CLI 手册 1：Cisco Secure Firewall ASA 系列常规操作 CLI 配置指南，9.22

上次修改日期: 2025 年 3 月 11 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. 保留所有权利。

目录

序言：

关于本指南 lix

文档目标 lix

相关文档 lix

文档约定 lix

通信、服务和其他信息 lx

第 I 部分：

ASA 入门 63

第 1 章

Cisco Secure Firewall ASA 简介 1

硬件和软件兼容性 1

VPN 兼容性 1

新增功能 1

ASA 9.22(1.1) 的新功能 2

防火墙功能概述 4

安全策略概述 5

通过访问规则允许或拒绝流量 5

应用 NAT 5

保护 IP 片段 5

应用 HTTP、HTTPS 或 FTP 过滤 5

应用应用检测 5

应用 QoS 策略 5

应用连接限制和 TCP 规范化 5

启用威胁检测 6

防火墙模式概述 6

状态监测概述 6
VPN 功能概述 8
安全情景概述 8
ASA 集群概述 9
特殊服务和传统服务 9

第 2 章 使用入门 11
访问命令行界面的控制台 11
访问 ISA 3000 控制台 11
访问 Firepower 1000和 Cisco Secure Firewall 1200/3100/4200 控制台 12
访问 Firepower 4100/9300 机箱上的 ASA 控制台 14
配置 ASDM 访问 15
使用出厂默认配置进行 ASDM 访问 15
自定义 ASDM 访问 16
启动 ASDM 18
出厂默认配置 20
恢复出厂默认配置 20
恢复 ASA Virtual 部署配置 22
Firepower 1010 默认配置 23
Firepower 1100 默认配置 25
Cisco Secure Firewall 1210/1220 默认配置 26
Cisco Secure Firewall 3100 默认配置 28
Cisco Secure Firewall 4200默认配置 29
Firepower 4100/9300 机箱 默认配置 30
ISA 3000 默认配置 31
ASA Virtual 部署配置 32
处理配置 34
关于启动配置和运行配置 34
保存配置更改 35
在单情景模式下保存配置更改 35
在多情景模式下保存配置更改 35

将启动配置复制到运行配置 37
查看配置 37
清除和删除配置设置 37
离线创建文本配置文件 39
将配置更改应用于连接 39
重新加载 ASA 39

第 3 章 许可证：用于 ISA 3000 的产品授权密钥许可 41
关于 PAK 许可证 41
预安装的许可证 41
永久许可证 41
基于时间的许可证 42
基于时间的许可证激活准则 42
基于时间的许可证计时器工作方式 42
永久许可证与基于时间的许可证的合并方式 42
堆叠基于时间的许可证 43
基于时间的许可证到期 43
许可证说明 44
Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 44
其他 VPN 许可证 44
合并后的各个类型的 VPN 会话总数 44
VPN 负载均衡 45
传统 VPN 许可证 45
加密许可证 45
TLS 代理会话总数 45
最大 VLAN 数量 46
共享 Secure Client 高级版许可证（AnyConnect 3 及更早版本） 46
故障转移 46
故障转移许可证要求和例外 46
如何合并故障转移许可证 47
故障转移或设备之间的通信丢失 47

升级故障转移对 47
无负载加密型号 48
许可证 FAQ 48
PAK 许可证准则 49
配置 PAK 许可证 50
订购许可证 PAK 并获取激活密钥 50
获取强加密许可证 51
激活或停用密钥 54
配置共享许可证（Secure Client 3 及更早版本） 55
关于共享许可证 55
关于共享许可服务器和参与者 55
参加者和服务器之间的通信问题 56
关于共享许可备用服务器 56
故障转移和共享许可证 57
最大参与者数 58
配置共享许可服务器 59
配置共享许可备份服务器（可选） 60
配置共享许可参与者 61
每个型号支持的功能许可证 62
每个型号的许可证 62
ISA 3000 许可证功能 62
监控 PAK 许可证 63
查看您当前的许可证 63
监控共享许可证 71
PAK 许可证的历史记录 73

第 4 章 许可证：智能软件许可 79
关于智能软件许可 79
Firepower 4100/9300 机箱上 ASA 的智能软件许可 80
智能软件管理器和账户 80
离线管理 80

永久许可证预留 80
智能软件管理器本地版 84
按虚拟帐户管理的许可证和设备 85
评估许可证 85
关于按类型划分的许可证 86
Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 86
其他 VPN 对等体数 86
VPN 对等体总数，所有类型 87
加密许可证 87
运营商许可证 88
TLS 代理会话总数 89
最大 VLAN 数量 89
僵尸网络流量过滤器许可证 89
故障转移或 ASA 集群许可证 90
ASAv 的故障转移许可证 90
Firepower 1010 的故障转移许可证 90
Firepower 1100 的故障转移许可证 90
Cisco Secure Firewall 1210/1220 的故障转移许可证 92
Cisco Secure Firewall 3100 的故障转移许可证 93
Cisco Secure Firewall 4200 的故障转移许可证 94
适用于 Firepower 4100/9300 的故障转移许可证 95
Cisco Secure Firewall 3100 的 ASA 群集许可证 96
Cisco Secure Firewall 4200 的 ASA 群集许可证 97
ASAv 的 ASA 集群许可证 98
Firepower 4100/9300 的 ASA 集群许可证 99
智能软件许可的前提条件 100
智能软件管理器常规版和本地版前提条件 100
永久许可证预留前提条件 100
智能软件许可准则 101
智能软件许可的默认设置 101
ASA Virtual: 配置智能软件许可 102

ASA Virtual：配置常规智能软件许可 102
ASA Virtual：为许可配置本地智能软件管理器 108
ASA Virtual：配置实用程序 (MSLA) 智能软件许可 112
ASA Virtual：配置永久许可证预留 118
安装 ASA Virtual 永久许可证 119
（可选）返还 ASA Virtual 永久许可证 121
（可选）取消注册 ASA Virtual（常规和本地） 122
（可选）续约 ASA Virtual ID 证书或许可证授权 （常规和本地） 122
1000/1200/3100/4200：配置智能软件许可 123
1000/1200/3100/4200：配置常规智能软件许可 123
1000/1200/3100/4200：配置智能软件本地许可 128
1000/1200/3100/4200：配置永久许可证预留 132
安装 1000/1200/3100/4200 永久许可证 132
（可选）返还 1000/1200/3100/4200 永久许可证 135
（可选）取消注册 1000/1200/3100/4200（常规和本地） 136
（可选）续约 1000/1200/3100/4200 ID 证书或许可证授权（常规和本地） 137
Firepower 4100/9300: 配置智能软件许可 137
每个型号的许可证 139
ASA Virtual 139
Firepower 1010 145
Firepower 1100 系列 145
Cisco Secure Firewall 1210 和 1220 147
Cisco Secure Firewall 3100 系列 148
Firepower 4100 149
Cisco Secure Firewall 4200 系列 150
Firepower 9300 151
每个型号的许可证 PID 152
监控智能软件许可 156
查看您当前的许可证 156
查看智能许可证状态 157
查看 UDI 160

调试智能软件许可 160
智能软件管理器通信 160
设备注册和令牌 160
与智能软件管理器的定期通信 161
不合规状态 161
Smart Call Home 基础设施 161
智能许可证证书管理 162
智能软件许可的历史记录 162

第 5 章 逻辑设备 Firepower 4100/9300 167
关于接口 167
机箱管理接口 167
接口类型 168
FXOS 接口与应用接口 169
关于逻辑设备 170
独立和集群逻辑设备 170
硬件和软件组合的要求与前提条件 170
逻辑设备的准则和限制 171
接口的准则和限制 171
一般准则和限制 172
高可用性的要求和前提条件 172
配置接口 172
配置物理接口 173
添加 EtherChannel（端口通道） 175
配置逻辑设备 177
添加独立 ASA 177
添加高可用性对 183
更改 ASA 逻辑设备上的接口 184
连接到应用控制台 185
逻辑设备的历史记录 186

第 6 章 透明或路由防火墙模式 189
关于防火墙模式 189
关于路由防火墙模式 189
关于透明防火墙模式 189
在网络中使用透明防火墙 190
管理 接口 190
允许路由模式功能通过流量 190
关于网桥组 191
网桥虚拟接口 (BVI) 191
透明防火墙模式下的网桥组 191
路由防火墙模式下的网桥组 192
传递路由模式下不允许的流量 193
允许第 3 层流量 193
允许的 MAC 地址 194
BPDU 处理 194
MAC 地址与路由查找 194
透明模式下网桥组不支持的功能 195
路由模式下网桥组不支持的功能 196
默认设置 197
防火墙模式准则 197
设置防火墙模式 198
防火墙模式示例 199
数据如何通过处于路由防火墙模式下的 ASA 199
内部用户访问 Web 服务器 200
外部用户访问 DMZ 上的 Web 服务器 201
内部用户访问 DMZ 上的 Web 服务器 202
外部用户尝试访问内部主机 202
DMZ 用户尝试访问内部主机 203
数据如何通过透明防火墙 204
内部用户访问 Web 服务器 205

内部用户使用 NAT 访问 Web 服务器 206
外部用户访问内部网络上的 Web 服务器 208
外部用户尝试访问内部主机 209
防火墙模式的历史记录 210

第 II 部分： 高可用性和可扩展性 213

第 7 章 多情景模式 215
关于安全情景 215
安全情景的公共用途 215
情景配置文件 216
情景配置 216
系统配置 216
管理情景配置 216
ASA 如何对数据包分类 216
有效分类器条件 216
分类示例 217
级联安全情景 219
对安全情景的管理访问 220
系统管理员访问 220
情景管理员访问 220
管理接口使用情况 221
关于资源管理 221
资源类 221
资源限制 221
默认类 221
使用超订用资源 222
使用不受限制的资源 223
关于 MAC 地址 223
多情景模式下的 MAC 地址 224
自动 MAC 地址 224

VPN 支持 224
多情景模式许可 225
多情景模式的先决条件 226
多情景模式准则 226
多情景模式默认设置 228
配置多情景 228
启用或禁用多情景模式 228
启用多情景模式 228
恢复单情景模式 230
配置用于资源管理的类 230
配置安全情景 234
自动为情景接口分配 MAC 地址 238
在情景和系统执行空间之间更改 239
管理安全情景 239
删除安全情景 239
更改管理情景 240
更改安全情景 URL 241
重新加载安全情景 242
通过清除配置来重新加载 242
通过删除和重新添加情景来重新加载 243
监控安全情景 243
查看情景信息 243
查看资源分配 245
查看资源使用情况 248
监控情景中的 SYN 攻击 250
查看分配的 MAC 地址 252
在系统配置中查看 MAC 地址 252
查看情景中的 MAC 地址 254
多情景模式示例 254
多情景模式的历史记录 255

第 8 章 通过故障转移实现高可用性 259
关于故障转移 259
故障转移模式 259
故障转移系统要求 260
硬件要求 260
软件要求 260
许可证要求 261
故障转移和状态故障转移链路 261
故障转移链路 261
状态故障转移链路 262
避免中断故障转移和数据链路 263
故障转移中的 MAC 地址和 IP 地址 264
无状态故障转移和有状态故障转移 266
无状态故障转移 266
状态故障转移 266
故障转移的网桥组要求 268
设备、ASAv 的网桥组要求 268
故障转移运行状态监控 269
设备运行状况监控 269
心跳模块冗余 269
接口监控 270
故障转移时间 271
配置同步 272
运行配置复制 272
文件复制 273
命令复制 273
config-sync 优化 274
关于主用/备用故障转移 275
主/辅助角色和主用/备用状态 275
启动时的主用设备确定 275

故障转移事件 275
关于主用/主用故障转移 276
主用/主用故障转移概述 276
故障转移组的主/辅助角色和主用/备用状态 277
启动时的故障转移组主用设备确定 277
故障转移事件 277
故障转移许可 278
故障转移准则 279
故障转移的默认设置 282
配置主用/备用故障转移 282
为主用/备用故障转移配置主设备 282
为主用/备用故障转移配置辅设备 286
配置主用/主用故障转移 287
为主用/主用故障转移配置主设备 287
为主用/主用故障转移配置辅助设备 292
配置可选故障转移参数 293
配置故障转移条件和其他设置 293
配置接口监控 297
配置非对称路由数据包支持（主用/主用模式） 297
管理故障转移 301
强制故障转移 301
禁用故障转移 302
恢复故障设备 303
重新同步配置 303
测试故障转移功能 304
远程命令执行 304
发送命令 305
更改命令模式 305
安全注意事项 306
远程命令执行的限制 306
监控 故障转移 307

故障转移消息 307
故障转移系统日志消息 307
故障转移调试消息 307
SNMP 故障转移陷阱 307
监控故障转移状态 308
故障转移的历史记录 308

第 9 章 公共云中的高可用性故障转移 311
关于公共云中的故障转移 311
关于主用/备份故障转移 312
主/辅助角色和主用/备份状态 312
故障转移连接 312
轮询和 Hello 消息 312
启动时的主用设备确定 313
故障转移事件 313
准则和限制 314
公共云中的故障转移许可 315
公共云中的故障转移默认值 316
关于 Microsoft Azure 中的 ASA Virtual 高可用性 316
关于 Azure 服务主体 317
Azure 中的 ASA Virtual 高可用性配置要求 318
配置主用/备份故障转移 319
配置主用/备份故障转移的主设备 319
配置主用/备份故障转移的辅助设备 320
配置可选故障转移参数 320
配置故障转移条件和其他设置 321
配置 Azure 服务主体的身份验证凭证 322
配置 Azure 路由表 324
启用主用/备份故障转移 325
启用主用/备份故障转移的主设备 325
启用主用/备份故障转移的辅助设备 326

管理公共云中的故障转移 327
强制故障转移 327
更新路由 328
验证 Azure 身份验证 329
监控公共云中的故障转移 329
故障转移状态 329
故障转移消息 330
公共云中的故障转移历史记录 331

第 10 章 为 Cisco Secure Firewall 3100/4200部署 ASA 集群 333
关于 ASA 集群 333
集群如何融入网络中 333
集群成员 334
引导程序配置 334
控制和数据节点角色 334
集群接口 334
集群控制链路 334
配置复制 335
ASA 集群管理 335
管理网络 335
管理接口 335
控制设备管理与数据设备管理 336
加密密钥复制 336
ASDM 连接证书 IP 地址不匹配 336
站点间集群 336
ASA 集群许可证 337
ASA 集群要求和前提条件 338
ASA 集群准则 340
配置 ASA 集群 345
使用电缆连接设备并配置接口 345
关于集群接口 346

使用电缆连接集群设备并配置上游和下游设备 352
上在每个设备上配置集群接口模式 352
在控制节点上配置接口 353
创建引导程序配置 359
配置控制节点引导程序设置 359
配置数据节点引导程序设置 364
自定义集群操作 366
配置基本 ASA 集群参数 367
配置运行状态监控并自动重新加入设置 367
配置连接再均衡和集群 TCP 复制延迟 371
配置站点间功能 372
管理集群节点 378
成为非活动节点 378
停用节点 379
重新加入集群 380
离开集群 381
更改控制节点 382
在整个集群范围内执行命令 382
监控 ASA 集群 383
监控集群状态 383
捕获整个集群范围内的数据包 388
监控集群资源 388
监控集群流量 388
监控集群路由 393
配置集群日志记录 393
监控集群接口 394
调试集群 394
ASA 集群示例 395
ASA 和交换机配置示例 395
ASA 配置 396
思科 IOS 交换机配置 397

单臂防火墙 398
流量分隔 400
路由模式站点间集群的 OTV 配置 402
站点间集群示例 405
独立接口路由模式南北站点间集群示例 405
具有站点特定的 MAC 和 IP 地址的跨区以太网通道路由模式示例 406
跨区以太网通道透明模式南北站点间集群示例 407
跨区以太网通道 透明模式东西站点间集群示例 408
集群参考 409
ASA 功能和集群 409
集群不支持的功能 409
集群集中化功能 410
应用到单个节点的功能 411
用于网络访问的 AAA 和集群 411
连接设置和集群 412
FTP 和集群 412
ICMP检测和集群 412
组播路由和集群 412
NAT 和集群 412
动态路由和集群 414
SCTP 和集群 416
SIP 检测和集群 417
SNMP 和集群 417
STUN 和集群 417
系统日志与 NetFlow 和集群 417
思科 TrustSec 和集群 417
VPN 和集群 417
性能换算系数 418
控制节点选择 418
集群中的高可用性 418
节点运行状况监控 419

接口监控 419
发生故障后的状态 419
重新加入集群 420
数据路径连接状态复制 420
集群管理连接的方式 421
连接角色 421
新连接所有权 422
TCP 的数据流示例 423
ICMP 和 UDP 的数据流示例 423
跨集群实现新 TCP 连接再均衡 424
Cisco Secure Firewall 3100/4200 的 ASA 集群的历史记录 425

第 11 章 **Firepower 4100/9300 的 ASA 集群** 427
关于 Firepower 4100/9300 机箱上的集群 427
引导程序配置 428
集群成员 428
集群控制链路 428
确定集群控制链路规格 429
集群控制链路冗余 429
机箱间集群的集群控制链路可靠性 430
集群控制链路网络 430
集群接口 430
连接到冗余交换机系统 430
配置复制 431
Cisco Secure Firewall ASA集群管理 431
管理网络 431
管理接口 431
控制设备管理与数据设备管理 431
加密密钥复制 432
ASDM 连接证书 IP 地址不匹配 432
跨网络 EtherChannel（推荐） 432

站点间集群 433
Firepower 4100/9300 机箱上的集群要求和前提条件 433
集群许可证 Firepower 4100/9300 机箱 435
集群准则和限制 436
在 Firepower 4100/9300 机箱上配置集群 441
FXOS：添加 ASA 集群 441
创建 ASA 集群 441
添加更多集群成员 451
ASA：配置防火墙模式和情景模式 452
ASA：配置数据接口 452
ASA：自定义集群配置 455
配置基本 ASA 集群参数 455
配置运行状态监控并自动重新加入设置 457
配置连接再均衡和集群 TCP 复制延迟 461
配置站点间功能 461
配置分布式站点间 VPN 468
FXOS：删除集群设备 474
ASA：管理集群成员 476
成为非活动成员 476
停用单元 477
重新加入集群 477
变更控制单元 478
在整个集群范围内执行命令 479
ASA：监控 Firepower 4100/9300 机箱上的 ASA 集群 480
监控集群状态 480
捕获整个集群范围内的数据包 484
监控集群资源 484
监控集群流量 484
监控集群路由 489
监控分布式站点间 VPN 489
配置集群日志记录 490

调试集群 490
分布式站点间 VPN 故障排除 491
ASA 集群示例 492
单臂防火墙 492
流量分隔 493
路由模式站点间集群的 OTV 配置 493
站点间集群示例 496
具有站点特定的 MAC 和 IP 地址的跨区以太网通道路由模式示例 496
跨区以太网通道透明模式南北站点间集群示例 497
跨区以太网通道 透明模式东西站点间集群示例 498
集群参考 499
ASA 功能和集群 499
集群不支持的功能 499
集群集中化功能 500
应用到单台设备的功能 501
用于网络访问的 AAA 和集群 502
连接设置 502
FTP 和集群 502
ICMP 检查 502
组播路由和集群 502
NAT 和集群 502
动态路由和集群 504
SCTP 和集群 504
SIP 检测和集群 505
SNMP 和集群 505
STUN 和集群 505
系统日志与 NetFlow 和集群 505
思科 TrustSec 和集群 505
Cisco Secure Firewall eXtensible 操作系统 (FXOS) 机箱上的 VPN 和集群 505
性能换算系数 506
控制设备选择 506

集群中的高可用性 507
机箱应用程序监控 507
设备运行状况监控 507
接口监控 507
修饰符应用监控 507
发生故障后的状态 508
重新加入集群 508
数据路径连接状态复制 508
集群管理连接的方式 509
连接角色 509
新连接所有权 511
TCP 的数据流示例 511
ICMP 和 UDP 的数据流示例 512
跨集群实现新 TCP 连接再均衡 513
Firepower 4100/9300上 ASA 集群的历史记录 513

第 12 章 **ASA 集群部署集群** 519
关于 ASA Virtual 集群 519
集群如何融入网络中 520
集群节点 520
引导程序配置 520
控制和数据节点角色 520
独立接口 520
基于策略的路由 521
同等成本的多路径路由 522
集群控制链路 522
集群控制链路流量概述 522
集群控制链路故障 523
配置复制 523
ASA Virtual集群管理 523
管理网络 523

管理接口 523
控制节点管理与数据节点管理 524
加密密钥复制 524
ASDM 连接证书 IP 地址不匹配 524
站点间集群 524
ASA Virtual集群的许可证 525
ASA Virtual集群要求和前提条件 525
ASA Virtual集群的准则 526
使用 Day0 配置来配置 ASA Virtual集群 527
部署后配置 ASA Virtual 集群 530
配置接口设置 530
在每个节点上配置集群接口模式 530
配置独立接口 531
创建引导程序配置 534
配置控制节点引导程序设置 534
配置数据节点引导程序设置 539
自定义集群操作 542
配置基本 ASA 集群参数 542
配置运行状态监控并自动重新加入设置 543
配置连接再均衡和集群 TCP 复制延迟 546
配置站点间功能 547
启用导向器本地化 547
启用站点冗余 547
配置集群流移动性 548
管理集群节点 552
成为非活动节点 553
从控制节点停用数据节点 553
重新加入集群 554
离开集群 555
更改控制节点 556
在整个集群范围内执行命令 556

监控 ASA Virtual集群 557
监控集群状态 557
捕获整个集群范围内的数据包 561
监控集群资源 561
监控集群流量 561
监控集群路由 566
配置集群日志记录 567
监控集群接口 567
调试集群 567
ASA Virtual集群示例 568
独立接口路由模式南北站点间集群示例 568
集群参考 569
ASA 功能和集群 569
集群不支持的功能 569
集群集中化功能 570
应用到单个节点的功能 571
用于网络访问的 AAA 和集群 571
连接设置和集群 572
动态路由和集群 572
FTP 和集群 573
ICMP检测和集群 573
组播路由和集群 573
NAT 和集群 573
SCTP 和集群 575
SIP 检测和集群 575
SNMP 和集群 575
STUN 和集群 575
系统日志与 NetFlow 和集群 575
思科 TrustSec 和集群 576
VPN 和集群 576
性能换算系数 576

控制节点选择 576
ASA Virtual 集群中的高可用性 577
节点运行状况监控 577
接口监控 577
发生故障后的状态 577
重新加入集群 578
数据路径连接状态复制 578
ASA Virtual集群管理连接的方式 579
连接角色 579
新连接所有权 581
TCP 的数据流示例 581
ICMP 和 UDP 的数据流示例 582
跨集群实现新 TCP 连接再均衡 583
ASA Virtual集群的历史记录 583

第 13 章 在公共云中为 ASA Virtual 部署 ASA 集群 585
关于公共云中的 ASA Virtual 集群 585
集群如何融入网络中 586
集群节点 586
引导程序配置 586
控制和数据节点角色 586
独立接口 587
集群控制链路 587
集群控制链路流量概述 587
集群控制链路故障 588
配置复制 588
ASA Virtual集群管理 588
管理网络 588
管理接口 588
控制节点管理与数据节点管理 589
加密密钥复制 589

ASDM 连接证书 IP 地址不匹配 589
ASA Virtual 集群许可证 589
ASA Virtual 集群要求和前提条件 590
ASA Virtual 集群准则 591
在 AWS 中部署集群 592
AWS 网关负载均衡器和 Geneve 单臂代理 592
拓扑示例 593
在 AWS 上部署 ASA Virtual 集群的端到端流程 595
模板 597
在 AWS 中使用 GWLB 配置 ASA Virtual 集群的目标故障转移 597
使用 CloudFormation 模板在 AWS 中部署堆栈 598
自动缩放参数配置 604
通过更新堆叠在 ASA Virtual 集群中配置所需的 IMDSv2 模式 605
在 AWS 中手动部署集群 606
创建 AWS 的 Day-0 配置 606
部署集群节点 608
在 AWS 中为 ASA Virtual 启用目标故障转移 609
在 Azure 中部署集群 610
关于 Azure 中的集群部署 611
使用 Azure 资源管理器模板来部署集群 611
在 Azure 中配置集群 616
准备用于在 Azure 上创建集群的配置文件 616
使用配置文件手动配置集群 618
使用 Azure 函数应用来配置集群 618
Azure 中的 ASA Virtual 集群故障排除 620
自定义集群操作 621
配置基本 ASA 集群参数 622
配置运行状态监控并自动重新加入设置 622
管理集群节点 625
成为非活动节点 625
从控制节点停用数据节点 626

重新加入集群 627
离开集群 627
更改控制节点 628
在整个集群范围内执行命令 629
监控集群 629
监控集群状态 630
捕获整个集群范围内的数据包 634
监控集群资源 634
监控集群流量 634
监控集群路由 639
配置集群日志记录 640
监控集群接口 640
调试集群 640
集群参考 641
ASA 功能和集群 641
集群不支持的功能 641
集群集中化功能 642
应用到单个节点的功能 643
用于网络访问的 AAA 和集群 643
连接设置和集群 643
动态路由和集群 643
FTP 和集群 644
ICMP检测和集群 645
组播路由和集群 645
NAT 和集群 645
SCTP 和集群 646
SIP 检测和集群 647
SNMP 和集群 647
STUN 和集群 647
系统日志和集群 647
思科 TrustSec 和集群 647

VPN 和集群 647
性能换算系数 648
控制节点选择 648
集群中的高可用性 648
节点运行状况监控 649
接口监控 649
发生故障后的状态 649
重新加入集群 649
数据路径连接状态复制 650
集群管理连接的方式 650
连接角色 650
新连接所有权 652
TCP 的数据流示例 652
ICMP 和 UDP 的数据流示例 653
关于公共云中的 ASA Virtual 集群的历史记录 655

第 III 部分： 接口 657

第 14 章 基本接口配置 659
关于基本接口配置 659
Auto-MDI/MDIX 功能 659
管理接口 660
管理接口概述 660
管理插槽/端口接口 660
将任何接口用于管理专用流量 661
透明模式下的管理接口 661
基本接口配置的相关准则 661
基本接口配置的默认设置 662
启用物理接口和配置以太网参数 662
启用巨帧支持（ASA Virtual、ISA 3000） 665
管理 Cisco Secure Firewall 3100/4200的网络模块 666

配置分支端口 666
增加网络模块 667
热插拔网络模块 668
将网络模块更换为其他类型 669
拆卸网络模块 670
监控接口 670
基本接口示例 671
物理接口参数示例 671
多情景模式示例 671
基本接口配置的历史记录 672

第 15 章 **Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口的基本接口配置** 675
关于 Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口 675
了解交换机端口和接口 675
Auto-MDI/MDIX 功能 676
交换机端口准则和限制 676
配置交换机端口和以太网供电 678
启用或禁用交换机端口模式 678
配置 VLAN 接口 679
将交换机端口配置为接入端口 680
将交换机端口配置为中继端口 682
配置以太网供电 684
监控交换机端口 686
交换机端口示例 687
路由模式示例 687
透明模式示例 688
混合防火墙接口/交换机端口示例 688
集成的路由和桥接示例 689
故障转移示例 690
交换机端口的历史记录 691

第 16 章 **EtherChannel 接口** 693

关于 EtherChannels 693

关于 EtherChannel 693

通道组接口 694

连接到其他设备上的 EtherChannel 694

链路聚合控制协议 695

负载均衡 695

EtherChannel MAC 地址 696

EtherChannel 的准则 696

EtherChannel 的默认设置 698

配置 EtherChannel 698

将接口添加到 EtherChannel 698

自定义 EtherChannel（ISA 3000） 701

监控 EtherChannels 702

EtherChannel 示例 703

EtherChannels的历史记录 704

第 17 章 **环回接口** 705

关于环回接口 705

环回接口准则 706

配置环回接口 706

对流向环回接口的流量进行速率限制 706

监控环回接口 708

环回接口的历史记录 708

第 18 章 **VLAN 子接口** 711

关于 VLAN 子接口 711

VLAN 子接口的许可 711

VLAN 子接口的准则和限制 712

VLAN 子接口的默认设置 713

配置 VLAN 子接口和 802.1Q 中继 713
监控 VLAN 子接口 715
VLAN 子接口示例 715
VLAN 子接口的历史记录 716

第 19 章 VXLAN 接口 719
关于 VXLAN 接口 719
封装 719
VXLAN 隧道端点 720
VTEP 源接口 720
VNI 接口 721
VXLAN 数据包处理 721
对等体 VTEP 722
VXLAN 使用案例 723
VXLAN 网桥或网关概述 723
VXLAN 网桥 723
VXLAN 网关（路由模式） 723
VXLAN 域之间的路由器 724
AWS 网关负载均衡器和 Geneve 单臂代理 725
AWS 网关负载均衡器和 Geneve 双臂代理 726
Azure 网关负载均衡器和配对代理 727
VXLAN 接口的要求和前提条件 728
VXLAN 接口准则 728
VXLAN 接口默认设置 729
配置 VXLAN 接口 729
配置 VTEP 源接口 730
配置 VNI 接口 732
（可选）更改 VXLAN UDP 端口 735
配置 Geneve 接口 736
为 Geneve 配置 VTEP 源接口 736
为 Geneve 配置 VNI 接口 737

允许网关负载均衡器运行状况检查 739
监控 VXLAN 接口 740
VXLAN 接口示例 743
透明 VXLAN 网关示例 743
VXLAN 路由示例 745
VXLAN 接口的历史记录 746

第 20 章 路由模式接口和透明模式接口 749
关于路由和透明模式接口 749
安全级别 749
双 IP 堆栈（IPv4 和 IPv6） 750
31 位子网掩码 750
31 位子网和集群 750
31 位子网和故障转移 750
31 位子网和管理 751
31 位子网不支持的功能 751
路由和透明模式接口准则和限制 751
配置路由模式接口 753
配置常规路由模式接口参数 753
配置 PPPoE 756
配置网桥组接口 757
配置网桥虚拟接口 (BVI) 757
配置常规网桥组成员接口参数 759
为透明模式配置管理接口 761
配置 IPv6 寻址 763
关于 IPv6 763
IPv6 寻址 763
修改的 EUI-64 接口 ID 764
配置 IPv6 前缀代理客户端 764
关于 IPv6 前缀授权 764
启用 IPv6 前缀授权客户端 766

配置全局 IPv6 地址 768
配置 IPv6 邻居发现 770
监控路由模式和透明模式接口 774
接口统计信息和信息 775
DHCP 信息 775
PPPoE 778
IPv6 邻居发现 779
路由和透明模式接口示例 780
包括 2 个网桥组的透明模式示例 780
与 2 个网桥组的交换 LAN 网段示例 780
路由模式和透明模式接口的历史记录 783

第 21 章 高级接口配置 787
关于高级接口配置 787
关于 MAC 地址 787
默认 MAC 地址 787
自动 MAC 地址 788
关于 MTU 789
路径 MTU 发现 789
默认 MTU 789
MTU 和分段 789
MTU 和巨型帧 789
关于 TCP MSS 790
默认 TCP MSS 790
建议的最大 TCP MSS 设置 790
接口间通信 791
接口内通信（路由防火墙模式） 791
手动配置 MAC 地址 791
自动分配 MAC 地址 792
配置、MTU和 TCP MSS 793
允许同一安全级别的通信 794

高级接口配置的历史记录 795

第 22 章 流量区域 797

关于流量区域 797

未分区行为 797

为什么使用区域？ 797

非对称路由 798

丢失的路由 798

负载均衡 799

每区域连接和路由表 800

ECMP 路由 800

未划分区域的 ECMP 支持 800

划分区域的 ECMP 支持 801

如何对连接进行负载均衡 801

回退到另一区域中的路由 801

基于接口的安全策略 801

流量区域支持的服务 801

安全级别 802

流量的主接口和当前接口 802

加入或离开区域 802

区域内流量 802

流入流量和流出流量 802

区域内重叠的 IP 地址 803

流量区域的前提条件 803

流量区域准则 804

配置流量区域 806

监控流量区域 807

区域信息 807

区域连接 807

区域路由 808

流量区域示例 809

流量区域的历史记录 812

第 IV 部分： 基本设置 813

第 23 章 基本设置 815

设置主机名、域名及启用密码和 Telnet 密码 815

设置日期和时间 817

设置时区和夏令时日期 817

使用 NTP 服务器设置日期和时间 820

手动设置日期和时间 821

配置精确时间协议 (ISA 3000) 822

配置主密码 824

添加或更改主密码 824

禁用主密码 826

删除主密码 827

配置 DNS 服务器 828

配置硬件旁路和双重电源（思科 ISA 3000） 830

调整 ASP（加速安全路径）性能和行为 832

选择规则引擎交易提交模式 832

启用 ASP 负载均衡 833

监控 DNS 缓存 834

基本设置的历史记录 834

第 24 章 DHCP 和 DDNS 服务 839

关于 DHCP 和 DDNS 服务 839

关于 DHCPv4 服务器 839

DHCP 选项 839

关于 DHCPv6 无状态服务器 840

关于 DHCP 中继代理 840

VTI 上的 DHCP 中继服务器支持 840

DHCP 和 DDNS 服务准则 841

配置 DHCP 服务器 843
启用 DHCPv4 服务器 843
配置高级 DHCPv4 选项 845
配置 DHCPv6 无状态服务器 847
配置 DHCP 中继代理 849
配置 DHCPv4 中继代理 849
配置 DHCPv6 中继代理 851
配置动态 DNS 852
监控 DHCP 和 DDNS 服务 857
监控 DHCP 服务 857
故障排除 VTI 上的 DHCP 中继 860
监控 DDNS 状态 861
DHCP 和 DDNS 服务的历史记录 862

第 25 章 数字证书 865
关于数字证书 865
公钥加密 866
证书可扩展性 866
密钥对 867
信任点 867
证书注册 868
SCEP 请求的代理 868
撤销检查 868
支持的 CA 服务器 868
CRL 869
OCSP 870
证书和用户登录凭证 871
用户登录凭证 871
证书 871
数字证书准则 872
配置数字证书 875

配置密钥对 875
配置信任点 877
为信任点配置 CRL 882
导出或导入信任点配置 885
配置 CA 证书映射规则 886
配置引用标识 889
手动获取证书 890
使用 SCEP 自动获取证书 892
为 SCEP 请求配置代理支持 894
如何设置特定整数类型 896
CA 证书 896
CA 服务器管理 896
设置证书到期警报（对于身份或 CA 证书） 898
监控数字证书 898
证书管理的历史记录 900

第 26 章 的 ARP 检测和 MAC 地址表 905
关于 ARP 检测和 MAC 地址表 905
网桥组流量的 ARP 检测 905
MAC 地址表 906
默认设置 906
ARP 检测和 MAC 地址表准则 906
配置 ARP 检测和其他 ARP 参数 907
添加静态 ARP 条目并自定义其他 ARP 参数 907
启用 ARP 检测 908
自定义网桥组的 MAC 地址表 909
为网桥组添加静态 MAC 地址 909
设置 MAC 地址超时 909
配置 MAC 地址学习 910
监控 ARP 检测和 MAC 地址表 910
ARP 检测和 MAC 地址表的历史记录 911

第 V 部分： IP 路由 913

第 27 章 路由概述 915

确定路径 915
支持的路由类型 916
静态与动态 916
单路径与多路径 916
平面与分层 916
链路状态与距离矢量 917
支持的互联网路由协议 917
路由表 917
路由表的填充方式 918
路由的管理距离 918
备份动态和浮动静态路由 919
如何制定转发决策 919
动态路由和故障转移 920
动态路由和集群 920
跨区以太网通道模式下的动态路由 920
独立接口模式下的动态路由 921
多情景模式下的动态路由 922
路由资源管理 923
管理流量的路由表 923
管理接口识别 924
等价多路径 (ECMP) 路由 924
禁用代理 ARP 请求 925
显示路由表 926
路由概述的历史记录 926

第 28 章 静态和默认路由 927

关于静态路由和默认路由 927

默认路由 927
静态路由 927
使用到 null0 接口的路由丢弃不必要的流量 928
路由优先级 928
透明防火墙模式和网桥组路由 928
静态路由跟踪 928
静态和默认路由准则 929
配置默认路由和静态路由 930
配置默认路由 930
配置静态路由 931
配置静态路由跟踪 932
监控静态路由或默认路由 934
静态路由或默认路由示例 934
静态和默认的历史记录 934

第 29 章 策略型路由 937
关于策略型路由 937
为什么使用基于策略的路由？ 937
同等访问权限和源敏感路由 938
服务质量 938
成本节约 938
负载分担 939
实施 PBR 939
基于策略的路由准则 939
路径监控 941
配置路径监控 942
配置基于策略的路由 942
基于策略的路由示例 946
路由映射配置示例 946
PBR 配置示例 947
使用软件定义的 WAN 直接访问互联网 949

正在使用的基于策略的路由 951
基于策略的路由的历史记录 955

第 30 章 路由映射 957
关于路由映射 957
Permit 和 Deny 子句 958
Match 和 Set 子句值 958
路由映射准则 959
定义路由映射 959
自定义路由映射 959
定义路由以匹配特定的目标地址 959
为路由操作配置度量值 961
路由映射示例 962
路由映射的历史记录 962

第 31 章 双向转发检测路由 963
关于 BFD 路由 963
BFD 异步模式和回应功能 963
BFD 会话建立 964
BFD 计时器协商 965
BFD 故障检测 966
BFD 部署场景 966
BFD 路由准则 966
配置 BFD 967
创建 BFD 模板 967
配置 BFD 接口 969
配置 BFD 映射 970
BFD 监控 971
BFD 路由的历史记录 972

第 32 章 BGP 973

关于 BGP 973
何时使用 BGP 973
路由表更改 974
BGP 路径选择 975
BGP 多路径 975
BGP 准则 976
配置 BGP 977
启用 BGP 977
定义 BGP 路由进程的最佳路径 979
配置策略列表 980
配置 AS 路径过滤器 981
配置社区规则 982
配置 IPv4 地址系列设置 983
配置 IPv4 系列常规设置 983
配置 IPv4 系列汇聚地址设置 985
配置 IPv4 系列过滤设置 986
配置 IPv4 系列 BGP 邻居设置 987
配置 IPv4 网络设置 993
配置 IPv4 重新分发设置 994
配置 IPv4 路由注入设置 995
配置 IPv6 地址系列设置 995
配置 IPv6 系列常规设置 996
配置 IPv6 系列汇聚地址设置 997
配置 IPv6 系列 BGP 邻居设置 998
配置 IPv6 网络设置 1004
配置 IPv6 重新分发设置 1005
配置 Ipv6 路由注入设置 1006
监控 BGP 1007
BGP 示例 1009
BGP 的历史记录 1012

第 33 章 OSPF 1015

关于 OSPF 1015

快速呼叫数据包 OSPF 支持 1016

OSPF 支持快速呼叫数据包的前提条件 1017

关于快速呼叫数据包的 OSPF 支持 1017

OSPFv2 与 OSPFv3 之间的实施差异 1017

OSPF 准则 1018

配置 OSPFv2 1020

配置身份验证所用的密钥链 1022

配置 OSPFv2 路由器 ID 1024

手动配置 OSPF 路由器 ID 1024

迁移时的路由器 ID 行为 1025

配置 OSPF 快速呼叫数据包 1025

自定义 OSPFv2 1026

将路由重新分发到 OSPFv2 中 1026

配置将路由重新分发到 OSPFv2 时的路由汇总 1028

添加路由汇总地址 1028

配置 OSPFv2 区域之间的路由汇总 1029

配置 OSPFv2 接口参数 1030

配置 OSPFv2 区域参数 1033

配置 OSPFv2 过滤器规则 1034

配置 OSPFv2 NSSA 1035

为集群配置 IP 地址池（OSPFv2 和 OSPFv3） 1036

定义静态 OSPFv2 邻居 1037

配置路由计算计时器 1037

记录邻居启动或关闭 1038

配置身份验证所用的密钥链 1039

配置 OSPFv3 1041

启用 OSPFv3 1041

配置 OSPFv3 接口参数 1042

配置 OSPFv3 路由器参数 1048
配置 OSPFv3 区域参数 1051
配置 OSPFv3 被动接口 1053
配置 OSPFv3 管理距离 1053
配置 OSPFv3 计时器 1054
定义静态 OSPFv3 邻居 1056
重置 OSPFv3 默认参数 1057
发送系统日志消息 1058
抑制系统日志消息 1058
计算汇总路由成本 1059
生成到 OSPFv3 路由域中的默认外部路由 1059
配置 IPv6 汇总前缀 1060
重新分发 IPv6 路由 1061
配置无中断重启 1062
配置功能 1063
为 OSPFv2 配置无中断重启 1063
为 OSPFv2 配置思科 NSF 无中断重启 1063
为 OSPFv2 配置 IETF NSF 无中断重启 1064
为 OSPFv3 配置无中断重启 1065
为 OSPF 配置无中断重新启动等待计时器 1066
删除 OSPFv2 配置 1066
删除 OSPFv3 配置 1067
OSPFv2 示例 1067
OSPFv3 示例 1069
监控 OSPF 1070
OSPF 的历史记录 1073

第 34 章 IS-IS 1077
关于 IS-IS 1077
关于 NET 1077
IS-IS 动态主机名 1078

IS-IS PDU 类型 1078
IS-IS 在多接入回路上的操作 1079
指定 IS 的 IS-IS 选择 1080
IS-IS LSPDB 同步 1081
IS-IS 最短路径计算 1082
IS-IS 关机协议 1082
IS-IS 前提条件 1083
IS-IS 准则 1083
配置 IS-IS 1083
全局启用 IS-IS 路由 1084
启用 IS-IS 身份验证 1087
配置 IS-IS LSP 1091
配置 IS-IS 汇总地址 1095
配置 IS-IS 被动接口 1096
配置 IS-IS 接口 1097
配置 IS-IS 接口呼叫传送 1101
配置 IS-IS IPv4 地址系列 1103
配置 IS-IS IPv6 地址系列 1108
监控 IS-IS 1113
IS-IS 的历史记录 1115
IS-IS 示例 1115

第 35 章 EIGRP 1125
关于 EIGRP 1125
EIGRP 准则 1127
配置 EIGRP 1128
启用 EIGRP 1128
启用 EIGRP 末节路由 1128
自定义 EIGRP 1130
为 EIGRP 路由进程定义网络 1130
为 EIGRP 配置接口 1131

配置被动接口 1133
在接口上配置汇总汇聚地址 1134
更改接口延迟值 1134
在接口上启用 EIGRP 身份验证 1135
定义 EIGRP 邻居 1137
将路由重新分发到 EIGRP 中 1138
在 EIGRP 中过滤网络 1140
自定义 EIGRP 呼叫间隔和保持时间 1141
禁用自动路由汇总 1142
配置 EIGRP 中的默认信息 1143
禁用 EIGRP 水平分割 1144
重新启动 EIGRP 进程 1145
配置 EIGRPv6 进程 1145
启用 EIGRPv6 1145
EIGRPv6 中的过滤器规则 1145
为 EIGRPv6 配置接口 1146
为 EIGRPv6 配置被动接口 1147
将路由重新分发到 EIGRPv6 1148
定义 EIGRPv6 邻居 1150
EIGRP 监控 1150
EIGRP 示例 1152
EIGRP 的历史记录 1153

第 36 章 组播路由 1155
关于组播路由 1155
末节组播路由 1155
PIM 组播路由 1156
PIM 源特定组播支持 1156
PIM 自举路由器 (BSR) 1156
PIM 引导程序路由器 (BSR) 术语 1156
组播组概念 1157

组播地址 1157
集群 1157
组播路由准则 1158
启用组播路由 1158
自定义组播路由 1159
配置末节组播路由和转发 IGMP 消息 1159
配置静态组播路由 1160
配置 IGMP 功能 1160
禁用接口上的 IGMP 1161
配置 IGMP 组成员身份 1161
配置静态加入的 IGMP 组 1162
控制对组播组的访问 1162
限制接口上的 IGMP 状态数量 1163
修改发送到组播组的查询消息 1164
更改 IGMP 版本 1165
配置 PIM 功能 1165
启用和禁用接口上的 PIM 1166
配置静态交汇点地址 1166
配置指定路由器优先级 1167
配置和过滤 PIM 注册消息 1167
配置 PIM 消息间隔 1168
过滤 PIM 邻居 1168
配置双向邻居过滤器 1169
将 ASA 配置为候选 BSR 1170
配置组播边界 1171
PIM 监控 1171
组播路由示例 1172
组播路由的历史记录 1172

第 VI 部分： **AAA 服务器和本地数据库** 1175

第 37 章 AAA 和本地数据库 1177

关于 AAA 和本地数据库 1177

身份验证 1177

授权 1178

会计 1178

身份验证、授权和记账之间的交互 1178

AAA 服务器和服务器组 1178

关于本地数据库 1180

回退支持 1181

组中存在多个服务器时的回退方式 1181

本地数据库准则 1182

在本地数据库中添加用户帐户 1182

监控本地数据库 1184

本地数据库的历史记录 1184

第 38 章 用于 AAA 的 RADIUS 服务器 1189

关于用于 AAA 的 RADIUS 服务器 1189

受支持的身份验证方法 1189

VPN 连接的用户授权 1190

支持的 RADIUS 属性集 1190

支持的 RADIUS 授权属性 1190

支持的 IETF RADIUS 授权属性 1199

RADIUS 记帐连接断开原因代码 1200

AAA 的 RADIUS 服务器准则 1200

配置用于 AAA 的 RADIUS 服务器 1201

配置 RADIUS 服务器组 1201

向组中添加 RADIUS 服务器 1205

为 AAA 监控 RADIUS 服务器 1207

用于 AAA 的 RADIUS 服务器的历史记录 1208

第 39 章 用于 AAA 的 TACACS+ 服务器 1209
关于用于 AAA 的 TACACS+ 服务器 1209
TACACS+ 属性 1209
用于 AAA 的 TACACS+ 服务器准则 1210
配置 TACACS+ 服务器 1211
配置 TACACS+ 服务器组 1211
向组中添加 TACACS+ 服务器 1213
监控用于 AAA 的 TACACS+ 服务器 1214
用于 AAA 的 TACACS+ 服务器的历史记录 1215

第 40 章 用于 AAA 的 LDAP 服务器 1217
关于 LDAP 和 ASA 1217
身份验证如何与 LDAP 配合使用 1217
LDAP 层次结构 1218
搜索 LDAP 层次结构 1218
绑定到 LDAP 服务器 1219
LDAP 属性映射 1220
AAA 的 LDAP 服务器准则 1220
配置用于 AAA 的 LDAP 服务器 1221
配置 LDAP 属性映射 1221
配置 LDAP 服务器组 1223
使用 LDAP 为 VPN 配置授权 1226
监控用于 AAA 的 LDAP 服务器 1227
用于 AAA 的 LDAP 服务器的历史记录 1228

第 41 章 用于 AAA 的 RSA SecurID 服务器 1229
关于 RSA SecurID 服务器 1229
用于 AAA 的 RSA SecurID 服务器准则 1229
配置用于 AAA 的 RSA SecurID 服务器 1230
配置 RSA SecurID AAA 服务器组 1230

将 RSA SecurID 服务器添加到 SDI 服务器组 1231
导入 SDI 节点密钥文件 1232
监控用于 AAA 的 RSA SecurID 服务器 1233
用于 AAA 的 RSA SecurID 服务器的历史记录 1233

第 VII 部分： 系统管理 1235

第 42 章 管理访问 1237
配置管理远程访问 1237
配置 SSH 访问 1237
配置 Telnet 访问 1244
配置用于 ASDM 的 HTTPS 访问、其他客户端 1245
为 ASDM 访问或无客户端 SSL VPN 配置 HTTP 重定向 1248
配置 VPN 隧道上的管理访问 1249
更改控制台超时 1250
自定义 CLI 提示符 1250
配置登录横幅 1251
设置管理会话配额 1252
为系统管理员配置 AAA 1254
配置管理验证 1254
关于管理验证 1254
配置用于 CLI 和 ASDM访问的身份验证 1256
配置 Enable 身份验证（特权 EXEC 模式） 1256
配置 ASDM 证书身份验证 1257
使用管理授权控制 CLI 和 ASDM 访问 1259
配置命令授权 1261
关于命令授权 1261
配置本地命令授权 1263
在 Commands TACACS+ 服务器上配置命令 1265
配置 TACACS+ 命令授权 1268
为本地数据库用户配置密码策略 1269

更改密码 1271
启用和查看登录历史记录 1272
配置管理访问记帐 1273
从锁定中恢复 1273
监控设备访问 1274
管理访问的历史记录 1277

第 43 章 软件和配置 1285
升级软件 1285
使用 ROMMON 加载映像（ISA 3000） 1285
升级 ROMMON 映像（ISA 3000） 1287
降级软件 1288
降级的准则和限制 1288
降级后删除了不兼容的配置 1290
降级 Firepower 1000、Cisco Secure Firewall 1200/3100/4200 1291
降级 Firepower 4100/9300 1291
降级 ISA 3000 1292
管理文件 1293
查看闪存中的文件 1293
从闪存中删除文件 1294
擦除闪存文件系统 1294
配置文件访问 1295
配置 FTP 客户端模式 1295
配置 ASA 安全复制服务器 1295
配置 ASA TFTP 客户端路径 1297
将文件复制到 ASA 1298
将文件复制到启动配置或运行配置 1300
设置 ASA 映像、ASDM 和启动配置 1302
备份和恢复配置或其他文件 1305
执行全面系统备份或还原 1305
开始备份或恢复之前 1305

备份系统 1307
恢复备份 1308
配置自动备份和恢复 (ISA 3000) 1309
配置自动备份 (ISA 3000) 1310
配置自动恢复 (ISA 3000) 1310
备份单模式配置或多模式系统配置 1312
备份闪存中的情景配置或其他文件 1313
在情景中备份情景配置 1314
从终端显示复制配置 1315
使用 Export 和 Import 命令备份附加文件 1315
使用脚本备份和恢复文件 1316
在开始使用备份和恢复脚本之前 1316
运行脚本 1316
样本脚本 1317
Cisco Secure Firewall 3100/4200上的热插拔 SSD 1322
禁用 USB 端口 1324
软件和配置的历史记录 1326

第 44 章 系统事件的响应自动化 1329
关于 EEM 1329
支持的事件 1329
事件管理器小程序上的操作 1330
输出目标 1330
EEM 准则 1330
配置 EEM 1331
创建事件管理器小应用程序并配置事件 1331
配置操作和操作输出的目标 1333
运行事件管理器小程序 1335
跟踪内存分配和内存使用 1335
EEM 示例 1338
监控 EEM 1339

EEM 的历史记录 1340

第 45 章 测试和故障排除 1341

恢复启用密码和 Telnet 密码 1341

恢复 ISA 3000 上的密码 1341

恢复 ASA Virtual上的密码或映像 1343

禁用 ISA 3000 硬件的密码恢复 1344

查看调试消息 1345

数据包捕获 1345

数据包捕获准则 1345

捕获数据包 1346

查看数据包捕获 1349

查看崩溃转储 1351

查看核心转储 1351

CPU 使用情况和报告 1351

ASA Virtual 中的 vCPU 使用率 1351

CPU 使用率示例 1352

VMware CPU 使用率报告 1352

ASA Virtual 和 vCenter 图表 1352

Amazon CloudWatch CPU 使用情况报告 1353

ASA Virtual 和 Amazon CloudWatch Graphs 1353

Azure CPU 使用率报告 1354

ASA Virtual 和 Azure Graphs 1354

Hyper-V CPU 使用率报告 1355

ASA Virtual 和 Hyper-V 图形 1355

OCI CPU 使用率报告 1356

ASA Virtual 和 OCI 图形 1356

测试配置 1356

测试基本连接：Ping 通地址 1357

使用 Ping 可测试的信息 1357

在 ICMP 和 TCP ping 之间进行选择 1357

启用 ICMP 1357
Ping 主机 1359
系统地测试 ASA 连接 1360
跟踪主机路由 1363
使 ASA 在跟踪路由中可见 1363
确定数据包路由 1364
使用数据包跟踪器测试策略配置 1366
监控连接 1368
测试和故障排除的历史记录 1368

第 VIII 部分： 监控 1371

第 46 章 日志记录 1373
关于日志记录 1373
多情景模式下的日志记录 1374
系统日志消息分析 1374
系统日志消息格式 1374
严重性级别 1376
系统日志消息过滤 1377
系统日志消息类 1377
自定义消息列表 1380
集群 1380
日志记录准则 1381
配置日志记录 1382
启用日志记录 1382
配置输出目标 1383
将系统日志消息发送至外部系统日志服务器 1383
将系统日志消息发送至内部日志缓冲区 1386
将系统日志消息发送给邮件消息 1388
将系统日志消息发送到 ASDM 1389
将系统日志消息发送到控制台端口 1391

将系统日志消息发送到 SNMP 服务器 1391
将系统日志消息发送到 Telnet 或 SSH 会话 1391
配置系统日志消息 1392
在系统日志显示或隐藏无效用户名 1392
在系统日志消息中包含日期和时间 1392
禁用系统日志消息 1393
更改系统日志消息的严重性级别 1393
在备用设备上阻止系统日志消息 1394
在非 EMBLEM 格式系统日志消息中包含设备 ID 1394
创建自定义事件列表 1395
配置日志记录过滤器 1396
将类中的所有系统日志消息发送到指定输出目标 1396
限制系统日志消息生成速率 1397
监控日志 1397
日志记录示例 1398
日志记录功能历史记录 1399

第 47 章 SNMP 1403
关于 SNMP 1403
SNMP 术语 1404
MIB 和陷阱 1404
SNMP 对象标识符 1406
物理供应商类型值 1409
MIB 中支持的表格和对象 1409
支持的陷阱（通知） 1411
接口类型和示例 1416
SNMP 第 3 版概述 1417
安全模型 1417
SNMP 组 1418
SNMP 用户 1418
SNMP 主机 1418

ASA 和思科 IOS 软件之间的实施差异 1418
SNMP 系统日志消息传递 1419
应用服务和第三方工具 1419
SNMP 准则 1419
配置 SNMP 1422
启用 SNMP 代理和 SNMP 服务器 1423
配置 SNMP 陷阱 1423
配置 CPU 使用率阈值 1424
配置物理接口阀值 1425
配置 SNMP 版本 1 或版本 2c 的参数 1425
配置 SNMP 第 3 版的参数 1427
配置用户组 1430
将用户与网络对象关联 1431
监控 SNMP 1431
SNMP 示例 1433
SNMP 的历史记录 1433

第 48 章 思科成功网络和遥测数据 1439
关于思科成功网络 1439
支持的平台和所需的配置 1439
ASA 遥测数据如何到达 SSE 云 1440
启用或禁用思科成功网络 1440
查看 ASA 遥测数据 1441
思科成功网络 - 遥测数据 1441
调试遥测数据 1447

第 49 章 **Anonymous Reporting 和 Smart Call Home** 1449
关于 Anonymous Reporting 1449
DNS 要求 1450
关于 Smart Call Home 1450
订用警报组 1451

警报组的属性 1451
通过警报组发送给思科的消息 1452
消息严重性阈值 1454
订用配置文件 1455
Anonymous Reporting 和 Smart Call Home 准则 1456
配置 Anonymous Reporting 和 Smart Call Home 1457
配置 Anonymous Reporting 1457
配置 Smart Call Home 1458
启用 Smart Call Home 1458
声明和验证证书颁发机构信任点 1459
配置环境和快照警报组 1460
配置警报组订用 1460
配置客户联系信息 1462
配置邮件服务器 1463
配置流量速率限制 1464
发送 Smart Call Home 通信 1465
配置目标配置文件 1465
复制目标配置文件 1467
重命名目标配置文件 1467
监控 Anonymous Reporting 和 Smart Call Home 1468
Smart Call Home 示例 1469
Anonymous Reporting 和 Smart Call Home 的历史记录 1470

第 IX 部分： 参考 1473

第 50 章 使用命令行界面 1475
防火墙模式和安全情景模式 1475
命令模式和提示符 1476
语法格式 1477
缩写命令 1478
命令行编辑 1478

命令补全 1478
命令帮助 1478
查看运行配置 1479
过滤 show 和 more 命令输出 1479
重定向和待处理 show 命令输出 1480
获取 show 命令输出的行计数 1480
命令输出分页 1481
添加注释 1482
文本配置文件 1482
命令如何与文本文件中的行相对应 1482
命令特定配置模式命令 1482
自动文本条目 1482
行顺序 1482
文本配置中不包括的命令 1483
密码 1483
多个安全情景文件 1483
支持的字符集 1483

第 51 章 地址、协议和端口 1485
IPv4 地址和子网掩码 1485
类 1485
专用网络 1486
子网掩码 1486
确定子网掩码 1486
确定要与子网掩码配合使用的地址 1487
IPv6 地址 1489
IPv6 地址格式 1489
IPv6 地址类型 1490
单播地址 1490
组播地址 1492
任播地址 1493

必需地址 1493
IPv6 地址前缀 1494
协议和应用 1494
TCP 和 UDP 端口 1495
本地端口和协议 1499
ICMP 类型 1500

关于本指南

以下主题介绍如何使用本指南。

- 文档目标，第 lix 页
- 相关文档，第 lix 页
- 文档约定，第 lix 页
- 通信、服务和其他信息，第 lx 页

文档目标

本指南旨在帮助您使用命令行界面为 Cisco Secure Firewall ASA 系列配置常规操作。本指南仅介绍最常见的一些配置场景，并未涵盖所有功能。

也可以使用自适应安全设备管理器 (ASDM) 这一基于 Web 的 GUI 应用来配置和监控 ASA。ASDM 提供配置向导指导您完成一些常见配置场景，并提供联机帮助以使您获得不常见场景的信息。

在本指南中，除非有专门指定，否则术语“ASA”一般适用于受支持的模型。

相关文档

有关详细信息，请参阅思科 *ASA* 系列文档一览，网址：http://www.cisco.com/go/asadocs。

文档约定

本文档遵循以下文本、显示和警报约定。

文本约定

约定	指示
boldface	命令、关键字、按钮标签、字段名称及用户输入的文本以**boldface**字体显示。对于基于菜单的命令，显示指向该命令的完整路径。

约定	指示
斜体	为其赋值的变量以斜体字体显示。 斜体字体还用于文档标题和一般强调。
等宽字体	系统显示的终端会话和信息以等宽字体格式显示。
{x | y | z}	必需的备选关键字集中在大括号内，以竖线分隔。
[ ]	方括号中的元素是可选项。
[x | y | z]	可选的备选关键字集中在方括号内，以竖线分隔。
[]	对于系统提示符的默认响应也位于方括号内。
< >	非打印字符（例如密码）位于尖括号内。
!、#	一行代码开头带有叹号 (!) 或星号 (#) 表示这是注释行。

读者提示

本文档采用以下格式的读者提示：

注释 表示读者需要注意的地方。注释部分包含有用的建议或本文档未涵盖材料的引用信息。

提示 表示以下信息可帮助您解决问题。

注意 表示读者应当小心处理。在这种情况下，您的操作可能会导致设备损坏或数据丢失。

便捷程序 表示所述操作可以节省时间。按照该段落中的说明执行操作，有助于节省时间。

警告 **表示读者需要注意。在这种情况下，操作可能会造成人身伤害。**

通信、服务和其他信息

- 要及时从思科收到相关信息，请注册思科配置文件管理器。

- 要使用重要技术实现您期望实现的业务结果，请访问思科服务。
- 要提交服务请求，请访问思科支持。
- 要了解并浏览安全且经过验证的企业级应用、产品、解决方案和服务，请访问思科 DevNet。
- 要获取一般网络、培训和认证主题相关的信息，请访问 Cisco Press。
- 要查找有关特定产品或产品系列的保修信息，请访问思科保修服务查找工具。

思科漏洞搜索工具

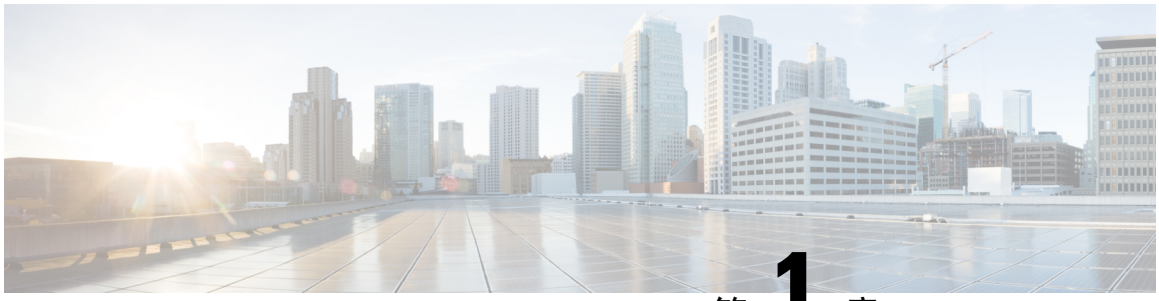
思科漏洞搜索工具 (BST) 是一款基于 Web 的工具，用作思科漏洞跟踪系统的网关，该系统包含一个关于思科产品和软件的缺陷和漏洞的综合列表。BST 提供关于您的产品和软件的详细漏洞信息。

关于本指南

第 部分

ASA 入门

- Cisco Secure Firewall ASA 简介， 第 1 页
- 使用入门， 第 11 页
- 许可证：用于 ISA 3000 的产品授权密钥许可， 第 41 页
- 许可证：智能软件许可， 第 79 页
- 逻辑设备 Firepower 4100/9300， 第 167 页
- 透明或路由防火墙模式， 第 189 页



第 1 章

Cisco Secure Firewall ASA 简介

Cisco Secure Firewall ASA 在一台设备提供高级状态防火墙和 VPN 集中器功能。ASA 包括许多高级功能，例如多安全情景（类似于虚拟化防火墙）、集群（将多个防火墙组合成一个防火墙）、透明（第 2 层）防火墙或路由（第 3 层）防火墙操作、高级检测引擎、IPsec VPN、SSL VPN 和无客户端 SSL VPN 支持以及许多其他功能。

- 硬件和软件兼容性， 第 1 页
- VPN 兼容性， 第 1 页
- 新增功能， 第 1 页
- 防火墙功能概述， 第 4 页
- VPN 功能概述， 第 8 页
- 安全情景概述， 第 8 页
- ASA 集群概述， 第 9 页
- 特殊服务和传统服务， 第 9 页

硬件和软件兼容性

有关受支持硬件和软件的完整列表，请参阅《思科 ASA 兼容性》。

VPN 兼容性

请参阅受支持的 VPN 平台（思科 ASA 系列）。

新增功能

本部分列出了每个版本的新功能。

注释 系统日志消息指南中列出了新增的、更改的和已弃用的系统日志消息。

ASA 9.22(1) 的新功能

发布日期：**2024** 年 **9** 月 **16** 日

注释 9.22(1) 未发布。

功能	说明
平台功能	
Cisco Secure Firewall 1210/1220	Cisco Secure Firewall 1210/1220 是一款紧凑型桌面防火墙，带有内置交换机和以太网供电+ (PoE+)，具体取决于型号。 • Cisco Secure Firewall 1210CE - 包括 8 个 1Gbps RJ-45 铜缆数据端口。 • Cisco Secure Firewall 1210CP - 其中四个端口上包含 PoE+。 • Cisco Secure Firewall 1220CX - 包括两个额外的 10Gbps SFP+ 端口和更高性能。
ASA Virtual 通过 GWLB 支持 AWS 上的双臂部署模式	ASA Virtual 现在支持在 AWS 上使用 GWLB 的双臂部署模式。此模式可使 ASA Virtual 在进行流量检查后，通过互联网网关直接将互联网流量转发到互联网，同时还可执行网络地址转换 (NAT)。 双臂模式不同于单臂模式，它有助于将检查到的出站流量路由回GWLB，然后通过互联网网关传输到互联网。 双臂模式支持在单 VPC 和多 VPC 网络环境中将已检查流量从 ASA Virtual转发到互联网。 ASA Virtual 中双臂模式的优势包括： • 最大限度地减少流量跳转，从而减少流量延迟，提高吞吐量性能。 • 整合并检查来自多个 VPC 的出站流量，然后再将其转发到互联网。 • 由于降低了基础设施要求，因此提供了一种经济高效的解决方案。 有关详细信息，请参阅《Cisco Secure Firewall ASA Virtual 入门指南，9.22》。
在 Kubernetes 或 Docker 环境中部署 Cisco Secure Firewall ASA 容器 (ASAc)	容器是一种软件包，它将代码和相关要求（如系统库、系统工具、默认设置等）捆绑在一起，以确保应用程序在计算环境中成功运行。您可以在开源 Kubernetes 或 Docker 环境中部署 ASA 容器 (ASAc)。
VMware ESXi 上的 ASA Virtual 支持	VMware 上的 ASA Virtual 现在支持 ESXi 版本 8.0。 有关详细信息，请参阅《Cisco Secure Firewall ASA Virtual 入门指南，9.22》。
防火墙功能	

功能	说明
对象组搜索优化。	对象组搜索功能得到了增强，可在评估访问控制规则以匹配连接时减少对象查找时间，并减少 CPU 开销。配置对象组搜索没有任何变化，优化行为会自动进行。 我们在设备 CLI 或增强的命令输出中添加了以下命令：**clear asp table network-object**、**debug ac logs**、**packet-tracer**、**show access-list**、**show asp table network-group**、**show object-group**。
高可用性和扩展性功能	
Cisco Secure Firewall 3100 和 4200 个最大集群节点增加到 16 个。	对于 Cisco Secure Firewall 3100 和 4200，最大节点数从 8 增加到 16。
Cisco Secure Firewall 3100 和 4200 集群独立接口模式	独立接口是正常的路由接口，每个接口都有自己的 本地 *IP* 地址 用于路由。每个接口的 主集群 *IP* 地址 是固定地址，始终属于控制节点。当控制节点更改时，主集群 IP 地址将转移到新的控制节点，使集群的管理得以无缝继续。 必须在上游交换机上分别配置负载均衡。 新增/修改的命令：**cluster interface-mode individual**
支持在 AWS 多可用性区域上部署 ASA Virtual 集群	现在，您可以在 AWS 区域的多个可用性区域内部署和配置 ASA Virtual 集群。集群还具有动态扩展能力 (Autoscale)，有助于根据需求增加或减少虚拟设备。 跨 AWS 区域中的多个可用性区域扩展 ASA Virtual 集群可以在灾难恢复期间实现持续的流量检测和动态扩展。 有关详细信息，请参阅在公共云中为 ASA Virtual 机部署群集。
许可证功能	
Smart Transport 是默认的智能许可传输	智能许可现在使用 Smart Transport 作为默认传输。如有必要，可以选择启用前一种类型 Smart Call Home 。 新增/修改的命令：**transport proxy**、**transport type**、**transport url**
ASAvU（无限制）许可证，用于部署具有 32 核和 64 核的 ASA Virtual	ASAvU 许可证可在 32 核和 64 核部署上实现最大吞吐量，仅在 VMware 和 KVM 上受支持。 新增/修改的命令：**throughput level unlimited**
管理、监控和故障排除功能	

功能	说明
禁用 USB 端口 (disk1)	默认情况下，type-A USB 端口 (disk1) 已启用并且无法禁用。现在，您可以在以下机型上出于安全目的禁用 USB 端口访问： • Firepower 1000 • Cisco Secure Firewall 3100 • Cisco Secure Firewall 4200 此设置存储在固件中，并且需要重新加载。此外，如果 USB 端口被禁用，并且您降级到不支持此功能的版本，则端口将保持禁用状态，并且在不清除NVRAM的情况下无法重新启用端口。 **注释** 此功能不会影响 type-B USB 控制台端口（如果有）。 新增/修改的命令： **usb-port disable**、**show usb-port**
VPN 功能	
DTLS 加密加速	Cisco Secure Firewall 4200 和 3100 系列支持 DTLS 加密加速。硬件执行 DTLS 加密和解密，并提高 DTLS 加密和 DTLS 解密流量的吞吐量。硬件还会对出口加密数据包执行优化，以改善延迟。 新增/修改的命令： **flow-offload-dtls**、**flow-offload-dtls egress-optimization**

防火墙功能概述

防火墙可防止外部网络上的用户在未经授权的情况下访问内部网络。防火墙同时可以为不同的内部网络提供保护，例如将人力资源网络与用户网络分开。如果需要向外部用户提供某些网络资源（例如 Web 服务器或FTP 服务器），可以将这些资源放置在防火墙后面单独的网络上（这种网络称为隔离区 (DMZ)）。防火墙允许有限访问 DMZ，但由于 DMZ 只包括公共服务器，因此发生在这个位置的攻击只会影响到服务器，而不会影响其他内部网络。还可以通过以下手段来控制内部用户何时可以访问外部网络（例如，访问互联网）：仅允许访问某些地址，要求身份验证或授权，配合使用外部 URL 过滤服务器。

讨论连接到防火墙的网络时，外部网络位于防火墙之前，内部网络可以得到保护，位于防火墙之后，*DMZ* 虽然位于防火墙之后，却可以限制外部用户的访问权限。由于 ASA 允许您配置许多安全策略不同的接口，包括许多内部接口、许多 DMZ 甚至许多外部接口（如果需要），则仅按照常规含义使用这些术语。

安全策略概述

安全策略确定哪些流量可通过防火墙来访问其他网络。默认情况下，ASA 允许流量从内部网络（较高安全性级别）自由流向外部网络（较低安全性级别）。可以将操作应用于流量，以自定义安全策略。

通过访问规则允许或拒绝流量

您可以应用访问规则，以限制从内部到外部的流量，或者允许从外部到内部的流量。对于网桥组接口，还可以应用 EtherType 访问规则来允许非 IP 流量。

应用 NAT

NAT 的一些优势如下：

- 可以在内部网络上使用专用地址。专用地址不能在互联网上进行路由。
- NAT 可隐藏其他网络的本地地址，使攻击者无法获悉主机的真实地址。
- NAT 可通过支持重叠 IP 地址来解决 IP 路由问题。

保护 IP 片段

ASA 提供 IP 片段保护。此功能对所有 ICMP 错误消息执行完全重组，并对通过 ASA 路由的剩余 IP 片段执行虚拟重组。系统会丢弃并记录未能通过安全检查的片段。不能禁用虚拟重组。

应用 HTTP、HTTPS 或 FTP 过滤

虽然可以使用访问列表来防止对于特定网站或 FTP 服务器的出站访问，但由于互联网的规模和动态性质，以这种方式配置和管理网络使用并不切合实际。

可以在 ASA 上配置云网络安全。您还可以将 ASA 与思科网络安全设备 (WSA) 等外部产品结合使用。

应用应用检测

针对在用户数据包内嵌入 IP 寻址信息的服务或在动态分配端口上打开辅助信道的服务，需要使用检测引擎。这些协议要求 ASA 执行深度数据包检测。

应用 QoS 策略

某些网络流量（例如声音和流传输视频）不允许出现长时间延迟。QoS 是一种网络功能，使您可以向此类流量赋予优先级。QoS 是指一种可以向所选网络流量提供更好服务的网络功能。

应用连接限制和 TCP 规范化

可以限制TCP连接、UDP连接和半开连接。限制连接和半开连接的数量可防止遭受DoS攻击。ASA 通过限制初期连接的数量来触发 TCP 拦截，从而防止内部系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。半开连接是源与目标之间尚未完成必要握手的连接请求。

TCP 规范化是指一种包含高级 TCP 连接设置的功能，用以丢弃有异常迹象的数据包。

启用威胁检测

可以配置扫描威胁检测和基本威胁检测，还可以配置如何使用统计信息来分析威胁。

基本威胁检测会检测可能与攻击（例如 DoS 攻击）相关的活动，并自动发送系统日志消息。

典型的扫描攻击包含测试子网中每个 IP 地址可达性（通过扫描子网中的多台主机或扫描主机或子网中的多个端口）的主机。扫描威胁检测功能确定主机何时执行扫描。ASA 扫描威胁检测功能与基于流量签名的 IPS 扫描检测不同，前者维护着一个广泛的数据库，其中包含可用来分析扫描活动的主机统计信息。

主机数据库跟踪可疑的活动（例如没有返回活动的连接、访问关闭的服务端口、如非随机 IPID 等易受攻击的 TCP 行为以及更多行为）。

您可以将 ASA 配置为发送有关攻击者的系统日志消息，也可以自动避开主机。

防火墙模式概述

ASA 在两种不同的防火墙模式下运行：

- 路由
- 透明

在路由模式下，ASA 被视为网络中的一个路由器跃点。

在透明模式下，ASA 如同是“线缆中的块”或“隐蔽的防火墙”，不被视为路由器跃点。ASA 在“网桥组”中连接至其内部和外部接口上的同一子网。

您可以使用透明防火墙简化网络配置。如果希望防火墙对攻击者不可见，透明模式同样有用。还可以针对在路由模式中会以其他方式被阻止的流量使用透明防火墙。例如，透明防火墙可通过 EtherType 访问列表允许组播数据流。

路由模式支持集成路由和桥接，因此也可以在路由模式下配置网桥组，并在网桥组和普通接口之间路由。在路由模式下，您可以复制透明模式功能；如果您不需要多情景模式或集群，可以考虑改用路由模式。

状态监测概述

系统使用自适应安全算法检测通过 ASA 的所有流量，要么允许通过，要么将其丢弃。简单的数据包过滤器可以检查源地址、目标地址和端口是否正确，但不会检查数据包序列或标记是否正确。过滤器还可以根据过滤器本身检查每个数据包，但这个过程可能比较慢。

注释 TCP 状态绕行功能使您可以自定义数据包流量。

但 ASA 等状态防火墙会考虑数据包的状态：

- 这是新连接吗？

  如果是新连接，ASA 必须对照访问列表检查数据包，并执行其他任务以确定允许还是拒绝数据包。为了执行此检查，会话的第一个数据包将通过“会话管理路径”，根据流量类型，它还可能通过“控制平面路径”。

  会话管理路径负责执行以下任务：

  - 执行访问列表检查
  - 执行路由查找
  - 分配 NAT 转换 (xlate)
  - 在“快速路径”中建立会话

  ASA 会在快速路径中为 TCP 流量创建转发和反向流；ASA 还会为无连接协议（例如 UDP、ICMP）创建连接状态信息（启用 ICMP 检测时），以便它们也可以使用快速路径。

  注释 对于其他 IP 协议，例如 SCTP，ASA 不会创建反向流路径。因此，涉及这些连接的 ICMP 错误数据包将被丢弃。

  需要第 7 层检测的某些数据包（必须检测或改变数据包负载）会传递到控制平面路径。具有两个或多个信道（一个使用已知端口号的数据信道，一个对每个会话使用不同端口号的控制信道，）的协议需要第 7 层检测引擎。这些协议包括 FTP、H.323 和 SNMP。

- 这是已建立的连接吗？

  如果连接已建立，则ASA不需要重新检查数据包；多数匹配的数据包都可以双向通过“快速”路径。快速路径负责执行以下任务：

  - IP 校验和验证
  - 会话查找
  - TCP 序列号检查
  - 基于现有会话的 NAT 转换
  - 第 3 层和第 4 层报头调整

  需要第 7 层检测的协议的数据包也可以通过快速路径。

  某些建立的会话数据包必须继续通过会话管理路径或控制平面路径。通过会话管理路径的数据包包括需要检测或内容过滤的 HTTP 数据包。通过控制平面路径的数据包包括需要第 7 层检测的协议的控制数据包。

VPN 功能概述

VPN 是一个跨 TCP/IP 网络（例如互联网）的安全连接，显示为私有连接。这种安全连接被称为隧道。ASA 使用隧道传输协议协商安全参数，创建和管理隧道，封装数据包，通过隧道收发数据包，然后再对它们解除封装。ASA 相当于一个双向隧道终端：可以接收普通数据包，封装它们，再将它们发送到隧道的另一端，在那里系统将对数据包解除封装并将其发送到最终目标。它也可以接收已封装的数据包，解除数据包封装，然后将它们发送到最终目标。ASA 可调用各种标准协议来完成这些功能。

ASA 可执行以下功能：

- 建立隧道
- 协商隧道参数
- 对用户进行身份验证
- 分配用户地址
- 数据加密和解密
- 管理安全密钥
- 管理隧道范围内的数据传输
- 按隧道终端或路由器方式管理入站和出站数据传输

ASA 可调用各种标准协议来完成这些功能。

安全情景概述

您可以将一台 ASA 设备分区成多个虚拟设备，这些虚拟设备被称为安全情景。每个 context 都是一台独立设备，拥有自己的安全策略、接口和管理员。多情景类似于拥有多台独立设备。多情景模式支持很多功能，包括路由表、防火墙功能、IPS 和管理；但是，某些功能不受支持。有关详细信息，请参阅相关功能章节。

在多情景模式中，ASA 包括用于每个情景的配置，其中确定安全策略、接口以及可以在独立设备中配置的几乎所有选项。系统管理员可在系统配置中配置情景以添加和管理情景；系统配置类似于单模式配置，是启动配置。系统配置可标识ASA的基本设置。系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。

管理情景类似于任何其他情景，唯一不同之处在于，当用户登录管理情景时，该用户拥有系统管理员权限并能访问系统和所有其他情景。

ASA 集群概述

通过ASA集群，您可以将多台ASA组合成单个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。

只能在控制设备上执行所有配置（引导程序配置除外）；然后配置将被复制到成员设备中。

特殊服务和传统服务

对于某些服务，可以在主配置指南和在线帮助以外找到相关文档。

特殊服务指南

特殊服务使 ASA 可以与其他思科产品实现互操作；例如，为电话服务提供安全代理（统一通信），同时提供僵尸网络流量过滤和思科更新服务器上的动态数据库，或者为思科网络安全设备提供 WCCP 服务。某些特殊服务在单独的指南中进行介绍：

- 思科 ASA 僵尸网络流量过滤器指南
- 思科 ASA NetFlow 实施指南
- 思科 ASA 统一通信指南
- 思科 ASA WCCP 流量重定向指南
- SNMP 版本 3 工具实施指南

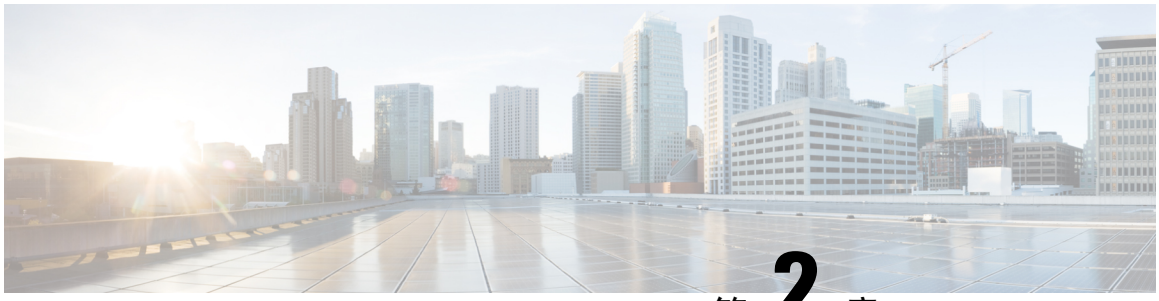
传统服务指南

ASA 仍支持传统服务，但可能还有更好的替代服务可供使用。传统服务在单独的指南中进行介绍：

思科 ASA 传统功能指南

本指南包含以下章节：

- 配置 RIP
- 适用于网络接入的 AAA 规则
- 使用保护工具，其中包括防止 IP 欺骗 (**ip verify reverse-path**)、配置分段大小 (**fragment**)、阻止不需要的连接 (**shun**)、配置 TCP 选项（适用于 ASDM）以及为基本 IPS 支持配置 IP 审核 (**ip audit**)。
- 配置过滤服务



第 2 章

使用入门

本章介绍如何开始使用 ASA。

- 访问命令行界面的控制台，第 11 页
- 配置 ASDM 访问，第 15 页
- 启动 ASDM，第 18 页
- 出厂默认配置，第 20 页
- 处理配置，第 34 页
- 将配置更改应用于连接，第 39 页
- 重新加载 ASA，第 39 页

访问命令行界面的控制台

对于初始配置，请从控制台端口直接访问 CLI。之后，您可以根据管理访问，第 1237 页使用 Telnet 或 SSH 配置远程访问。如果系统已处于多情景模式，则访问控制台端口会将您引导至系统执行空间。

注释 有关 ASA virtual 控制台访问，请参阅《 ASA virtual 快速入门指南》。

访问 ISA 3000 控制台

按照以下步骤访问设备控制台。

过程

步骤 1 使用所提供的控制台电缆将计算机连接到控制台端口，并使用已设置为 9600 波特、8 个数据位、无奇偶校验、1 个停止位、无流量控制功能的终端仿真器连接到控制台。

请参阅 ASA 硬件指南，了解有关控制台电缆的详细信息。

步骤 2 按 **Enter** 键将看到以下提示符：

```
ciscoasa>
```

此 提示符表明您正处于用户 EXEC 模式。用户 EXEC 模式仅能获取基本命令。

步骤 3 访问特权 EXEC 模式。

enable

第一次输入 **enable** 命令时，系统会提示您更改密码：

示例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

在特权 EXEC 模式中，所有非配置命令均可用。还可从特权 EXEC 模式进入 配置模式。

要退出特权模式，请输入 **disable**、**exit** 或 **quit** 命令。

步骤 4 访问全局配置模式。

configure terminal

示例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

可从全局配置模式开始配置 ASA。要退出全局配置模式，请输入 **exit**、 **quit** 或 **end** 命令。

访问 Firepower 1000和 Cisco Secure Firewall 1200/3100/4200 控制台

Firepower 1000 和 Cisco Secure Firewall 3100 1200/3100/4200 控制台端口可将您连接到 ASA CLI。然后，您可以在 ASA CLI 中使用 Telnet 连接到 FXOS CLI 进行故障排除。

过程

步骤 1 将管理计算机连接到控制台端口。确保为操作系统安装任何必要的串行驱动程序。使用以下串行设置：

- 9600 波特率
- 8 个数据位

- 无奇偶校验
- 1 个停止位

连接到 ASA CLI。默认情况下，访问控制台时不需要提供用户凭证。

步骤 2 访问特权 EXEC 模式。

enable

第一次输入 **enable** 命令时，系统会提示您更改密码。

示例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

如果 ASA 无法启动，并且您进入 FXOS 故障保护模式，则您在 ASA 上设置的启用密码也是 FXOS **管理员**用户密码。

在特权 EXEC 模式中，所有非配置命令均可用。还可从特权 EXEC 模式进入 配置模式。

要退出特权 EXEC 模式，请输入 **disable**、**exit** 或 **quit** 命令。

步骤 3 访问全局配置模式。

configure terminal

示例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

可从全局配置模式开始配置 ASA。要退出全局配置模式，请输入 **exit**、**quit** 或 **end** 命令。

步骤 4 （可选） 连接到 FXOS CLI。

connect fxos [**admin**]

- **admin**- 提供管理员级的访问权限。如果不选择此选项，用户将拥有只读访问权限。请注意，即使在管理员模式下，也没有任何配置命令可用。

系统不会提示您提供用户凭证。当前的 ASA 用户名将传递给FXOS，无需其他登录。要返回到 ASA CLI，请输入 **exit** 或键入 **Ctrl-Shift-6**、**x**。

在 FXOS 中，您可以使用 **scope security/show audit-logs** 命令查看用户活动。

示例：

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
```

```
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

访问 Firepower 4100/9300 机箱上的 ASA 控制台

对于初始配置，请通过依次连接到Firepower 4100/9300 机箱管理引擎（连接控制台端口或使用 Telnet 或 SSH 进行远程连接）和 ASA 安全模块来访问命令行界面。

过程

步骤 1 连接到 Firepower 4100/9300 机箱管理引擎 CLI（控制台或 SSH），然后将会话连接到 ASA：

connect module *slot* {**console** | **telnet**}

使用 Telnet 连接的优点在于，您可以同时对模块开展多个会话，并且连接速度更快。

首次访问模块时，您将访问 FXOS 模块 CLI。然后必须连接到 ASA 应用。

connect asa

示例：

```
Firepower# connect module 1 console
Firepower-module1> connect asa

asa>
```

步骤 2 访问授权的 EXEC 模式，该模式具有最高权限级别。

enable

第一次输入 **enable** 命令时，系统会提示您更改密码。

示例：

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa#
```

在特权 EXEC 模式中，所有非配置命令均可用。还可从特权 EXEC 模式进入 配置模式。

要退出特权模式，请输入 **disable**、**exit** 或 **quit** 命令。

步骤 3 进入全局配置 模式。

configure terminal

示例：

```
asa# configure terminal
asa(config)#
```

要退出全局配置模式，请输入 **disable**、**exit** 或 **quit** 命令。

步骤 4 输入 **Ctrl-a, d** 使应用程序控制台返回到 FXOS 模块 CLI

出于故障排除目的，您可能想使用 FXOS 模块 CLI。

步骤 5 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 **Telnet** 会话：

a) 输入 **Ctrl-],**。

配置 ASDM 访问

本节介绍如何通过默认配置访问 ASDM，以及在没有默认配置的情况下如何配置访问。

使用出厂默认配置进行 ASDM 访问

通过出厂默认配置，已采用默认网络设置对 ASDM 连接进行了预配置。

过程

使用以下接口和网络设置连接到 ASDM：

- 管理接口取决于设备型号：
  - Firepower 1010、Cisco Secure Firewall 1210/1220—Management 1/1 (192.168.45.1)，或内部以太网 1/2 至 1/8（1010 和 1210）或 1/10 (1220) (192.168.1.1)。管理主机限制为 192.168.45.0/24 网络，内部主机限制为 192.168.1.0/24 网络。

- 设备模式下的 Firepower 1100、 Cisco Secure Firewall 3100、4200 - 内部以太网 1/2 (192.168.1.1) 或 Management 1/1（来自 DHCP）。内部主机限制为 192.168.1.0/24 网络。管理主机允许来自任何网络。
- Firepower 4100/9300 - 部署时定义的管理类型接口和您选择的 IP 地址。管理主机允许来自任何网络。
- ASA Virtual- Managemetn 0/0（在部署期间设置）。管理主机仅限于管理网络。
- ISA 3000 - Management 1/1 (192.168.1.1)。管理主机受限于192.168.1.0/24 网络。

注释
如果更改为多情景模式，则可使用上述网络设置从管理情景访问 ASDM。

相关主题

出厂默认配置，第 20 页
启用或禁用多情景模式，第 228 页
启动 ASDM，第 18 页

自定义 ASDM 访问

如果满足一个或多个以下条件，可使用该程序：

- 没有出厂默认配置
- 想要更改管理 IP 地址
- 想要更改为透明防火墙模式
- 想要更改为多情景模式

对于单一路由模式，为了实现快速轻松的 ASDM 访问，我们建议应用出厂默认配置，但可选择设置您自己的管理 IP 地址。只有您有特殊需求（如设置透明或多情景模式）或有需要保留的其他配置时，才应使用本节所述程序。

注释 对于 ASAv，可以在部署过程中配置透明模式，所以此程序主要用在类似于部署之后需要清除配置等情况。

过程

步骤 1 在控制台端口访问 CLI。

步骤 2 （可选）启用透明防火墙模式：

该命令清除您的配置。

firewall transparent

步骤 3 配置管理接口：

```
interface interface_id
   nameif name
   security-level level
   no shutdown
   ip address ip_address mask
```

示例：

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

security-level 是介于 1 到 100 之间的数字，其中 100 为最安全级别。

步骤 4 （对于直连管理主机）为管理网络设置 DHCP 池：

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

示例：

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

确保此范围内不包括接口地址。

步骤 5 （对于远程管理主机）配置管理主机路由：

route *management_ifc management_host_ip mask gateway_ip* **1**

示例：

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

步骤 6 为 ASDM 启用 HTTP 服务器：

http server enable

步骤 7 允许管理主机访问 ASDM：

http *ip_address mask interface_name*

示例：

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

步骤 8 保存配置：

write memory

步骤 9 （可选）将模式设置为多模式：

mode multiple

出现提示时，请确认要将现有配置转换为管理情景。然后系统将提示重新加载 ASA。

示例

以下配置将防火墙模式转换为透明模式，配置 Management 0/0 接口，并为管理主机启用 ASDM：

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

相关主题

恢复出厂默认配置，第 20 页
设置防火墙模式，第 198 页
访问 ISA 3000 控制台，第 11 页
启动 ASDM，第 18 页

启动 ASDM

使用 ASDM-IDM 启动程序启动 ASDM。启动器是使用您可以连接用其连接到任意 ASA IP 地址的 Web 浏览器从 ASA 下载的一款应用。如果要连接至其他 ASA，无需重新下载该启动器。

在 ASDM 内，可以选择其他 ASA IP 地址进行管理。

本节介绍最初如何连接 ASDM，以及如何使用启动程序启动 ASDM。

ASDM 将文件存储在本地 \Users\<user_id>\.asdm 目录（包括缓存、日志和首选项）和临时目录中（包括 Secure Client 配置文件）中。

过程

步骤 1 在指定为 ASDM 客户端的计算机上，输入以下 URL：

https://*asa_ip_address*/**admin**

注释
确保指定 **https://**，而非指定 **http://** 或只指定 IP 地址（默认为 HTTP）；ASA 不会自动将 HTTP 请求转发到 HTTPS。

系统将显示 ASDM 启动页面和以下按钮：

安装 ASDM 启动程序 (Install ASDM Launcher)

步骤 2 要下载启动程序并开始 ASDM，请执行以下操作：

a) 点击**安装 ASDM 启动程序 (Install ASDM Launcher)**。

图 *1:* 安装 ***ASDM*** 启动程序

b) 将用户名和密码字段留空（适用于新安装），然后点击**确定 (OK)**。

如果未配置 HTTPS 身份验证，可以在没有用户名和 **enable** 密码（默认为空）的情况下获得对 ASDM 的访问权限。首次在 CLI 中输入 **enable** 命令时，系统会提示您更改密码；登录 ASDM 时不会强制执行此行为。建议您尽快更改启用密码，不要再保持空白状态；请参阅 设置主机名、域名及启用密码和 Telnet 密码，第 815 页。**注意**：如果您启用了 HTTPS 身份验证，则输入您的用户名及关联的密码。即使不使用身份验证，如果您在登录屏幕输入用户名和密码（而不是将用户名留空），ASDM 也会从本地数据库中检查是否有匹配项。

c) 将安装程序保存到计算机，然后启动安装程序。安装完成后，将自动打开 ASDM-IDM 启动程序。

d) 输入管理 IP 地址、同一个用户名和密码（新安装则留空），然后点击**确定 (OK)**。

出厂默认配置

出厂默认配置是思科对新的 ASA 应用的配置。

- Firepower 1010 - 出厂默认配置启用功能性内部/外部配置。您可以从管理接口或内部交换机端口使用 ASDM 管理 ASA。
- Firepower 1100 - 出厂默认配置启用功能性内部/外部配置。您可以从管理接口或内部接口使用 ASDM 管理 ASA。
- Secure Firewall 1210/1220 - 出厂默认配置启用功能性内部/外部配置。您可以从管理接口或内部交换机端口使用 ASDM 管理 ASA。
- Cisco Secure Firewall 3100 - 出厂默认配置启用功能性内部/外部配置。您可以从管理 1/1 接口或内部接口使用 ASDM 管理 ASA。
- Cisco Secure Firewall 4200 - 出厂默认配置启用功能性内部/外部配置。您可以从管理 1/1 接口或内部接口使用 ASDM 管理 ASA。
- Firepower 4100/9300 机箱 - 在部署独立 ASA 或 ASA 集群时，出厂默认配置可配置管理接口，以便可以使用 ASDM 与其连接，然后通过它完成配置。
- ASA Virtual- 根据虚拟机监控程序，在部署过程中，部署配置（初始虚拟部署设置）可配置管理接口，以便可以使用 ASDM 与其连接，然后通过它完成配置。还可以配置故障转移 IP 地址。还可应用“出厂默认”配置（如果需要）。
- ISA 3000 - 出厂默认配置是几乎完全透明的防火墙模式配置，所有内部和外部接口都位于同一网络中；您可以使用 ASDM 连接到管理接口来设置网络的 IP 地址。已为两个接口对 。

对于设备 ，出厂默认配置仅可用于路由防火墙模式和单一情景模式，除了 ISA 3000，后者的出厂默认配置仅在透明模式中可用。对于 ASA virtual 和 Firepower 4100/9300 机箱，可以在部署时选择透明模式或路由模式。

注释 除映像文件和（隐藏的）默认配置外，以下文件夹和文件是闪存中的标准配置：log/、crypto_archive/ 和 coredumpinfo/coredump.cfg。这些文件上的日期可能与闪存中映像文件的日期不匹配。这些文件有助于潜在的故障排除；它们不表示已发生故障。

恢复出厂默认配置

本节介绍如何恢复出厂默认配置。对于 ASA virtual，该程序可擦除部署配置并对各 ASA 5525-X 应用以下配置：

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
!
asdm logging informational
asdm history enable
!
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```

注释 在 Firepower 4100/9300 上，恢复出厂默认配置会擦除配置；要恢复默认配置，必须从管理引擎重新部署 ASA。

开始之前

此功能仅在路由防火墙模式下可用，但 ISA 3000 除外，ISA 3000 仅在透明模式下支持此命令。此外，该功能仅可用于单一情景模式；已清除配置的ASA没有任何定义的情景可使用该功能自动进行配置。

过程

步骤 1 恢复出厂默认配置：

configure factory-default [*ip_address* [*mask*]]

示例：

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

如果指定 *ip_address*，则根据设备型号设置内部或管理接口 IP 地址，而不是使用默认 IP 地址。有关由 *ip_address* 选项设置的接口，请参阅以下型号准则：

- Firepower 1010 - 设置**管理**界面 IP 地址。
- Firepower 1100-设置内部接口IP地址。
- Cisco Secure Firewall 1210/1220-设置 **管理** 接口 IP 地址。
- Cisco Secure Firewall 3100 - 设置**内部**接口IP地址。
- Cisco Secure Firewall 4200 - 设置**内部**接口IP地址。
- Firepower 4100/9300-无影响。
- ASA Virtual—设置 **管理** 接口 IP 地址。

- ISA 3000 - 设置管理接口 IP 地址。

http 命令使用您指定的子网。同样，**dhcpd address** 命令范围包含比你指定的 IP 地址更高的所有可用地址。例如，如果指定10.5.6.78，子网掩码为255.255.255.0，则DHCP地址范围为10.5.6.79-10.5.6.254。

对于 Firepower 1000 和Cisco Secure Firewall 1200、3100、4200：此命令会清除 **boot system** 命令（如有）以及配置的其余部分。此配置更改不会影响启动时的映像：继续使用当前加载的映像。

对于所有其他型号：此命令可清除 **boot system** 命令（如果存在）和其他配置。该命令允许您从特定映像启动。**boot system** 下次在恢复出厂配置后重新加载 ASA 时，它将从内部闪存的第一个映像启动；如果内部闪存中无映像，ASA 将不启动。

示例：

```
docs-bxb-asa3(config)# configure factory-default 10.86.203.151 255.255.254.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
WARNING: The new maximum-session limit will take effect after the running-config is saved
and the system boots next time. Command accepted
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.86.203.151 255.255.254.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.86.202.0 255.255.254.0 management
Executing command: dhcpd address 10.86.203.152-10.86.203.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

步骤 2 将默认配置保存到闪存：

write memory

该命令将运行配置保存到启动配置的默认位置，即使以前已将 **boot** config 命令配置为设置另一个位置也是如此；配置清除后，该路径也将清除。

恢复 ASA Virtual 部署配置

本节介绍如何恢复 ASA virtual 部署（第 0 天）配置。

过程

步骤 1 为了执行故障转移，请关闭备用设备。

为防止备用设备变成主用设备，必须将其关闭。如果让其处于打开状态，则当清除主用设备配置后，备用设备将变为主用设备。当原来的主用设备重新加载并且通过故障转移链路重新连接后，旧配置将从新主用设备同步，并且擦除所需要的部署配置。

步骤 2 重新加载后，恢复部署配置。为了执行故障转移，请在主用设备上输入以下命令：

write erase

注释
ASA virtual 会启动当前运行的映像，因此，不会恢复到原始启动映像。要使用原始启动映像，请参阅 **boot image** 命令。

请勿保存该配置。

步骤 3 重新加载 ASA virtual，并加载部署配置：

reload

步骤 4 为了执行故障转移，请开启备用设备。

主用设备重新加载后，开启备用设备。部署配置将同步备用设备。

Firepower 1010 默认配置

Firepower 1010 的出厂默认配置包含以下配置：

- **硬件交换机** - 以太网 1/2 至 1/8 属于 VLAN 1
- **内部→外部**流量 - 以太网 1/1（外部），VLAN1（内部）
- **管理** - 管理端口 1/1（管理），IP 地址 192.168.45.1
- **外部 IP 地址**来自 DHCP，**内部 IP 地址**—192.168.1.1
- 内部接口、管理接口上的 **DHCP 服务器**
- 来自外部 DHCP 的**默认路由**
- **ASDM** 访问 - 允许管理和内部主机。管理主机限制为 192.168.45.0/24 网络，内部主机限制为 192.168.1.0/24 网络。
- **NAT** - 从内部到外部所有流量的接口 PAT。
- **DNS** 服务器 - OpenDNS 服务器已预配置。

配置由以下命令组成：

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
```

```
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Firepower 1100 默认配置

Firepower 1100 的出厂默认配置包含以下配置：

- **内部→外部流量** - 以太网 1/1（外部），以太网 1/2（内部）
- **外部 IP 地址**来自 DHCP，**内部 IP 地址**—192.168.1.1
- **管理**—管理 1/1（管理），IP 地址来自 DHCP
- **DHCP 服务器**在内部接口上
- **默认路由** 来自外部 DHCP，管理 DHCP
- **ASDM** 访问 - 允许管理和内部主机。内部主机限制为 192.168.1.0/24 网络。
- **NAT** - 从内部到外部所有流量的接口 PAT。
- **DNS** 服务器 - OpenDNS 服务器已预配置。

配置由以下命令组成：

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
```

```
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 1210/1220 默认配置

Cisco Secure Firewall 1210/1220 的默认出厂配置用于配置以下内容：

- **硬件交换机** - 以太网 1/2 至 1/8 (1210) 或以太网 1/2 至 1/10 (1220) 属于 VLAN 1
- **内部→外部**流量 - 以太网 1/1（外部），VLAN1（内部）
- **管理** - 管理端口 1/1（管理），IP 地址 192.168.45.1
- **外部 IP 地址**来自 DHCP，**内部 IP 地址**—192.168.1.1
- 内部接口、管理接口上的 **DHCP 服务器**
- 来自外部 DHCP 的**默认路由**
- **ASDM** 访问 - 允许管理和内部主机。管理主机限制为 192.168.45.0/24 网络，内部主机限制为 192.168.1.0/24 网络。
- **NAT** - 从内部到外部所有流量的接口 PAT。
- **DNS** 服务器 - OpenDNS 服务器已预配置。

配置由以下命令组成：

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
```

```
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
! 1220
interface Ethernet1/9
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
! 1220
interface Ethernet1/10
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
!
dhcpd auto_config outside
```

```
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 3100 默认配置

Cisco Secure Firewall 3100 的默认出厂配置用于配置以下内容：

- **内部→外部流量** - 以太网 1/1（外部），以太网 1/2（内部）
- **外部 IP 地址**来自 DHCP，**内部 IP 地址**—192.168.1.1
- **管理**—管理 1/1（管理），IP 地址来自 DHCP
- **DHCP 服务器**在内部接口上
- **默认路由** 来自外部 DHCP，管理 DHCP
- **ASDM** 访问 - 允许管理和内部主机。内部主机限制为 192.168.1.0/24 网络。
- **NAT** - 从内部到外部所有流量的接口 PAT。
- **DNS** 服务器 - OpenDNS 服务器已预配置。

配置由以下命令组成：

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
```

```
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 4200默认配置

Cisco Secure Firewall 4200 的默认出厂配置用于配置以下内容：

- **内部→外部流量** - 以太网 1/1（外部），以太网 1/2（内部）
- **外部 IP 地址**来自 DHCP，**内部 IP 地址**—192.168.1.1
- **管理**—管理 1/1（管理），IP 地址来自 DHCP
- **DHCP 服务器**在内部接口上
- **默认路由** 来自外部 DHCP，管理 DHCP
- **ASDM** 访问 - 允许管理和内部主机。内部主机限制为 192.168.1.0/24 网络。
- **NAT** - 从内部到外部所有流量的接口 PAT。
- **DNS** 服务器 - OpenDNS 服务器已预配置。

配置由以下命令组成：

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
```

```
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Firepower 4100/9300 机箱 默认配置

在 Firepower 4100/9300 机箱上部署 ASA 时，可预设置许多可供您使用 ASDM 连接到 Management 0/0 接口的参数。典型配置包括以下设置：

- 管理接口：
  - 您选择的管理类型接口已在 Firepower 4100/9300 机箱管理引擎上定义
  - 命名为“management”
  - 您选择的 IP 地址
  - 安全级别为 0
  - 管理专用
- 通过管理接口的默认路由
- ASDM 访问 - 允许所有主机。

独立设备的配置包括以下命令。有关集群设备的其他配置，请参阅创建 ASA 集群，第 441 页。

```
interface <management_ifc>
  management-only
  ip address <ip_address> <mask>
  ipv6 address <ipv6_address>
  ipv6 enable
  nameif management
  security-level 0
  no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

ISA 3000 默认配置

ISA 3000 的默认出厂配置如下：

- **透明防火墙模式** - 透明防火墙是第 2 层防火墙，充当“嵌入式防火墙”或“隐藏防火墙”，并且不会被视为所连接设备的路由器跃点。
- **1 个网桥虚拟接口** - 所有成员接口都位于同一网络中（**IP 地址未预先配置；必须进行设置以与您的网络相匹配**）：GigabitEthernet 1/1 (outside1)、GigabitEthernet 1/2 (inside1)、GigabitEthernet 1/3 (outside2)、GigabitEthernet 1/4 (inside2)
- 所有**内部和外部**接口均可互相通信。
- **管理 1/1 接口** - 192.168.1.1/24 用于 ASDM 访问。
- 用于管理上的客户端的 **DHCP**。
- **ASDM** 访问 - 允许管理主机。
- 为以下接口对启用了**硬件旁路**：GigabitEthernet 1/1 和 1/2；GigabitEthernet 1/3 和 1/4

注释 当ISA 3000断电并进入硬件旁路模式时，只有上述接口对能够通信；inside1 和 inside2 以及 outside1 和 outside2 将不再能通信。这些接口之间的任何现有连接都将断开。在恢复供电后，将随着 ASA 接管流而发生短暂的连接中断。

配置由以下命令组成：

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
```

```
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management
```

ASA Virtual 部署配置

部署 ASA virtual 时，可预设置许多可供您使用 ASDM 连接到 Management 0/0 接口的参数。典型配置包括以下设置：

- 路由或透明防火墙模式
- Management 0/0 接口：
  - 命名为“management”
  - IP 地址或 DHCP
  - 安全级别为 0
- 管理主机 IP 地址的静态路由（如果其没有位于管理子网中）
- 启用或禁用 HTTP 服务器
- 管理主机 IP 地址的 HTTP 访问
- （可选）GigabitEthernet 0/8 的故障转移链路 IP 地址和 Management0/0 备用 IP 地址
- DNS 服务器
- 智能许可 ID 令牌
- 智能许可吞吐量水平和 基础 功能层
- 智能传输 URL (https://smartreceiver.cisco.com/licservice/license) 和端口 80。
- （可选）Smart Transport 代理 URL 和端口
- （可选）SSH 管理设置：

- 客户端 IP 地址
- 本地用户名和密码
- 使用本地数据库进行 SSH 所需的身份验证

- （可选）启用或禁用 REST API

注释 要向思科许可颁发机构成功注册 ASA virtual，ASA virtual需要访问互联网。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

有关独立设备，请参阅以下配置示例：

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
http server enable
http managemment_host_IP mask management
route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
```

注释 基础许可证过去称为“标准”许可证。

有关故障转移对中的主要设备，请参阅以下配置示例：

```
nameif management
  security-level 0
  ip address ip_address standby standby_ip

  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
```

```
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

处理配置

本节介绍如何处理配置。除非另有说明，否则本节中的信息适用于单一安全情景和多安全情景。

关于启动配置和运行配置

启动配置

当ASA启动时，它会从文本文件（称为启动配置）加载配置。默认情况下，该文件作为隐藏文件驻留在内部闪存中。但是，您可以为可视文件系统中的启动配置指定不同的文件。请使用以下命令来指定新的启动配置：

boot config {**disk0:/** | **disk1:/**} [*path*/]*filename*

保存新位置：

write memory

例如：

```
ciscoasa (config)# boot config disk0:/startup.cfg
ciscoasa (config)# write memory
```

使用大型配置

隐藏的启动目录的空间有限。如果配置非常大（例如，超过了 16 MB），那么您将无法保存启动配置。在这种情况下，您必须使用 **boot config** 命令将启动配置保存到可视文件系统。例如，如果您将大型配置加载到运行内存中并尝试保存，如果输入 **write memory** 并且配置过大，您可能会看到以下错误消息：

```
%错误写入。nvram:/startup-config（设备上没有剩余空间）
```

在这种情况下，请确保在重新加载 ASA 之前将运行配置重新保存到新的文件位置。否则，ASA 可能无法加载完整的配置。

运行配置

输入命令时，仅对内存中的运行配置进行更改。必须将运行配置手动保存到启动配置，以便重新加载后更改仍旧有效。

保存配置更改

本节介绍如何保存配置。

在单情景模式下保存配置更改

要将运行配置保存到启动配置，请执行以下程序。

过程

将运行配置保存到启动配置中。

write memory

注释
copy running-config startup-config 命令等同于 **write memory** 命令。

在多情景模式下保存配置更改

可分别保存每个情景（和系统）配置，或者，也可同时保存所有情景配置。

分别保存每个情景和系统

使用以下程序保存系统或情景配置。

过程

从情景或系统中，将运行配置保存到启动配置：

write memory

对于多情景模式，情景启动配置可以驻留在外部服务器。在这种情况下，ASA 会将配置重新保存至您在情景 URL 中标识的服务器，但 HTTP 或 HTTPS URL 除外，它们不允许您将配置保存至服务器。

注释
copy running-config startup-config 命令等同于 **write memory** 命令。

同时保存所有情景配置

请按照以下操作步骤同时保存所有情景配置以及系统配置。

过程

从系统执行空间，将运行配置保存到所有情景的启动配置和系统配置：

write memory all [**/noconfirm**]

如果不输入 **/noconfirm** 关键字，则将看到以下提示：

```
Are you sure [Y/N]:
```

在输入 **Y** 后，ASA 会保存系统 配置和每个情景。情景启动配置可驻留在外部服务器上。在这种情况下，ASA 会将配置保存回 您在情景 URL 中标识的服务器，但 HTTP 或 HTTPS URL 除外， 它们不允许您将配置保存到服务器。

在 ASA 保存每个情景后，系统将显示以下消息：

```
‘Saving context ‘b’ ... ( 1/3 contexts saved ) ’
```

有时，情景会由于出错 而不能保存。请参阅以下错误的相关信息：

- 对于因内存不足而未保存的情景，系统将显示以下消息：

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- 对于因无法到达远程目标而未保存的情景，系统将显示以下消息：

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- 对于因情景被锁定而无法保存的情景，系统将显示以下消息：

  ```
  Unable to save the configuration for the following contexts as these contexts are locked.
  context ‘a’ , context ‘x’ , context ‘z’ .
  ```

  仅在其他用户已 在保存配置或正在删除情景时，才会锁定情景。

- 对于因启动配置为只读配置而不能保存的情景（例如，在 HTTP 服务器上），在所有其他消息的末尾将显示以下消息报告：

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context ‘a’ , context ‘b’ , context ‘c’ .
  ```

- 对于因闪存扇区错误而未保存的情景，系统将显示以下消息：

```
The context 'context a' could not be saved due to Unknown errors
```

将启动配置复制到运行配置

使用以下命令之一，将新启动配置复制到运行配置：

- **copy startup-config running-config**

  将启动配置与运行配置合并。合并会将新配置中的所有新命令添加到运行配置中。如果配置相同，则不会发生任何更改。如果命令冲突或命令影响情景的运行，则合并的影响取决于命令。可能会发生错误，也可能出现意外结果。

- **reload**

  重新加载 ASA，即加载启动配置并丢弃运行配置。

- **clear configure all**，然后 **copy startup-config running-config**

  加载启动配置并丢弃运行配置，无需重新加载。

查看配置

以下命令可供您查看运行配置和启动配置：

- **show running-config**

  查看运行配置。

- **show running-config** *command*

  查看特定命令的运行配置。

- **show startup-config**

  查看启动配置。

清除和删除配置设置

要擦除设置，请输入以下命令之一：

- **clear configure** *configurationcommand* [*level2configurationcommand*]

  清除指定命令的所有配置。如果只想清除特定版本命令的配置，则可输入 *level2configurationcommand* 的值。

  例如，要清除所有 **aaa** 命令的配置，请输入以下命令：

```
ciscoasa(config)# clear configure aaa
```

要仅清除 **aaa authentication** 命令的配置，请输入以下命令：

```
ciscoasa(config)# clear configure aaa authentication
```

- **no** *configurationcommand* [*level2configurationcommand*] *qualifier*

  禁用命令的特定参数或选项。在这种情况下，可使用 **no** 命令删除 *qualifier* 识别的特定配置。

  例如，要删除特定 **access - list** 命令，请输入足够命令对其进行唯一标识；可能必须输入整个命令：

```
ciscoasa(config)# no access-list abc extended permit icmp any any object-group obj_icmp_1
```

- **write erase**

  擦除启动配置。

注释 对于 ASA virtual，此命令将在重新加载后恢复部署配置。要完全擦除配置，请使用 **clear configure all** 命令。

- **clear configure all**

  擦除运行配置。

注释 在多情景模式下，如果从系统配置输入 **clear configure all**，还将删除所有情景并使它们停止运行。情景配置文件将不擦除，仍保留在原始位置。

注释 对于 Firepower 1000 和Cisco Secure Firewall 1200、3100、4200：此命令会清除 **boot system** 命令（如有）以及配置的其余部分。此配置更改不会影响启动时的映像：继续使用当前加载的映像。

对于所有其他型号：此命令可清除 **boot system** 命令（如果存在）和其他配置。**boot** system 命令使您可以从特定映像上启动，包括外部闪存卡上的映像。下次重新加载 ASA 时，它将从内部闪存的第一个映像启动；如果内部闪存中无映像，则 ASA 将不启动。

离线创建文本配置文件

本指南介绍如何使用 CLI 配置 ASA；保存命令时，更改将写入文本文件。但是，如果不使用 CLI，则可以直接在计算机上编辑文本文件，并将配置完整地或逐行粘贴在配置模式命令行提示符处。或者，也可将文本文件下载至 ASA 内部闪存。有关如何将配置文件下载至 ASA 的信息，请参阅软件和配置，第 1285 页。

在大多数情况下，本指南所述的命令之前都有CLI提示符。以下示例中的提示为“ciscoasa(config)#”：

```
ciscoasa(config)# context a
```

在文本配置文件中，系统不提示您输入命令，因此提示符省略如下：

```
context a
```

有关格式化文件的其他 信息，请参阅 使用命令行界面，第 1475 页。

将配置更改应用于连接

更改配置的安全策略后，所有新连接将使用新安全策略。现有连接将继续使用在连接建立时配置的策略。原连接的 **show** 命令输出反映原配置，在某些情况下将不包括关于原连接的数据。

例如，如果要从接口删除 QoS **service-policy**，然后重新添加修改版本，则 **show service-policy** 命令仅显示与匹配新服务策略的新连接相关联的 QoS 计数器；旧策略的现有连接不再显示在命令输出中。

要确保所有连接使用新策略，需要断开当前连接，以便其使用新策略重新连接。

要断开连接，请输入以下命令：

- **clear conn** [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip* [*-src_ip*] [**netmask** *mask*]] [**port** *src_port* [*-src_port*]] [**address** *dest_ip* [*-dest_ip*] [**netmask** *mask*]] [**port** *dest_port* [*-dest_port*]]

  该命令可在任何状态中终止连接。要查看所有当前连接，请参阅 **show conn** 命令。

  如果不带参数，该命令将清除所有受影响的出站连接。要清除入站连接（包括当前的管理会话），请使用 **all** 关键字。要根据源 IP 地址、目标 IP 地址、端口和/或协议清除特定连接，可以指定所需选项。

重新加载 ASA

要重新加载 ASA，请完成以下操作步骤。

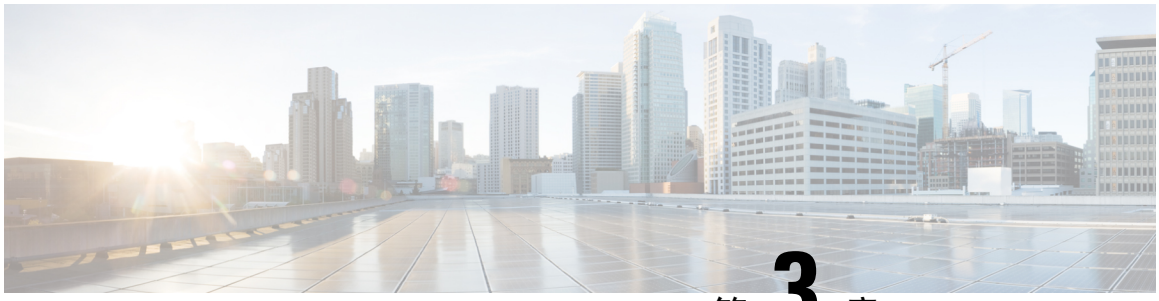
reload 命令不会复制到数据节点以进行集群，也不会复制到备用/辅助设备进行故障转移。

在多情景模式下，仅可从系统执行空间重新加载。

过程

重新加载 ASA。

reload



第 3 章

许可证：用于 ISA 3000 的产品授权密钥许可

许可证指定在给定 ASA 上启用的选项。本文档介绍所有物理 ISA 3000 的产品授权密钥 (PAK) 许可证。有关其他型号，请参阅 许可证：智能软件许可，第 79 页。

- 关于 PAK 许可证，第 41 页
- PAK 许可证准则，第 49 页
- 配置 PAK 许可证，第 50 页
- 配置共享许可证（Secure Client 3 及更早版本），第 55 页
- 每个型号支持的功能许可证，第 62 页
- 监控 PAK 许可证，第 63 页
- PAK 许可证的历史记录，第 73 页

关于 PAK 许可证

许可证指定在给定 ASA 上启用的选项。它由一个表示 160 位（5 个 32 位字或 20 个字节）值的激活密钥表示。该值对序列号（11 个字符的字符串）和已启用的功能进行编码。

预安装的许可证

默认情况下，ASA 已预安装了一个许可证。此许可证可能是基础许可证，您要向其添加更多许可证，或者其可能已经安装所有许可证，具体取决于您的订购以及供应商为您安装的内容。

相关主题

监控 PAK 许可证，第 63 页

永久许可证

您可以安装一个永久激活密钥。永久激活密钥在单个密钥中包含所有许可功能。如果您还安装了基于时间的许可证，则 ASA 会将永久许可证和基于时间的许可证合并为运行许可证。

相关主题

永久许可证与基于时间的许可证的合并方式，第 42 页

基于时间的许可证

除永久许可证以外，您还可以购买基于时间的许可证，或者接收具有时间限制的评估许可证。例如，您可能会购买基于时间的 Secure Client 高级版许可证，以处理并发 SSL VPN 用户数的短期激增。

基于时间的许可证激活准则

- 您可以安装多个基于时间的许可证，包括同一功能的多个许可证。但是，每个功能一次只能有一个基于时间的许可证处于活动状态。非活动许可证保持已安装状态，并可随时使用。例如，如果安装一个 1000 会话的 Secure Client 高级版许可证和一个 2500 会话的 Secure Client 高级版许可证，则其中仅有一个许可证可处于活动状态。
- 如果激活在密钥中具有多个功能的评估许可证，则无法为所包含的其中一个功能也同时激活另一基于时间的许可证。

基于时间的许可证计时器工作方式

- 当在 ASA 上激活基于时间的许可证时，其计时器便开始倒计时。
- 如果在基于时间的许可证超时之前停止对其进行使用，则计时器会停止。仅当重新激活基于时间的许可证时，计时器才会再次启动。
- 如果基于时间的许可证处于活动状态，并且您关闭 ASA，则计时器会停止倒计时。仅当 ASA 正在运行时，基于时间的许可证才会倒计时。系统时钟设置不影响许可证；只有 ASA 正常运行时间会计入许可证持续时间。

永久许可证与基于时间的许可证的合并方式

激活基于时间的许可证时，通过永久许可证与基于时间的许可证获得的功能将合并以形成正在运行的许可证。永久许可证与基于时间的许可证的合并方式取决于许可证的类型。下表列出了每个功能许可证的合并规则。

注释　即使使用了永久许可证，如果基于时间的许可证处于活动状态，也会继续倒计时。

表 *1:* 基于时间的许可证合并规则

基于时间的功能	合并许可证规则
Secure Client 高级会话	使用基于时间的许可证或永久许可证两者中的较高值。例如，如果永久许可证是 1000 个会话，基于时间的许可证是 2500 个会话，则会启用 2500 个会话。通常，不会安装功能弱于永久许可证的基于时间的许可证，但是，如果您这么做，则会使用永久许可证。

基于时间的功能	合并许可证规则
统一通信代理会话	基于时间的许可证会话会添加到永久会话中，最高值为平台限制。例如，如果永久许可证为 2500 个会话，基于时间的许可证为 1000 个会话，则只要基于时间的许可证处于活动状态，就会启用 3500 个会话。
其他所有	使用基于时间的许可证或永久许可证两者中的较高值。对于状态为启用或禁用的许可证，将会使用状态为启用的许可证。对于具有数字层的许可证，将使用较高的值。通常，不会安装功能弱于永久许可证的基于时间的许可证，但是，如果您这么做，则会使用永久许可证。

相关主题

监控 PAK 许可证，第 63 页

堆叠基于时间的许可证

在许多情况下，您可能需要续订基于时间的许可证，并从旧许可证无缝过渡到新许可证。对于只有基于时间的许可证时才可提供的功能，在应用新许可证之前，许可证没有到期尤为重要。ASA 允许堆叠基于时间的许可证，从而让您不必担忧许可证到期或由于提前安装了新许可证而损害许可证上的时间。

当安装与已安装的许可证相同的基于时间的许可证时，许可证会进行合并，并且持续时间等于合并后的持续时间。

例如：

1. 您安装有一个 8 周的 1000 会话 Secure Client 高级版许可证，并且该许可证已使用 2 周（剩余 6 周）。
2. 然后，您又安装了另一个 8 周 1000 个会话许可证，许可证合并具有 14 周 1000 个会话（8 周加上 6 周）。

如果许可证不同（例如，1000 会话 Secure Client 高级版许可证和 2500 会话许可证），则许可证 不会 合并。由于每个功能仅能有一个基于时间的许可证处于活动状态，这些许可证中仅有一个许可证可以处于活动状态。

虽然不能合并不相同的许可证，但在当前许可证到期时，ASA 会自动激活已安装的功能相同的许可证（如果可用）。

相关主题

激活或停用密钥，第 54 页
基于时间的许可证到期，第 43 页

基于时间的许可证到期

当某个功能的当前许可证到期时，ASA 会自动激活同一功能的已安装许可证（如果适用）。如果没有其他适用于此功能的基于时间的许可证，则会使用永久许可证。

如果为某个功能安装了多个额外的基于时间的许可证，则ASA会使用其找到的第一个许可证；将会使用哪个许可证不是用户可配置的，而是取决于内部操作。如果您希望使用的许可证不是ASA激活的基于时间的许可证，则必须手动激活您希望使用的许可证。

例如，您有一个基于时间的 2500 个会话 Secure Client 高级许可证（活动）、一个基于时间的 1000 个会话 Secure Client 高级许可证（非活动），以及一个永久的 500 个会话的 Secure Client 高级许可证。当 2500 个会话许可证到期时，ASA 会激活 1000 个会话许可证。在 1000 个会话许可证到期后，ASA 会使用 500 个会话永久许可证。

相关主题

激活或停用密钥，第 54 页

许可证说明

以下部分包括有关许可证的其他信息。

Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证

Secure Client Advantage或 Premier 许可证是可应用于多个 ASA 的多用途许可证，所有这些 ASA 都共享许可证指定的一个用户池。仅 仅限 Secure Client VPN 许可证适用于特定的 ASA。请参阅 https://www.cisco.com/go/license，并单独为每个 ASA 分配 PAK。将生成的激活密钥应用于 ASA 时，会将 VPN 功能切换到允许的最大值，但共享该许可证的所有 ASA 中唯一用户的实际数量不应超出此许可证限制。有关详情，请参阅：

- Cisco Secure Client 订购指南
- Secure Client 许可常见问题解答 (FAQ)

注释 Secure Client Premier 许可证是唯一支持多语境模式的 Secure Client Premier 许可证。此外，在多情景模式下，此许可证必须应用于故障转移对中的每台设备；该许可证不进行聚合。

其他 VPN 许可证

其他 VPN 对等体包括以下 VPN 类型：

- 使用 IKEv1 的 IPsec 远程访问 VPN
- 使用 IKEv1 的 IPsec 站点间 VPN
- 使用 IKEv2 的 IPsec 站点间 VPN

此许可证包含在基础许可证中。

合并后的各个类型的 VPN 会话总数

- VPN 对等体总数是 Secure Client 和其他 VPN 对等体允许的最大 VPN 对等体数。例如，如果总数为 1000，则可以同时允许 500 个 Secure Client 和 500 个其他 VPN 对等体；或 700 个 Secure

Client 和 300 个其他 VPN；或对 Secure Client 使用全部 1000 个。如果超出了 VPN 对等体总数，可以对 ASA 实施过载，以确保相应地调整网络大小。

VPN 负载均衡

VPN 负载均衡需要强加密 (3DES/AES) 许可证。

传统 VPN 许可证

有关许可的所有相关信息，请参阅 Secure Client补充最终用户许可协议 。

注释 Secure Client Premier 许可证时多情景模式下支持的唯一 Secure Client 许可证；您无法使用默认或传统许可证。

加密许可证

无法禁用 DES 许可证。如果您安装有 3DES 许可证，则 DES 仍然可用。要在希望仅使用强加密时防止使用 DES，请务必将所有相关命令都配置为仅使用强加密。

TLS 代理会话总数

用于加密语音检测的每个 TLS 代理会话都会计入 TLS 许可证限制中。

使用 TLS 代理会话的其他应用不计入 TLS 限制，例如移动性优势代理（无需许可证）。

某些应用可能会在一个连接中使用多个会话。例如，如果为一部电话配置了主用和备用思科 Unified Communications Manager，则有 2 个 TLS 代理连接。

使用 **tls-proxy maximum-sessions** 命令，或在 ASDM 中使用 **Configuration > Firewall > Unified Communications > TLS Proxy** 窗格，单独设置 TLS 代理限制。要查看型号的限制，请输入 **tls-proxy maximum-sessions ?** 命令。如果应用的 TLS 代理许可证高于默认的 TLS 代理限制，则 ASA 自动设置 TLS 代理限制以与许可证匹配。TLS 代理限制的优先级高于许可证限制；如果设置的 TLS 代理限制低于许可证限制，则无法使用许可证中的所有会话。

注释 对于以“K8”结尾的许可证部件号（例如，用户数少于 250 的许可证），TLS 代理会话数限制为 1000。对于以“k9”结尾的许可证部件号（例如，用户数为 250 或更多的许可证），TLS 代理限制取决于配置，最高值为型号限制。K8 和 K9 是指许可证是否有出口限制：K8 不受限制，K9 受限制。

如果清除配置（例如使用 **clear configure all** 命令），TLS 代理限制将设置为模型的默认值；如果默认值低于许可证限制，会显示一条错误消息，让您使用 **tls-proxy maximum-sessions** 命令再次增加该限制（在 ASDM 中，使用 **TLS Proxy** 窗格）。如果使用故障转移并输入 **write standby** 命令，或者在 ASDM 中，在主设备上使用 **File > Save Running Configuration to Standby Unit** 来强制进行配置同步，则会在辅助设备上自动生成 **clear configure all** 命令，因此，您可能会在辅助设备上看到警告消息。由于配置同步会恢复在主设备上设置的 TLS 代理限制，因此可以忽略该警告。

您也可能为连接使用 SRTP 加密会话：

- 对于 K8 许可证，SRTP 会话数限制为 250。
- 对于 K9 许可证，则没有任何限制。

注释 只有需要对媒体进行加密/解密的呼叫会计入 SRTP 限制；如果将呼叫设置为直通式，即使两端均为 SRTP，这些呼叫也不计入限制。

最大 VLAN 数量

对于根据 VLAN 限制计数的接口，您必须向其分配 VLAN。 例如：

```
interface gigabitethernet 0/0.100
vlan 100
```

共享 Secure Client 高级版许可证（AnyConnect 3 及更早版本）

注释 AnyConnect 4 及更高版本的许可不支持 ASA 上的共享许可证功能。 Secure Client 许可证是共享的，不再需要共享服务器或参与者许可证。

通过共享许可证，您可以购买大量的 Secure Client 高级会话，并且通过将一组 ASA 中的一个 ASA 配置为共享许可服务器，将剩余 ASA 配置为共享许可参与者，来根据需要在这组 ASA 之间共享会话。

故障转移

除一些例外情况之外，故障转移设备不要求每台设备上具有相同的许可证。对于早期版本，请参阅您的版本的许可文档。

故障转移许可证要求和例外

型号	许可证要求
ISA 3000	两个设备上都有增强型安全许可证。 注释 每台设备必须拥有相同的加密许可证。

注释 需要有效的永久密钥；在极少数情况下，在 ISA 3000 可以删除您的 PAK 身份验证密钥。如果密钥全部由 0 组成，则需要重新安装有效的身份验证密钥，然后才能启用故障转移。

如何合并故障转移许可证

对于故障转移对，每台设备上的许可证会合并为单个运行集群许可证。如果您为每台设备购买单独的许可证，则合并的许可证使用以下规则：

- 对于具有数字层（例如，会话数）的许可证，每台设备的许可证的值会合并，最高值为平台限制。如果正在使用的所有许可证都基于时间，则许可证将同时倒计时。

  例如，对于故障转移：

  - 您有两台 ASA，每台安装了 10 个 TLS 代理会话；许可证将进行合并以获得总共 20 个 TLS 代理会话。
  - 您有一台具有 1000 个 TLS 代理会话的 ASA，以及另一台具有 2000 个会话的 ASA 5545-X；由于平台限制为 2000 个，因此合并的许可证可允许 2000 个 TLS 代理会话。

- 对于状态为启用或禁用的许可证，将会使用状态为启用的许可证。
- 对于启用或禁用的基于时间的许可证（并且没有数字层），持续时间是所有许可证的合并后的持续时间。主/控制单位首先对其许可证进行倒计时，当其许可证到期时，辅助/数据单位开始对其许可证进行倒计时，依此类推。

相关主题

监控 PAK 许可证，第 63 页

故障转移或设备之间的通信丢失

如果设备丢失通信超过 30 天，则每台设备将还原到本地安装的许可证。在 30 天宽限期内，所有设备将继续使用合并的运行许可证。

如果在 30 天的宽限期内恢复通信，则对于基于时间的许可证，将从主/主许可证中减去耗用时间；如果主/主许可证已到期，则仅在此时辅助/从属许可证才会开始倒计时。

如果在30天内没有恢复通信，则对于基于时间的许可证，将从所有设备许可证（如果已安装）中减去耗用时间。它们会被视为独立许可证，不会受益于合并后的许可证。耗用时间包括 30 天的宽限期。

升级故障转移对

由于故障转移对不要求在两台设备上具有同一许可证，因此可以将新许可证应用于每台设备而不会产生任何停机时间。如果应用要求重新加载的永久许可证，则可以在重新加载时故障转移到另一台设备。如果两台设备都需要重新加载，则可以将其分开重新加载，以便不会产生停机时间。

相关主题

激活或停用密钥，第 54 页

无负载加密型号

您可以购买一些具有无负载加密功能的型号。如要出口至某些国家/地区，则在 ASA 系列上不能启用负载加密。ASA 软件可感知无负载加密型号，并会禁用以下功能：

- 统一通信
- VPN

您仍然可以安装强加密 (3DES/AES) 许可证，以便用于管理连接。例如，可以使用 ASDM HTTPS/SSL、SSHv2、Telnet 和 SNMPv3。

当您查看许可证时，将不会列出 VPN 许可证和统一通信许可证。

相关主题

监控 PAK 许可证，第 63 页

许可证 FAQ

我是否可以激活多个基于时间的许可证？

是。对于每个功能，您可以一次使用一个基于时间的许可证。

我是否可以“堆叠”基于时间的许可证，以便在时间限制解除时，将自动使用下一个许可证？

是。对于相同的许可证，当安装多个基于时间的许可证时，时间限制会合并。对于不相同的许可证（例如一个 1000 会话 Secure Client 高级版许可证和一个 2500 会话许可证），ASA 将自动激活它所发现的适用于此功能的基于下次的许可证。

我是否可以在使基于时间的许可证保持活动的同时，安装新的永久许可证？

是。激活永久许可证不会影响基于时间的许可证。

对于故障转移，我是否可以将共享许可服务器用作主设备，并将共享许可备用服务器用作辅助设备？

否。辅助设备具有与主设备相同的运行许可证；对于共享许可服务器，它们需要服务器许可证。备用服务器需要参与者许可证。备用服务器可以处于由两台备用服务器组成的一个单独故障转移对中。

我是否需要为故障转移对中的辅助设备购买相同的许可证？

否。从版本 8.3(1) 开始，不必在两台设备上拥有匹配的许可证。通常，您仅为主设备购买许可证；辅助设备在变为主用状态时会继承主许可证。对于您在辅助设备上也有独立许可证的情况（例如，如果您为版本 8.3 之前的软件购买了匹配的许可证），这些许可证会合并为运行故障转移集群许可证，其数量最高值为型号限制。

除共享型 AnyConnect 高级版许可证之外，我是否可以使用基于时间的或永久的 Secure Client 高级版许可证？

是。仅在本地安装的许可证（基于时间的许可证或永久许可证）中的会话用尽后，才会使用共享许可证。

注释 在共享许可服务器上，不使用永久 Secure Client 高级版许可证；但您可以与共享许可服务器许可证同时使用基于时间的许可证。在这种情况下，基于时间的许可证会话仅适用于本地 Secure Client 高级版会话；不能将其添加到共享许可池供参与者使用。

PAK 许可证准则

情景模式准则

在多情景模式下，请在系统执行空间中应用激活密钥。

故障转移准则

请参阅故障转移，第 46 页。

型号准则

- 仅在 ASA virtual 上支持智能许可。
- 在 ASA virtual、ASA 5506-X、ASA 5508-X 和 ASA 5516-X 上不支持共享许可。
- ASA 5506-X 和 ASA 5506W-X 不支持基于时间的许可证。

升级和降级准则

如果从任何之前版本升级到最新版本，则您的激活密钥保持兼容。但如果要维护降级功能，则可能会遇到问题：

- 降级到版本 8.1 或更早版本 - 在升级后，如果激活在版本 *8.2* 之前引入的其他功能许可证，则执行降级后激活密钥会继续与早期版本兼容。但是，如果激活在版本 *8.2* 或更高版本中引入的功能许可证，则激活密钥不会向后兼容。如果您有不兼容的许可证密钥，请参阅以下准则：
  - 如果以前输入了早期版本的激活密钥，则 ASA 会使用该密钥（没有您在版本 8.2 或更高版本中激活的任何新许可证）。
  - 如果您有新系统且没有早期的激活密钥，则需要请求与早期版本兼容的新激活密钥。
- 降级到版本 8.2 或更早版本 - 版本 8.3 中引入了更稳健的基于时间的密钥用法以及故障转移许可证变更：
  - 如果您有多个基于时间的激活密钥处于活动状态，则在降级后，只有最新激活的基于时间的密钥可以处于活动状态。所有其他密钥都会变为非活动状态。如果最后的基于时间的许可证是用于版本 8.3 中引入的功能，则该许可证即使无法在早期版本中使用，也仍会保持活动状态。重新输入永久密钥或有效的基于时间的密钥。
  - 如果在故障转移对上有不匹配的许可证，则降级将禁用故障转移。即使密钥匹配，所使用的许可证也将不再是合并许可证。

- 如果您安装有一个基于时间的许可证，但是它用于版本 8.3 中引入的功能，则在降级之后，该基于时间的许可证保持活动状态。您需要重新输入永久密钥，以禁用该基于时间的许可证。

其他准则

- 激活密钥不会存储在配置文件中；它会以隐藏文件的形式存储在闪存中。
- 激活密钥会绑定到设备的序列号。功能许可证无法在设备之间转移（除非发生硬件故障）。如果您由于硬件故障而必须更换设备，并且思科 TAC 涵盖该设备，请联系思科许可团队，以便将您的现有许可证转移至新的序列号。思科许可团队将要求您提供产品许可密钥参考编号和现有序列号。
- 用于许可的序列号显示在 **show version** 输出中。此序列号与印制在硬件外部的机箱序列号不同。机箱序列号用于技术支持，但不用于许可。
- 一旦购买，您将无法退还许可证来获取退款或已升级的许可证。
- 在单个设备上，无法将用于同一功能的两个单独许可证合并；例如，如果您购买了一个 25 个会话 SSL VPN 许可证，此后又购买了 50 个会话许可证，则无法使用 75 个会话；您可以使用最多 50 个会话。（您能以升级价格购买更大的许可证，例如从 25 个到 75 个会话；应将这种升级与将两个单独许可证合并区分开来）。
- 虽然您可以激活所有许可证类型，但有些功能互不兼容。对于 AnyConnect 高级版许可证，此许可证与以下许可证不兼容：AnyConnect 高级版许可证、共享型 AnyConnect 高级版许可证以及高级终端评估许可证。默认情况下，如果安装了 AnyConnect 高级版许可证（如果其适用于您的型号），则会使用该许可证，而不是上述许可证。您可以依次使用**webvpn** 和 **no anyconnect-essentials** 命令，在配置中禁用 AnyConnect 基础版许可证，以恢复使用其他许可证。

配置 PAK 许可证

本节介绍如何获取激活密钥以及如何将其激活。您也可以停用密钥。

订购许可证 PAK 并获取激活密钥

要在 ASA 上安装许可证，您需要生产授权密钥，您可以向 Cisco.com 注册该密钥以获取激活密钥。然后，可以在 ASA 上输入激活密钥。每个功能许可证都需要一个单独的生产授权密钥。PAK 合并在一起可为您提供一个激活密钥。您可能已随设备的包装箱收到所有的许可证 PAK。ASA 预安装了基础许可证和增强型安全许可证，以及强加密 (3DES/AES) 许可证（如果您有资格使用该许可证）。如果需要手动请求强机密许可证（免费），请访问 http://www.cisco.com/go/license。

开始之前

在为设备购买一个或多个许可证时，可在思科智能软件管理器中对其进行管理：

https://software.cisco.com/#module/SmartLicensing

如果您还没有帐户，请设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。

过程

步骤 1 要购买额外许可证，请参阅 http://www.cisco.com/go/ccw。请参阅以下 Secure Client 订购指南和常见问题解答：

- Cisco Secure Client 订购指南
- Secure Client 许可常见问题解答 (FAQ)

订购许可证后，您会收到一封包含产品授权密钥 (PAK) 的邮件。对于 Secure Client 许可证，您将收到多用途 PAK，该 PAK 可应用于多个使用相同用户会话池的 ASA。有时，PAK 邮件可能需要几天才能收到。

步骤 2 通过输入以下命令获取 ASA 的序列号。

show version | grep Serial

许可使用的序列号与硬件铭牌上标示的机箱序列号不同。机箱序列号用于获取技术支持，而非获取许可。

步骤 3 要获取激活密钥，请转至以下许可网站：

http://www.cisco.com/go/license

步骤 4 系统提示时，输入以下信息：

- 产品授权密钥（如果您有多个密钥，请先输入其中一个密钥。您必须单独输入每个密钥。）
- ASA 的序列号
- 您的邮件地址

系统会自动生成激活密钥，并将其发送到您提供的邮件地址。此密钥包含迄今为止已注册的永久许可证的所有功能。对于基于时间的许可证，每个许可证具有单独的激活密钥。

步骤 5 如果您有其他产品授权密钥，请针对每个产品授权密钥重复此过程。输入所有产品授权密钥后，所提供的最终激活密钥会包含已注册的所有永久功能。

步骤 6 根据激活或停用密钥，第 54 页安装激活密钥。

获取强加密许可证

要使用 ASDM（和许多其他功能），您需要安装强加密 (3DES/AES) 许可证。如果 ASA 未预装强加密许可证，您可以免费申请一个。您必须符合所在国家/地区的强加密许可证条件。

过程

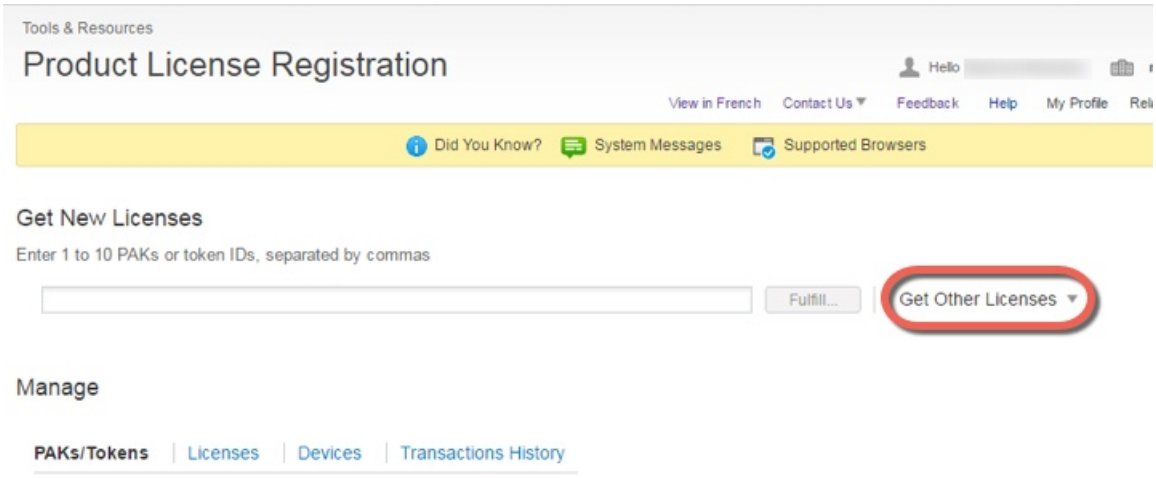
步骤 1 通过输入以下命令获取 ASA 的序列号：

show version | grep Serial

此序列号与印制在硬件外部的机箱序列号不同。机箱序列号用于技术支持，但不用于许可。

步骤 2 访问 https://www.cisco.com/go/license，然后点击**获取其他许可证**。

图 *2:* 获取其他许可证

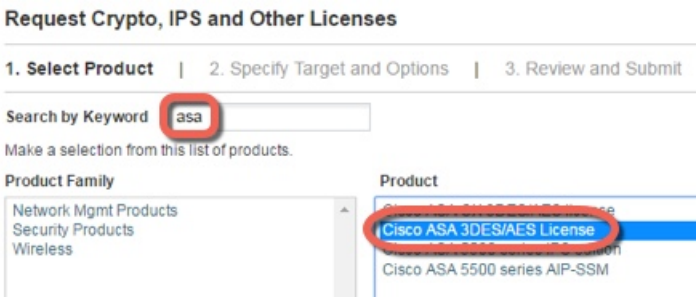


步骤 3 选择 **IPS, Crypto, Other**。

图 *3: IPS*、加密、其他

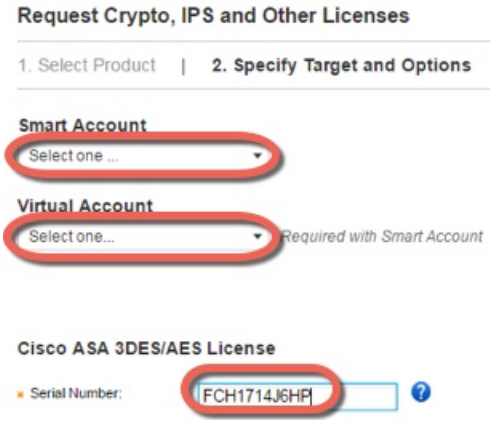
步骤 4 在 **Search by Keyword** 字段中，输入 **asa**，并选择 **Cisco ASA 3DES/AES License**。

图 *4:* 思科 ***ASA 3DES/AES*** 许可证



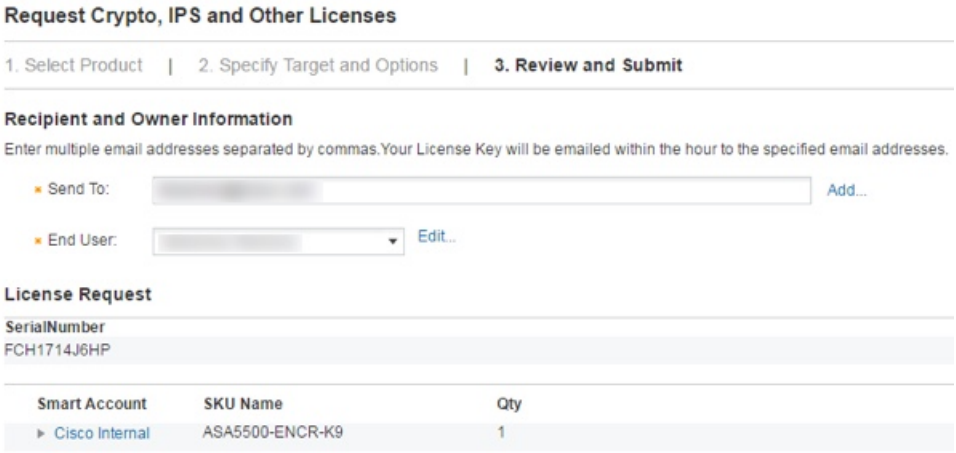
步骤 5 选择您的智能帐户 **(Smart Account)**、虚拟帐户 **(Virtual Account)**，输入 ASA 序列号 **(Serial Number)**，然后点击下一步 **(Next)**。

图 *5:* 智能帐户、虚拟帐户和序列号



步骤 6 系统将自动填充您的 Send To 邮箱地址和 End User 名称；必要时输入其他邮箱地址。选中**我同意 (I Agree)** 复选框，然后点击**提交 (Submit)**。

图 *6:* 提交



步骤 7 之后，您将会收到一封包含激活密钥的邮件，但您也可以立即从**管理 (Manage)** > **许可证 (Licenses)** 区域下载该密钥。

步骤 8 根据激活或停用密钥，第 54 页应用激活密钥。

激活或停用密钥

本节介绍如何输入新的激活密钥，以及如何激活和停用基于时间的密钥。

开始之前

- 如果您已处于多情景模式下，请在系统执行空间中输入激活密钥。
- 某些永久许可证会在激活后要求重新加载 ASA。下表列出了要求重新加载的许可证。

表 *2:* 永久许可证重新加载要求

型号	要求重新加载的许可证操作
所有型号	降级加密许可证。

过程

步骤 1 将激活密钥应用于 ASA：

activation-key *key* [**activate** | **deactivate**]

示例：

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

key 是包括五个元素的十六进制字符串，各元素之间以空格分隔。前导 0x 区分符是可选的；系统假定所有值都是十六进制值。

您可以安装一个永久密钥和 多个基于时间的密钥。如果输入新的永久密钥，则它会覆盖已安装的永久密钥。

activate 和 **deactivate** 关键字仅适用于基于时间的密钥。如果不输入任何值，则 **activate** 为默认值。您为给定功能激活的最后一个基于时间的密钥是活动密钥。要停用所有活动的基于时间的密钥，请输入 **deactivate** 关键字。如果您是第一次输入密钥，之后指定 **deactivate**，则在 ASA 上安装的密钥处于不活动状态。

步骤 2 （可能需要）。重新加载 ASA：

reload

输入新的激活密钥之后，某些永久许可证会要求您重新加载 ASA。如果您需要重新加载，将会看到以下消息：

```
WARNING: The running activation key was not updated with the requested key.
The flash activation key was updated with the requested key, and will become
active after the next reload.
```

相关主题

基于时间的许可证，第 42 页

配置共享许可证（Secure Client 3 及更早版本）

注释 Secure Client 4 及更高版本的许可不支持 ASA 上的共享许可证功能。 Secure Client 许可证是共享的，不再需要共享服务器或参与者许可证。

本节介绍如何配置共享许可服务器和参与者。

关于共享许可证

通过共享许可证，您可以购买大量的 Secure Client 高级会话，并且通过将一组 ASA 中的一个 ASA 配置为共享许可服务器，将剩余 ASA 配置为共享许可参与者，来根据需要在这组 ASA 之间共享会话。

关于共享许可服务器和参与者

以下步骤说明共享许可证的工作方式：

1. 确定哪一台ASA应充当共享许可服务器，然后使用该设备的序列号购买共享许可服务器许可证。
2. 确定哪些 ASA 应充当共享许可参与者（包括共享许可备用服务器），并使用每台设备的序列号获取每台设备的共享许可参与者许可证。
3. （可选）将另一台 ASA 指定为共享许可备用服务器。只能指定一台备用服务器。

注释 共享许可备用服务器仅需要参与者许可证。

4. 请在共享许可服务器上配置一个共享密钥；具有该共享密钥的所有参与者都可以使用共享许可证。
5. 将 ASA 配置为参与者时，它通过发送有关自身的信息（包括本地许可证和型号信息）向共享许可服务器注册。

注释 参与者需要能够通过 IP 网络与服务器通信；它不必在同一子网中。

6. 共享许可服务器会使用参与者应轮询服务器的频率的有关信息进行响应。
7. 当参与者用尽本地许可证的会话时，它会向共享许可服务器发出请求，从而获取更多会话（以 50 个会话为增量）。
8. 共享许可服务器使用共享许可证进行响应。参与者使用的会话总数不能超过平台型号的最大会话数。

注释 共享许可服务器也可以参与共享许可证池。它进行参与既不需要参与者许可证，也不需要服务器许可证。

   1. 如果在共享许可证池中没有为参与者留下足够多的会话，则服务器通过提供尽可能多的可用会话进行响应。
   2. 参与者会继续发送请求更多会话的刷新消息，直到服务器可以充分满足请求。

9. 当参与者的负载减少时，它会向服务器发送消息，以释放共享会话。

注释 ASA 在服务器和参与者之间使用 SSL 来加密所有通信。

参加者和服务器之间的通信问题

有关参与者和服务器之间的通信问题的信息，请参阅以下准则：

- 如果参与者在 3 倍刷新间隔后未能发送刷新信息，则服务器会将会话释放回共享许可证池。
- 如果参与者无法访问许可证服务器以发送刷新消息，则参与者可以继续使用其从服务器收到的共享许可证，最多可使用 24 小时。
- 如果在24小时后，参与者仍无法与许可证服务器通信，则参与者将释放共享许可证，即使其仍然需要会话也如此。参与者会保留已建立的现有连接，但无法接受超过许可证限制的新连接。
- 如果在24小时的时间到期之前且服务器使参与者会话到期之后，参与者与服务器重新连接，则参与者需要为会话发送新的请求；服务器通过可向该参与者发送尽可能多的会话进行响应。

关于共享许可备用服务器

共享许可备用服务器必须先成功向主共享许可服务器注册，然后才能承担备用角色。当其注册时，主共享许可服务器将与备用服务器同步服务器设置以及共享许可证信息，其中包括已注册参与者的列表以及当前的许可证使用情况。主服务器和备用服务器以10秒为间隔同步数据。在最初的同步之后，即使经过重新加载，备份服务器也能够成功履行备用职责。

当主服务器发生故障时，备用服务器会接管服务器操作。备用服务器可以连续运行最多30天，在此之后，备用服务器会停止向参与者发出会话，而且现有会话将会超时。请务必在此30天的时段内恢复主服务器。关键级别的系统日志消息会在 15 天时发送，并在 30 天时再次发送。

当主服务器恢复正常运行时，它将与备用服务器同步，然后接管服务器操作。

当备用服务器不处于主用状态时，它会充当主共享许可服务器的普通参与者。

注释 首次启动主共享许可服务器时，备用服务器仅可独立运行 5 天。运行限制将逐日延长，直至达到 30 天。此外，如果此后主服务器停止运行任意时长，则备用服务器的运行限制会逐日缩短。当主服务器恢复正常运行时，备用服务器的运行限制会开始再次逐日延长。例如，如果主服务器停止运行 20 天，在此期间备用服务器处于主用状态，则备用服务器的运行限制将仅剩余10天。备份服务器在继续充当非主用的备用服务器 20 天后，将“充值”至最长的 30 天运行限制。实施此“充值”功能是为了防止滥用共享许可证。

故障转移和共享许可证

本节介绍共享许可证如何与故障转移交互。

故障转移和共享许可证服务器

本节介绍主服务器和备用服务器如何与故障转移交互。由于共享许可服务器与ASA一样也会执行常规职责，包括执行VPN网关和防火墙等功能，则您可能需要为主和备用共享许可服务器配置故障转移，以提高可靠性。

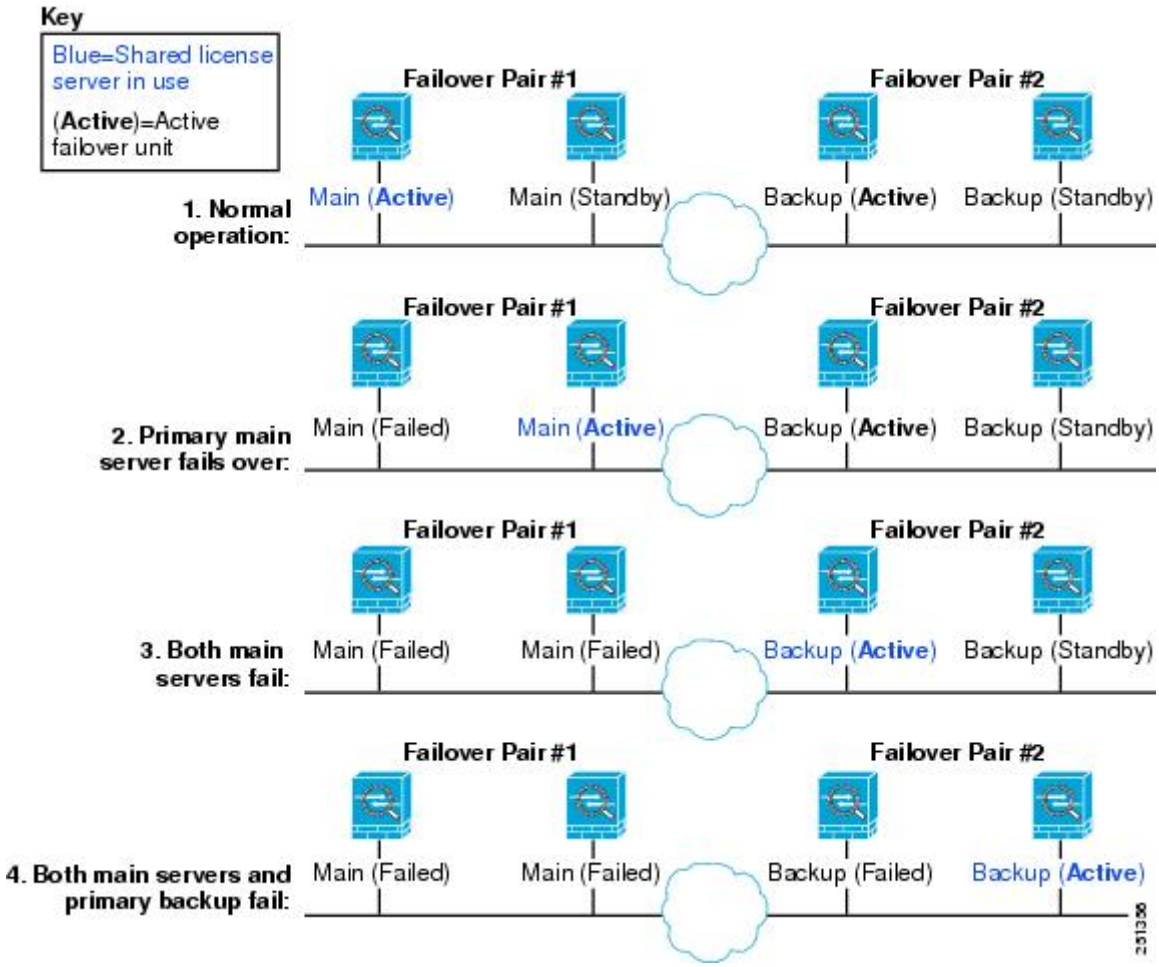
注释 备用服务器机制独立于故障转移，但与其兼容。

仅在单情景模式下支持共享许可证，因此不支持主用/主用故障转移。

对于主用/备用故障转移，主设备将充当主共享许可服务器，发生故障转移后，备用设备将充当主共享许可服务器。备用设备不会充当备用共享许可证服务器。相反，您可以视需要让另一对设备充当备用服务器。

例如，您具有包含 2 个故障转移对的网络。第 1 对包含主许可服务器。第 2 对包含备用服务器。第 1 对中的主设备发生故障时，备用设备会立即变为新的主许可服务器。绝不会使用第 2 对中的备用服务器。仅当第1对中的两台设备均发生故障时，第2对中的备用服务器才会用作共享许可服务器。如果第 1 对保持关闭，并且第 2 对中的主设备关闭，则第 2 对中的备用设备将用作共享许可服务器（请见下图）。

图 7: 故障转移和共享许可证服务器



辅助备用服务器与主备用服务器共享相同的运行限制；如果辅助设备变为主用设备，它会在主设备停止的位置继续倒计时。

相关主题

关于共享许可备用服务器，第 56 页

故障转移和共享许可证参与者

对于参与者对，两台设备均会使用单独的参与者 ID 向共享许可服务器注册。主用设备会将其参与者 ID 与备用设备同步。当备用设备切换到主用角色时，它会使用此 ID 生成转移请求。此转移请求用于将来自先前主用设备的共享会话移至新的主用设备。

最大参与者数

ASA 不限制共享许可证的参与者数量；但是，超大共享网络可能会潜在影响许可服务器的性能。在这种情况下，您可以增大参与者刷新之间的延迟，也可以创建两个共享网络。

配置共享许可服务器

此部分介绍如何将 ASA 配置为共享许可服务器。

开始之前

服务器必须具有共享许可服务器密钥。

过程

步骤 1 设置共享密钥：

license-server secret *secret*

示例：

```
ciscoasa(config)# license-server secret farscape
```

secret 是由 4 至 128 个 ASCII 字符组成的字符串。拥有此密钥的任何参与者都可以使用许可服务器。

步骤 2 （可选）设置刷新间隔：

license-server refresh-interval *seconds*

示例：

```
ciscoasa(config)# license-server refresh-interval 100
```

间隔介于 10 和 300 秒之间；此值会提供给参与者，用于设置其应与服务器通信的频率。默认值为 30 秒。

步骤 3 （可选）设置服务器侦听来自参与者的 SSL 连接的端口。

license-server port *port*

示例：

```
ciscoasa(config)# license-server port 40000
```

port 介于 1 和 65535 之间。默认值为 TCP 端口 50554。

步骤 4 （可选）确定备用服务器 IP 地址和序列号：

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]

示例：

```
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
```

如果备用服务器属于某个故障转移对，请另外确定备用设备序列号。只能确定 1 台备用服务器及其可选的备用设备。

步骤 5 使此设备成为共享许可服务器：

license-server enable *interface_name*

示例：

```
ciscoasa(config)# license-server enable inside
```

指定参与者与服务器进行连接的接口。您可以为所需数量的接口重复此命令。

示例

以下示例设置共享密钥、更改刷新间隔和端口、配置备用服务器，并在内部接口和 dmz 接口上使此设备成为共享许可服务器：

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

配置共享许可备份服务器（可选）

本节介绍如何使共享许可参与者在主服务器发生故障时充当备用服务器。

开始之前

备用服务器必须具有共享许可参与者密钥。

过程

步骤 1 确定共享许可服务器 IP 地址和共享密钥：

license-server address *address* **secret** *secret* [**port** *port*]

示例：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

如果更改服务器配置中的默认端口，请设置该端口，以便备用服务器能够匹配。

步骤 2 使此设备成为共享许可备用服务器：

license-server backup enable *interface_name*

示例：

```
ciscoasa(config)# license-server backup enable inside
```

指定参与者与服务器进行连接的接口。您可以为所需数量的接口重复此命令。

示例

以下示例确定许可服务器和共享密钥，并在内部接口和 dmz 接口上使此设备成为备用共享许可服务器：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

配置共享许可参与者

本部分配置共享许可参与者以与共享许可服务器进行通信。

开始之前

参与者必须具有共享许可参与者密钥。

过程

步骤 1 确定共享许可服务器 IP 地址和共享密钥：

license-server address *address* **secret** *secret* [**port** *port*]

示例：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

如果更改服务器配置中的默认端口，请设置该端口，以便参与者能够匹配。

步骤 2 （可选）如果配置了备用服务器，请输入备用服务器地址：

license-server backup address *address*

示例：

```
ciscoasa(config)# license-server backup address 10.1.1.2
```

示例

以下示例设置许可服务器 IP 地址和共享密钥，以及备用许可服务器 IP 地址：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

每个型号支持的功能许可证

本节介绍适用于每个型号的许可证，以及有关这些许可证的重要说明。

每个型号的许可证

本节列出了适用于每个型号的功能许可证：

显示为斜体的项是可以替代基础许可证（或增强型安全许可证等）版本的独立可选许可证。可混合和匹配可选许可证。

注释 某些功能互不兼容。有关兼容性信息，请参阅单独的功能章节。

如果您拥有一个无负载加密型号，则无法支持下面的部分功能。有关不支持功能的列表，请参阅无负载加密型号，第 48 页。

有关许可证的详细信息，请参阅许可证说明，第 44 页。

ISA 3000 许可证功能

下表显示了 ISA 3000 已获许可的功能。

许可证	基础许可证	增强型安全许可证
防火墙许可证		
僵尸网络流量过滤器	不支持	不支持
并发防火墙连接数	20,000	50,000
Carrier	不支持	不支持
TLS 代理会话总数	160	160

许可证	基础许可证		增强型安全许可证	
VPN 许可证				
Secure Client 对等体	禁用	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证：最多 *25* 个	禁用	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证：最多 *25* 个
其他 VPN 对等体数	10		50	
VPN 对等体总数（包括所有类型）	25		50	
VPN 负载均衡	不支持		不支持	
通用许可证				
加密	基本 (DES)	可选许可证：强 *(3DES/AES)*	基本 (DES)	可选许可证：强 *(3DES/AES)*
故障转移	不支持		主用/备用	
安全情景	不支持		不支持	
集群	不支持		不支持	
最大 VLAN 数量	5		25	

监控 PAK 许可证

本节介绍如何查看许可证信息。

查看您当前的许可证

此部分介绍如何查看您的当前许可证，以及与基于时间的激活密钥对应的许可证的剩余时间。

开始之前

如果您拥有的是无负载加密型号，则在查看许可证时，将不会列出VPN许可证和统一通信许可证。有关详细信息，请参阅无负载加密型号，第 48 页。

过程

显示永久许可证、活动的基于时间的许可证以及运行许可证（包括永久许可证和活动的基于时间的许可证）：

show activation-key [**detail**]

detail 关键字还显示非活动的基于时间的许可证。

对于故障转移或集群设备，该命令还显示“集群”许可证，该许可证包括所有设备的密钥。

示例

示例 1：独立设备运行 show activation-key 命令时的输出

以下是独立设备运行 **show activation-key** 命令时的样本输出，其中显示运行许可证（包括永久许可证和活动的基于时间的许可证）以及每个活动的基于时间的许可证：

```
ciscoasa# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

示例 2：独立设备运行 show activation-key detail 时的输出

以下是独立设备运行 **show activation-key detail** 命令时的样本输出，其中显示运行许可证（合并的永久许可证和基于时间的许可证），以及永久许可证和每个已安装的基于时间的许可证（活动和非活动）：

```
ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5512-X Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days
```

```
Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                  : 25     7 days
```

示例 3：故障转移对中的主设备运行 show activation-key detail 时的输出

以下是主故障转移设备运行 **show activation-key detail** 命令时的样本输出，其中显示：

- 主设备许可证（合并的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证（来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 主设备永久许可证。
- 主设备安装的基于时间的许可证（活动和非活动）。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers       : 4            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
```

```
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2               perpetual
AnyConnect Essentials             : Disabled        perpetual
Other VPN Peers                   : 750             perpetual
Total VPN Peers                   : 750             perpetual
Shared License                    : Disabled         perpetual
AnyConnect for Mobile             : Disabled        perpetual
AnyConnect for Cisco VPN Phone    : Disabled        perpetual
Advanced Endpoint Assessment      : Disabled        perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts               : 2          7 days
AnyConnect Premium Peers                   : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions         : 100        14 days
```

示例 4：故障转移对中的辅助设备运行 show activation-key detail 时的输出

以下是辅助故障转移设备运行 **show activation-key detail** 命令时的样本输出，其中显示：

- 辅助设备许可证（合并的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证（来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 辅助设备永久许可证。
- 辅助设备安装的基于时间的许可证（活动和非活动）。此设备没有任何基于时间的许可证，因此在此样本输出中不会显示任何内容。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 10             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
```

```
GTP/GPRS                        : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions         : 2              perpetual
Total UC Proxy Sessions         : 2              perpetual
Botnet Traffic Filter           : Disabled       perpetual
Intercompany Media Engine       : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
```

示例 5：故障转移对中的 ASA 服务模块的主设备运行 show activation-key 时的输出

以下是主故障转移设备运行 **show activation-key** 命令时的样本输出，其中显示：

- 主设备许可证（合并的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证（来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 主设备安装的基于时间的许可证（活动和非活动）。

```
ciscoasa# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50 perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
```

```
Botnet Traffic Filter           : Enabled    330 days
```

示例 6：故障转移对中的 ASA 服务模块的辅助设备运行 show activation-key 时的输出

以下是辅助故障转移设备运行 **show activation-key** 命令时的样本输出，其中显示：

- 辅助设备许可证（合并的永久许可证和基于时间的许可证）。
- “故障转移集群”许可证（来自主设备和辅助设备的合并许可证）。这是 ASA 上实际运行的许可证。此许可证中反映主许可证和辅助许可证组合的值以粗体显示。
- 辅助设备安装的基于时间的许可证（活动和非活动）。此设备没有任何基于时间的许可证，因此在此样本输出中不会显示任何内容。

```
ciscoasa# show activation-key detail

Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Disabled       perpetual
Botnet Traffic Filter             : Disabled       perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50 perpetual
GTP/GPRS                          : Enabled perpetual
Botnet Traffic Filter             : Enabled 330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.
```

示例 7：集群运行 show activation-key 时的输出

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
```

```
Security Contexts : 2 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster : Enabled perpetual

This platform has an ASA 5585-X base license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 100 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
Encryption-DES : Enabled perpetual
Encryption-3DES-AES : Enabled perpetual
Security Contexts : 4 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 4 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 4 perpetual
Total UC Proxy Sessions : 4 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster : Enabled perpetual

This platform has an ASA 5585-X base license.

The flash permanent activation key is the SAME as the running permanent key.
```

监控共享许可证

要监控共享许可证，请输入以下命令之一。

- **show shared license** [**detail** | **client** [*hostname*] | **backup**]

  显示共享许可证统计信息。可选关键字仅适用于许可服务器：**detail** 关键字用于显示每个参与者的统计信息。要将显示内容限制为一个参与者的相关信息，请使用 **client** 关键字。**backup** 关键字用于显示有关备用服务器的信息。

  要清除共享许可证统计信息，请输入 **clear shared license** 命令。

  以下是许可证参与者上 **show shared license** 命令的样本输出：

  ```
  ciscoasa>  show shared license
  ```

```
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
```

以下是许可证服务器上 **show shared license detail** 命令的样本输出：

```
ciscoasa>  show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0


Client Info:

  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

- **show activation-key**

  显示 ASA 上安装的许可证。**show version** 命令也可用于显示许可证信息。

- **show vpn-sessiondb**

  显示有关 VPN 会话的许可证信息。

PAK 许可证的历史记录

功能名称	平台版本	说明
增加了连接数和 VLAN 数量	7.0(5)	提高了以下限制： • ASA5510 基础许可证连接数从 32000 增加到 50000；VLAN 数从 0 增加到 10。 • ASA5510 基础许可证连接数从 64000 增加到 130000；VLAN 数从 10 增加到 25。 • ASA5520 连接数从 130000 增加到 280000；VLAN 数从 25 增加到 100。 • ASA5540 连接数从 280000 增加到 400000；VLAN 数从 100 增加到 200。
SSL VPN 许可证	7.1(1)	引入了 SSL VPN 许可证。
增加了 SSL VPN 许可证数量	7.2(1)	为 ASA 5550 和更高版本引入了 5000 用户 SSL VPN 许可证。
ASA 5510 上的基础许可证增加了接口数	7.2(2)	对于 ASA 5510 上的基础许可证，最大接口数从 3 加管理接口数增加到无限个。
增加了 VLAN 数量	7.2(2)	ASA 5505 上增强型安全许可证 VLAN 的最大数量从 5（3 个全功能；1 个故障转移；1 个限用于备用接口）增加到 20 个全功能接口。此外，中继端口数量也从 1 增加到 8。现在有 20 个全功能接口，您不需要使用 backup interface 命令禁用备用 ISP 接口的功能；您可以为其使用全功能接口。备用接口命令对于 Easy VPN 配置仍非常有用。 以下型号的 VLAN 数量限制也有所增加：ASA 5510（对于基础许可证，从 10 增加到 50；对于增强型安全许可证，从 25 增加到 100）、ASA 5520（从 100 增加到 150）和 ASA 5550（从 200 增加到 250）。

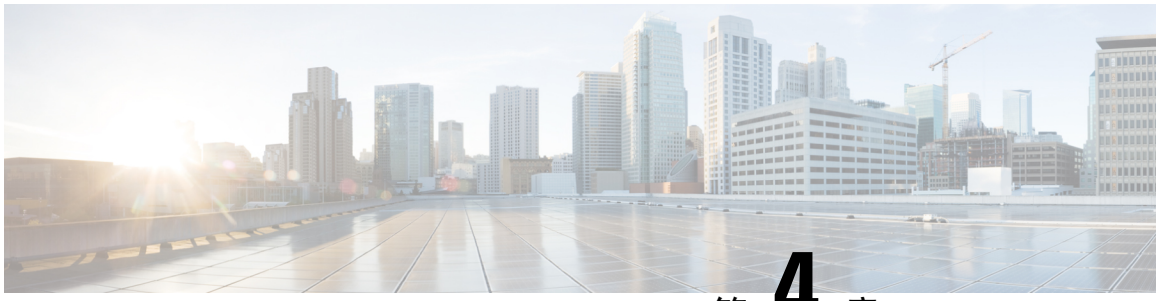
功能名称	平台版本	说明
对于 ASA 5510 增强型安全许可证的千兆以太网支持	7.2(3)	具有增强型安全许可证的 ASA 5510 现在在 Ethernet 0/0 和 0/1 端口上支持千兆以太网 (1000 Mbps)。在基础许可证中，它们将继续用作快速以太网 (100 Mbps) 端口。对于两种许可证，Ethernet 0/2、0/3 和 0/4 仍为快速以太网端口。 注释 接口名称仍为 Ethernet 0/0 和 Ethernet 0/1。 使用 **speed** 命令可更改接口上的速度，使用 **show interface** 命令可查看为每个接口当前配置的速度。
高级终端评估许可证	8.0(2)	引入了高级终端评估许可证。作为 Cisco AnyConnect 或无客户端 SSL VPN 连接完成的一个条件，远程计算机将对一系列规模大幅扩展的防病毒软件和反间谍软件应用、防火墙、操作系统以及相关更新进行扫描。它还会扫描您指定的所有注册表项、文件名和进程名称，它会将扫描结果发送至 ASA。ASA 使用用户登录凭证和计算机扫描结果来指定动态访问策略 (DAP)。 借助高级终端评估许可证，您可以进行相关配置，以尝试对不合规计算机进行更新（使其符合版本要求），从而增强主机扫描。 思科可通过独立于思科安全桌面的软件包，对主机扫描所支持的应用和版本的列表进行及时更新。
ASA 5510 的 VPN 负载均衡	8.0(2)	ASA 5510 增强型安全许可证现在支持 VPN 负载均衡。
适用于移动设备的 AnyConnect 许可证	8.0(3)	引入了适用于移动设备的 AnyConnect 许可证。通过它，Windows 移动设备可以使用 Secure Client连接至 ASA。
基于时间的许可证	8.0(4)/8.1(2)	引入了对基于时间的许可证的支持。
增加了 ASA 5580 的 VLAN 数量	8.1(2)	在 ASA 5580 上支持的 VLAN 数量从 100 增加到 250。
统一通信代理会话许可证	8.0(4)	引入了 UC 代理会话许可证。电话代理、状态联合代理和加密语音检测应用会在其连接中使用 TLS 代理会话。根据 UC 许可证限制对每个 TLS 代理会话进行计数。所有这些应用都在 UC 代理伞状结构下获得许可，并且可以混合搭配使用。 此功能在版本 8.1 中不可用。
僵尸网络流量过滤器许可证	8.2(1)	引入了僵尸网络流量过滤器许可证。僵尸网络流量过滤器可以跟踪通向已知不良域名和 IP 地址的连接，从而防御恶意软件网络活动。

功能名称	平台版本	说明
AnyConnect 基础版许可证	8.2(1)	引入了 AnyConnect 基础版许可证。此许可证支持 AnyConnect VPN 客户端访问 ASA。此许可证不支持基于浏览器的 SSL VPN 访问或思科安全桌面。对于这些功能，请激活 AnyConnect 高级版许可证而不是 AnyConnect 基础版许可证。 注释 借助 AnyConnect 基础版许可证，VPN 用户可以使用 Web 浏览器来进行登录，然后下载并启动 (WebLaunch) Secure Client。 Secure Client 软件提供一系列相同的客户端功能，无论是通过此许可证还是通过 AnyConnect 高级版许可证启用。 AnyConnect 基础版许可证不能与给定 ASA 上的以下许可证同时处于活动状态：AnyConnect 高级版许可证（所有类型）或高级终端评估许可证。但您可以在同一网络内的不同 ASA 上运行 AnyConnect 基础版和 AnyConnect 高级版许可证。 默认情况下，ASA 使用 AnyConnect 基础版许可证，但您可以通过如下方式将其禁用，以使用其他许可证：使用 **webvpn**，然后使用 **no anyconnect-essentials** 命令。
SSL VPN 许可证更改为 AnyConnect 高级版 SSL VPN 版本许可证	8.2(1)	SSL VPN 许可证的名称更改为 AnyConnect 高级版 SSL VPN 版本许可证。
SSL VPN 共享许可证	8.2(1)	引入了 SSL VPN 共享许可证。多个 ASA 可以按需共享一个 SSL VPN 会话池。
移动代理应用不再需要统一通信代理许可证	8.2(2)	移动代理不再需要 UC 代理许可证。
10 GE I/O 许可证（用于带 SSP-20 的 ASA 5585-X）	8.2(3)	引入了 10 GE I/O 许可证（用于带 SSP-20 的 ASA 5585-X），以便在光纤端口上支持 10 千兆以太网速度。默认情况下，SSP-60 支持 10 千兆以太网速度。 注释 在 8.3(x) 版本中不支持 ASA 5585-X。
10 GE I/O 许可证（用于带 SSP-10 的 ASA 5585-X）	8.2(4)	引入了 10 GE I/O 许可证（用于带 SSP-10 的 ASA 5585-X），以便在光纤端口上支持 10 千兆以太网速度。默认情况下，SSP-40 支持 10 千兆以太网速度。 注释 在 8.3(x) 版本中不支持 ASA 5585-X。

功能名称	平台版本	说明
不相同的故障转移许可证	8.3(1)	不再要求每个设备上的故障转移许可证相同。来自主设备和辅助设备的合并许可证是同时用于这两种设备的许可证。 修改了以下命令：**show activation-key** 和 **show version**。
可堆叠的基于时间的许可证	8.3(1)	基于时间的许可证现在可以堆叠。在许多情况下，您可能需要续订基于时间的许可证，并从旧许可证无缝过渡到新许可证。对于只有基于时间的许可证时才可提供的功能，在应用新许可证之前，许可证没有到期尤为重要。ASA 允许堆叠基于时间的许可证，从而让您不必担忧许可证到期或由于提前安装了新许可证而损害许可证上的时间。
公司间媒体引擎许可证	8.3(1)	引入了 IME 许可证。
多个基于时间的许可证同时处于活动状态	8.3(1)	您现在可以安装多个基于时间的许可证，每个功能一次只能有一个许可证处于活动状态。 修改了以下命令：**show activation-key** 和 **show version**。
基于时间的许可证的独立激活和停用。	8.3(1)	您现在可以使用一个命令来激活或停用基于时间的许可证。 修改了以下命令：**activation-key** [**activate** | **deactivate**]。
AnyConnect 高级版 SSL VPN 版本许可证更改为 AnyConnect 高级版 SSL VPN 许可证	8.3(1)	AnyConnect 高级版 SSL VPN 版本许可证的名称更改为 AnyConnect 高级版 SSL VPN 许可证。
用于出口的无负载加密映像	8.3(2)	如果您在 ASA 5505 至 5550 上安装无负载加密软件，则会禁用统一通信、强加密 VPN 和强加密管理协议。 **注释** 此特殊映像仅在 8.3(x) 中受支持；要想在 8.4(1) 及更高版本中支持无负载加密，您需要购买ASA的特殊硬件版本。
增加了 ASA 5550、5580 和 5585-X 的情景数	8.4(1)	对于带 SSP-10 的 ASA 5550 和 ASA 5585-X，最大情景数从 50 增加到 100。对于带 SSP-20 和更高版本的 ASA 5580 和 5585-X，最大数量从 50 增加到 250。
增加了 ASA 5580 和 5585-X 的 VLAN 数量	8.4(1)	对于 ASA 5580 和 5585-X，最大 VLAN 数量从 250 增加到 1024。

功能名称	平台版本	说明
增加了 ASA 5580 和 5585-X 的连接数	8.4(1)	提高了防火墙连接限制： • ASA 5580-20 - 1,000,000 至 2,000,000。 • ASA 5580-40 - 2,000,000 至 4,000,000。 • 带 SSP-10 的 ASA 5585-X：750,000 至 1,000,000。 • 带 SSP-20 的 ASA 5585-X：1,000,000 至 2,000,000。 • 带 SSP-40 的 ASA 5585-X：2,000,000 至 4,000,000。 • 带 SSP-60 的 ASA 5585-X：2,000,000 至 10,000,000。
AnyConnect 高级版 SSL VPN 许可证更改为 AnyConnect 高级版许可证	8.4(1)	AnyConnect 高级版 SSL VPN 许可证的名称更改为 AnyConnect 高级版许可证。许可证信息显示从“SSL VPN Peers”更改为“AnyConnect Premium Peers”。
增加了 ASA 5580 的 AnyConnect VPN 会话数	8.4(1)	AnyConnect VPN 会话限制从 5,000 增加到 10,000。
增加了 ASA 5580 的其他 VPN 会话数	8.4(1)	其他 VPN 会话数限值从 5,000 增加到 10,000。
使用 IKEv2 的 IPsec 远程访问 VPN	8.4(1)	向 AnyConnect 基础版和 AnyConnect 高级版许可证中添加了使用 IKEv2 的 IPsec 远程访问 VPN。 **注释** ASA 上对 IKEv2 的支持存在以下限制： 我们当前不支持重复的安全关联。 IKEv2 站点间会话已添加到其他 VPN 许可证（以前为 IPsec VPN）。其他 VPN 许可证包含在基础许可证中。
用于出口的无负载加密硬件	8.4(1)	对于支持无负载加密的型号（例如 ASA 5585-X），ASA 软件将禁用统一通信和 VPN 功能，从而使 ASA 可以出口至某些国家/地区。
适用于 SSP-20 和 SSP-40 的双 SSP	8.4(2)	对于 SSP-40 和 SSP-60，您可以在同一机箱中使用两个相同级别的 SSP。不支持混合级别的 SSP（例如，不支持混用 SSP-40 和 SSP-60）。每个 SSP 均作为独立设备，可单独配置和管理。如果需要，可以将两个 SSP 用作故障转移对。当在机箱中使用两个 SSP 时不支持 VPN；但请注意，VPN 并没有被禁用。
ASA 5512-X 至 ASA 5555-X 的 IPS 模块许可证	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 上的 IPS SSP 软件模块需要 IPS 模块许可证。
ASA 5580 和 5585-X 的集群许可证	9.0(1)	为 ASA 5580 和 5585-X 添加了集群许可证。

功能名称	平台版本	说明
ASASM 上支持 VPN	9.0(1)	ASASM 现在支持所有 VPN 功能。
ASASM 上支持统一通信	9.0(1)	ASASM 现在支持所有统一通信功能。
SSP-10 和 SSP-20 的 ASA 5585-X 双 SSP 支持（SSP-40 和 SSP-60 除外）；双 SSP 的 VPN 支持	9.0(1)	ASA 5585-X 现在支持所有 SSP 型号使用双 SSP（在同一机箱中，您可以使用两个相同级别的 SSP）。使用双 SSP 时，现在支持 VPN。
ASA 5500-X 对集群的支持	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X 现在支持由 2 台设备组成的集群。默认情况下，在基础许可证中支持两台设备的集群；对于 ASA 5512-X，您需要增强型安全许可证。
对 ASA 5585-X 支持 16 个集群成员	9.2(1)	ASA 5585-X 现在支持由 16 台设备组成的集群。
引入了 ASAv4 和 ASAv30 标准版和高级版型号许可证	9.2(1)	ASAv 带有一种简单的许可方案：标准版和高级版级别的 ASAv4 和 ASAv30 永久许可证。无可用的附加许可证。



第 4 章

许可证：智能软件许可

通过智能软件许可，您可以集中购买和管理许可证池。与产品授权密钥 (PAK) 许可证不同，智能许可证未绑定到特定序列号。您可以轻松部署或停用 ASA，而不必管理每台设备的许可密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。

注释 有关每个平台的智能许可功能和行为的详细信息，请参阅支持智能的产品系列。

- 关于智能软件许可， 第 79 页
- 智能软件许可的前提条件， 第 100 页
- 智能软件许可准则， 第 101 页
- 智能软件许可的默认设置， 第 101 页
- ASA Virtual: 配置智能软件许可， 第 102 页
- 1000/1200/3100/4200：配置智能软件许可， 第 123 页
- Firepower 4100/9300: 配置智能软件许可， 第 137 页
- 每个型号的许可证， 第 139 页
- 每个型号的许可证 PID， 第 152 页
- 监控智能软件许可， 第 156 页
- 智能软件管理器通信， 第 160 页
- 智能软件许可的历史记录， 第 162 页

关于智能软件许可

思科智能许可是一种灵活的许可模式，为您提供一种更简便、更快速、更一致的方式来购买和管理整个思科产品组合和整个组织中的软件。此外它很安全，您可以控制用户可访问的内容。借助智能许可，您可以：

- **轻松激活：** 智能许可建立了可在整个组织中使用的软件许可证池，不再需要产品激活密钥 (PAK)。
- **统一管理：** 利用 My Cisco Entitlements (MCE)，您可以在一个易于使用的门户中全面了解您的所有 Cisco 产品和服务，始终了解您拥有以及正在使用的产品和服务。

- **许可证灵活性：** 您的软件没有与硬件节点锁定，因此您可以根据需要轻松使用和传输许可证。

要使用智能许可，您必须先在 Cisco Software Central (software.cisco.com) 上创建智能帐户。

有关思科许可的更详细概述，请访问 cisco.com/go/licensingguide

Firepower 4100/9300 机箱上 ASA 的智能软件许可

对于 Firepower 4100/9300 机箱上的 ASA，智能软件许可配置，划分为 Firepower 4100/9300 机箱管理引擎和 ASA 两部分。

- Firepower 4100/9300 机箱- 在机箱上配置所有智能软件许可基础设施，包括用于与智能软件管理器进行通信的参数。Firepower 4100/9300 机箱本身无需任何许可证即可运行。

注释 机箱间集群需要您在集群的每个机箱上启用相同的智能许可方法。

- ASA 应用 - 在 ASA 中配置所有许可证授权。

智能软件管理器和账户

在为设备购买一个或多个许可证时，可在思科智能软件管理器中对其进行管理：

https://software.cisco.com/#module/SmartLicensing

通过智能软件管理器，您可以为组织创建一个主账户。

注释 如果您还没有账户，请点击此链接以设置新账户。通过智能软件管理器，您可以为组织创建一个主帐户。

默认情况下，许可证分配给主账户下的默认虚拟账户。作为账户管理员，您可以选择创建其他虚拟账户；例如，您可以为区域、部门或子公司创建账户。通过多个虚拟账户，您可以更轻松地管理大量许可证和设备。

离线管理

如果您的设备无法访问互联网，也不能向智能软件管理器注册，您必须配置离线许可。

永久许可证预留

如果您的设备出于安全原因而无法访问互联网，您可以选择为每个ASA请求永久许可证。永久许可证不需要定期访问智能软件管理器。与 PAK 许可证一样，您可以购买许可证并为 ASA 安装许可证密钥。与PAK许可证不同的是，您可以通过智能软件管理器获取和管理许可证。您可以在定期智能许可模式与永久许可证预留模式之间轻松切换。

注释 ASA 不支持特定许可证预留 (SLR)。在 SLR 中，特定功能授权将永久启用。ASA 仅支持永久启用所有功能的 PLR。

ASA Virtual 永久许可证预留

注释 仅在 VMware 和 KVM 上支持永久许可证预留。

您可以获得启用以下所有功能的型号特定许可证：

- 模式的最大吞吐量
- 基础 层
- 强加密 (3DES/AES) 许可证，如果您已在智能许可账户中启用该功能
- 为平台启用的 Secure Client 功能

  能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 86 页）。

基于内存和 vCPU 的永久许可证预留模式

您可以根据分配给 ASA virtual 的 RAM 和 vCPU 来配置型号特定许可证。例如，具有 8 GB RAM 和 4 个 vCPU 的 ASA virtual 始终使用具有 2G 吞吐量的 ASAv30 许可证。

vCPU 和内存与许可证的关系如下：

- 2 GB，1 个 vCPU - ASAv5 (100M)（必须运行 **license smart set_plr5** 命令；否则，ASAv10 许可证会分配为允许 1 G 吞吐量。）

注释 在版本 9.13 中，ASAv5 RAM 要求被提高到了 2 GB。由于 RAM 的增加，ASAv5 永久许可证不再有效，因为 ASA 检查了分配的内存并确定 2 GB RAM 实际上是 ASAv10，而不是 ASAv5。要允许 ASAv5 永久许可证工作，您必须将 ASA 配置为为此模式识别额外的内存。

- 2 GB，1 个 vCPU - ASAv10 (1G)
- 8 GB，4 个 vCPU - ASAv30 (2G)
- 16 GB，8 个 vCPU - ASAv50 (10G)
- 32 GB，16 个 vCPU - ASAv100 (20G)
- 64 GB，32 个 vCPU - ASAvU

- 128 GB，64 个 vCPU - ASAvU

稍后，如果要更改设备的型号级别，则必须退回当前许可证并在正确的型号级别请求新的许可证。要更改已部署的 ASA virtual 的型号，在虚拟机监控程序中，可以更改 vCPU 和 DRAM 设置以匹配新的型号要求。有关这些值，请参阅《*ASA virtual Virtual* 入门指南》。

如果您停止使用许可证，则必须通过在 ASA virtual 上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。您必须正确遵循退回过程，以避免为未使用的许可证付费。

有关配置永久许可证预留的详细信息，请参阅ASA Virtual：配置永久许可证预留 ，第 118 页。

Firepower 1010 永久许可证预留

您可以获得启用所有功能的许可证：

- 基础 层
- Security Plus
- 强加密 (3DES/AES) 许可证（如果您的帐户符合条件）
- Secure Client 功能已启用并设为平台最大值。

  能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 ，第 86 页）。

注释 您还需要在 ASA 配置中请求授权，以便 ASA 允许使用它们。

如果您停止使用许可证，则必须通过在ASA上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。确保正确遵循退回过程，以避免为未使用的许可证付费。

Firepower 1100 永久许可证预留

您可以获得启用所有功能的许可证：

- 基础 层
- 最大安全情景数
- 强加密 (3DES/AES) 许可证（如果您的帐户符合条件）
- Secure Client 功能已启用并设为平台最大值。

  能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 ，第 86 页）。

注释 您还需要在 ASA 配置中请求授权，以便 ASA 允许使用它们。

如果您停止使用许可证，则必须通过在ASA上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。确保正确遵循退回过程，以避免为未使用的许可证付费。

Cisco Secure Firewall 1210/1220 永久许可证预留

您可以获得启用所有功能的许可证：

- 基础 层
- 强加密 (3DES/AES) 许可证（如果您的帐户符合条件）
- Secure Client 功能已启用并设为平台最大值。

  能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 86 页）。

注释 您还需要在 ASA 配置中请求授权，以便 ASA 允许使用它们。

如果您停止使用许可证，则必须通过在ASA上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。确保正确遵循退回过程，以避免为未使用的许可证付费。

Cisco Secure Firewall 3100/4200 永久许可证预留

您可以获得启用所有功能的许可证：

- 基础 层
- 最大安全情景数
- 运营商许可证
- 强加密 (3DES/AES) 许可证（如果您的帐户符合条件）
- Secure Client 功能已启用并设为平台最大值。

  能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 86 页）。

注释 您还需要在 ASA 配置中请求授权，以便 ASA 允许使用它们。

如果您停止使用许可证，则必须通过在ASA上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。确保正确遵循退回过程，以避免为未使用的许可证付费。

Firepower 4100/9300 机箱永久许可证预留

您可以获得启用所有功能的许可证：

- 基础 层。
- 最大安全情景数
- 运营商许可证
- 强加密 (3DES/AES) 许可证（如果您的帐户符合条件）
- Secure Client 功能已启用并设为平台最大值。

  能否使用 Secure Client 功能取决于是否购买了让您能够使用 Secure Client 的 Secure Client 许可证（请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 86 页）。

注释 许可证在 Firepower 4100/9300 机箱上管理，但您还需要请求 ASA 配置授权，以便 ASA 允许使用它们。

如果您停止使用许可证，则必须通过在 Firepower 4100/9300 机箱 上生成退回代码，然后将该代码输入智能软件管理器中以退回许可证。确保正确遵循退回过程，以避免为未使用的许可证付费。

注释 将 ASA Virtual 版本 9.20 反向升级到较早的未许可版本时，在 ASA Virtual 版本 9.20 注册期间生成的 PLR 令牌将返回到智能许可证服务器。此 PLR 令牌与未经许可的 ASA Virtual（升级后）的许可证安装不兼容。

智能软件管理器本地版

如果您的设备出于安全原因无法访问互联网，您可以选择以虚拟机 (VM) 形式安装本地智能软件管理器卫星（也称为“智能软件卫星服务器”）服务器。该本地智能软件管理器提供智能软件管理器功能的子集，并允许您为所有本地设备提供必要的许可服务。只有本地智能软件管理器需要定期连接到主智能软件管理器，才能同步您的许可证使用情况。您可以按时间表执行同步，也可以手动同步。

您可以在本地智能软件管理器上执行以下功能：

- 激活或注册许可证
- 查看公司的许可证
- 在公司实体之间传输许可证

有关更多信息，请参阅思科智能软件管理器本地部署产品手册。

按虚拟帐户管理的许可证和设备

仅当虚拟账户可以使用分配给该账户的许可证时，才能按虚拟账户对许可证和设备进行管理。如果您需要其他许可证，则可以从另一个虚拟账户传输未使用的许可证。您还可以在虚拟账户之间迁移设备。

对于 Firepower 4100/9300 机箱上的 ASA - 仅机箱注册为设备，而机箱中的 ASA 应用会请求自己的许可证。例如，对于配有 3 个安全模块的 Firepower 9300 机箱，机箱计为一个设备，但模块使用 3 个单独的许可证。

评估许可证

ASA Virtual

ASA virtual 不支持评估模式。在 ASA virtual 向智能软件管理器注册之前，它会在严格限制速率的状态下运行。

Firepower 1000

在 Firepower 1000 向智能软件管理器注册之前，它会在评估模式下运行 90 天（总用量）。仅已启用默认授权。当此期限结束时，Firepower 1000 将变为不合规。

注释 您不能接收评估许可证进行强加密 (3DES/AES)；您必须向智能软件管理器注册，以接收可启用强加密 (3DES/AES) 许可证的导出合规性令牌。

Firepower 2100

在 Firepower 2100 向智能软件管理器注册之前，它会在评估模式下运行 90 天（总用量）。仅已启用默认授权。当此期限结束时，Firepower 2100 将变为不合规。

注释 您不能接收评估许可证进行强加密 (3DES/AES)；您必须向智能软件管理器注册，以接收可启用强加密 (3DES/AES) 许可证的导出合规性令牌。

Cisco Secure Firewall 3100/4200

在 Cisco Secure Firewall 3100/4200 向智能软件管理器注册之前，它会在评估模式下运行 90 天（总使用量）。仅已启用默认授权。当此期限结束时，Cisco Secure Firepower 3100/4200 将变为不合规。

注释 您不能接收评估许可证进行强加密 (3DES/AES)；您必须向智能软件管理器注册，以接收可启用强加密 (3DES/AES) 许可证的导出合规性令牌。

Firepower 4100/9300 机箱

Firepower 4100/9300 机箱支持两种类型的评估许可证：

- 机箱级评估模式 - 在 Firepower 4100/9300 机箱 向智能软件管理器注册之前，会在评估模式下运行 90 天（总使用量）。ASA 在此模式下无法请求特定授权，只能启用默认授权。当此期限结束时，Firepower 4100/9300 机箱会变为不合规。
- 基于授权的评估模式 - 在 Firepower 4100/9300 机箱向智能软件管理器注册之后，您可以获取基于时间的评估许可证，并可将这些许可证分配给 ASA。在 ASA 中，可照常请求授权。当该基于时间的许可证到期时，您需要续订基于时间的许可证或获取永久许可证。

注释 您不能接收评估许可证进行强加密 (3DES/AES)；您必须向智能软件管理器注册并获取永久许可证，以接收可启用强加密 (3DES/AES) 许可证的导出合规性令牌。

关于按类型划分的许可证

以下部分包括有关按类型分类的许可证的其他信息。

Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证

Secure Client 许可证不会直接应用于 ASA。但是，您需要购买许可证并将其添加到您的智能账户，以保证将 ASA 用作 Secure Client 前端。

- 对于 Secure Client Advantage 和 Secure Client Premier 许可证，将您打算在智能账户中的所有 ASA 中使用的对等体数量相加，并为该数量的对等体购买许可证。
- 对于 仅限 Secure Client VPN，请为每个 ASA 购买一个许可证。与提供可由多个 ASA 共享的对等体池的其他许可证不同， 仅限 Secure Client VPN 许可证是按前端划分的。

有关详情，请参阅：

- Cisco Secure Client 订购指南
- Secure Client 许可常见问题解答 (FAQ)

其他 VPN 对等体数

其他 VPN 对等体包括以下 VPN 类型：

- 使用 IKEv1 的 IPsec 远程访问 VPN
- 使用 IKEv1 的 IPsec 站点间 VPN
- 使用 IKEv2 的 IPsec 站点间 VPN

此许可证包含在基础许可证中。

VPN 对等体总数，所有类型

- VPN 对等体总数是 Secure Client 和其他 VPN 对等体允许的最大 VPN 对等体数。例如，如果总数为 1000，则可以同时允许 500 个 Secure Client 和 500 个其他 VPN 对等体；或 700 个 Secure Client 和 300 个其他 VPN；或对 Secure Client 使用全部 1000 个。如果超出了 VPN 对等体总数，可以对 ASA 实施过载，以确保相应地调整网络大小。

加密许可证

强加密：ASA Virtual

在连接到智能软件管理器或智能软件管理器本地服务器之前，强加密 (3DES/AES) 可用于管理连接，因此您可以启动 ASDM 并连接到智能软件管理器。对于需要强加密（如 VPN）的通过设备的流量，在您连接到智能软件管理器并获得强加密许可证之前，吞吐量会受到严格限制。

当您向智能软件许可帐户请求 ASA virtual 的注册令牌时，请选中 **允许在通过此令牌注册的产品上使用导出控制功能** 复选框，以便应用强加密 (3DES/AES) 许可证（您的帐户必须符合其使用条件）。如果 ASA virtual 之后变为不合规状态，只要已成功应用导出合规性令牌， ASA virtual 将会保留许可证，并且不会恢复到速率受限状态。如果您重新注册 ASA virtual，并且禁用了导出合规性，或者如果您将 ASA virtual 还原到出厂默认设置，系统将会删除该许可证。

如果最初注册 ASA virtual 时未使用强加密，之后又添加了强加密，则必须重新加载 ASA virtual 才能使新许可证生效。

对于永久许可证预留许可证，如果您的帐户符合使用条件，则启用强加密 (3DES/AES) 许可证。

如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。

强加密：设备模式下的 Firepower 1000、Cisco Secure Firewall 1200/3100/4200

ASA 默认情况下包含 3DES 功能，仅用于管理访问，因此您可以连接到智能软件管理器，还可以立即使用 ASDM。如果之后在 ASA 上配置了 SSH 访问，也可以使用 SSH 和 SCP。其他需要强加密（例如 VPN）的功能必须启用强加密，这要求您先向智能软件管理器注册。

注释 如果您在注册之前尝试配置任何可使用强加密的功能（即使您仅配置了弱加密），您的 HTTPS 连接会在该接口上断开，并且您无法重新连接。此规则的例外是您连接到仅限管理的接口，例如管理 1/1。SSH 不受影响。如果您丢失了 HTTPS 连接，可以连接到控制台端口以重新配置 ASA、连接到仅管理接口，或者连接到没有为强加密功能配置的接口。

当您向智能软件许可帐户请求 ASA 的注册令牌时，请选中 **允许在通过此令牌注册的产品上使用导出控制功能** 复选框，以便应用强加密 (3DES/AES) 许可证（您的帐户必须符合其使用条件）。如果 ASA 之后变为不合规状态，只要已成功应用导出合规性令牌，ASA 将会继续允许通过设备的流量。即使您重新注册 ASA 并禁用导出合规性，许可证仍将保持启用状态。如果您将 ASA 恢复到出厂默认设置，系统将会删除该许可证。

如果最初注册 ASA 时未使用强加密，之后又添加了强加密，则必须重新加载 ASA 才能使新许可证生效。

对于永久许可证预留许可证，如果您的帐户符合使用条件，则启用强加密 (3DES/AES) 许可证。

如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。

强加密：Firepower 4100/9300 机箱

当ASA部署为逻辑设备时，您可以立即启动ASDM。在您连接并获取强加密许可证之前，不允许通过需要强加密（如 VPN）设备的流量。

当您向智能软件许可帐户请求机箱的注册令牌时，请选中 **允许在通过此令牌注册的产品上使用导出控制功能** 复选框，以便应用强加密 (3DES/AES) 许可证（您的帐户必须符合其使用条件）。

如果 ASA 之后变为不合规状态，只要已成功应用导出合规性令牌，ASA 将会继续允许通过设备的流量。如果您重新注册机箱，并且禁用了导出合规性，或者如果您将机箱还原到出厂默认设置，系统将会删除该许可证。

如果最初注册机箱时未使用强加密，之后又添加了强加密，则必须重新加载ASA应用程序才能使新许可证生效。

对于永久许可证预留许可证，如果您的帐户符合使用条件，则启用强加密 (3DES/AES) 许可证。

如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。

DES：所有型号

无法禁用 DES 许可证。如果您安装有 3DES 许可证，则 DES 仍然可用。要在希望仅使用强加密时防止使用 DES，请务必将所有相关命令都配置为仅使用强加密。

运营商许可证

借助运营商许可证，可以实现以下检查功能：

- Diameter - Diameter是用于下一代移动和固定电信网络（例如用于 LTE（长期演进）和 IMS（多媒体子系统）的 EPS（演进的数据包系统）的身份验证、授权和记账 (AAA) 协议。在这些网络中，该协议将取代 RADIUS 和 TACACS。
- GTP/GPRS—GPRS 隧道协议用于 GSM、UMTS 和 LTE 网络的通用分组无线服务 (GPRS) 流量。GTP 提供隧道控制和管理协议，通过创建、修改和删除隧道来为移动站提供 GPRS 网络接入。此外，GTP 还使用隧道机制来传送用户数据包。
- M3UA—MTP3 User Adaptation (M3UA) 是客户端/服务器协议，为基于 IP 的应用提供连接 SS7 网络的网关，以便连接 SS7 消息传递部分 3 (MTP3) 层。使用 M3UA，可以通过 IP 网络运行 SS7 用户部分（例如 ISUP）。M3UA 在 RFC 4666 中定义。
- RFC 4960 中介绍了 SCTP—SCTP（流控制传输协议）。该协议支持基于 IP 的电话信令协议 SS7，也是适用于 4G LTE 移动网络架构中多个接口的传输协议。

TLS 代理会话总数

用于加密语音检测的每个 TLS 代理会话都会计入 TLS 许可证限制中。

使用 TLS 代理会话的其他应用不计入 TLS 限制，例如移动性优势代理（无需许可证）。

某些应用可能会在一个连接中使用多个会话。例如，如果为一部电话配置了主用和备用思科Unified Communications Manager，则有 2 个 TLS 代理连接。

使用 **tls-proxy maximum-sessions** 命令，或在 ASDM 中使用 **Configuration > Firewall > Unified Communications > TLS Proxy** 窗格，单独设置 TLS 代理限制。要查看型号的限制，请输入 **tls-proxy maximum-sessions ?** 命令。如果应用的 TLS 代理许可证高于默认的 TLS 代理限制，则 ASA 自动设置 TLS 代理限制以与许可证匹配。TLS 代理限制的优先级高于许可证限制；如果设置的 TLS 代理限制低于许可证限制，则无法使用许可证中的所有会话。

注释 对于以“K8”结尾的许可证部件号（例如，用户数少于 250 的许可证），TLS 代理会话数限制为 1000。对于以“k9”结尾的许可证部件号（例如，用户数为 250 或更多的许可证），TLS 代理限制取决于配置，最高值为型号限制。K8 和 K9 是指许可证是否有出口限制：K8 不受限制，K9 受限制。

如果清除配置（例如使用 **clear configure all** 命令），TLS 代理限制将设置为模型的默认值；如果默认值低于许可证限制，会显示一条错误消息，让您使用 **tls-proxy maximum-sessions** 命令再次增加该限制（在 ASDM 中，使用 **TLS Proxy** 窗格）。如果使用故障转移并输入 **write standby** 命令，或者在 ASDM 中，在主设备上使用 **File > Save Running Configuration to Standby Unit** 来强制进行配置同步，则会在辅助设备上自动生成 **clear configure all** 命令，因此，您可能会在辅助设备上看到警告消息。由于配置同步会恢复在主设备上设置的 TLS 代理限制，因此可以忽略该警告。

您也可能为连接使用 SRTP 加密会话：

- 对于 K8 许可证，SRTP 会话数限制为 250。
- 对于 K9 许可证，则没有任何限制。

注释 只有需要对媒体进行加密/解密的呼叫会计入 SRTP 限制；如果将呼叫设置为直通式，即使两端均为 SRTP，这些呼叫也不计入限制。

最大 VLAN 数量

对于根据 VLAN 限制计数的接口，您必须向其分配 VLAN。 例如：

```
interface gigabitethernet 0/0.100
vlan 100
```

僵尸网络流量过滤器许可证

要下载动态数据库，需要强加密 (3DES/AES) 许可证。

故障转移或 ASA 集群许可证

ASAv 的故障转移许可证

备用设备需要与主设备相同型号的许可证。

Firepower 1010 的故障转移许可证

智能软件管理器常规版和本地版

两台 Firepower 1010 设备都必须向智能软件管理器或智能软件管理器本地服务器注册。两台设备都要求您先启用基础许可证和安全加许可证，然后才能配置故障转移。

通常，您也不需要在 ASA 中启用强加密（3DES/AES）功能许可证，因为在注册设备时，两台设备都应获得强加密令牌。使用注册令牌时，两台设备必须具有相同的加密级别。

如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。在这种情况下，请在启用故障转移后在主用设备上启用它。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。只有主用设备需要向服务器请求许可证。许可证将聚合为一个单独的故障转移许可证，供该故障转移对共享，并且此聚合许可证还将缓存在备用设备上，以便在该设备将来成为主用设备时使用。在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使用聚合许可证的期限是30天，如果该故障转移对在宽限期后仍不合规，且没有使用强加密令牌，则将无法对需要强加密 (3DES/AES) 功能许可证的功能进行配置更改；否则操作不会受到影响。新主用设备每隔35秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

Firepower 1100 的故障转移许可证

智能软件管理器常规版和本地版

只有主用设备需要向服务器请求许可证。许可证聚合为故障转移对共享的单个故障转移许可证。辅助设备不会产生额外成本。

为主用/备用故障转移启用故障转移后，只能在主用设备上配置智能许可。对于主用/主用故障转移，只能在故障转移组 1 为主用的设备上配置智能许可。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。聚合许可证也会缓存在备用设备上，以便在该设备将来成为主用设备时使用。

注释 每个 ASA 在形成故障转移对时必须具有相同的加密许可证。将 ASA 注册到智能许可服务器时，当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。由于此要求，在使用具有故障转移功能的强加密令牌时，您有两种许可选择：

- 在启用故障转移之前，请将两台设备注册到智能许可服务器。在这种情况下，两台设备将具有强加密功能。然后，在启用故障转移后，继续在主用设备上配置许可证授权。如果为故障转移链路启用加密，系统将会使用 AES/3DES（强加密）。
- 在将主用设备注册到智能许可服务器之前，请启用故障转移。这种情况下，两台设备都还不能进行强加密。然后，配置许可证授权并将主用设备注册到智能许可服务器；两台设备都将从聚合许可证中获得强加密。请注意，如果您在故障转移链路上启用了加密，系统将使用 DES（弱加密），因为故障转移链路是在设备获得强加密之前建立的。您必须重新加载两台设备，才能在链路上使用 AES/3DES。如果仅重新加载一台设备，则该设备将尝试使用 AES/3DES，而原始设备则使用 DES，这将导致两台设备变为活动状态（脑裂）。

各个插件许可证类型将按以下方式进行管理：

- 基础—虽然只有主用设备需要向服务器请求此许可证，但默认情况下备用设备已启用了基础许可证；它不需要向服务器注册来使用它。
- 情景 - 只有主用设备需要请求此许可证。不过，默认情况下基础许可证包括 2 个情景，并存在于两台设备上。每台设备的基础许可证的值与主用设备上的情景许可证的值合并之和为平台限制。例如：
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 1120 设备，这些许可证总计包括 4 个情景。您在主用/备用对中的主用设备上配置 3 个情景的许可证。因此，聚合故障转移许可证包括 7 个情景。不过，由于一台设备的平台限制为 5，因此合并许可证最多仅允许 5 个情景。在此情况下，只能将主用情景许可证配置为 1 个情景。
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 Firepower 1140 设备，这些许可证总计包括 4 个情景。您在主用/主用对中的主设备上配置 4 个情景的许可证。因此，聚合故障转移许可证包括 8 个情景。例如，一台设备可以使用 5 个情景，而另一台设备可以使用 3 个情景，例如；但在失败期间，一台设备将使用所有 8 个情景。由于一台设备的平台限制为 10，因此合并许可证最多允许 10 个情景；8 个情景在该限制范围内。
- 强加密 (3DES/AES) - 如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使用聚合许可证的期限是30天，如果该故障转移对在宽限期后仍不合规，则将无法对需要特殊许可证的功能（例如，添加一个额外的情景）进行配置更改；否则操作不会受到影响。新主用设备每隔 35 秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布

授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

Cisco Secure Firewall 1210/1220 的故障转移许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议您在启用故障转移之前使用许可服务器对每台设备进行许可，以避免许可不匹配问题，以及在使用强加密许可证时出现的故障转移链路加密问题。

数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在 ASA 许可证配置中，默认情况下，两台设备上的 基础 许可证始终处于启用状态。为主用/备用故障转移启用故障转移后，只能在主用设备上配置智能许可。对于主用/主用故障转移，只能在故障转移组 1 为主用的设备上配置智能许可。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。聚合许可证也会缓存在备用设备上，以便在该设备将来成为主用设备时使用。

各个插件许可证类型将按以下方式进行管理：

- 基础 — 每台设备都会向服务器请求一个基础许可证。
- 情景 - 只有主用设备需要请求此许可证。不过，默认情况下基础许可证包括 2 个情景，并存在于两台设备上。每台设备的基础许可证的值与主用设备上的情景许可证的值合并之和为平台限制。例如：
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 1210 设备，这些许可证总计包括 4 个情景。您在主用/备用对中的主用设备上配置 5 个情景的许可证。因此，聚合故障转移许可证包括 9 个情景。不过，由于一台设备的平台限制为 5，因此合并许可证最多仅允许 5 个情景。在此情况下，只能将主用情景许可证配置为 1 个情景。
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 1220 设备，这些许可证总计包括 4 个情景。您在主用/主用对中的主设备上配置 5 个情景的许可证。因此，聚合故障转移许可证包括 9 个情景。例如，一台设备可以使用 5 个情景，而另一台设备可以使用 4 个情景；但在故障期间，一台设备将使用全部 9 个情景。由于一台设备的平台限制为 10，因此合并许可证最多允许 10 个情景；9 个情景在该限制范围内。
- 强加密 (3DES/AES) - 如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使

用聚合许可证的期限是30天，如果该故障转移对在宽限期后仍不合规，则将无法对需要特殊许可证的功能进行配置更改；否则操作不会受到影响。新主用设备每隔35秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

Cisco Secure Firewall 3100 的故障转移许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议您在启用故障转移之前使用许可服务器对每台设备进行许可，以避免许可不匹配问题，以及在使用强加密许可证时出现的故障转移链路加密问题。

故障转移功能本身不需要任何许可证。数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在 ASA 许可证配置中，默认情况下，两台设备上的 基础 许可证始终处于启用状态。为主用/备用故障转移启用故障转移后，只能在主用设备上配置智能许可。对于主用/主用故障转移，只能在故障转移组 1 为主用的设备上配置智能许可。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。聚合许可证也会缓存在备用设备上，以便在该设备将来成为主用设备时使用。

各个插件许可证类型将按以下方式进行管理：

- 基础 — 每台设备都会向服务器请求一个基础许可证。
- 情景 - 只有主用设备需要请求此许可证。不过，默认情况下基础许可证包括 2 个情景，并存在于两台设备上。每台设备的基础许可证的值与主用设备上的情景许可证的值合并之和为平台限制。例如：
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 3130 设备，这些许可证总计包括 4 个情景。您在主用/备用对中的主用设备上配置 100 个情景的许可证。因此，聚合故障转移许可证包括 104 个情景。不过，由于一台设备的平台限制为 100，因此合并许可证最多仅允许 100 个情景。在此情况下，只能将主用情景许可证配置为 95 个情景。
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 3130 设备，这些许可证总计包括 4 个情景。您在主用/主用对中的主设备上配置 10 个情景的许可证。因此，聚合故障转移许可证包括 14 个情景。例如，一台设备可以使用 9 个情景，而另一台设备可以使用 5 个情景，例如；但在失败期间，一台设备将使用所有14个情景。由于一台设备的平台限制为 100，因此合并许可证最多允许 100 个情景；14 个情景在该限制范围内。
- 强加密 (3DES/AES) - 如果您的智能账户未获得强加密授权，但Cisco已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使用聚合许可证的期限是30天，如果该故障转移对在宽限期后仍不合规，则将无法对需要特殊许可证的功能（例如，添加一个额外的情景）进行配置更改；否则操作不会受到影响。新主用设备每隔 35 秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

Cisco Secure Firewall 4200 的故障转移许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议您在启用故障转移之前使用许可服务器对每台设备进行许可，以避免许可不匹配问题，以及在使用强加密许可证时出现的故障转移链路加密问题。

故障转移功能本身不需要任何许可证。数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在 ASA 许可证配置中，默认情况下，两台设备上的 基础 许可证始终处于启用状态。为主用/备用故障转移启用故障转移后，只能在主用设备上配置智能许可。对于主用/主用故障转移，只能在故障转移组 1 为主用的设备上配置智能许可。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。聚合许可证也会缓存在备用设备上，以便在该设备将来成为主用设备时使用。

各个插件许可证类型将按以下方式进行管理：

- 基础 - 每台设备从服务器请求一个基础许可证。
- 情景 - 只有主用设备需要请求此许可证。不过，默认情况下基础许可证包括 2 个情景，并存在于两台设备上。每台设备的基础许可证的值与主用设备上的情景许可证的值合并之和为平台限制。例如：
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 4215 设备，这些许可证总计包括 4 个情景。您在主用/备用对中的主用设备上配置 250 个情景的许可证。因此，聚合故障转移许可证包括 254 个情景。不过，由于一台设备的平台限制为 250，因此合并许可证最多仅允许 250 个情景。在此情况下，只能将主用情景许可证配置为 246 个情景。
  - 主用/备用： 基础 许可证包括 2 个情景；对于两个 FirePower 4215 设备，这些许可证总计包括 4 个情景。您在主用/主用对中的主设备上配置 10 个情景的许可证。因此，聚合故障转移许可证包括 14 个情景。例如，一台设备可以使用 9 个情景，而另一台设备可以使用 5 个情景，例如；但在失败期间，一台设备将使用所有 14 个情景。由于一台设备的平台限制为 250，因此合并许可证最多允许 250 个情景；14 个情景在该限制范围内。

- 强加密 (3DES/AES) - 如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使用聚合许可证的期限是 30 天，如果该故障转移对在宽限期后仍不合规，则将无法对需要特殊许可证的功能（例如，添加一个额外的情景）进行配置更改；否则操作不会受到影响。新主用设备每隔 35 秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

适用于 Firepower 4100/9300 的故障转移许可证

智能软件管理器常规版和本地版

在配置故障转移之前，两个 Firepower 4100/9300 都必须向智能软件管理器或智能软件管理器本地服务器注册。辅助设备不会产生额外成本。

当您应用注册令牌时，对于符合条件的用户，系统会自动启用强加密许可证。使用令牌时，每个机箱必须具有相同的加密许可证。对于在 ASA 配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

为主用/备用故障转移启用故障转移后，只能在主用设备上配置用于主用/备用故障转移的 ASA 许可证配置智能许可。对于主用/主用故障转移，只能在故障转移组 1 为主用的设备上配置智能许可。该配置将被复制到备用设备，但备用设备不会使用该配置；它将保持在缓存状态。只有主用设备需要向服务器请求许可证。许可证将聚合为一个单独的故障转移许可证，供该故障转移对共享，并且此聚合许可证还将缓存在备用设备上，以便在该设备将来成为主用设备时使用。各个许可证类型将按以下方式进行管理：

- 基础—虽然只有主用设备需要向服务器请求此许可证，但默认情况下备用设备已启用了基础许可证；它不需要向服务器注册来使用它。
- 情景 - 只有主用设备需要请求此许可证。不过，默认情况下基础许可证包括 10 个情景，并存在于两台设备上。每台设备的基础许可证的值与主用设备上的情景许可证的值合并之和为平台限制。例如：
  - 主用/备用： 基础 许可证包括 10 个情景；对于 2 台设备，这些许可证相加之和为 20 个情景。您在主用/备用对中的主用设备上配置 250 个情景的许可证。因此，聚合故障转移许可证包括 270 个情景。不过，由于一台设备的平台限制为 250，因此合并许可证最多仅允许 250 个情景。在此情况下，只能将主用情景许可证配置为 230 个情景。
  - 主用/主用： 基础 许可证包括 10 个情景；对于 2 台设备，这些许可证相加之和为 20 个情景。您在主用/主用对中的主设备上配置 10 个情景的许可证。因此，聚合故障转移许可证包括 30 个情景。例如，一台设备可以使用 17 个情景，而另一台设备可以使用 13 个情景，

例如；但在失败期间，一台设备将使用所有 30 个情景。由于一台设备的平台限制为 250，因此合并许可证最多允许 250 个情景；30 个情景在该限制范围内。

- 运营商 - 只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。
- 强加密 (3DES) - 如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

在故障转移后，新的主用设备将继续使用聚合许可证。它将使用缓存许可证配置向服务器重新请求授权。当旧的主用设备作为备用设备重新加入该对时，它将发布许可证授权。在备用设备发布授权之前，如果帐户中没有可用的许可证，则新主用设备的许可证可能处于不合规状态。故障转移对使用聚合许可证的期限是30天，如果该故障转移对在宽限期后仍不合规，则将无法对需要特殊许可证的功能进行配置更改；否则操作不会受到影响。新主用设备每隔35秒发送一个权限授权续约请求，直到许可证合规为止。如果解散该故障转移对，则主用设备将发布授权，并且两台设备会将许可配置保留在缓存状态。要重新激活许可，需要清除每台设备上的配置，然后再重新配置它。

永久许可证预留

对于永久许可证预留，必须在配置故障转移之前为每台机箱单独购买许可证并启用。

Cisco Secure Firewall 3100 的 ASA 群集许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议在启用集群之前使用许可服务器对每台设备进行许可，避免出现许可不匹配的问题，并在使用强加密许可证时出现集群控制链路加密问题。

集群功能本身不需要任何许可证。数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在ASA许可证配置中，默认情况下，始终在所有设备上启用基础许可证。您只能在控制设备上配置智能许可。该配置会复制到数据设备，但某些许可证不使用该配置；它仍处于缓存状态，只有控制设备才会请求许可证。这些许可证将聚合成一个由集群设备共享的集群许可证，此聚合许可证也会缓存在数据设备上，以便将来某个从属设备变为控制设备时使用。各个许可证类型将按以下方式进行管理：

- 基础 — 每台设备都会向服务器请求一个基础许可证。
- 情景 - 只有控制设备从服务器请求情景许可证。默认情况下，基础许可证包括 2 个情景，并且位于所有集群成员上。每台设备的基础许可证的值加上控制设备上的情景许可证的值共同形成了聚合集群许可证中的平台限制。例如：
  - 您在集群中有 6 个 Cisco Secure Firewall 3100。基础许可证包括 2 个情景；因为有 6 台设备，因此这些许可证加起来总共包括 12 个情景。您在控制设备上额外配置一个包含 20 个情景的许可证。因此，聚合的集群许可证包括32个情景。由于一台机箱的平台限制为100，因此合并许可证最多允许 100 个情景；32 个情景在该限制范围内。因此，您可以在控制设备上配置最多 32 个情景；每台数据设备通过配置复制也将拥有 32 个情景。

- 您在集群中有 3 个 Cisco Secure Firewall 3100。基础许可证包括 2 个情景；因为有 3 台设备，因此这些许可证加起来总共包括 6 个情景。您在控制设备上额外配置一个包含 100 个情景的许可证。因此，聚合的集群许可证包括 106 个情景。由于一台设备的平台限制为 100，因此合并许可证最多允许 100 个情景；106 个情景超出限制范围。因此，您仅可以在控制设备上配置最多 100 个情景；每台数据设备通过配置复制也将拥有 100 个情景。在此情况下，只能将控制设备情景许可证配置为 94 个情景。

- 强加密 (3DES) - 如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有控制设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

如果选择了新的控制设备，新的控制设备继续使用聚合的许可证。它还会使用缓存的许可证配置再次请求控制设备许可证。当旧的控制设备作为数据设备重新加入集群后，它会释放控制设备许可证授权。在数据设备释放该许可证之前，如果帐户中没有可用的许可证，则控制设备的许可证可能处于一个非合规状态。保留的许可证的有效期为30天，但如果它在此宽限期过后仍处于非合规状态，您将无法对需要特殊许可证的功能进行配置更改；否则操作将不受影响。新主用设备会每隔35秒发送一次权限授权续约请求，直到许可证合规为止。在对许可证请求进行完整的处理之前，应避免进行配置更改。如果某台设备退出集群，缓存的控制配置将被删除，而按设备进行的授权将会保留。尤其是，您需要在非集群设备上重新请求情景许可证。

永久许可证预留

对于永久许可证预留，必须在配置集群之前为每个机箱单独购买许可证并启用。

Cisco Secure Firewall 4200 的 ASA 群集许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议在启用集群之前使用许可服务器对每台设备进行许可，避免出现许可不匹配的问题，并在使用强加密许可证时出现集群控制链路加密问题。

集群功能本身不需要任何许可证。数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在ASA许可证配置中，默认情况下，始终在所有设备上启用基础许可证。您只能在控制设备上配置智能许可。该配置会复制到数据设备，但某些许可证不使用该配置；它仍处于缓存状态，只有控制设备才会请求许可证。这些许可证将聚合成一个由集群设备共享的集群许可证，此聚合许可证也会缓存在数据设备上，以便将来某个从属设备变为控制设备时使用。各个许可证类型将按以下方式进行管理：

- 基础 — 每台设备都会向服务器请求一个基础许可证。
- 情景 - 只有控制设备从服务器请求情景许可证。默认情况下，基础许可证包括 2 个情景，并且位于所有集群成员上。每台设备的基础许可证的值加上控制设备上的情景许可证的值共同形成了聚合集群许可证中的平台限制。例如：

- 您在集群中有 6 个 Cisco Secure Firewall 4200。基础许可证包括 2 个情景；因为有 6 台设备，因此这些许可证加起来总共包括 12 个情景。您在控制设备上额外配置一个包含 20 个情景的许可证。因此，聚合的集群许可证包括32个情景。由于一台机箱的平台限制为250，因此合并许可证最多允许 250 个情景；32 个情景在该限制范围内。因此，您可以在控制设备上配置最多 32 个情景；每台数据设备通过配置复制也将拥有 32 个情景。
- 您在集群中有 3 个 Cisco Secure Firewall 4200。基础许可证包括 2 个情景；因为有 3 台设备，因此这些许可证加起来总共包括 6 个情景。您在控制设备上额外配置一个包含 250 个情景的许可证。因此，聚合的群集许可证包括 256 个情景。由于一台设备的平台限制为 250，则聚合后的许可证最多允许 250 个情景；256 个情景超出了此限制。因此，您仅可以在控制设备上配置最多 250 个情景；每台数据设备通过配置复制也将拥有 250 个情景。在此情况下，只能将控制设备情景许可证配置为 244 个情景。

- 强加密 (3DES) - 如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有控制设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

如果选择了新的控制设备，新的控制设备继续使用聚合的许可证。它还会使用缓存的许可证配置再次请求控制设备许可证。当旧的控制设备作为数据设备重新加入集群后，它会释放控制设备许可证授权。在数据设备释放该许可证之前，如果帐户中没有可用的许可证，则控制设备的许可证可能处于一个非合规状态。保留的许可证的有效期为30天，但如果它在此宽限期过后仍处于非合规状态，您将无法对需要特殊许可证的功能进行配置更改；否则操作将不受影响。新主用设备会每隔35秒发送一次权限授权续约请求，直到许可证合规为止。在对许可证请求进行完整的处理之前，应避免进行配置更改。如果某台设备退出集群，缓存的控制配置将被删除，而按设备进行的授权将会保留。尤其是，您需要在非集群设备上重新请求情景许可证。

永久许可证预留

对于永久许可证预留，必须在配置集群之前为每个机箱单独购买许可证并启用。

ASAv 的 ASA 集群许可证

智能软件管理器常规版和本地版

每台设备需要相同的吞吐量许可证和相同的加密许可证。我们建议在启用集群之前使用许可服务器对每台设备进行许可，避免出现许可不匹配的问题，并在使用强加密许可证时出现集群控制链路加密问题。

集群功能本身不需要任何许可证。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在ASA许可证配置中，只能在控制设备上配置智能许可。该配置会复制到数据设备，但某些许可证不使用该配置；它仍处于缓存状态，只有控制设备才会请求许可证。这些许可证将聚合成一个由集群设备共享的集群许可证，此聚合许可证也会缓存在数据设备上，以便将来某个从属设备变为控制设备时使用。各个许可证类型将按以下方式进行管理：

- 基础 - 只有控制设备从服务器请求基础许可证，并且由于许可证汇聚，所有设备都可以使用标准许可证。

- 吞叶量 - 每台设备都会向服务器请求其自己的吞吐量许可证。
- 强加密 (3DES) - 如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有控制设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

永久许可证预留

对于永久许可证预留，必须在配置集群之前为每台设备单独购买许可证并启用。

Firepower 4100/9300 的 ASA 集群许可证

智能软件管理器常规版和本地版

集群功能本身不需要任何许可证。要使用强加密和其他可选许可证，每个 Firepower 4100/9300 机箱都必须注册到许可证颁发机构或智能软件管理器常规版和本地版中。数据设备不会产生额外成本。

当您应用注册令牌时，对于符合条件的用户，系统会自动启用强加密许可证。使用令牌时，每个机箱必须具有相同的加密许可证。对于在 ASA 配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在ASA许可证配置中，只能在控制设备上配置智能许可。该配置会复制到数据设备，但某些许可证不使用该配置；它仍处于缓存状态，只有控制设备才会请求许可证。这些许可证将聚合成一个由集群设备共享的集群许可证，此聚合许可证也会缓存在数据设备上，以便将来某个从属设备变为控制设备时使用。各个许可证类型将按以下方式进行管理：

- 基础 - 只有控制设备从服务器请求基础许可证，并且由于许可证汇聚，两个设备都可以使用标准许可证。
- 情景 - 只有控制设备从服务器请求情景许可证。默认情况下，基础许可证包括 10 个情景，并且位于所有集群成员上。每台设备的基础许可证的值加上控制设备上的情景许可证的值共同形成了聚合集群许可证中的平台限制。例如：
  - 集群中有 6 个 Firepower 9300 模块。基础许可证包括 10 个情景；对于 6 台设备，这些许可证相加之和为 60 个情景。您在控制设备上额外配置一个包含 20 个情景的许可证。因此，聚合的集群许可证包括 80 个情景。由于一个模块的平台限制为 250，因此聚合后的许可证最多允许 250 个情景；80 个情景没有超出此限制。因此，您可以在控制设备上配置最多 80 个情景；每台数据设备通过配置复制也将拥有 80 个情景。
  - 集群中有 3 台 Firepower 4112 设备。基础许可证包括 10 个情景；对于 3 台设备，这些许可证相加之和为 30 个情景。您在控制设备上额外配置一个包含 250 个情景的许可证。因此，聚合的集群许可证包括 280 个情景。由于一台设备的平台限制为 250，则聚合后的许可证最多允许 250 个情景；280 个情景超出了此限制。因此，您仅可以在控制设备上配置最多 250 个情景；每台数据设备通过配置复制也将拥有 250 个情景。在此情况下，只能将控制设备情景许可证配置为 220 个情景。
- 运营商 - 分布式站点间 VPN 所需。此许可证按设备进行授权，每台设备从服务器请求其自己的许可证。

- 强加密 (3DES) - 对于 2.3.0 前 Cisco Software Manager 本地部署；或如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。此许可证按设备进行授权，每台设备从服务器请求其自己的许可证。

如果选择了新的控制设备，新的控制设备继续使用聚合的许可证。它还会使用缓存的许可证配置再次请求控制设备许可证。当旧的控制设备作为数据设备重新加入集群后，它会释放控制设备许可证授权。在数据设备释放该许可证之前，如果帐户中没有可用的许可证，则控制设备的许可证可能处于一个非合规状态。保留的许可证的有效期为30天，但如果它在此宽限期过后仍处于非合规状态，您将无法对需要特殊许可证的功能进行配置更改；否则操作将不受影响。新的主用设备每12小时发送一次权利授权续约请求，直到许可证合规为止。在对许可证请求进行完整的处理之前，应避免进行配置更改。如果某台设备退出集群，缓存的控制配置将被删除，而按设备进行的授权将会保留。尤其是，您需要在非集群设备上重新请求情景许可证。

永久许可证预留

对于永久许可证预留，必须在配置集群之前为每个机箱单独购买许可证并启用。

智能软件许可的前提条件

智能软件管理器常规版和本地版前提条件

Firepower 4100/9300

在配置 ASA 许可授权之前，请在 Firepower 4100/9300 机箱上配置智能软件许可基础设施。

所有其他型号

- 确保来自设备的互联网访问、HTTP 代理访问或本地服务器访问上的智能软件管理器 。
- 配置 DNS 服务器，以使设备能够解析智能软件管理器的名称。
- 设置设备的时钟。
- 在思科智能软件管理器上创建账户：

  https://software.cisco.com/#module/SmartLicensing

  如果您还没有账户，请点击此链接以设置新账户。通过思科智能软件管理器，您可以为组织创建一个账户。

永久许可证预留前提条件

- 在思科智能软件管理器上创建主账户：

  https://software.cisco.com/#module/SmartLicensing

如果您还没有账户，请点击此链接以设置新账户。通过智能软件管理器，您可以为组织创建一个主帐户。即使ASA确实需要互联网连接到智能许可服务器以进行永久许可证预留，但智能软件管理器仍用于管理您的永久许可证。

- 获得许可团队的永久许可证预留支持。您必须提供使用永久许可证预留的正当理由。如果您的帐户未获得批准，则无法购买和应用永久许可证。
- 购买特殊的永久许可证（请参阅 每个型号的许可证 PID，第 152 页）。如果您的帐户中没有正确的许可证，则当您尝试在ASA上保留许可证时，将会看到类似于以下内容的错误消息：“许可证无法保留，因为虚拟帐户没有足够的剩余以下永久许可证：1-Firepower 4100 ASA PERM UNIV（永久）。“
- 永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅 Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 86 页）。
- ASA Virtual： Azure 虚拟机监控程序不支持永久许可证预留。

智能软件许可准则

- 仅支持智能软件许可。对于 ASA virtual上的较早软件，如果升级现有 PAK 许可的 ASA virtual，则以前安装的激活密钥将被忽略，但会保留在设备上。如果将 ASA virtual 降级，则将恢复激活密钥。
- 对于永久许可证预留，您必须在停用设备之前退回该许可证。如果不正式退回该许可证，该许可证会保持已使用状态，且无法退回用于新设备。
- 由于思科传输网关使用具有不合规国家/地区代码的证书，因此在将 ASA 与该产品一起使用时，无法使用 HTTPS。您必须对思科传输网关使用 HTTP。

智能软件许可的默认设置

Smart Transport

默认情况下，所有设备型号都使用 Smart Transport 进行智能软件许可证通信，并使用以下 URL：

```
https://smartreceiver.cisco.com/licservice/license
```

对于 Firepower 4100/9300，必须在机箱级别启用智能软件许可证通信。

ASA Virtual

- 在部署 ASA virtual时，您可设置功能层和吞吐量级别。此时仅 基础 级别可用。对于永久许可证预留，您不需要设置这些参数。当您启用永久许可证预留时，这些命令将从配置中删除。

注释 Essentials 许可证过去称为标准许可证，CLI 仍使用“标准”术语。

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G | unlimited}
```

注释 如果您在 VMware 或 KVM 上使用的是 32 或 64 核心部署，则在 **throughput level** 命令中只能使用 **unlimited** 选项。

ASA Virtual: 配置智能软件许可

本节介绍如何为 ASA Virtual 配置智能软件许可。

ASA Virtual：配置常规智能软件许可

在部署 ASA virtual 时，您可以预配置设备并包含一个注册令牌，以便其向智能软件管理器注册并启用智能软件许可。如果您需要更改 HTTP 代理服务器、许可证授权，或注册 ASA virtual（例如，如果您未在 Day0 配置中包含 ID 令牌），请执行此任务。

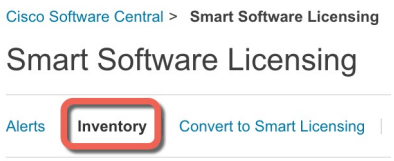
注释 您可能已经在部署您的 ASA virtual时预配置了 HTTP 代理服务器和许可证授权。您还可能在部署 ASA virtual时在 Day0 配置中包含了注册令牌；如果是这样，您就不需要使用此程序重新注册。

过程

步骤 1 （思科智能软件管理器）中，为要将此设备添加到其中的虚拟帐户请求一个注册令牌并复制该令牌。

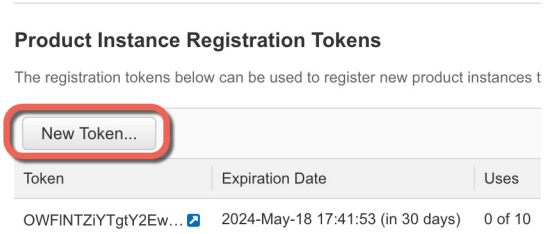
a) 点击**清单 (Inventory)**。

图 *8:* 清单



b) 在**常规 (General)** 选项卡上，点击**新建令牌 (New Token)**。

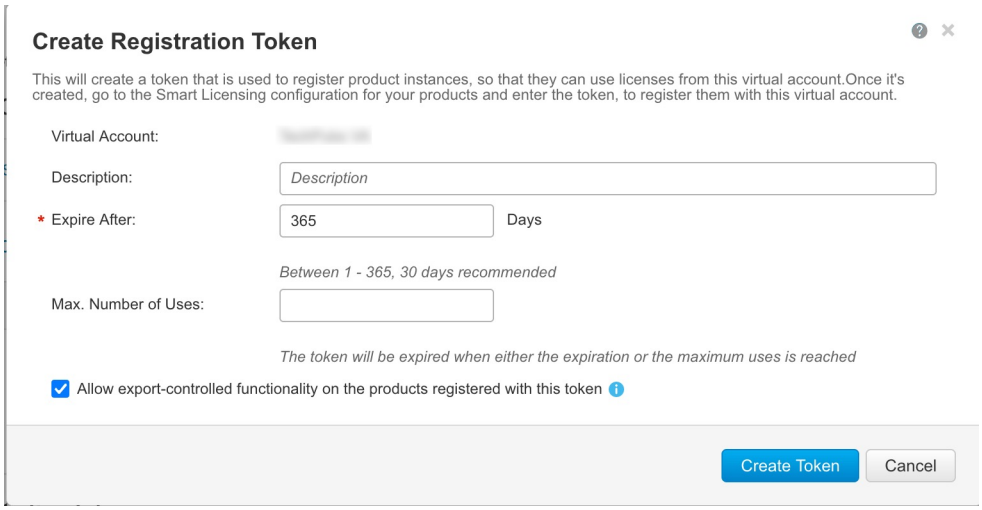
图 *9:* 新建令牌



c) 在 **Create Registration Token** 对话框中，输入以下设置，然后点击 **Create Token**：

- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- 最大使用次数
- **Allow export-controlled functionaility on the products registered with this token** - 启用导出合规性标志。

图 *10:* 创建注册令牌



系统将令牌添加到您的清单中。

d) 点击令牌右侧的箭头图标可以打开 **Token** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册 ASA 时，请准备好此令牌，以在该程序后面的部分使用。

图 *11:* 查看令牌

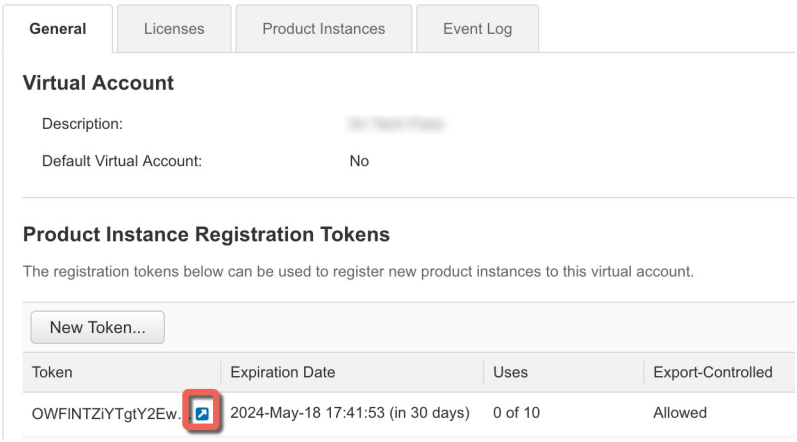
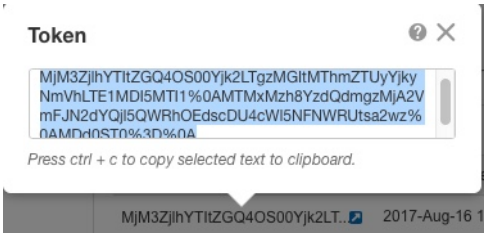


图 *12:* 复制令牌



步骤 2 （可选） 在 ASA virtual 上，指定 Smart Transport 的 HTTP 代理 URL。

license smart

transport proxy *proxy_server_ip* **port** *port*

要使用 Smart Call Home 而不使用 Smart Transport，请参阅步骤 4，第 106 页。

注释

- 不支持认证的HTTP代理。
- 配置代理服务器 URL 时，请勿指定协议。

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy proxy.esl.cisco.com port 80
```

步骤 3 配置许可证授权：

a) 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用。基础版许可证以前称为标准版许可证，在 CLI 中仍称为“标准版”。

c) 设置吞吐量级别，以便确定从智能软件管理器请求的许可证：

吞吐量级别 {**100M** | **1G** | **2G** | **10G** | **20G** | **无限制**}

注释
如果您使用的是 32 核或 64 核部署，则只有**无限制**选项可用。

请参阅以下吞吐量/许可证关系：

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100
- 无限制 - ASAvU

示例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

d) （可选） 启用强加密。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

a) 退出许可证智能模式以应用更改：

exit

在通过以下方式退出许可证智能配置模式之前，更改将不会生效：明确退出该模式（**exit** 或 **end**），或输入使您进入其他模式的任何命令。

示例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

步骤 4 （可选） 使用 Smart Call Home 而不是默认 Smart Transport 来与智能许可服务器进行通信。

如果您确定要使用 Smart Call Home 而不是 Smart Transport，请完成以下步骤。否则，应使用默认的 Smart Transport 。

a) 将传输类型设置为 Smart Call Home。

license smart

transport type callhome

配置包括一个名为 **License** 的 Smart Call Home 配置文件，其中指定了智能软件管理器的 URL。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

b) （可选） 指定 HTTP 代理 URL。

call-home

http-proxy *ip_address* **port** *port*

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

步骤 5 将 ASA virtual 注册到智能软件管理器。

license smart register idtoken *id_token* [**force**]

ASA virtual 尝试向智能软件管理器注册并请求对已配置的许可证授权进行授权。

注册 ASA virtual时，智能软件管理器会为 ASA virtual 和智能软件管理器之间的通信颁发 ID 证书。它还会将 ASA virtual 分配到相应的虚拟账户。通常情况下，此程序是一次性实例。但是，如果 ID 证书由于诸如通信问题等原因而到期，则稍后可能需要重新注册 ASA virtual。

勾选 **强制** 关键词以注册已注册但可能与智能软件管理器不同步的 ASA virtual 。例如，如果从智能软件管理器中意外删除了 ASA virtual，请使用 **force**。

示例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

步骤 6 检查许可证状态。

show license status或**show running-config license**

如果与智能软件管理器的通信失败，请检查您是否配置了 DNS 服务器以及可访问服务器的正确路由。

示例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Supported
  VRF:
    Not Supported

Registration:
  Status: UNREGISTERED - REGISTRATION FAILED
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Feb 27 2024 06:34:02 UTC
    Failure reason: {"token":["The token 'sgdgdsdg' is not valid."]}

License Authorization:
  Status: No Licenses in Use

Export Authorization Key:
  Features Authorized:
    <none>

Miscellaneous:
  Custom Id: <empty>

Device Telemetry Report Summary:
================================
Data Channel: NOT AVAILABLE
Reports on disk: 0
```

示例：

```
ciscoasa(config)# show running-config license
license smart
feature tier standard
throughput level 1G
transport proxy proxy.esl.cisco.com port 80
```

ASA Virtual：为许可配置本地智能软件管理器

此程序适用于使用本地智能软件管理器的 ASA virtual 。

开始之前

- 从 Cisco.com 下载智能软件管理器本地 OVA 文件，并在 VMwareESXi 服务器上安装和配置此文件。有关更多信息，请参阅思科智能软件管理器本地部署产品手册。
- 在 7.0 版中，本地智能软件管理器中添加了 Smart Transport 。如果您使用的是旧版本，请按照此程序在 ASA virtual 上启用 Smart Call Home。
- 在将设备置于气隙网络中之前，请下载加密 CA 信任池。该信任池通常会自动下载，但在气隙网络中可能会过期：

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

过程

步骤 1 在智能软件管理器本地上请求注册令牌。

步骤 2 （可选） 在 ASA virtual 上，为 Smart Transport 指定 HTTP 代理 URL。

license smart

transport proxy *proxy_server_ip* **port** *port*

要使用 Smart Call Home 而不使用 Smart Transport，请参阅步骤 5 ，第 110 页。

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

步骤 3 更改许可证服务器 URL 以转到智能软件管理器本地。

license smart

transport url https://*on-Prem_ip_address***/SmartTransport**

要使用 Smart Call Home 而不使用 Smart Transport，请参阅步骤 5 ，第 110 页。

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport url https://10.1.5.5/SmartTransport
```

步骤 4 配置许可证授权。

a) 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用。基础版许可证以前称为标准版许可证，在 CLI 中仍称为“**标准版**”。

c) 设置吞吐量级别，以便确定从智能软件管理器请求的许可证：

吞吐量级别 {**100M** | **1G** | **2G** | **10G** | **20G** | **无限制**}

注释
如果您使用的是 32 核或 64 核部署，则只有**无限制**选项可用。

请参阅以下吞吐量/许可证关系：

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100
- 无限制 - ASAvU

示例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

d) （可选） 启用强加密。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

a) 退出许可证智能模式以应用更改：

exit

在通过以下方式退出许可证智能配置模式之前，更改将不会生效：明确退出该模式（**exit** 或 **end**），或输入使您进入其他模式的任何命令。

示例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

步骤 5 （可选） 使用 Smart Call Home 而不是默认 Smart Transport 来与智能许可服务器进行通信。

如果您确定要使用 Smart Call Home 而不是 Smart Transport，请完成以下步骤。否则，应使用默认的 Smart Transport。

a) 将传输类型设置为 Smart Call Home。

license smart

transport type callhome

配置包括一个名为 **License** 的 Smart Call Home 配置文件，其中指定了智能软件管理器的 URL。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

b) （可选） 指定 HTTP 代理 URL。

call-home

http-proxy *ip_address* **port** *port*

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

c) 更改许可证服务器 URL 以转到智能软件管理器本地：

call-home

profile License

destination address http
https://*on-Prem_ip_address***/Transportgateway/services/DeviceRequestHandler**

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile)#destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

步骤 6 使用您在第 1 步中请求的令牌注册 ASA：

license smart register idtoken *id_token*

ASA 向本地智能软件管理器注册，并申请配置的许可证授权。如果您的帐户允许，则智能软件管理器本地还会应用强加密 (3DES/AES) 许可证。

注册 ASA virtual时，智能软件管理器会为 ASA virtual 和智能软件管理器本地部署之间的通信颁发 ID 证书。它还会将 ASA virtual 分配到相应的虚拟账户。通常情况下，此程序是一次性实例。但是，如果 ID 证书由于诸如通信问题等原因而到期，则稍后可能需要重新注册 ASA virtual。

示例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

步骤 7 检查许可证状态。

show license status

如果与智能软件管理器的通信失败，请检查您是否配置了 DNS 服务器以及可访问服务器的正确路由。

示例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://10.1.5.5/SmartTransport
  Proxy:
    Not Supported
```

```
  VRF:
    Not Supported

Registration:
  Status: UNREGISTERED - REGISTRATION FAILED
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Feb 27 2024 06:34:02 UTC
    Failure reason: {"token":["The token 'sgdgdsdg' is not valid."]}

License Authorization:
  Status: No Licenses in Use

Export Authorization Key:
  Features Authorized:
    <none>

Miscellaneous:
  Custom Id: <empty>

Device Telemetry Report Summary:
================================
Data Channel: NOT AVAILABLE
Reports on disk: 0
```

ASA Virtual：配置实用程序 (MSLA) 智能软件许可

通过托管服务许可协议 (MSLA) 的实用程序许可，您可以按许可证的使用时间来付费，而不是为许可证订用或永久许可证支付一次性费用。在实用程序许可模式下，ASA virtual 会以时间为单位（15 分钟间隔）来跟踪许可证使用情况。ASA virtual 智能代理每四个小时向智能软件管理器发送许可证使用情况报告（被称为 RUM 报告）。然后，使用情况报告将被转发到计费服务器。使用实用程序许可时，Smart Call Home 不会被用作许可消息的传输。消息将改为使用智能传输通过 HTTP/HTTPS 直接发送。

开始之前

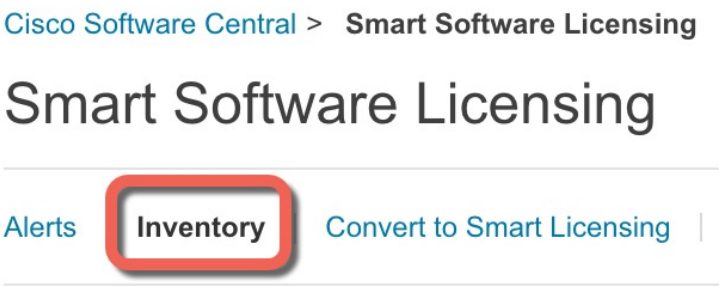
您可以使用本地智能软件管理器从 Cisco.com 下载智能软件管理器本地 OVA 文件，并在 VMware ESXi 服务器上安装和配置此文件。有关更多信息，请参阅思科智能软件管理器本地部署产品手册。

过程

步骤 1 在智能软件管理器（思科智能软件管理器）中，为要将此设备添加到其中的虚拟帐户请求一个注册令牌并复制该令牌。

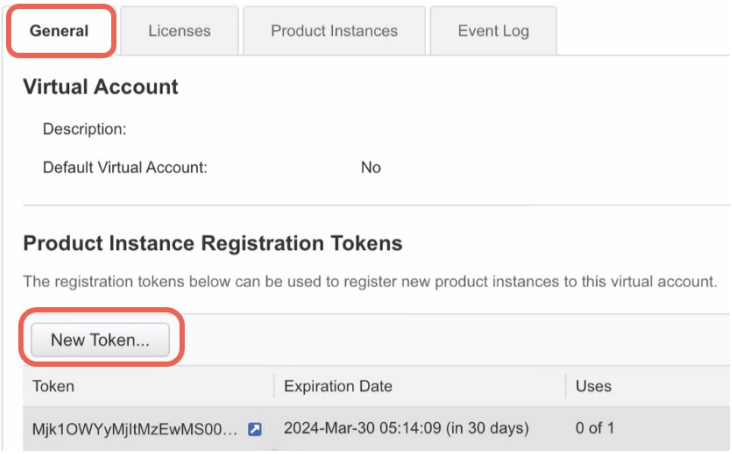
a) 点击**清单 (Inventory)**。

图 *13:* 清单



b) 在常规 **(General)** 选项卡上，点击新建令牌 **(New Token)**。

图 *14:* 新建令牌

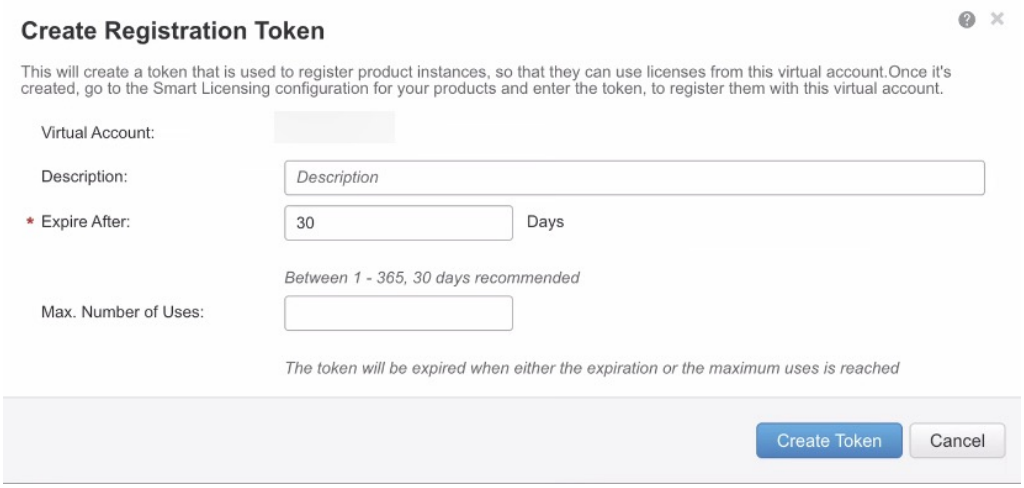


c) 在 **Create Registration Token** 对话框中，输入以下设置，然后点击 **Create Token**：

- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- 最大值使用次数 - 令牌的最大使用次数。

  令牌在到期日期或最大使用次数后到期。

图 *15:* 创建注册令牌



系统将令牌添加到您的清单中。

d) 点击令牌右侧的箭头图标可以打开 **Token** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册 ASA 时，请准备好此令牌，以在该程序后面的部分使用。

图 *16:* 查看令牌

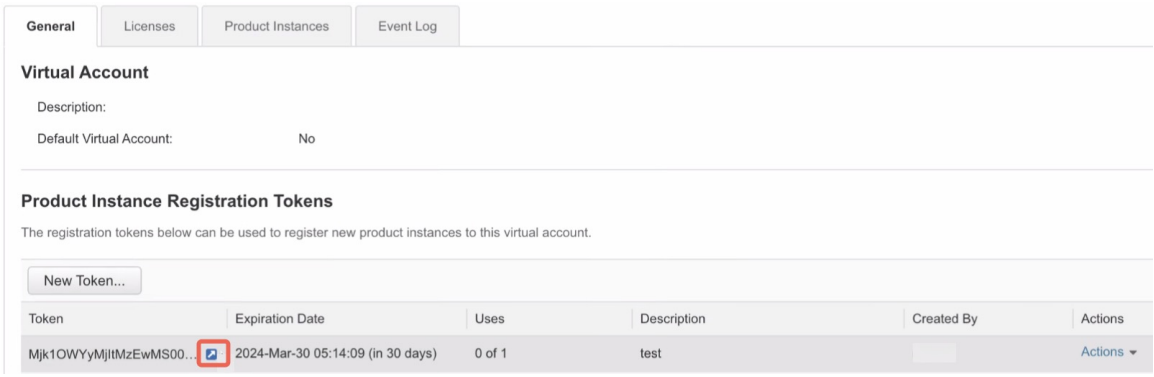
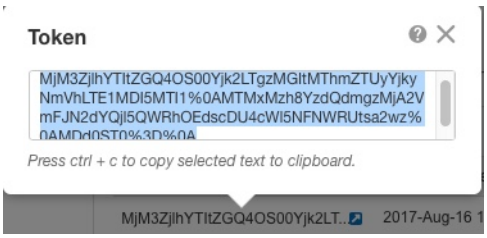


图 *17:* 复制令牌



步骤 2 在 ASA virtual 上，配置智能许可参数。

a) 进入许可证智能配置模式。

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 启用智能传输。

transport type smart

实用程序许可需要使用 Smart Transport 而不是 Smart Call Home。

示例：

```
ciscoasa(config-smart-lic)# transport type smart
```

c) （可选） 指定智能软件管理器常规或本地部署的 URL。或者，您可以为许可证使用情况报告指定一个备选目标。

transport url {*transport_url* | **utility** *utility_url* | **default** }

如果未设置 URL，它将同时对智能传输和许可证使用情况报告使用 **default**，即 **https://smartreceiver.cisco.com/licservice/license**。

示例：

```
ciscoasa(config-smart-lic)# transport url http://server99.cisco.com/SmartTransport
ciscoasa(config-smart-lic)# transport url utility
http://server-utility.cisco.com/SmartTransport
```

d) （可选） 如果您的网络使用 HTTP 代理进行互联网访问，请配置代理地址。

transport proxy *proxy-url* **port** *proxy-port-number*

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 443
```

e) 在许可消息中隐藏许可设备的主机名或智能代理版本号。

privacy {**all** | **hostname** | **version**}

示例：

```
ciscoasa(config-smart-lic)# privacy all
```

f) 设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用。基础版许可证以前称为标准版许可证，在 CLI 中仍称为“标准版”。

g) 设置吞吐量级别，以便确定从智能软件管理器请求的许可证：

吞吐量级别 {**100M** | **1G** | **2G** | **10G** | **20G** | **无限制**}

注释
如果您使用的是 32 核或 64 核部署，则只有**无限制**选项可用。

请参阅以下吞吐量/许可证关系：

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100
- 无限制 - ASAvU

示例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

h) （可选） 启用强加密。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

i) 退出许可证智能模式以应用更改：

exit

在通过以下方式退出许可证智能配置模式之前，更改将不会生效：明确退出该模式（**exit** 或 **end**），或输入使您进入其他模式的任何命令。

示例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

步骤 3 配置实用程序许可。

a) 进入实用程序配置模式。

utility

示例：

```
ciscoasa(config-smart-lic)# utility
ciscoasa(config-smart-lic-util)#
```

b) 创建唯一的客户标识符。此标识符包含在实用程序许可使用情况报告消息中。

custom-id *custom-identifier*

示例：

```
ciscoasa(config-smart-lic-util)# custom-id MyCustomID
```

c) 创建唯一的客户配置文件。此信息包含在实用程序许可使用情况报告中。

customer-info {**city** | **country** | **id** | **name** | **postalcode** | **state** |**street**} *value*

示例：

```
ciscoasa(config-smart-lic-util)# customer-info city MyCity
ciscoasa(config-smart-lic-util)# customer-info country MyCountry
ciscoasa(config-smart-lic-util)# customer-info id MyID
ciscoasa(config-smart-lic-util)# customer-info name MyName
ciscoasa(config-smart-lic-util)# customer-info postalcode MyPostalCode
ciscoasa(config-smart-lic-util)# customer-info state MyState
ciscoasa(config-smart-lic-util)# customer-info street MyStreet
```

d) 启用实用程序许可。

mode standard

示例：

```
ciscoasa(config-smart-lic-util)# mode standard
```

步骤 4 使用您在第 1 步中请求的令牌注册 ASA：

license smart register idtoken *id_token*

示例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

步骤 5 检查许可证状态。

show license status

如果与智能软件管理器的通信失败，请检查您是否配置了 DNS 服务器以及可访问服务器的正确路由。

示例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: ENABLED
  Utility report:
    Last success: May 14 2018 21:37:25 UTC
    Last attempt: SUCCEEDED on May 14 2018 21:37:24 UTC
    Next attempt: May 15 2018 01:37:24 UTC

  Customer Information:
    Id: MyID
    Name: MyName
    Street: MyStreet
    City: MyCity
    State: MyState
    Country: MyCountry
    Postal Code: MyPostalCode

Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Smart
  Registration URL: http://server99.cisco.com/SmartTransport
  Utility URL: http://server-utility.cisco.com/SmartTransport

Registration:
  Status: REGISTERED
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on May 14 2018 21:37:20 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Sep 13 2018 13:34:40 UTC
  Registration Expires: May 14 2019 21:29:20 UTC

License Authorization:
  Status: AUTHORIZED on May 14 2018 21:37:22 UTC
  Last Communication Attempt: NOT STARTED
    Failure reason: Device in Thirdparty Utility Mode
  Next Communication Attempt: None
  Communication Deadline: Aug 12 2018 21:37:24 UTC
```

ASA Virtual：配置永久许可证预留

您可以为 ASA virtual分配一个永久许可证。本部分介绍在您停用 ASA virtual 时，或在更改模型层并且需要新的许可证时，如何退回许可证。

过程

步骤 1 安装 ASA Virtual 永久许可证，第 119 页

步骤 2 （可选）返还 ASA Virtual 永久许可证，第 121 页

安装 ASA Virtual 永久许可证

对于无法访问互联网的 ASA virtual，您可以向智能软件管理器请求永久许可证。有关 ASA virtual 永久许可证预留的详细信息，请参阅ASA Virtual 永久许可证预留，第 81 页。

注释 对于永久许可证预留，您必须在停用 ASA virtual之前退回该许可证。如果不正式退回该许可证，该许可证会保持已使用状态，且无法退回用于新的 ASA virtual。请参阅（可选）返还 ASA Virtual 永久许可证，第 121 页。

注释 如果在安装永久许可证后清除配置（例如使用 **write erase**），则只需使用不带任何参数的 **license smart reservation** 命令重新启用永久许可证预留（如步骤 1 所示）；您不需要完成此程序的其余部分。

开始之前

- 购买永久许可证，以便其在智能软件管理器中可用。并非所有账户都被批准使用永久许可证预留。在您尝试配置此功能之前，请确保已获得思科批准。
- 在 ASA virtual 启动之后，您必须请求永久许可证；您不能在 Day 0 配置期间安装永久许可证。

过程

步骤 1 （仅限 ASAv5）当 DRAM 为 2GB（9.13 及更高版本中的最低要求）时，允许使用 ASAv5 永久许可证。

license smart set_plr5

步骤 2 在 ASA virtual CLI 中，启用永久许可证预留：

license smart reservation

示例：

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

要使用常规智能许可，请使用此命令的 **no** 形式。

删除了以下命令：

```
license smart
  feature tier standard
```

```
throughput level {100M | 1G | 2G | 10G | 20G| unlimited}
```

步骤 3 请求要在智能软件管理器中输入的许可证代码：

license smart reservation request universal

示例：

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

如果更改内存或vCPU，则必须退回当前许可证，并申请新型号级别的新许可证。请求的许可证必须与安装的内存和 vCPU 相匹配。有关 ASA virtual 永久许可证预留的 vCPU 和内存到许可证矩阵的详细信息，请参阅ASA Virtual 永久许可证预留 ，第 81 页。

要更改已部署的 ASA virtual的型号，在虚拟机监控程序中，可以更改 vCPU 和 DRAM 设置以匹配新的型号要求；有关这些值，参阅 ASA virtual 快速入门指南。要查看您当前的型号，请使用 **show vm** 命令。

如果重新输入此命令，则会显示同一代码，即使在重新加载后也是如此。如果您尚未将此代码输入智能软件管理器，并且希望取消该请求，请输入：

license smart reservation cancel

如果禁用永久许可证预留，则所有待处理请求也会被取消。如果您已将该代码输入智能软件管理器，则必须完成此程序才能将该许可证应用于ASA virtual，然后可以根据需要退回该许可证。请参阅（可选）返还 ASA Virtual 永久许可证 ，第 121 页。

步骤 4 访问“智能软件管理器清单”(Smart Software Manager Inventory) 屏幕，点击**许可证 (Licenses)** 选项卡：

https://software.cisco.com/#SmartLicensing-Inventory

Licenses 选项卡显示与您的帐户相关的所有现有许可证（普通和永久）。

步骤 5 点击**许可证预留 (License Reservation)**，然后在**预留请求代码 (Reservation Request Code)** 字段中键入 ASA virtual 代码。

步骤 6 点击**预留许可证 (Reserve License)**。

智能软件管理器将生成授权码。您可以下载该授权码或将其复制到剪贴板。根据智能软件管理器，许可证现已处于使用状态。

如果您没有看到 **License Reservation** 按钮，则您的帐户未被授权执行永久许可证预留。在这种情况下，您应禁用永久许可证预留并重新输入普通的智能许可证命令。

步骤 7 在 ASA virtual中输入授权码：

license smart reservation install *code*

示例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

```
ciscoasa#
```

ASA virtual 现在完全获得许可。

（可选）返还 ASA Virtual 永久许可证

如果您不再需要永久许可证（例如，您要停用ASA virtual或更改其型号级别使得它需要新许可证），必须使用此程序将该许可证正式返还给智能软件管理器。如果您不按照所有步骤操作，则该许可证仍将保持使用状态，并且无法轻松释放用于其他地方。

过程

步骤 1 在 ASA virtual上生成返还代码：

license smart reservation return

示例：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ASA virtual会立即变成未获许可并转变为“评估”状态。如果您需要再次查看此代码，请重新输入此命令。请注意，如果您请求新的永久许可证 (**license smart reservation request universal**)，或更改 ASA virtual 型号级别（通过断开电源并更换 vCPU/RAM），则将无法重新显示此代码。确保捕获该代码以完成返还。

步骤 2 查看 ASA virtual 通用设备标识符 (UDI)，以便在智能软件管理器中找到此 ASA virtual 实例：

show license udi

示例：

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

步骤 3 访问智能软件管理器的“清单”(Inventory) 屏幕，然后点击**产品实例 (Product Instances)** 选项卡：

https://software.cisco.com/#SmartLicensing-Inventory

Product Instances 选项卡通过 UDI 显示所有获得许可的产品。

步骤 4 找到您想要取消许可的 ASA virtual，依次选择**操作 (Actions)** > **删除 (Remove)**，然后在**预留退回码 (Reservation Return Code)** 字段中键入 ASA virtual。点击**删除产品实例 (Remove Product Instance)**。

永久许可证被返还到可用池。

步骤 5 要禁用永久许可证预留，请执行以下操作：

a) 禁用永久许可证预留。

no license smart reservation

b) 使用以下命令确认许可证已取消注册：

show license features

（可选）取消注册 ASA Virtual（常规和本地）

对 ASA virtual 取消注册会从帐户中删除 ASA virtual。系统会删除 ASA virtual 中的所有许可证授权和证书。您可能希望取消注册来为新的 ASA virtual 释放许可证。或者，也可以从智能软件管理器删除 ASA virtual。

注释 如果取消注册 ASA virtual，则在重新加载 ASA virtual后，它将恢复到严格的速率限制状态。

过程

取消注册 ASA virtual：

license smart deregister

然后 ASA virtual 会重新加载。

（可选）续约 ASA Virtual ID 证书或许可证授权 （常规和本地）

默认情况下，ID证书每6个月自动更新，许可证授权每30天更新。如果您访问互联网的时间有限，或者在智能软件管理器中进行了任何许可更改等操作，则可能要为这些项目手动续订注册。

过程

步骤 1 更新 ID 证书：

license smart renew id

步骤 2 更新许可证授权：

license smart renew auth

1000/1200/3100/4200：配置智能软件许可

本节介绍如何为 1000/1200/3100/4200 配置智能软件许可。选择以下方法之一：

- 1000/1200/3100/4200：配置常规智能软件许可，第 123 页

  您也可以（可选）取消注册 1000/1200/3100/4200（常规和本地），第 136 页或（可选）续约 1000/1200/3100/4200 ID 证书或许可证授权（常规和本地），第 137 页。

- 1000/1200/3100/4200：配置智能软件本地许可，第 128 页

  您也可以（可选）取消注册 1000/1200/3100/4200（常规和本地），第 136 页或（可选）续约 1000/1200/3100/4200 ID 证书或许可证授权（常规和本地），第 137 页。

- 1000/1200/3100/4200：配置永久许可证预留，第 132 页

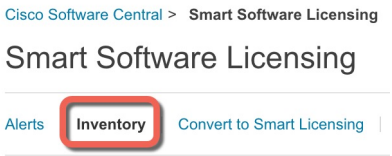
1000/1200/3100/4200：配置常规智能软件许可

此程序适用于使用智能软件管理器的 ASA。

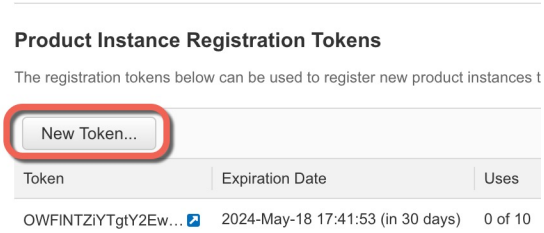
过程

步骤 1 在 Cisco Smart Software Manager 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

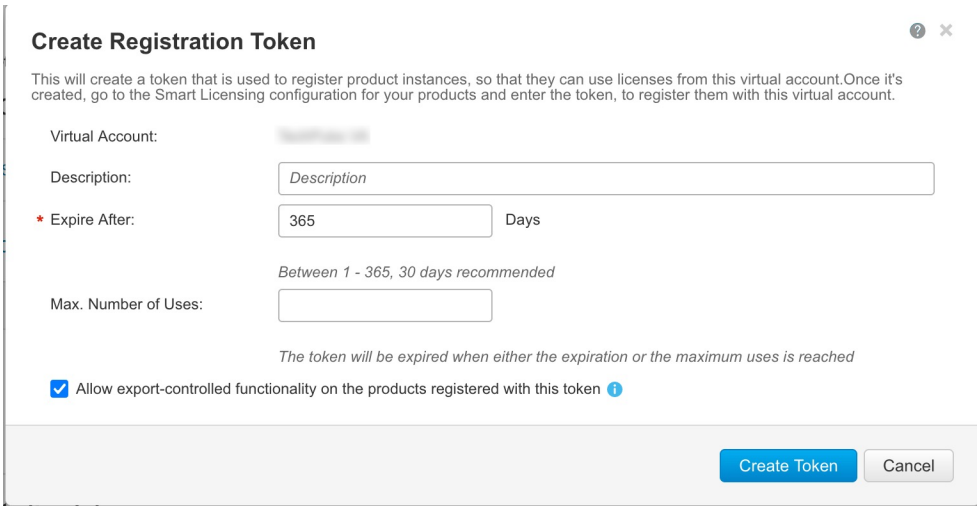
a) 点击**清单 (Inventory)**。



b) 在 **General** 选项卡上，点击 **New Token**。



c) 在 **Create Registration Token** 对话框中，输入以下设置，然后点击 **Create Token**：



- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- 最大使用次数
- **Allow export-controlled functionaility on the products registered with this token** - 启用导出合规性标志。

系统将令牌添加到您的清单中。

d) 点击令牌右侧的箭头图标可以打开 **Token** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册ASA时，请准备好此令牌，以在该程序后面的部分使用。

图 *18:* 查看令牌

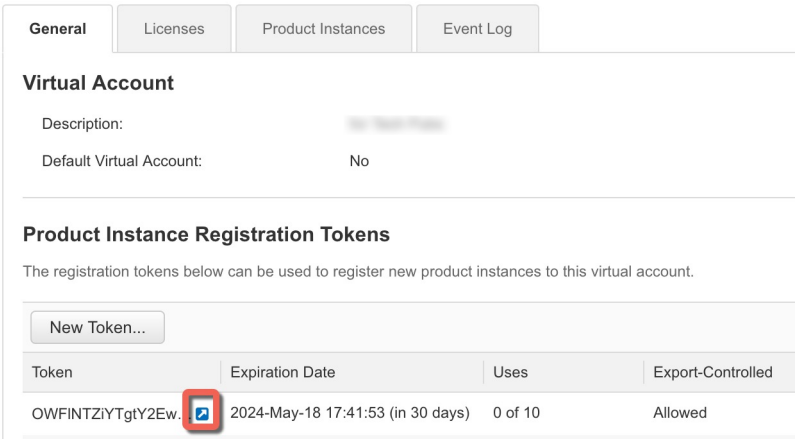
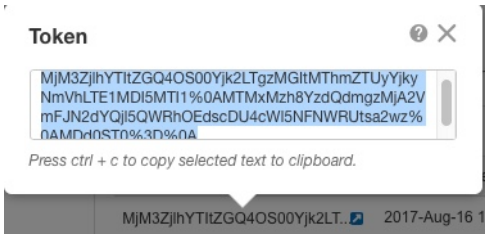


图 *19:* 复制令牌



步骤 2 （可选） 在 ASA 上，为 Smart Transport 指定 HTTP 代理 URL。

license smart

transport proxy *proxy_server_ip* **port** *port*

要使用 Smart Call Home 而不是 Smart Transport，请参阅步骤步骤 4 ，第 127 页。

注释

- 不支持认证的HTTP代理。
- 配置代理服务器 URL 时，请勿指定协议。

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy proxy.esl.cisco.com port 80
```

步骤 3 在 ASA 上请求许可证授权。

a) 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) （Firepower 1000）设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用；层许可证是添加其他功能许可证的前提条件。基础版许可证以前称为标准版许可证，在 CLI 中仍称为“标准版”。Cisco Secure Firewall 模型的 基础 许可证始终处于启用状态，无法禁用。

c) 请求安全情景许可证。

feature context 编号

注释
Firepower 1010 和 Cisco Secure Firewall 1210/1220 不支持此许可证。

默认情况下，ASA 支持 2 个情景，因此您应该请求的情景数量为需要的数量减去 2 个默认情景。情景的最大数量取决于您使用的型号：

- Firepower 1120 - 5 种情景
- Firepower 1140 - 10 种情景
- Firepower 1150 - 25 种情景
- Cisco Secure Firewall 3100 — 100 个情景
- Cisco Secure Firewall 4200 - 100 个情景

例如，对于 Firepower 1150 而言，要使用最大值 - 25 种情景，请为情景数输入 23；此值将与默认值 2 相加。

示例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （可选） (Firepower 1010) 请求增强型安全许可证以启用故障转移。

feature security-plus

示例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （可选） (Cisco Secure Firewall 3100/4200) 请求 Diameter、GTP/GPRS、SCTP 检测的运营商许可证。

feature carrier

示例：

```
ciscoasa(config-smart-lic)# feature carrier
```

f) （可选） 启用强加密。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

步骤 4 （可选） 使用 Smart Call Home 而不是默认 Smart Transport 来与智能许可服务器进行通信。

如果您确定要使用 Smart Call Home 而不是 Smart Transport，请完成以下步骤。否则，应使用默认的 Smart Transport。

a) 将传输类型设置为 Smart Call Home。

license smart

transport type callhome

配置包括一个名为 **License** 的 Smart Call Home 配置文件，其中指定了智能软件管理器的 URL。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

b) （可选） 指定 HTTP 代理 URL。

call-home

http-proxy *ip_address* **port** *port*

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

步骤 5 使用您在第 1 步中复制的令牌注册 ASA：

license smart register idtoken *id_token*

示例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA 向智能软件管理器注册，并申请配置的许可证授权。如果您的帐户允许，则智能软件管理器还会应用强加密 (3DES/AES) 许可证。使用 **show license summary** 或 **show running-config license** 命令检查许可证状态和使用情况。

示例：

```
ciscoasa# show license summary
```

```
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP1010-ASA-Std)                     1 AUTHORIZED
```

示例：

```
ciscoasa(config)# show running-config license
license smart
feature tier standard
throughput level 1G
transport proxy proxy.esl.cisco.com port 80
```

1000/1200/3100/4200：配置智能软件本地许可

此程序适用于使用本地智能软件管理器的 ASA。

开始之前

- 从 Cisco.com 下载智能软件管理器本地 OVA 文件，并在 VMwareESXi 服务器上安装和配置此文件。有关更多信息，请参阅思科智能软件管理器本地部署产品手册。
- 在 7.0 版中，本地智能软件管理器中添加了 Smart Transport 。如果您使用的是旧版本，请按照此程序在 ASA 上启用 Smart Call Home。
- 在将设备置于气隙网络中之前，请下载加密 CA 信任池。该信任池通常会自动下载，但在气隙网络中可能会过期：

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

过程

步骤 1 在智能软件管理器本地服务器上请求注册令牌。

步骤 2 （可选） 在 ASA 上，为 Smart Transport 指定 HTTP 代理 URL。

license smart

transport proxy *proxy_server_ip* **port** *port*

要使用 Smart Call Home 而不是 Smart Transport，请参阅步骤步骤 5，第 130 页。

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

步骤 3 更改许可证服务器 URL 以转到智能软件管理器本地。

license smart

transport url https://*on-Prem_ip_address***/SmartTransport**

要使用 Smart Call Home 而不是 Smart Transport，请参阅步骤步骤 5，第 130 页。

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport url https://10.1.5.5/SmartTransport
```

步骤 4 在 ASA 上请求许可证授权。

a) 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) （Firepower 1000）设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用；层许可证是添加其他功能许可证的前提条件。基础版许可证以前称为标准版许可证，在 CLI 中仍称为“标准版”。Cisco Secure Firewall 模型的 基础 许可证始终处于启用状态，无法禁用。

c) （可选） 请求安全情景许可证。

feature context 编号

注释
Firepower 1010 和 Cisco Secure Firewall 1210/1220 不支持此许可证。

默认情况下，ASA 支持 2 个情景，因此您应该请求的情景数量为需要的数量减去 2 个默认情景。情景的最大数量取决于您使用的型号：

- Firepower 1120 - 5 种情景
- Firepower 1140 - 10 种情景
- Firepower 1150 - 25 种情景
- Cisco Secure Firewall 3100 — 100 个情景
- Cisco Secure Firewall 4200 - 100 个情景

例如，对于 Firepower 1150 而言，要使用最大值 - 25 种情景，请为情景数输入 23；此值将与默认值 2 相加。

示例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （可选） (Firepower 1010) 请求增强型安全许可证以启用故障转移。

feature security-plus

示例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （可选） (Cisco Secure Firewall 3100/4200) 请求 Diameter、GTP/GPRS、SCTP 检测的运营商许可证。

feature carrier

示例：

```
ciscoasa(config-smart-lic)# feature carrier
```

f) （可选） 启用强加密。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

步骤 5 （可选） 使用 Smart Call Home 而不是默认 Smart Transport 来与智能许可服务器进行通信。

如果您确定要使用 Smart Call Home 而不是 Smart Transport，请完成以下步骤。否则，应使用默认的 Smart Transport。

a) 将传输类型设置为 Smart Call Home。

license smart

transport type callhome

配置包括一个名为 **License** 的 Smart Call Home 配置文件，其中指定了智能软件管理器的 URL。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

b) （可选）指定 HTTP 代理 URL。

call-home

http-proxy *ip_address* **port** *port*

注释
不支持认证的HTTP代理。

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

c) 更改许可证服务器 URL 以转到智能软件管理器本地：

call-home

profile License

destination address http
https://*on-Prem_ip_address***/Transportgateway/services/DeviceRequestHandler**

示例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile)#destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

步骤 6 使用您在第 1 步中请求的令牌注册 ASA：

license smart register idtoken *id_token*

示例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA 向本地智能软件管理器服务器注册，并申请配置的许可证授权。如果您的帐户允许，则智能软件管理器还会应用强加密 (3DES/AES) 许可证。使用 **show license summary** 命令检查许可证状态和使用情况。

示例：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP1010-ASA-Std)                    1 AUTHORIZED
```

1000/1200/3100/4200：配置永久许可证预留

您可以为 Firepower 1000, Cisco Secure Firewall 1200/3100/4200分配一个永久许可证。本节还介绍在停用 ASA 时如何退回许可证。

过程

步骤 1 安装 1000/1200/3100/4200 永久许可证，第 132 页。

步骤 2 （可选）返还 1000/1200/3100/4200 永久许可证，第 135 页。

安装 1000/1200/3100/4200 永久许可证

对于无法访问互联网 ASA，您可以向智能软件管理器请求永久许可证。永久许可证启用所有功能：具有最多安全情景的 基础 许可证。

注释 对于永久许可证预留，您必须在停用ASA之前退回该许可证。如果不正式退回该许可证，该许可证会保持已使用状态，且无法退回用于新的ASA。请参阅（可选）返还 1000/1200/3100/4200 永久许可证，第 135 页。

开始之前

购买永久许可证，以便其在智能软件管理器中可用。并非所有账户都被批准使用永久许可证预留。在您尝试配置此功能之前，请确保已获得思科批准。

过程

步骤 1 在 ASA CLI 中，启用永久许可证预留：

license smart reservation

示例：

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

步骤 2 请求要在智能软件管理器中输入的许可证代码：

license smart reservation request universal

示例：

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
BB-ZFPR-2140:JAD200802RR-AzKmHcc71-2A
ciscoasa#
```

如果重新输入此命令，则会显示同一代码，即使在重新加载后也是如此。如果您尚未将此代码输入智能软件管理器，并且希望取消该请求，请输入：

license smart reservation cancel

如果禁用永久许可证预留，则所有待处理请求也会被取消。如果您已将该代码输入智能软件管理器，则必须完成此程序才能将该许可证应用于 ASA，然后可以根据需要退回该许可证。请参阅（可选）返还 1000/1200/3100/4200 永久许可证，第 135 页。

步骤 3 访问“智能软件管理器清单”(Smart Software Manager Inventory) 屏幕，点击**许可证 (Licenses)** 选项卡：

https://software.cisco.com/#SmartLicensing-Inventory

Licenses 选项卡显示与您的帐户相关的所有现有许可证（普通和永久）。

步骤 4 点击**许可证预留**，并在框中键入 ASA 代码。点击 **Reserve License**。

智能软件管理器将生成授权码。您可以下载该授权码或将其复制到剪贴板。根据智能软件管理器，许可证现已处于使用状态。

如果您没有看到 **License Reservation** 按钮，则您的帐户未被授权执行永久许可证预留。在这种情况下，您应禁用永久许可证预留并重新输入普通的智能许可证命令。

步骤 5 在 ASA 中输入授权码：

license smart reservation install *code*

示例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

步骤 6 在 ASA 上请求许可证授权。

注释
虽然永久许可证允许完全使用所有的许可证，但您仍需要打开 ASA 配置中的授权，以便 ASA 知道它可以使用它们。

a) 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) （Firepower 1000）设置功能层：

feature tier standard

只有标准（基本）层可用，但您需要在配置中将其启用；层许可证是添加其他功能许可证的前提条件。基础版许可证以前称为标准版许可证，在 CLI 中仍称为“标准版”。Cisco Secure Firewall 模型的 基础 许可证始终处于启用状态，无法禁用。

c) （可选） 启用安全情景许可证。

feature context 编号

注释
Firepower 1010 和 Cisco Secure Firewall 1210/1220 不支持此许可证。

默认情况下，ASA 支持 2 个情景，因此您应该启用的情景数量为需要的数量减去 2 个默认情景。由于永久许可证允许最大数量，因此您可以为自己的型号启用最大数量。情景的最大数量取决于您使用的型号：

- Firepower 1120 - 5 种情景
- Firepower 1140 - 10 种情景
- Firepower 1150 - 25 种情景

- Cisco Secure Firewall 3100 — 100 个情景
- Cisco Secure Firewall 4200 - 100 个情景

例如，对于 Firepower 1150 而言，要使用最大值 - 25 种情景，请为情景数输入 23；此值将与默认值 2 相加。

示例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （可选） (Firepower 1010) 启用增强型安全许可证以启用故障转移。

feature security-plus

示例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （可选） (Cisco Secure Firewall 3100/4200) 启用 Diameter、GTP/GPRS、SCTP 检测的运营商许可证。

feature carrier

示例：

```
ciscoasa(config-smart-lic)# feature carrier
```

f) （可选） 启用强加密。

feature strong-encryption

如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

示例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

（可选）返还 1000/1200/3100/4200 永久许可证

如果不再需要永久许可证（例如，您正在停用 ASA），您必须使用以下程序将该许可证正式返还给智能软件管理器。如果您不按照所有步骤操作，则该许可证仍将保持使用状态，并且无法轻松释放用于其他地方。

过程

步骤 1 在 ASA 上生成返还代码：

license smart reservation return

示例：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ASA 将立即变为未许可并进入“评估”状态。如果您需要再次查看此代码，请重新输入此命令。请注意，如果您请求新的永久许可证 (**license smart reservation request universal**)，则您无法重新显示此代码。确保捕获该代码以完成返还。如果评估期已过期，则ASA会进入过期状态。有关不合规状态的详细信息，请参阅 不合规状态，第 161 页。

步骤 2 查看 ASA 通用设备标识符 (UDI)，以便在智能软件管理器中找到此 ASA 实例：

show license udi

示例：

```
ciscoasa# show license udi
UDI: PID:FPR-2140,SN:JAD200802RR
ciscoasa#
```

步骤 3 访问智能软件管理器的“清单”(Inventory) 屏幕，然后点击**产品实例 (Product Instances)** 选项卡：

https://software.cisco.com/#SmartLicensing-Inventory

Product Instances 选项卡通过 UDI 显示所有获得许可的产品。

步骤 4 找到您想要取消许可的ASA，依次选择**操作**>**删除**，然后在方框中键入ASA返还代码。点击**Remove Product Instance**。

永久许可证被返还到可用池。

（可选）取消注册 1000/1200/3100/4200（常规和本地）

取消注册 ASA 将从您的帐户删除 ASA。系统会删除 ASA 上的所有许可证授权和证书。您可能需要取消注册才能释放许可证以用于新的 ASA。或者，可以将 ASA 从智能软件管理器中删除。

过程

取消注册 ASA：

license smart deregister

（可选）续约 1000/1200/3100/4200 ID 证书或许可证授权（常规和本地）

默认情况下，ID证书每6个月自动更新，许可证授权每30天更新。如果您访问互联网的时间有限，或者例如在智能软件管理器中进行了任何许可更改，则可能需要为其中任一项手动续约注册。

过程

步骤 1 更新 ID 证书：

license smart renew id

步骤 2 更新许可证授权：

license smart renew auth

Firepower 4100/9300: 配置智能软件许可

此程序适用于使用智能软件管理器、本地智能软件管理器的机箱，或永久许可证预留；请参阅《FXOS 配置指南》，以将你的方法配置为前提条件。

对于永久许可证预留，许可证可启用所有功能：具有最多安全情景和运营商许可证的标准层。但是，要让 ASA“知道”可以使用这些功能，您需要在 ASA 上启用它们。

开始之前

对于 ASA 集群，您需要访问控制单元进行配置。查看 机箱管理器 ，确定哪一台设备为控制单元。如该程序所示，您也可以从 ASA CLI 执行检查。

过程

步骤 1 连接到 Firepower 4100/9300 机箱 CLI（控制台或 SSH），然后将会话连接到 ASA：

connect module 插槽 **console connect asa**

示例：

```
Firepower> connect module 1 console
Firepower-module1> connect asa

asa>
```

下次连接到 ASA 控制台时，您会直接进入 ASA，不需要再次输入 **connect asa**。

对于 ASA 集群，您仅需要访问控制单元以进行许可证配置和其他配置。通常，控制单元位于插槽 1，因此，您首先应连接到该模块。

步骤 2 在 ASA CLI 中，进入全局配置模式。默认情况下，除非在部署逻辑设备时设置了启用密码，否则启用密码为空，但系统会在首次输入命令**enable**时提示您更改密码。

enable configure terminal

示例：

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa# configure terminal
asa(config)#
```

步骤 3 对于 ASA 集群，如果需要，请确认此设备是控制单元：

show cluster info

示例：

```
asa(config)# show cluster info
Cluster stbu: On
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
Other members in the cluster:
  Unit "unit-1-2" in state SLAVE
    ID : 1
    Version : 9.5(2)
    Serial No.: P3000000001
    CCL IP : 127.2.1.2
    CCL MAC : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2015
    Last leave: N/A
  Unit "unit-1-3" in state MASTER
    ID : 2
    Version : 9.5(2)
    Serial No.: JAB0815R0JY
    CCL IP : 127.2.1.3
    CCL MAC : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2015
    Last leave: N/A
```

如果其他设备才是控制设备，请退出当前连接，并连接到正确的设备。有关如何退出连接，请参阅下文。

步骤 4 进入许可证智能配置模式：

license smart

示例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

步骤 5 设置功能层：

feature tier standard

仅标准层可用。层许可证是添加其他功能许可证的前提条件。您的帐户中必须有足够的级别许可证。否则，无法配置任何其他功能许可证或需要许可证的任何功能。

步骤 6 请求以下功能中的一种或多种：

- 运营商 (GTP/GPRS、Diameter 和 SCTP 检测)

  feature carrier

- 安全情景

  feature context *<1-248>*

  对于永久许可证预留，您可以指定最大情景数 (248)。

- 强加密 (3DES/AES)

  feature strong-encryption

  如果您从智能软件管理器收到强加密令牌，则不需要此许可证。然而，如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有主用设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

示例：

```
ciscoasa(config-smart-lic)# feature carrier
ciscoasa(config-smart-lic)# feature context 50
```

步骤 7 要退出 ASA 控制台，在提示符中输入输入 **~** 即可退出 Telnet 应用。输入 **quit** 以退回管理引擎 CLI。

每个型号的许可证

本部分列出可用于 ASAv 和 Firepower 4100/9300 机箱 ASA 安全模块的许可证授权。

ASA Virtual

使用 **throughput level** 命令在 ASA 配置中设置吞吐量水平，它将确定从智能软件管理器申请的许可证。请参阅以下吞吐量级别/许可证关系：

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100
- 无限制 — ASAvU

吞吐量级别还决定了最大 Secure Client 和 TLS 代理会话数。但是，较低的 ASA virtual 内存配置文件将限制您的实际会话数，因此要确定您的会话，需要检查吞吐量级别和安装的内存。

ASA virtual 的内存决定了最大并发防火墙连接数和 VLAN，而不是由吞吐量级别决定。

下表显示 ASA virtual 系列已获许可的功能。

许可证	说明
许可证授权	
吞吐量级别	可以使用 **throughput level** 命令在 ASA 配置中设置吞吐量水平。该级别会确定您需要的许可证。 100M: ASAv5 1G: ASAv10 2G: ASAv30 10G: ASAv50 20G: ASAv100 无限制：ASAvU
防火墙许可证	
僵尸网络流量过滤器	启用
防火墙连接数，并发	防火墙连接由 ASA virtual 内存决定。 2 GB 至 7.9 GB：100,000 8 GB 至 15.9 GB：500,000 16 GB 至 31.9 GB：2,000,000 32 GB 至 64 GB：4,000,000 ASAvU：如果使用最小内存为 64 GB 的 ASAvU，则防火墙连接的最大数量为 8,000,000。
运营商	启用

许可证	说明
Total TLS Proxy Sessions	TLS 代理会话由吞吐量级别和 ASA virtual 内存决定。 100M 吞吐量 + 任何内存：500 1G 吞吐量 + 任意内存：500 2G 吞吐量 • 2 GB 至 7.9 GB 内存：500 • 8 GB+ 内存：1000 10G 吞吐量 • 2 GB 至 7.9 GB 内存：500 • 8 GB 至 15.9 GB 内存：1000 • 16 GB 以上内存：10,000 20G 吞吐量 • 2 GB 至 7.9 GB 内存：500 • 8 GB 至 15.9 GB 内存：1000 • 16 GB 至 31.9 GB 内存：10,000 • 32 GB+ 内存：20,000 无限制吞吐量：如果您使用的是 ASAvU（最小内存为 64 GB），则 TLS 代理会话的最大数量为 40,000 个。
VPN 许可证	

许可证	说明	
Secure Client 对等体	未获得许可	Secure Client 对等体由吞吐量级别和 ASA virtual 内存决定。 可选 *Secure Client Advantage* 或 *Secure Client Premier* 许可证，最多： *100M* 吞吐量 + 任何内存：*50* *1G* 吞吐量 + 任意内存：*250* *2G* 吞吐量 • *2 GB* 至 *7.9 GB* 内存：*250* • *8 GB*+ 内存：*750* *10G* 吞吐量 • *2 GB* 至 *7.9 GB* 内存：*250* • *8 GB* 至 *15.9 GB* 内存：*750* • *16 GB* 以上内存：*10,000* *20G* 吞吐量： • *2 GB* 至 *7.9 GB* 内存：*250* • *8 GB* 至 *15.9 GB* 内存：*750* • *16 GB* 至 *31.9 GB*：*10,000* • *32 GB*+ 内存：*20,000* 无限制吞吐量：如果您使用的是 ASAvU（其最小内存为 64 GB），则 Secure Client 对等体的最大数量为 40,000。

许可证	说明
其他 VPN 对等体	注释 其他 VPN 对等体由吞吐量级别和 ASA virtual 内存决定。 100M 吞吐量 + 任何内存：50 1G 吞吐量 + 任意内存：250 2G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB+ 内存：750 10G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB 至 15.9 GB 内存：750 • 16 GB 以上内存：10,000 20G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB 至 15.9 GB 内存：750 • 16 GB 至 31.9 GB：10,000 • 32 GB+ 内存：20,000 无限制吞吐量：如果您使用的是ASAvU（其最小内存为64GB），则其他 VPN 对等体的最大数量为 40,000。

许可证	说明
VPN 对等体总数（包括所有类型）	注释 VPN 对等体总数由吞吐量级别和 ASA virtual 内存决定。 100M 吞吐量 + 任何内存：50 1G 吞吐量 + 任意内存：250 2G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB+ 内存：750 10G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB 至 15.9 GB 内存：750 • 16 GB 以上内存：10,000 20G 吞吐量 • 2 GB 至 7.9 GB 内存：250 • 8 GB 至 15.9 GB 内存：750 • 16 GB 至 31.9 GB：10,000 • 32 GB+ 内存：20,000 无限制吞吐量：如果使用的是 ASAvU（它使用的最小内存为 64 GB），则最大 VPN 对等体数为 40,000。
通用许可证	
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置
故障转移	主用/备用
安全情景	不支持
集群	已启用
最大 VLAN 数量	VLAN 由 ASA virtual 内存决定。 2 GB 至 7.9 GB - 50 8 GB 至 15.9 GB - 200 16 GB 至 31.9 GB - 1024 32 GB 至 64 GB - 1024

Firepower 1010

下表显示 Firepower 1010 已获许可的功能。

许可证	基础 许可证	
防火墙许可证		
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	100,000	
运营商	不支持。虽然不支持 SCTP 检测映射，但支持使用 ACL 的 SCTP 状态检测：	
TLS 代理会话总数	4,000	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证，最多：*75*
其他 VPN 对等体	75	
VPN 对等体总数（包括所有类型）	75	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
增强型安全（故障转移、VPN 负载均衡）	禁用	可选
安全情景	不支持。	
集群	不支持。	
最大 VLAN 数量	60	

Firepower 1100 系列

下表显示 Firepower 1100 系列已获许可的功能。

许可证	基础 许可证
防火墙许可证	

许可证	基础 许可证	
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	Firepower 1120：200,000 Firepower 1140：400,000 Firepower 1150：600,000	
运营商	不支持。虽然不支持 SCTP 检测映射，但支持使用 ACL 的 SCTP 状态检测：	
TLS 代理会话总数	Firepower 1120：4,000 Firepower 1140：8,000 Firepower 1150：8,000	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证，最多： *Firepower 1120：150* *Firepower 1140：400* *Firepower 1150：800*
其他 VPN 对等体	Firepower 1120：150 Firepower 1140：400 Firepower 1150：800	
VPN 对等体总数（包括所有类型）	Firepower 1120：150 Firepower 1140：400 Firepower 1150：800	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
安全情景	2	可选许可证，最多： *Firepower 1120：5* *Firepower 1140：10* *Firepower 1150：25*

许可证	基础 许可证
集群	不支持。
最大 VLAN 数量	1024

Cisco Secure Firewall 1210 和 1220

下表显示 Cisco Secure Firewall 1210 和 1220 系列已获许可的功能。

许可证	基础 许可证	
防火墙许可证		
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	Cisco Secure Firewall 1210：200,000 Cisco Secure Firewall 1220：300,000	
运营商	不支持。虽然不支持 SCTP 检测映射，但支持使用 ACL 的 SCTP 状态检测：	
TLS 代理会话总数	Cisco Secure Firewall 1210: 320 Cisco Secure Firewall 1220: 320	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证，最多： *Cisco Secure Firewall 1210*：*200* *Cisco Secure Firewall 1220*：*300*
其他 VPN 对等体数	Cisco Secure Firewall 1210：200 Cisco Secure Firewall 1220：300	
VPN 对等体总数（包括所有类型）	Cisco Secure Firewall 1210：200 Cisco Secure Firewall 1220：300	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
集群	不支持。	

许可证	基础 许可证
最大 VLAN 数量	1024

Cisco Secure Firewall 3100 系列

下表显示 Cisco Secure Firewall 3100 系列已获许可的功能。

许可证	基础 许可证	
防火墙许可证		
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	Cisco Secure Firewall 3105: 2,000,000 Cisco Secure Firewall 3110: 2,000,000 Cisco Secure Firewall 3120: 4,000,000 Cisco Secure Firewall 3130: 6,000,000 Cisco Secure Firewall 3140: 10,000,000	
运营商	禁用	可选许可证：运营商
TLS代理会话总数	Cisco Secure Firewall 3105: 10,000 Cisco Secure Firewall 3110: 10,000 Cisco Secure Firewall 3120: 15,000 Cisco Secure Firewall 3130: 15,000 Cisco Secure Firewall 3140: 15,000	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证，最多： *Cisco Secure Firewall 3105: 3000* *Cisco Secure Firewall 3110: 3000* *Cisco Secure Firewall 3120: 7000* *Cisco Secure Firewall 3130: 15,000* *Cisco Secure Firewall 3140: 20,000*

许可证	基础 许可证	
其他 VPN 对等体数	Cisco Secure Firewall 3105: 3000 Cisco Secure Firewall 3110: 3000 Cisco Secure Firewall 3120: 7000 Cisco Secure Firewall 3130: 15,000 Cisco Secure Firewall 3140: 20,000	
VPN 对等体总数（包括所有类型）	Cisco Secure Firewall 3105: 3000 Cisco Secure Firewall 3110: 3000 Cisco Secure Firewall 3120: 7000 Cisco Secure Firewall 3130: 15,000 Cisco Secure Firewall 3140: 20,000	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
安全情景	2	可选许可证，最多：*100*
集群	启用	
最大 VLAN 数量	1024	

Firepower 4100

下表显示 Firepower 4100 已获许可的功能。

许可证	基础 许可证	
防火墙许可证		
僵尸网络流量过滤器	不支持。	
并发防火墙连接数	Firepower 4112：10,000,000 Firepower 4115：15,000,000 Firepower 4125：25,000,000 Firepower 4145：40,000,000	
运营商	禁用	可选许可证：运营商
TLS代理会话总数	15,000	
VPN 许可证		

许可证	基础 许可证	
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*或 仅限 *Secure Client VPN* 许可证： *Firepower 4112: 10,000* *Firepower 4115: 15,000* *Firepower 4125: 20,000* *Firepower 4145: 20,000*
其他 VPN 对等体	Firepower 4112: 10,000 Firepower 4115: 15,000 Firepower 4125: 20,000 Firepower 4145: 20,000	
VPN 对等体总数（包括所有类型）	Firepower 4112: 10,000 Firepower 4115: 15,000 Firepower 4125: 20,000 Firepower 4145: 20,000	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
安全情景	10	可选许可证：最多 *250*
集群	启用	
最大 VLAN 数量	1024	

Cisco Secure Firewall 4200 系列

下表显示 Cisco Secure Firewall 4200 系列已获许可的功能。

许可证	基础 许可证
防火墙许可证	
僵尸网络流量过滤器	不支持。
并发防火墙连接数	Cisco Secure Firewall 4215：40,000,000 Cisco Secure Firewall 4225：80,000,000 Cisco Secure Firewall 4245：80,000,000

许可证	基础 许可证	
运营商	禁用	可选许可证：运营商
TLS代理会话总数	15,000	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证，最多： *Cisco Secure Firewall 4215: 20,000* *Cisco Secure Firewall 4225: 25,000* *Cisco Secure Firewall 4245: 30,000*
其他 VPN 对等体数	Cisco Secure Firewall 4215: 20,000 Cisco Secure Firewall 4225: 25,000 Cisco Secure Firewall 4245: 30,000	
VPN 对等体总数（包括所有类型）	Cisco Secure Firewall 4215: 20,000 Cisco Secure Firewall 4225: 25,000 Cisco Secure Firewall 4245: 30,000	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
安全情景	10	可选许可证，最多：*250*
集群	启用	
最大 VLAN 数量	1024	

Firepower 9300

下表显示 Firepower 9300 已获许可的功能。

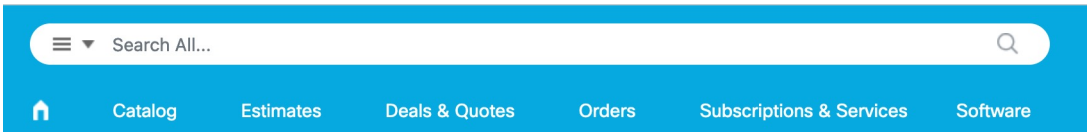
许可证	基础 许可证
防火墙许可证	
僵尸网络流量过滤器	不支持。

许可证	基础 许可证	
并发防火墙连接数	Firepower 9300 SM-56: 60,000,000 Firepower 9300 SM-48: 60,000,000 Firepower 9300 SM-40: 55,000,000	
Carrier	禁用	可选许可证：运营商
TLS 代理会话总数	15,000	
VPN 许可证		
Secure Client 对等体	未获得许可	可选 *Secure Client Advantage*、*Secure Client Premier*、或 仅限 *Secure Client VPN* 许可证：最多 *20,000* 个
其他 VPN 对等体数	20,000	
VPN 对等体总数（包括所有类型）	20,000	
通用许可证		
加密	基础 (DES) 或强 (3DES/AES)，取决于帐户的导出合规性设置	
安全情景	10	可选许可证：最多 *250*
集群	启用	
最大 VLAN 数量	1024	

每个型号的许可证 PID

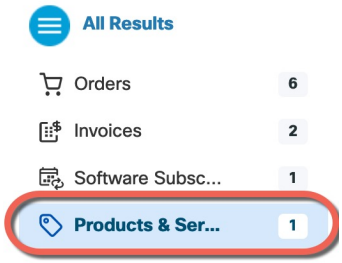
当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用思科商务工作空间上的**搜索全部 (Search All)** 字段。

图 *20*: 许可证搜索



从结果中选择**产品和服务 (Products & Services)**。

图 *21:* 结果



ASA Virtual PID

ASA Virtual 智能软件管理器常规版和本地版PID：

- ASAv5 许可证—L-ASAV5S-K9=
- ASAv10 许可证—L-ASAV10S-K9=
- ASAv30 许可证—L-ASAV30S-K9=
- ASAv50 许可证—L-ASAV50S-K9=
- ASAv100 许可证—L-ASAV100S-1Y=
- ASAv100 许可证—L-ASAV100S-3Y=
- ASAv100 许可证—L-ASAV100S-5Y=
- ASAvU 许可证—L-ASA-V-U-K9=

注释 ASAv 100 是基于预订的许可证，许可期限为 1 年、3 年或 5 年。

ASA Virtual 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 ， 第 86 页）。

- ASAv5 许可证—L-ASAV5SR-K9=
- ASAv10 许可证—L-ASAV10SR-K9=
- ASAv30 许可证—L-ASAV30SR-K9=
- ASAv50 许可证—L-ASAV50SR-K9=
- ASAv100 许可证—L-ASAV100SR-K9=
- ASAvU 许可证—ASA-V-U-ULR-K9=

Firepower 1010 PID

Firepower 1010 智能软件管理器常规版和本地版 PID：

- 基础版 — L-FPR1000-ASA=。Required.
- 增强型安全 — L-FPR1010-SEC-PL=。增强型安全许可证启用了故障转移。
- 强加密 (3DES/AES)—L-FPR1K-ENC-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 1010 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 ， 第 86 页）。

- L-FPR1K-ASA-BPU=

Firepower 1100 PID

Firepower 1100 智能软件管理器常规版和本地版 PID：

- 基础版 — L-FPR1000-ASA=。Required.
- 5 情景 — L-FPR1K-ASASC-5=。情景许可证是累加的，可购买多个许可证。
- 10 情景 —L-FPR1K-ASASC-10=。情景许可证是累加的，可购买多个许可证。
- 强加密 (3DES/AES)—L-FPR1K-ENC-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 1100 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 ， 第 86 页）。

- L-FPR1K-ASA-BPU=

Cisco Secure Firewall 1210/1220 PIDs

Secure Firepower 1210/1220 智能软件管理器常规版和本地版 PID：

- 基础—自动包含。
- 强加密 (3DES/AES)—L-CSF1200-ENCK9=。仅当帐户未获授权使用强加密时需要。

Cisco Secure Firewall 1210/1220 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 ， 第 86 页）。

- L-CSF1200-ASA-BPU=

Cisco Secure Firewall 3100 PID

Secure Firepower 3100 智能软件管理器常规版和本地版 PID：

- 基础—自动包含。
- 5 情景—L-FPR3K-ASASC-5=。情景许可证是累加的，可购买多个许可证。
- 10 情景—L-FPR3K-ASASC-10=。情景许可证是累加的，可购买多个许可证。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP) — L-FPR3K-ASA-CAR=
- 强加密 (3DES/AES)—L-FPR3K-ENC-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 3100 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 86 页）。

- L-FPR3K-ASA-BPU=

Firepower 4100 PID

Firepower 4100 智能软件管理器常规版和本地版 PID：

- 基础版 — L-FPR4100-ASA=。Required.
- 10 情景 — L-FPR4K-ASASC-10=。情景许可证是累加的，可购买多个许可证。
- 230 情景 — L-FPR4K-ASASC-230=。情景许可证是累加的，可购买多个许可证。
- 250 情景 — L-FPR4K-ASASC-250=。情景许可证是累加的，可购买多个许可证。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP) — L-FPR4K-ASA-CAR=
- 强加密 (3DES/AES)—L-FPR4K-ENC-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 4100 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证，第 86 页）。

- L-FPR4K-ASA-BPU =

Cisco Secure Firewall 4200 PID

Secure Firepower 4200 智能软件管理器常规版和本地版 PID：

- 基础—自动包含。
- 5 情景—L-FPR4200-ASASC-5=。情景许可证是累加的，可购买多个许可证。
- 10 情景—L-FPR4200-ASASC-10=。情景许可证是累加的，可购买多个许可证。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP)—L-FPR4200-ASA-CAR=
- 强加密 (3DES/AES)—L-FPR4200-ENC-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 4200 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 ， 第 86 页）。

- L-FPR4200-ASA-BPU=

Firepower 9300 PID

Firepower 9300 智能软件管理器常规版和本地版 PID：

- 基础 - L-F9K-ASA =。Required.
- 10 情景 — L-F9K-ASA-SC-10=。情景许可证是累加的，可购买多个许可证。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP) — L-F9K-ASA-CAR=
- 强加密 (3DES/AES)—L-F9K-ASA-ENCR-K9=。仅当帐户未获授权使用强加密时需要。

Firepower 9300 永久许可证预留 PID：

永久许可证包括所有可用功能，包括强加密 (3DES/AES) 许可证（如果您的帐户符合条件）。Secure Client 功能也会根据平台购买的最大数量启用，具体取决于您购买的 Secure Client 许可证是否具有权使用 Secure Client （请参阅Secure Client Advantage、 Secure Client Premier和 仅限 Secure Client VPN 许可证 ， 第 86 页）。

- L-FPR9K-ASA-BPU =

监控智能软件许可

您可以监控许可证功能、状态和证书，以及启用调试消息。

查看您当前的许可证

如需查看许可证，请参阅以下命令：

- **show license features**

  以下示例显示仅有 基础 许可证（无最新许可证授权）的 ASA virtual ：

```
Serial Number:  9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
```

查看智能许可证状态

请参阅以下命令来查看许可证状态：

- **show license all**

  显示智能软件许可的状态、智能代理版本、UDI 信息、智能代理状态、全局合规性状态、授权状态、许可证书信息和排定的智能代理任务。

  以下示例显示 ASA virtual 许可证：

```
ciscoasa# show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 21 21:17:35 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 21 21:17:35 2015 UTC
  Next Communication Attempt: Sep 24 00:44:10 2015 UTC
```

```
  Communication Deadline: Dec 20 21:14:33 2015 UTC

License Usage
==============

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
====================
UDI: PID:ASAv,SN:9AHV3KJBEKE

Agent Version
=============
Smart Agent for Licensing: 1.6_reservation/36
```

- **show license status**

  显示智能许可证状态。

  以下示例显示使用普通智能软件许可的 ASA virtual 的状态：

```
ciscoasa# show license status

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 23 01:41:26 2015 UTC
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC
  Communication Deadline: Dec 22 01:38:25 2015 UTC
```

  以下 示例显示使用永久许可证预订的 ASA virtual 的状态：

```
ciscoasa# show license status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jan 28 16:42:45 2016 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Jan 28 16:42:45 2016 UTC
```

```
Licensing HA configuration error:
    No Reservation Ha config error
```

- **show license summary**

  显示智能许可证状态和使用情况摘要。

  以下示例显示使用普通智能软件许可的 ASA virtual 的摘要：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2016 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (ASAv-STD-1G)                     1 AUTHORIZED
```

  以下示例显示使用永久许可证预订的 ASA virtual 的摘要：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed

License Authorization:
  Status: AUTHORIZED - RESERVED
```

- **show license usage**

  显示智能许可证使用情况。

  以下示例显示 ASA virtual的使用情况：

```
ciscoasa# show license usage

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
```

```
Version: 1.0
Status: AUTHORIZED
```

查看 UDI

如需查看通用产品标识符 (UDI)，请参阅以下命令：

show license udi

以下示例显示 ASAv 的 UDI：

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

调试智能软件许可

请参阅以下用于调试集群的命令：

- **debug license agent** {**error** | **trace** | **debug** | **all**}

  从智能代理打开调试。

- **debug license** *level*

  打开各种级别的智能软件许可管理器调试。

智能软件管理器通信

本部分介绍您的设备如何与智能软件管理器通信。

设备注册和令牌

对于每个虚拟账户，您可以创建注册令牌。默认情况下，此令牌有效期为30天。当部署每个设备或注册现有设备时，请输入此令牌 ID 以及授权级别。如果现有令牌已过期，则可以创建新的令牌。

注释 Firepower 4100/9300 机箱 - 设备注册是在机箱中而不是在 ASA 逻辑设备上进行配置。

在部署后或在现有设备上手动配置这些参数后启动时，设备会向智能软件管理器进行注册。使用令牌注册设备时，智能软件管理器会为设备和智能软件管理器之间的通信颁发ID证书。此证书有效期为 1 年，但需要每 6 个月续签一次。

与智能软件管理器的定期通信

设备每30天与智能软件管理器通信一次。如果您在智能软件管理器中进行更改，则可以刷新设备上的授权，以使更改立即生效。或者，也可以等待设备按计划通信。

您可以随意配置 HTTP 代理。

ASA Virtual

ASA virtual 必须可以直接访问互联网，或者至少可每 90 天通过 HTTP 代理访问互联网。常规许可证通信每30天进行一次，但如果设备具有宽限期，则最多保持合规状态90天，而不会进行自动通报。宽限期后，您应该联系智能软件管理器，否则您的 ASA virtual 将不合规；其他操作不受影响。

所有其他型号

ASA 必须可以直接访问互联网，或者至少每 90 天一次通过 HTTP 代理访问互联网。常规许可证通信每 30 天进行一次，但如果设备具有宽限期，则会最多运行 90 天，而不会进行自动通报。在宽限期后，您必须联系智能软件管理器，否则您将无法对需要特殊许可证的功能进行配置更改，但操作则不受影响。

不合规状态

设备在以下情况下可能会处于不合规状态：

- 过度使用 - 当设备使用不可用的许可证时。
- 许可证到期 - 当基于时间的许可证到期时。
- 通信不畅 - 当设备无法访问许可证颁发机构以重新获得授权时。

要验证您的帐户是否处于或接近不合规状态，必须将设备当前正在使用的授权与智能帐户中的授权进行比较。

根据具体型号，设备在不合规状态下可能受到限制：

- ASA Virtual- ASA virtual 不受影响。
- 所有其他模型-您将无法对需要特殊许可证的功能进行配置更改，但操作则不受影响。例如，基于 基础 许可证限制的现有环境可以继续运行，您可以修改它们的配置，但无法添加 新 环境。如果首次注册时没有足够的 基础 许可证，则无法配置任何许可功能，包括强加密功能。

Smart Call Home 基础设施

默认情况下，Smart Call Home 配置文件存在于用于指定智能软件管理器的 URL 的配置中。不能移除此配置文件。请注意，许可证配置文件的唯一可配置选项是智能软件管理器的目的地址 URL。除非获得 Cisco TAC 的指示，否则不应更改智能软件管理器 URL。

注释 对于 Firepower 4100/9300 机箱，用于许可的 Smart Call Home 在 Firepower 4100/9300 机箱管理引擎中，而不是 ASA 上进行配置。

不能为智能软件许可禁用 Smart Call Home。例如，即使使用 **no service call-home** 命令禁用 Smart Call Home，也不会禁用智能软件许可。

除非您专门配置其他 Smart Call Home 功能，否则不会开启这些功能。

智能许可证证书管理

ASA 会自动创建一个信任点，其中包含颁发 Smart Transport 或 Smart Call Home 服务器证书的 CA 的证书。为避免在服务器证书的颁发层次发生更改时出现服务中断，请配置 **auto-update** 命令以启用按照定期间隔自动更新信任池捆绑包。

从智能许可证服务器收到的服务器证书必须在 Extended Key Usage 字段中包括“ServAuth”。此检查仅在非自签名证书上完成；自签名证书在此字段中不提供任何值。

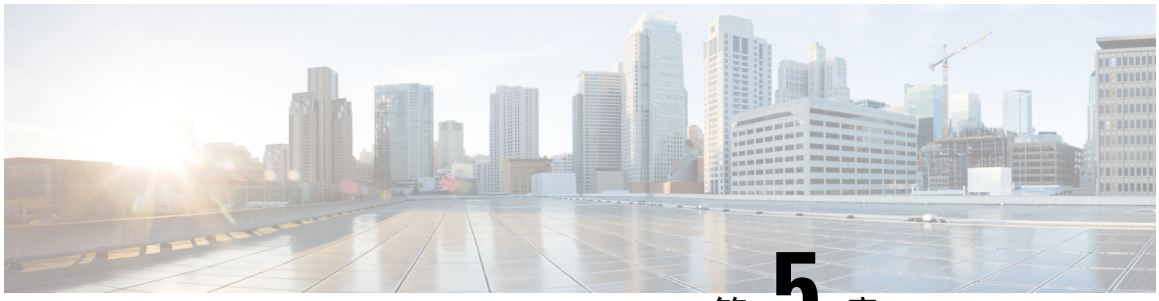
智能软件许可的历史记录

功能名称	平台版本	说明
Smart Transport 是与 CSSM 服务器通信的默认传输机制	9.22(1)	智能许可使用 Smart Transport 而不是 Smart Call Home 作为所有设备的默认传输。
ASAvU 许可证	9.22(1)	ASAvU 许可证在具有 32 核和 64 核的部署上实现最大吞吐量。此许可证仅在 VMware 和 KVM 上受支持。 新增/修改的命令：**throughput level unlimited**
增加了 Cisco Secure Firewall 4200 的连接限制	9.20(2)	已增加连接限制： • 4215: 15M → **40M** • 4225: 30M → **80M** • 4245: 60M → **80M**
Cisco Secure Firewall 3100 支持运营商许可证	9.18(1)	运营商许可证启用 Diameter、GTP/GPRS、SCTP 检测。 新增/修改的命令：**feature carrier**
ASAv100 永久许可证预留	9.14(1.30)	ASAv100现在支持使用产品ID L-ASAV100SR-K9=进行永久许可证预留。**请注意**：并非所有账户都被批准使用永久许可证预留。

功能名称	平台版本	说明
ASA Virtual MSLA 支持	9.13(1)	ASA virtual 支持思科托管服务许可协议（MSLA）程序，这是一种软件许可和消费体系，专为向第三方提供托管软件服务的思科客户和合作伙伴而设计。 MSLA 是一种新的智能许可形式，其中许可智能代理在时间单位内跟踪许可授权的使用情况。 新增/修改的命令：**license smart**、**mode**、**utility**、**custom-id**、**custom-info**、**privacy**、**transport type**、**transport url**、**transport proxy**
ASA Virtual 灵活许可	9.13(1)	灵活许可是智能许可的一种新形式，其中可以在受支持的 ASA virtual vCPU/内存配置中使用任何 ASA virtual 许可证。 Secure Client 和 TLS 代理的会话限制由安装的 ASA virtual 平台授权确定，而不是与型号相关的平台限制。 新增/修改的命令：**show version**、**show vm**、**show cpu**、**show license features**
更改了 Firepower 4100/9300 机箱 上故障转移对的许可	9.7(1)	只有主用单元能够请求许可权利。过去，两种设备都需请求许可证授权。支持 FXOS 2.1.1。
适用于 ASA virtual 短字符串增强的永久许可证预留	9.6(2)	由于智能代理的更新（更新至 1.6.4），请求和授权代码现在使用更短的字符串。 未修改任何命令。
卫星服务器对 ASA virtual的支持	9.6(2)	如果您的设备出于安全原因无法访问互联网，您可以选择以虚拟机 (VM) 形式安装本地智能软件管理器卫星服务器。 未修改任何命令。
适用于 Firepower 4100/9300 机箱 上 ASAv 的永久许可证预留	9.6(2)	在不允许与思科智能软件管理器之间进行通信的高安全性环境中，您可以为 Firepower 9300 和 Firepower 4100 上的 ASA 请求永久许可证。所有可用许可证授权均包括在永久许可证中，包括标准层、强加密（如果符合条件）、安全情景和运营商许可证。需要 FXOS 2.0.1。 所有配置均在 Firepower 4100/9300 机箱 上执行；无需对 ASA 进行配置。
ASA virtual 永久许可证预留	9.5(2.200) 9.6(2)	在不允许与思科智能软件管理器之间进行通信的高安全性环境中，您可以请求提供 ASA virtual永久许可证。 在 9.6(2) 中，我们还为 Amazon Web 服务上的 ASA virtual 添加了对此功能的支持。Microsoft Azure 不支持此功能。 引入了以下命令：**license smart reservation**、**license smart reservation cancel**、**license smart reservation install**、**license smart reservation request universal**、**license smart reservation return**

功能名称	平台版本	说明
智能代理升级至 v1.6	9.5(2.200) 9.6(2)	智能代理从1.1版本升级到1.6版本。此升级支持永久许可证预留，同时也支持依据许可证账号中的权限集设置强加密 (3DES/AES) 许可证授权。 **注释** 如果您从 9.5(2.200) 版本降级， ASA virtual 将不保留许可注册状态。您需要在中，使用 **license smart register idtoken** *id_token* **force** 命令重新注册，并从智能软件管理器获取 ID 令牌。 引入了以下命令：**show license status**、**show license summary**、**show license udi**、**show license usage** 修改了以下命令：**show license all**、**show tech-support license** 弃用了以下命令：**show license cert**、**show license entitlement**、**show license pool**、**show license registration**
强加密 (3DES) 许可证已自动应用于 Firepower 9300 上的 ASA	9.5(2.1)	对于一般的思科智能软件管理器用户，当他们在 Firepower 9300 上应用注册令牌时，只要符合相应条件，系统会自动启用强加密许可证。 **注释** 如果您通过智能软件管理器卫星部署使用 ASDM 和其他强加密功能，您必须在部署 ASA 之后使用 ASA CLI 启用强加密 (3DES) 许可证。 此功能要求具有 FXOS 1.1.3 版本。 删除了以下非卫星配置中的命令：**feature strong-encryption**
如果服务器证书的颁发层次结构出现更改，思科智能报障服务 (Smart Call Home)/智能许可 (Smart Licensing) 证书需进行验证	9.5(2)	智能许可使用 Smart Call Home 基础设施。当 ASA 首次在后台配置智能报障服务的匿名报告时，它会自动创建一个信任点，这个信任点包含颁发过智能报障服务证书的 CA 的证书。ASA 现在支持在服务器证书颁发层次结构出现变更时对证书进行验证；您可以按一定时间间隔定期启用 trustpool 捆绑的自动更新功能。 引入了以下命令：**auto-import**
新运营商许可证	9.5(2)	用于替换现有的 GTP/GPRS 许可证的新运营商许可证提供的支持包括 SCTP 和 Diameter 检测。对于 Firepower 9300 上的 ASA，**feature mobile-sp** 命令将自动迁移到 **feature carrier** 命令。 引入或修改了以下命令：**feature carrier**、**show activation-key**、**show license**、**show tech-support**、**show version**
Firepower 9300 ASA 的思科智能软件许可	9.4(1.150)	我们为 Firepower 9300 ASA 引入了智能软件许可。 引入了以下命令：**feature strong-encryption, feature mobile-sp, feature context**

功能名称	平台版本	说明
面向 ASA virtual 的思科智能软件许可	9.3(2)	通过智能软件许可，您可以购买和管理许可证池。与 PAK 许可证不同，智能许可证未绑定到特定序列号。您可以轻松部署或停用 ASA virtual，而不必管理每台设备的许可证密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。 引入了以下命令：**clear configure license**、**debug license agent**、**feature tier**、**http-proxy**、**license smart**、**license smart deregister**、**license smart register**、**license smart renew**、**show license**、**show running-config license**、**throughput level**



第 5 章

逻辑设备 Firepower 4100/9300

Firepower 4100/9300 是具有灵活性的安全平台，可在其中安装一个或多个逻辑设备。本章介绍基本的接口配置以及如何使用 机箱管理器添加独立或高可用性逻辑设备。要添加集群逻辑设备，请参阅 Firepower 4100/9300 的 ASA 集群，第 427 页。要使用 FXOS CLI，请参阅 FXOS CLI 配置指南。有关更多高级 FXOS 程序和故障排除，请参阅 FXOS 配置指南。

- 关于接口，第 167 页
- 关于逻辑设备，第 170 页
- 硬件和软件组合的要求与前提条件，第 170 页
- 逻辑设备的准则和限制，第 171 页
- 配置接口，第 172 页
- 配置逻辑设备，第 177 页
- 逻辑设备的历史记录，第 186 页

关于接口

Firepower 4100/9300 机箱支持物理接口和 EtherChannel（端口通道）接口。EtherChannel 接口最多可以包含同一类型的 16 个成员接口。

机箱管理接口

机箱管理接口用于通过 SSH 或 机箱管理器来管理 FXOS 机箱。此接口独立于分配给应用管理用逻辑设备的 MGMT 型接口。

要配置此接口参数，必须从 CLI 进行配置。要在 FXOS CLI 中查看此接口，请连接到本地管理并显示管理端口：

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

请注意，即使将物理电缆或小型封装热插拔模块拔下，或者执行了 **mgmt-port shut** 命令，机箱管理接口仍会保持正常运行状态。

注释 机箱管理接口不支持巨型帧。

接口类型

物理接口 和 EtherChannel（端口通道）接口可以是下列类型之一：

- 数据 - 用于常规数据。不能在逻辑设备之间共享数据接口，且逻辑设备无法通过背板与其他逻辑设备通信。对于数据接口上的流量，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。
- 数据共享 - 用于常规数据。仅容器实例支持这些数据接口，可由一个或多个逻辑设备/容器实例（仅限威胁防御-使用-管理中心 ）共享。
- 管理 - 用于管理应用程序实例。这些接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。只能为每个逻辑设备分配一个管理接口。根据您的应用和管理器，您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。有关独立机箱管理接口的信息，请参阅机箱管理接口，第 167 页。

注释 管理接口更改会导致逻辑设备重新启动，例如将管理接口从 e1/1 更改为 e1/2 会导致逻辑设备重新启动以应用新的管理接口。

- 事件 - 用作 威胁防御-using-管理中心 设备的辅助管理接口。

注释 安装每个应用实例时，会分配一个虚拟以太网接口。如果应用不使用事件接口，则虚拟接口将处于管理员关闭状态。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- 集群 - 用作集群逻辑设备的集群控制链路。默认情况下，系统会在端口通道 48 上自动创建集群控制链路。“集群”类型仅在 EtherChannel 接口上受支持。

有关独立部署和集群部署中威胁防御和 ASA 应用的接口类型支持，请参阅下表。

表 3: 接口类型支持

应用		数据	数据：子接口	数据共享	数据共享：子接口	管理	事件	集群（仅 EtherChannel）	集群：子接口
威胁防御	独立本地实例	是	-	—	—	是	是	-	—
	独立容器实例	是	是	是	是	是	是	-	—
	集群本地实例	是（EtherChannel 仅用于机箱间集群）	-	—	—	是	是	是	—
	集群容器实例	是（EtherChannel 仅用于机箱间集群）	-	—	—	是	是	是	是
ASA	独立本地实例	是	-	—	—	是	—	是	—
	集群本地实例	是（EtherChannel 仅用于机箱间集群）	-	—	—	是	—	是	—

FXOS 接口与应用接口

Firepower 4100/9300 管理物理接口和 EtherChannel（端口通道）接口的基本以太网设置。在应用中，您可以配置更高级别的设置。例如，您只能在 FXOS 中创建 EtherChannel；但是，您可以为应用中的 EtherChannel 分配 IP 地址。

下文将介绍 FXOS 接口与应用接口之间的交互。

VLAN 子接口

对于所有逻辑设备，您可以在应用内创建 VLAN 子接口。

机箱和应用中的独立接口状态

您可以从管理上启用和禁用机箱和应用中的接口。必须在两个操作系统中都启用能够正常运行的接口。由于接口状态可独立控制，因此机箱与应用之间可能出现不匹配的情况。

关于逻辑设备

逻辑设备允许您运行一个应用实例（ASA 或威胁防御）和一个可选修饰器应用 (Radware DefensePro) 以形成服务链。

当您添加逻辑设备时，还应定义应用实例类型和版本，分配接口，并配置推送至应用配置的引导程序设置。

注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 威胁防御）。还可以在独立模块上运行一种应用实例的不同版本。

独立和集群逻辑设备

您可以添加以下类型的逻辑设备：

- 独立 - 独立逻辑设备作为独立单元或高可用性对中的单元运行。
- 集群 - 集群逻辑设备允许您将多个单元集合在一起，具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。Firepower 9300 等多模块设备支持机箱内集群。对于 Firepower 9300，所有三个模块必须参与集群，同时适用于本地实例和容器实例。

硬件和软件组合的要求与前提条件

Firepower 4100/9300支持多种型号、安全模块、应用类型以及高可用性和可扩展性功能。请参阅以下要求，了解允许的组合。

Firepower 9300 的要求

Firepower 9300 包括 3 个安全模块插槽和多种类型的安全模块。请参阅以下要求：

- 安全模块类型 - 您可以在 Firepower 9300 中安装不同类型的模块。例如，您可以将 SM-48 作为模块 1、SM-40 作为模块 2、SM-56 作为模块 3 安装。
- 本地和容器实例 - 在安全模块上安装容器实例时，该模块只能支持其他容器实例。本地实例将使用模块的所有资源，因此只能在模块上安装一个本地实例。可以在某些模块上使用本地实例，在其他模块上使用容器实例。例如，您可以在模块 1 和模块 2 上安装本地实例，但在模块 3 上安装容器实例。

- 集群 - 集群中的所有安全模块（无论是机箱内还是机箱间）都必须为同一类型。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。例如，您可以在机箱 1 中安装 2 个 SM-40，在机箱 2 中安装 3 个 SM-40。 如果在同一机箱中安装了 1 个 SM-48 和 2 个 SM-40，则无法使用集群。
- 高可用性 - 仅在 Firepower 9300 上的同类模块间支持高可用性。 但是，这两个机箱可以包含混合模块。例如，每个机箱都设有 SM-40、SM-48 和 SM-56。可以在 SM-40 模块之间、SM-48 模块之间和 SM-56 模块之间创建高可用性对。
- ASA 和 威胁防御 应用类型-您可以在机箱中的独立模块上安装不同类型的应用。例如，您可以在模块 1 和模块 2 上安装 ASA，在模块 3 上安装 威胁防御 。
- ASA 或 威胁防御 版本 - 您可以在单独的模块上运行不同版本的应用实例类型，或在同一模块上运行单独的容器实例。例如，您可以在模块 1 上安装 威胁防御 6.3，在模块 2 上安装 威胁防御 6.4，在模块 3 上安装 威胁防御 6.5。

Firepower 4100 的要求

Firepower 4100 有多个型号。请参阅以下要求：

- 本地和容器实例 - 在 Firepower 4100 上安装容器实例时，该设备只能支持其他容器实例。本地实例将使用设备的所有资源，因此只能在设备上安装一个本地实例。
- 集群 - 集群内的所有机箱都必须为同一型号。
- 高可用性 - 仅在同类模块间支持高可用性。
- ASA 和 威胁防御 应用类型 - Firepower 4100 只能运行一种应用类型。

逻辑设备的准则和限制

有关准则和限制，请参阅以下章节。

接口的准则和限制

默认 MAC 地址

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。
- EtherChannel - 对于 EtherChannel，属于通道组的所有接口共用同一个 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。

一般准则和限制

防火墙模式

您可以在 威胁防御和 ASA 的引导程序配置中将防火墙模式设置为路由或透明模式。

高可用性

- 在应用配置中配置高可用性。
- 可以将任何数据接口用作故障转移和状态链路。 不支持数据共享接口。

情景模式

- 部署后，请在 ASA 中启用多情景模式。

高可用性的要求和前提条件

- 高可用性故障转移配置中的两个设备必须：
  - 位于单独的机箱上；不支持 Firepower 9300 的机箱内高可用性。
  - 型号相同。
  - 将同一接口分配至高可用性逻辑设备。
  - 拥有相同数量和类型的接口。启用高可用性之前，所有接口必须在 FXOS 中进行相同的预配置。
- 仅 Firepower 9300 上同种类型模块之间支持高可用性；但是两个机箱可以包含混合模块。例如，每个机箱都设有 SM-56、SM-48 和 SM-40。可以在 SM-56 模块之间、SM-48 模块之间和 SM-40 模块之间创建高可用性对。
- 有关其他高可用性系统要求，请参阅 故障转移系统要求，第 260 页一章。

配置接口

默认情况下，物理接口处于禁用状态。可以启用接口，添加 Etherchannel，编辑接口属性。

注释 如果在 FXOS 中删除一个接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中删除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

配置物理接口

您可以通过物理方式启用和禁用接口，并设置接口速度和双工。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在应用中以逻辑方式启用它。

注释 对于 QSFPH40G-CUxM，默认情况下自动协商会始终处于启用状态，并且您无法将其禁用。

开始之前

- 不能单独修改已经是 EtherChannel 成员的接口。务必在将接口添加到 EtherChannel 之前为其配置设置。

过程

步骤 1 进入接口模式。

scope eth-uplink

scope fabric a

步骤 2 启用接口。

enter interface *interface_id*

enable

示例：

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

注释
不能单独修改作为端口通道成员的接口。如果您在作为端口通道成员的接口上使用 **enter interface** 或 **scope interface** 命令，将会收到一条错误消息，说明对象不存在。应先使用 **enter interface** 命令编辑接口，然后在将接口添加到端口通道。

步骤 3 （可选）设置防反跳时间。

set debounce-time 5000 {Enter a value between 0-15000 milli-seconds}

示例：

```
Firepower /eth-uplink/fabric/interface # set debounce-time 5000
```

示例：

注释
不支持在 1G 接口上配置防反跳时间。

步骤 4 （可选）设置接口类型。

set port-type {**data** | **mgmt** | **cluster**}

示例：

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

data 关键字为默认类型。请勿选择 **cluster** 关键字；默认情况下，系统会自动在端口通道 48 上创建集群控制链路。

步骤 5 启用或禁用自动协商（如果您的接口支持）。

set auto-negotiation {**on** | **off**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

步骤 6 设置接口速度。

set admin-speed {**1gbps** | **10gbps** | **40gbps** | **100gbps**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

步骤 7 设置接口双工模式。

set admin-duplex {**fullduplex** |**halfduplex**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

步骤 8 如果您编辑了默认流量控制策略，则它已应用于接口。如果您创建了新策略，请将其应用于接口。

set flow-control-policy *name*

示例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

步骤 9 保存配置。

commit-buffer

示例：

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

添加 EtherChannel（端口通道）

EtherChannel（也称为端口通道）最多可以包含 16 个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。链路聚合控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

您可以将 EtherChannel 中的每个物理数据接口配置为：

- Active - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- 开启 - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

注释 如果将其模式从打开更改为主用或从主用更改为打开状态，则可能需要多达三分钟的时间才能使 EtherChannel 进入运行状态。

非数据接口仅支持主用模式。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。 如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

Firepower 4100/9300 机箱 创建 EtherChannel 时，EtherChannel 将处于**挂起**状态（对于主动 LACP 模式）或**关闭**状态（对于打开 LACP 模式），直到将其分配给逻辑设备，即使物理链路是连通的。EtherChannel 在以下情况下将退出**挂起**状态：

- 将 EtherChannel 添加为独立逻辑设备的数据或管理端口
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的管理接口或集群控制链路
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的数据端口，并且至少有一个单元已加入该集群

请注意，EtherChannel 在您将它分配到逻辑设备前不会正常工作。如果从逻辑设备移除 EtherChannel 或删除逻辑设备，EtherChannel 将恢复为**挂起**或**关闭**状态。

过程

步骤 1 进入接口模式：

scope eth-uplink

scope fabric a

步骤 2 创建端口通道：

create port-channel *id*

enable

步骤 3 分配成员接口：

create member-port *interface_id*

您最多可以添加相同介质类型和容量的16个成员接口。成员接口必须设置为相同的速度和双工，并且必须与您为此端口通道配置的速度和双工相匹配。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

步骤 4 （可选） 设置接口类型。

set port-type {**data** | **mgmt** | **cluster**}

示例：

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

data关键字为默认类型。请勿选择**cluster**关键字，除非要将此端口通道用作集群控制链路，而不是默认设置。

步骤 5 为端口通道的成员设置所需的接口速度。

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

如果添加未达到指定速度的成员接口，接口将无法成功加入端口通道。默认值为 **10gbps**。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

步骤 6 （可选） 为端口通道的成员设置所需的双工。

set duplex {**fullduplex** | **halfduplex**}

如果添加以指定双工配置的成员接口，接口将无法成功加入端口通道。默认值为 **fullduplex**。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

步骤 7 启用或禁用自动协商（如果您的接口支持）。

set auto-negotiation {**on** | **off**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

步骤 8 设置数据接口的 LACP 端口通道模式。

对于非数据接口，模式始终是主用模式。

set port-channel-mode {**active** | **on**}

示例：

```
Firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

步骤 9 如果您编辑了默认流量控制策略，则它已应用于接口。如果您创建了新策略，请将其应用于接口。

set flow-control-policy *name*

示例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

步骤 10 提交配置：

commit-buffer

配置逻辑设备

在 Firepower 4100/9300 机箱上添加独立逻辑设备或高可用性对。

有关集群，请参阅#unique_219。

添加独立 ASA

独立逻辑设备可单独使用，也可在高可用性对中使用。在具有多个安全模块的 Firepower 9300 上，可以配置集群或独立设备。集群必须使用所有模块，因此无法将双模块集群和独立设备进行混用和搭配。

您可以通过 Firepower 4100/9300 机箱部署一个路由或透明防火墙模式的 ASA。

对于多情景模式，您必须先部署逻辑设备，然后在 ASA 应用中启用多情景模式。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像下载到 Firepower 4100/9300 机箱。

注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 威胁防御）。还可以在独立模块上运行一种应用实例的不同版本。

- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口不同于仅用于机箱管理的机箱管理端口（在 FXOS 中，可能会看到该接口显示为 MGMT、management0 或其他类似名称）。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址

过程

步骤 1 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 2 设置应用实例映像版本。

a) 查看可用映像。请注意您想要使用的版本号。

show app

示例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

b) 将范围设置为安全模块/引擎插槽。

scope slot *slot_id*

对于 Firepower 4100，*slot_id*始终为 1；对于 Firepower 9300，则始终为 1、2 或 3。

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) 创建应用实例。

enter app-instance asa *device_name*

device_name 可介于 1 至 64 个字符之间。在对此实例创建逻辑设备时，您将使用此设备名称。

示例：

```
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* #
```

d) 设置 ASA 映像版本。

set startup-version *version*

示例：

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

e) 退出到插槽模式。

exit

示例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) 退出到 ssa 模式。

exit

示例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

步骤 3 创建逻辑设备。

enter logical-device *device_name* **asa** *slot_id* **standalone**

使用与您之前添加的应用实例相同的 *device_name*。

示例：

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

步骤 4 向逻辑设备分配管理和数据接口。对各个接口重复此步骤。

create external-port-link *name interface_id* **asa**

set description *description*

exit

- *name* - 由 Firepower 4100/9300 机箱管理引擎使用；它不是在 ASA 配置中使用的接口名称。
- *description* - 在含有空格的短语两侧使用引号 (")。

管理接口与机箱管理端口不同。稍后您需要在 ASA 上启用和配置数据接口，包括设置 IP 地址。

示例：

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

步骤 5 配置管理引导程序信息。

a) 创建引导程序对象。

create mgmt-bootstrap asa

示例：

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 指定防火墙模式：路由或透明。

create bootstrap-key FIREWALL_MODE

set value {**routed** |**transparent**}

exit

在路由模式中，设备被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第2层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 指定管理员并启用密码。

create bootstrap-key-secret PASSWORD

set value

输入值： 密码

确认值： 密码

exit

示例：

预配置的 ASA 管理员用户和启用密码在进行密码恢复时非常有用；如果您有 FXOS 访问权限，在您忘记了管理员用户密码时，可以将其重置。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 配置 IPv4 管理接口设置。

create ipv4 *slot_id* **default**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) 配置 IPv6 管理接口设置。

create ipv6 *slot_id* **default**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) 退出管理引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

步骤 6 保存配置。

commit-buffer

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。使用 **show app-instance** 命令检查部署状态。当**管理状态**为**已启用**且**运行状态**为**在线**时，应用实例正在运行且可供使用。

示例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ ---------- -------------- -------------
asa        asa1       2          Disabled    Not Installed                   9.12.1
    Native                    Not Applicable  None
ftd        ftd1       1          Enabled     Online           6.4.0.49       6.4.0.49
    Container   Default-Small Not Applicable  None
```

步骤 7 请参阅 ASA 配置指南，以开始配置安全策略。

示例

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
```

```
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

添加高可用性对

威胁防御ASA 高可用性（也称为故障转移）是在应用中配置，而不是在 FXOS 中配置。但为了让您的机箱做好配置高可用性的准备，请参阅以下步骤。

开始之前

请参阅故障转移系统要求，第 260 页。

过程

步骤 1 将相同的接口分配给各个逻辑设备。

步骤 2 为故障转移和状态链路分配 1 个或 2 个数据接口。

这些接口用于交换 2 个机箱之间的高可用性流量。我们建议您将一个 10 GB 数据接口用于组合的故障转移和状态链路。如果您有可用的接口，可以使用单独的故障转移和状态链路；状态链路需要的带宽最多。不能将管理类型的接口用于故障转移或状态链路。我们建议您在机箱之间使用一个交换机，并且不将同一网段中的其他任何设备作为故障转移接口。

步骤 3 在逻辑设备上启用高可用性。请参阅通过故障转移实现高可用性，第 259 页。

步骤 4 如果您在启用高可用性后需要更改接口，请先在备用设备上执行更改，然后再在主用设备上执行更改。

注释
对于 ASA，如果在 FXOS 中移除一个接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中移除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

更改 ASA 逻辑设备上的接口

可以在 ASA 逻辑设备上分配、取消分配或替换管理接口。ASDM 会自动发现新接口。

添加新接口或删除未使用的接口对 ASA 配置的影响很小。但是，如果在 FXOS 中删除已分配的接口（例如，如果删除网络模块、删除 EtherChannel，或将分配的接口重新分配给 EtherChannel），并且在安全策略中使用该接口，则删除操作会影响 ASA 配置。在这种情况下，ASA 配置会保留原始命令，以便您可以进行任何必要的调整。您可以在 ASA OS 中手动移除旧的接口配置。

注释 您可以编辑已分配的 EtherChannel 的成员，而不影响逻辑设备。

开始之前

- 根据配置物理接口，第 173 页和添加 EtherChannel（端口通道），第 175 页配置您的接口，并添加任何 EtherChannel。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到 EtherChannel。对于新的 EtherChannel，您可以随后将 EtherChannel 分配到设备。
- 对于集群或故障转移，请确保添加或移除所有设备上的接口。我们建议先在数据/备用设备上更改接口，然后再在控制/主用设备上更改接口。新的接口在管理性关闭的状态下添加，因此，它们不会影响接口监控。

过程

步骤 1 进入安全服务模式：

Firepower# **scope ssa**

步骤 2 编辑逻辑设备：

Firepower /ssa # **scope logical-device** *device_name*

步骤 3 从逻辑设备取消分配接口：

Firepower /ssa/logical-device # **delete external-port-link** *name*

输入 **show external-port-link** 命令以查看接口名称。

对于管理接口，请删除当前接口，然后在添加新的管理接口之前，使用 **commit-buffer** 命令确认更改。

步骤 4 将新的接口分配到逻辑设备：

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **asa**

步骤 5 提交配置：

commit-buffer

提交系统配置任务。

连接到应用控制台

使用以下程序连接至应用的控制台。

过程

步骤 1 使用控制台连接或 Telnet 连接来连接至模块 CLI。

connect module *slot_number* {**console** | **telnet**}

要连接至不支持多个安全模块的设备的安全引擎，请使用 **1** 作为 *slot_number*。

使用 Telnet 连接的优点在于，您可以同时对模块开展多个会话，并且连接速度更快。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

步骤 2 连接到应用控制台。

connect asa *name*

要查看实例名称，请输入不含名称的命令。

示例：

```
Firepower-module1> connect asa asa1
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
```

```
asa>
```

步骤 3 退出应用控制台到 FXOS 模块 CLI。

- ASA - 输入 **Ctrl-a, d**

步骤 4 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 Telnet 会话：

a) 输入 **Ctrl-],**。

示例

以下示例连接至安全模块 1 上的 ASA，然后退回到 FXOS CLI 的管理引擎层。

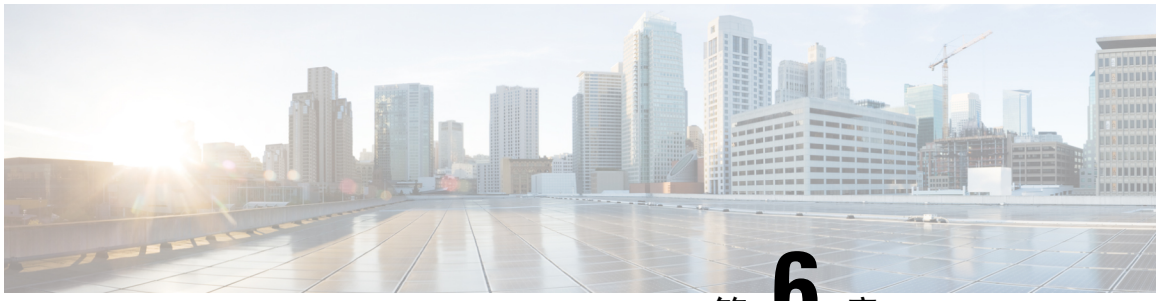
```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa asa1
asa> ~
telnet> quit
Connection closed.
Firepower#
```

逻辑设备的历史记录

特性	Version	详细信息
用于 Firepower 4112 的 ASA	9.14(1)	我们推出了 Firepower 4112。 **注释** 需要 FXOS 2.8.1。

特性	Version	详细信息
Firepower 9300 SM-56 支持	9.12.2	我们推出了 SM-56 安全模块。 **注释** 需要 FXOS 2.6.1.157。
适用于 Firepower 4115、4125 和 4145 的 ASA	9.12(1)	我们推出了 Firepower 4115、4125 和 4145。 **注释** 需要 FXOS 2.6.1。
Firepower 9300 SM-40 和 SM-48 支持	9.12.1	我们引入了 SM-40 和 SM-48 安全模块。 **注释** 需要 FXOS 2.6.1。
支持在同一个 Firepower 9300 上使用独立的 ASA 和 威胁防御 模块	9.12.1	您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 威胁防御 逻辑设备。 **注释** 需要 FXOS 2.6.1。
Firepower 4100/9300 的集群控制链路可自定义 IP 地址	9.10.1	默认情况下， 集群控制链路使用 127.2.0.0/16 网络。现在，可以在 FXOS 中部署集群时设置网络。机箱根据机箱 ID 和插槽 ID 自动生成每个设备的集群控制链路接口 IP 地址：127.2.*chassis_id*.*slot_id*。但是，某些网络部署不允许 127.2.0.0/16 流量通过。因此，您现在可以为 FXOS 中的集群控制链路设置一个自定义的 /16 子网（环回 (127.0.0.0/8) 和组播 (224.0.0.0/4 地址除外）。 **注释** 需要 FXOS 2.4.1。 新增/修改的 FXOS 命令：**set cluster-control-link network**
支持保存模式下的数据 Etherchannel	9.10.1	现在可以将数据和数据共享 Etherchannel 设置为“主用”LACP 模式或“保持”模式。其他类型 Etherchannel 仅支持“主用”模式。 **注释** 需要 FXOS 2.4.1。 新增/修改的 FXOS 命令：**set port-channel-mode**
Firepower 4100/9300 机箱上的 ASA 的站点间集群改进	9.7(1)	现在，您可以在部署 ASA 集群时为每个 Firepower 4100/9300 机箱配置站点 ID。以前，您必须在 ASA 应用中配置站点 ID；此新功能简化了最初的部署。请注意，您不能再在 ASA 配置中设置站点 ID。此外，为了实现与站点间集群的最佳兼容性，我们建议您升级到 ASA 9.7(1) 和 FXOS 2.1.1，升级版包含对稳定性和性能的多项改进。 修改了以下命令：**site-id**
支持 Firepower 4100 系列	9.6(1)	使用 FXOS 1.1.4，ASA 在 Firepower 4100 系列上支持机箱间集群。 未修改任何命令。

特性	Version	详细信息
6 个模块的机箱间集群，以及 Firepower 9300 ASA 应用的站点间集群	9.5(2.1)	现在您可利用 FXOS 1.1.3 启用机箱内集群，并扩展至站点间集群。在最多 6 个机箱中最多可以包含 6 个模块。 未修改任何命令。
Firepower 9300 的机箱内 ASA 集群	9.4(1.150)	最多可对 Firepower 9300 机箱内的 3 个安全模块建立集群。机箱中的所有模块都必须属于该集群。 引入了以下命令：**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis**



第 6 章

透明或路由防火墙模式

本章介绍如何将防火墙模式设置为路由或透明模式，以及防火墙在各种防火墙模式下的工作方式。

可以在多情景模式下为每个情景独立设置防火墙模式。

- 关于防火墙模式， 第 189 页
- 默认设置， 第 197 页
- 防火墙模式准则， 第 197 页
- 设置防火墙模式， 第 198 页
- 防火墙模式示例， 第 199 页
- 防火墙模式的历史记录， 第 210 页

关于防火墙模式

ASA支持两种防火墙模式：路由防火墙模式和透明防火墙模式。

关于路由防火墙模式

在路由模式中，ASA被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。您可以在情景之间共享第 3 层接口。

通过集成路由和桥接，您可以使用您用来对网络的多个接口进行分组的“网桥组”，ASA使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。ASA在 BVI 与正规的路由接口之间进行路由。如果您不需要多情景模式或集群或 EtherChannel 或 VNI 成员接口，则可以考虑使用路由模式而非透明模式。在路由模式下，可以像在透明模式下一样具有一个或多个隔离的网桥组，但也可以使用正常的路由接口进行混合部署。

关于透明防火墙模式

通常情况下，防火墙是一个路由跃点，并充当与其中一个被屏蔽子网连接的主机的默认网关。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。但是，与其他防火墙一样，接口之间的访问控制是受控制的，需要进行通常的所有防火墙检查。

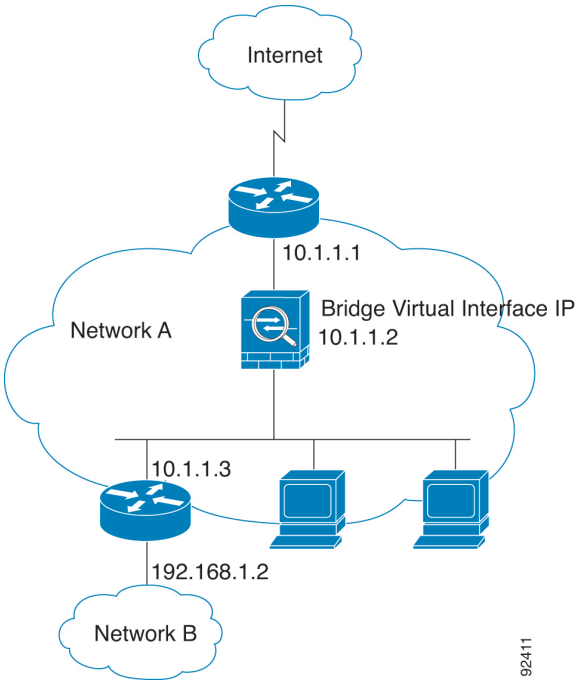
第 2 层连接使用您用来对网络的内部和外部接口进行分组的“网桥组”来实现，ASA使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。多个网络可以有多个网桥组。在透明模式下，这些网桥组无法相互通信。

在网络中使用透明防火墙

ASA 在其接口之间连接同一个网络。由于防火墙不是路由跃点，因此可以将透明防火墙轻松引入到现有网络中。

下图显示典型的透明防火墙网络，其中的外部设备与内部设备在同一个子网上。内部路由器和主机显示为与外部路由器直接连接。

图 *22*: 透明防火墙网络



管理 接口

除了每个网桥虚拟接口 (BVI) IP 地址，您可以添加不属于任何网桥组的独立管理 插槽/端口接口，这样将仅允许管理流量通过 ASA。有关详细信息，请参阅管理接口，第 660 页。

允许路由模式功能通过流量

对于透明防火墙不直接支持的功能，您可以允许流量通过，以便上游和下游路由器能够支持这些功能。例如，通过使用访问规则，可以允许 DHCP 流量（而不是不受支持的 DHCP 中继功能）或组播流量（例如 IP/TV 产生的流量）。还可以通过透明防火墙建立路由协议邻接；可以根据扩访问规则允许 OSPF、RIP、EIGRP 或 BGP 流量通过。同样，诸如 HSRP 或 VRRP 之类的协议也可以通过 ASA。

关于网桥组

网桥组是指 ASA 网桥（而非路由）的接口组。 网桥组在透明和路由防火墙模式下受支持。与任何其他防火墙接口一样，接口之间的访问控制将受控制，并将部署所有普通防火墙检查。

网桥虚拟接口 (BVI)

每个网桥组包括一个网桥虚拟接口 (BVI)。ASA使用该 BVI IP 地址作为源自网桥组的数据包的源地址。BVI IP 地址必须与网桥组成员接口位于同一子网。BVI 不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。

在透明模式下：只有网桥组成员接口会被命名并可以与基于接口的功能配合使用。

在路由模式下：BVI 充当网桥组和其他路由接口之间的网关。要在网桥组/路由接口之间进行路由，必须为 BVI 命名。对于一些基于接口的功能，您可以单独使用 BVI：

- 访问规则 - 可以为网桥组成员接口和BVI配置访问规则；对于入站规则，会首先检查成员接口。对于出站规则，会首先检查 BVI。
- DHCPv4 服务器 - 只有 BVI 支持 DHCPv4 服务器配置。
- 静态路由 - 可以为 BVI 配置静态路由；不能为成员接口配置静态路由。
- 系统日志服务器和其他源自 ASA的流量 - 当指定系统日志服务器（或 SNMP 服务器，或流量源自 ASA的其他服务）时，可以指定 BVI 或成员接口。

如果您在路由模式下没有命名 BVI，则 ASA不会路由网桥组流量。此配置将为网桥组复制透明防火墙模式。如果您不需要多情景模式或集群或 EtherChannel 或 VNI 成员接口，则可以考虑改用路由模式。在路由模式下，可以像在透明模式下一样具有一个或多个隔离的网桥组，但也可以使用正常的路由接口进行混合部署。

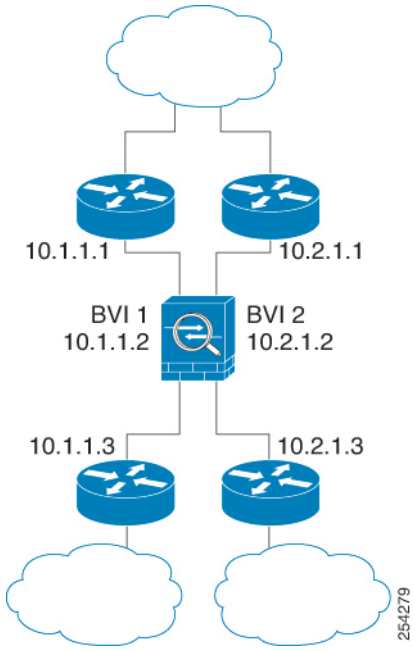
透明防火墙模式下的网桥组

网桥组的流量相互分离；流量不会路由至 ASA 中的另一个网桥组，并且流量必须退出 ASA 后才能通过外部路由器路由回ASA中的另一个网桥组。虽然每个网桥组的桥接功能是独立的，但所有网桥组之间可共享很多其他功能。例如，所有网桥组都共享系统日志服务器或AAA服务器的配置。为完全分离安全策略，请在每个情景中对一个网桥组使用安全情景。

可以在每个网桥组中包含多个接口。有关支持的网桥组和接口的确切数量，请参阅防火墙模式准则，第 197 页。如果您在每个网桥组中使用的接口数超过 2 个，则可以控制同一网络上多个网段之间的通信，而不只是在内部和外部之间的通信。例如，如果您有三个不需要彼此通信的内部网段，则可以将每个网段设置在单独的接口上，并且仅允许它们与外部接口通信。或者，您可以自定义接口之间的访问规则，以根据需要允许任意程度的访问。

下图显示连接到 ASA且具有两个网桥组的两个网络。

图 *23:* 具有两个网桥组的透明防火墙网络

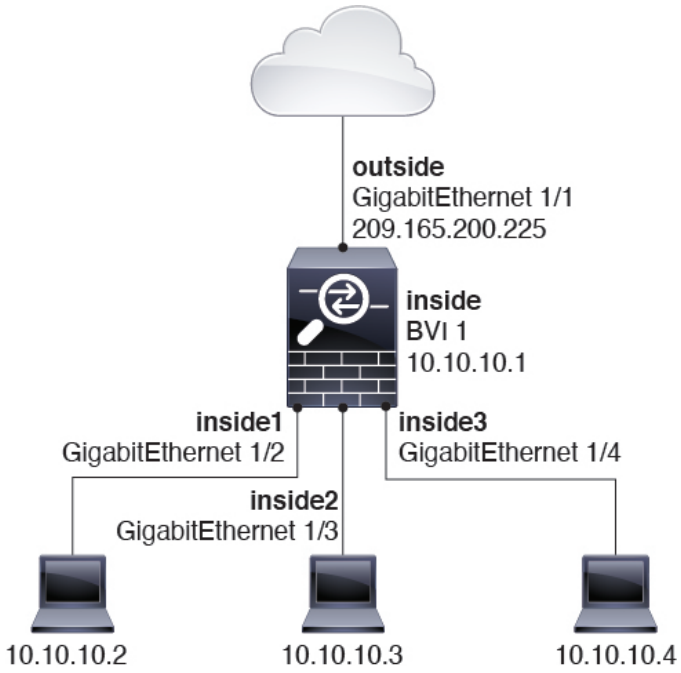


路由防火墙模式下的网桥组

网桥组流量可以路由到其他网桥组或路由接口。您可以选择通过不为网桥组的 BVI 接口分配名称来隔离网桥组流量。如果命名了 BVI，则 BVI 将像其他任何普通接口一样参与路由。

路由模式下网桥组的一种用途是在 ASA上而非外部交换机上使用额外接口。例如，某些设备的默认配置包括一个外部接口作为普通接口，还包括分配给内部网桥组的其他接口。由于此网桥组的目的是替换外部交换机，因此您需要配置访问策略，以便所有网桥组接口都可以自由通信。 例如，就像默认配置一样，将所有接口设置为同一安全级别，然后启用相同安全接口通信；无需访问规则。

图 *24:* 具有内部网桥组和外部路由接口的路由防火墙网络



传递路由模式下不允许的流量

在路由模式下，某些类型的流量无法通过 ASA，即使在访问规则中允许该流量也不行。但网桥组使用访问规则（对于 IP 流量）或 EtherType 规则（对于非 IP 流量）几乎可以允许所有流量通过。

- IP 流量 - 在路由防火墙模式下，即便访问规则（包括不支持的动态路由协议和 DHCP）中允许广播和组播流量，它们也会受到阻拦，除非配置了 DHCP 中继。在网桥组内，您可以通过访问规则（使用扩展 ACL）允许此流量。
- 非 IP 流量 - AppleTalk、IPX、BPDU 和 MPLS 等都可使用 EtherType 规则配置为通过。

注释 网桥组不传递 CDP 数据包，也不传递有效 EtherType 大于或等于 0x600 的任何数据包。BPDU 和 IS-IS 除外，它们受支持。

允许第 3 层流量

- 单播 IPv4 和 IPv6 流量可通过网桥组从安全性较高的接口自动流向安全性较低的接口，而无需访问规则。
- 对于从低安全性接口传播到高安全性接口的第3层流量，要求低安全性接口上有一个访问规则。
- 允许 ARP 双向通过网桥组，而无需访问规则。ARP 流量可通过 ARP 检测进行控制。
- IPv6 邻居发现和路由器请求数据包可以使用访问规则传递。

- 可使用访问规则允许广播和组播流量通过。

允许的 MAC 地址

如果得到您的访问策略的允许，将允许以下目标 MAC 地址通过网桥组（请参阅允许第 3 层流量，第 193 页）。系统会丢弃此列表中未列出的任何 MAC 地址。

- 实际广播目标 MAC 地址等于 FFFF.FFFF.FFFF
- IPv4 组播 MAC 地址的范围是 0100.5E00.0000 至 0100.5EFE.FFFF
- IPv6 组播 MAC 地址的范围是 3333.0000.0000 至 3333.FFFF.FFFF
- BPDU 组播地址等于 0100.0CCC.CCCD
- AppleTalk 组播 MAC 地址的范围是 0900.0700.0000 至 0900.07FF.FFFF

BPDU 处理

为防止环路使用生成树协议，默认情况下允许 BPDU 通过。要阻止 BPDU，需要将 EtherType 规则配置为拒绝 BPDU。您还可以阻止外部交换机上的 BPDU。例如，如果同一网桥组的成员连接到不同 VLAN 中的交换机端口，则可以阻止交换机上的 BPDU。在这种情况下，来自一个 VLAN 的 BPDU 将在另一个 VLAN 中可见，这可能会导致生成树根网桥选择过程问题。

如果使用故障转移功能，则可能要阻止 BPDU，以防止交换机端口在拓扑结构更改时进入阻止状态。有关详细信息，请参阅故障转移的网桥组要求，第 268 页。

MAC 地址与路由查找

对于网桥组中的流量，通过执行目标 MAC 地址查找而不是路由查找来确定数据包的传出接口。

但是，路由查找对于以下情况是必要的：

- 源自 ASA的流量 - 例如，在 ASA上为发往系统日志服务器所在的远程网络的流量添加一个默认/静态路由。
- 已启用检测的 IP 语音 (VoIP) 和 TFTP 流量，并且终端至少在一跳之外 - 在 ASA上为发往成功建立辅助连接的远程终端的流量添加静态路由。ASA会在访问控制策略中创建一个临时“针孔”以允许辅助连接；由于连接可能会使用一组不同于主连接的 IP 地址，所以 ASA需要执行路由查找以便在正确的接口上安装针孔。

  受影响的应用包括：

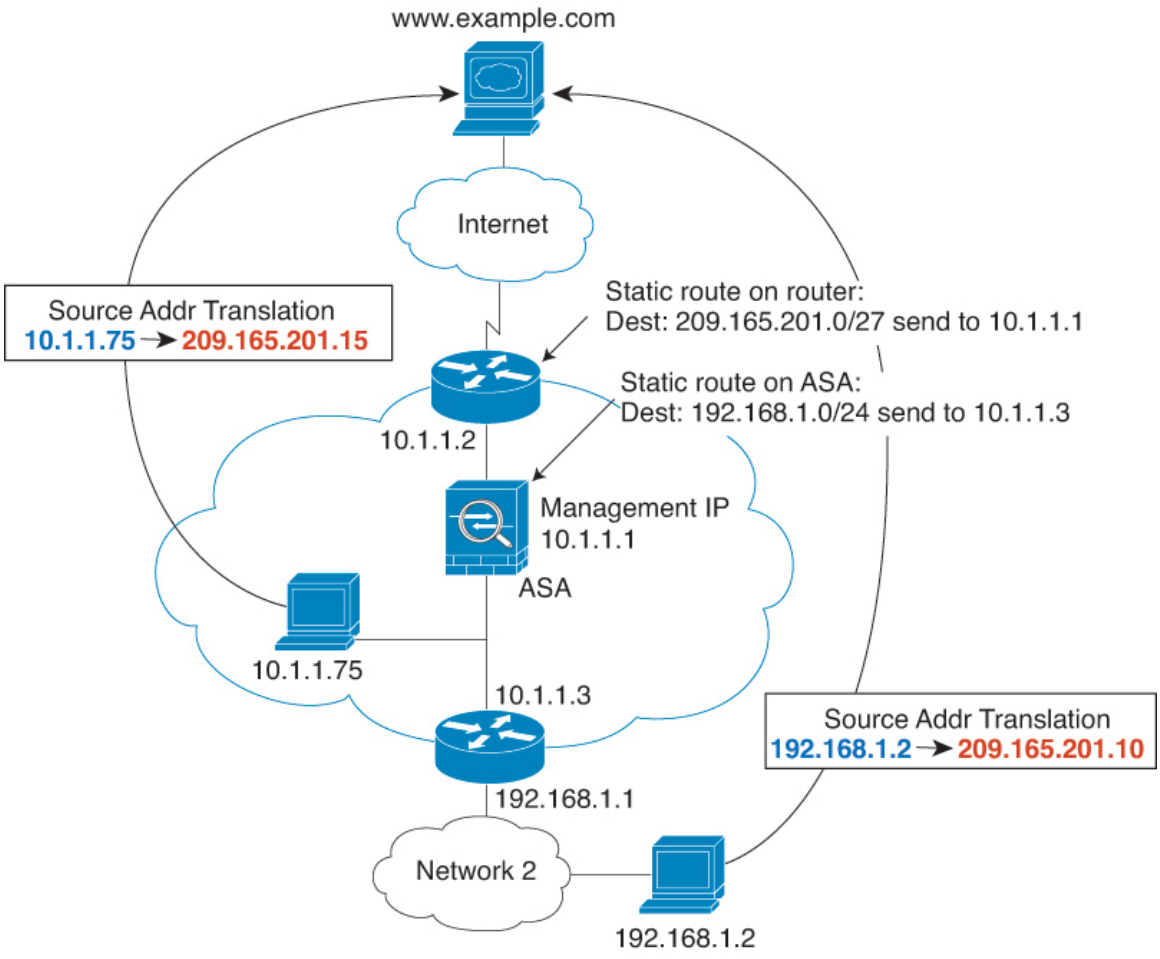
  - CTIQBE
  - GTP
  - H.323
  - MGCP
  - RTSP

- SIP
- Skinny (SCCP)
- SQL*Net
- SunRPC
- TFTP

- ASA对其执行 NAT 的至少一跳开外的流量 - 在 ASA上为发往远程网络的流量配置静态路由。您还需要在上游路由器上为要发送到 ASA的已映射地址的流量配置静态路由。

  此路由要求也适用已启用检测和 NAT 的 VoIP 和 DNS 的嵌入式 IP 地址，这些嵌入式 IP 地址都必须至少在一跳之外。ASA需要识别正确的出口接口，以便可以执行转换。

图 *25: NAT* 示例：网桥组中的 *NAT*



透明模式下网桥组不支持的功能

下表列出了在透明模式下网桥组中不受支持的功能。

表 *4:* 在透明模式下不支持的功能

功能	说明
动态 DNS	-
DHCPv6 无状态服务器	在网桥组成员接口上仅支持 DHCPv4 服务器。
DHCP 中继	透明防火墙可作为 DHCPv4 服务器，但它不支持 DHCP 中继。不需要使用 DHCP 中继，因为可使用两个访问规则来允许 DHCP 流量通过：一个规则用于允许从内部接口向外部发送 DCHP 请求；另一个用于允许来自另一个方向的服务器的应答。
动态路由协议	但是，对于网桥组成员接口，可以为 ASA上发起的流量添加静态路由。您还可以使用访问规则来允许动态路由协议通过 ASA。
组播 IP 路由	通过在访问规则中允许组播流量，可以允许组播流量通过 ASA。
QoS	-
针对直通流量终止 VPN	透明防火墙仅支持在网桥组成员接口上使用站点间的 VPN 隧道传输管理连接。它不会针对通过 ASA 的流量终止 VPN 连接。您可以使用访问规则允许 VPN 流量通过 ASA，但它不会终止非管理连接。无客户端 SSL VPN 也不受支持。
统一通信	—

路由模式下网桥组不支持的功能

下表列出了在路由模式下网桥组中不支持的功能。

表 *5:* 路由模式下不受支持的功能

功能	说明
EtherChannel 或 VNI 成员接口	仅支持物理接口和子接口作为网桥组成员接口。 管理 接口也不受支持。
集群	集群中不支持网桥组。
动态 DNS	-
DHCPv6 无状态服务器	只有 DHCPv4 服务器在 BVI 上受支持。
DHCP 中继	路由防火墙可以作为 DHCPv4 服务器，但它不支持在 BVI 或网桥组成员接口上使用 DHCP 中继。
动态路由协议	但您可以为 BVI 添加静态路由。您还可以使用访问规则来允许动态路由协议通过 ASA。非网桥组接口支持动态路由。

功能	说明
组播 IP 路由	通过在访问规则中允许组播流量，可以允许组播流量通过 ASA。非网桥组接口支持组播路由。
多情景模式	在多情景模式下，不支持网桥组。
QoS	非网桥组接口支持 QoS。
针对直通流量终止 VPN	您无法终止 BVI 上的 VPN 连接。非网桥组接口支持 VPN。 网桥组成员接口仅支持将站点间 VPN 隧道用于管理连接。它不会针对通过 ASA 的流量终止 VPN 连接。您可以使用访问规则通过网桥组传递 VPN 流量，但它不会终止非管理连接。无客户端 SSL VPN 也不受支持。
统一通信	非网桥组接口支持统一通信。

默认设置

默认模式

默认模式为路由模式。

网桥组默认设置

默认情况下，所有 ARP 数据包都在网桥组内通过。

防火墙模式准则

情景模式准则

根据情景设置防火墙模式。

桥接组准则（透明和路由模式）

- 您可以创建最多 250 个桥接组，每个桥接组 64 个接口。
- 各个直连网络必须在同一子网上。
- ASA不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。
- 每个桥接组都需要 BVI 的 IP 地址，以用于管理往返设备的流量和使流量通过 ASA。对于 IPv4 流量，请指定 IPv4 地址。对于 IPv6 流量，请指定 IPv6 地址。
- 您仅可手动配置 Ipv6 地址。

- BVI IP 地址必须与已连接网络位于同一子网上。您不能将该子网设置为主机子网 (255.255.255.255)。
- 不支持将管理接口作为桥接组成员。
- 对于具有桥接 ixgbevf 接口的 VMware 上的 ASAv50，透明模式不受支持，在路由模式中网桥组不受支持。
- 对于 Firepower 1010 和 Cisco Secure Firewall 1210/20，不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个桥接组中。
- 在透明模式下，必须至少使用 1 个桥接组；数据接口必须属于桥接组。
- 在透明模式下，请勿将 BVI IP 地址指定为所连接设备的默认网关；设备需要将位于 ASA另一端的路由器指定为默认网关。
- 在透明模式下，默认路由（为管理流量提供返回路径所需的路由）仅适用于来自一个桥接组网络的管理流量。这是因为默认路由会指定网桥组中的接口以及网桥组网络上的路由器 IP 地址，而您只能定义一个默认路由。如果您具有来自多个桥接组网络的管理流量，则需要指定常规静态路由来确定预期会发出管理流量的网络。
- 在透明模式下，管理接口不支持 PPPoE。
- 在路由模式下，要在桥接组和其他路由接口之间路由，您必须指定 BVI。
- 在路由模式下，ASA - 不支持将 EtherChannel 和 VNI 接口定义为网桥组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。
- 使用网桥组成员时，不允许双向转发检测 (BFD) 回应数据包通过 ASA。如果 ASA 的一端有两个邻居运行 BFD，则 ASA 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。

其他准则和限制

- 在更改防火墙模式时，ASA 会清除正在运行的配置，因为许多命令不能同时支持两种模式。启动配置会保持不变。如果重新加载而不保存，则会加载启动配置，且模式会恢复为原始设置。有关备份配置文件的信息，请参阅设置防火墙模式，第 198 页。
- 如果将文本配置下载到 ASA 且使用 **firewall transparent** 命令来更改模式，请确保将该命令放在配置的顶部；ASA 会在读取命令后立即更改模式并继续读取下载的配置。如果此命令显示在配置的后面部分，则ASA会清除配置中在此命令前面的所有行。有关下载文本文件的信息，请参阅设置 ASA 映像、ASDM 和启动配置，第 1302 页。

设置防火墙模式

本节介绍如何 更改防火墙模式。

注释 我们建议先设置防火墙模式再执行任何其他配置，因为更改防火墙模式会清除运行配置。

开始之前

在更改模式时，ASA 将清除运行的配置（有关详细信息，请参阅防火墙模式准则，第 197 页）。

- 如果您已经具有填充的配置，请务必在更改模式之前备份配置；在创建新配置时，可以使用此备份作为参考。请参阅备份和恢复配置或其他文件，第 1305 页。
- 在控制台端口处使用 CLI 更改模式。如果使用任何其他类型的会话（包括 ASDM 命令行界面工具或SSH），当清除配置时您将被断开，在任何情况下您必须使用控制台断开重新连接到ASA。
- 在情景中设置模式。

注释 要将防火墙模式设置为透明模式，并要在清除配置后配置 ASDM 管理访问，请参阅配置 ASDM 访问，第 15 页。

过程

将防火墙模式设置为透明：

firewall transparent

示例：

```
ciscoasa(config)# firewall transparent
```

要将模式更改为路由模式，请输入 **no firewall transparent** 命令。

注释
系统不会提示您确认防火墙模式更改；更改会立即发生。

防火墙模式示例

本节包含流量如何通过处于路由和透明防火墙模式下的 ASA 的示例。

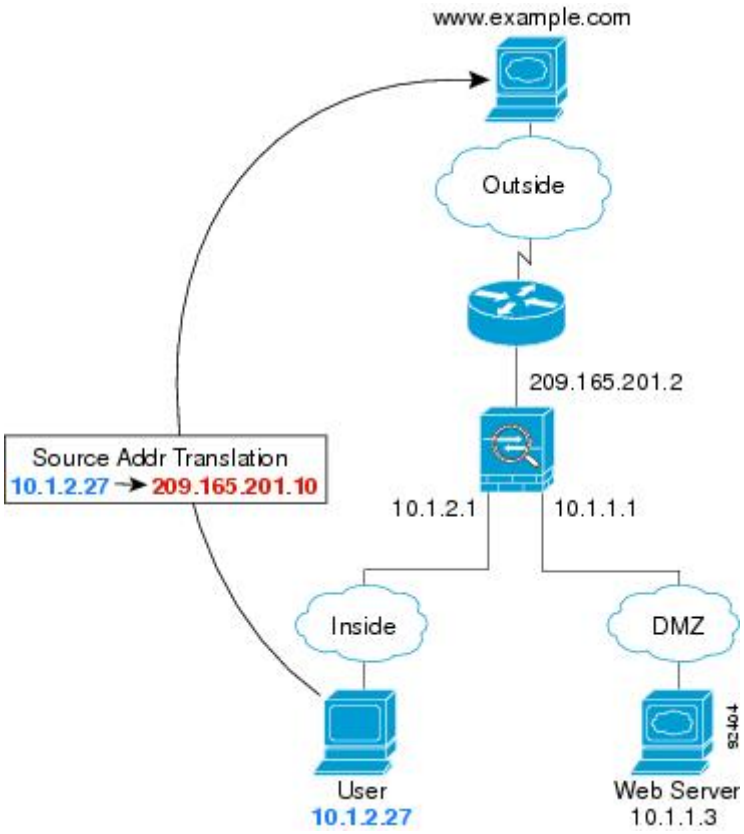
数据如何通过处于路由防火墙模式下的 ASA

以下各节介绍在多个情景中，数据如何通过处于路由防火墙模式下的 ASA。

内部用户访问 Web 服务器

下图显示了内部用户对外部 Web 服务器的访问。

图 *26:* 内部至外部



以下步骤介绍数据如何通过 ASA：

1. 内部网络中的用户从 www.example.com 请求访问网页。
2. ASA 接收数据包，由于是新会话，因此它会根据安全策略条款验证数据包是否获得允许。

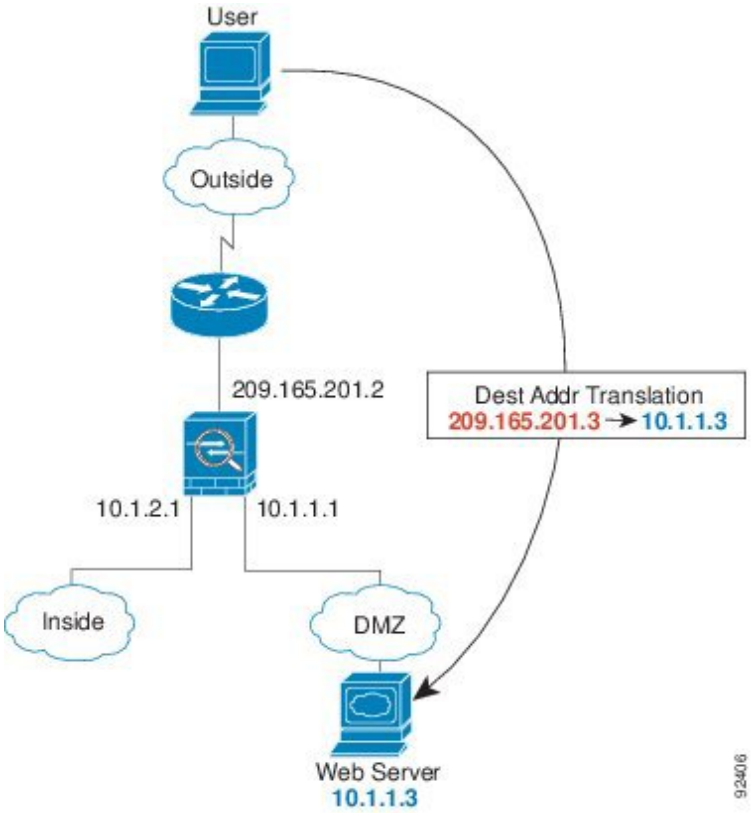
   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. ASA 将实际地址 (10.1.2.27) 转换为映射的地址 209.165.201.10，后者位于外部接口子网上。

   映射的地址可能位于任意子网上，但当它位于外部接口子网上时，才会简化路由。
4. 然后，ASA 会记录有关会话已建立的信息，并从外部接口转发数据包。
5. 当 www.example.com 响应请求时，数据包会通过 ASA，由于已建立会话，因此数据包会绕过许多与新连接关联的查找。ASA 通过将全局目标地址逆向转换为本地用户地址 10.1.2.27 来执行 NAT。
6. ASA 将数据包转发给内部用户。

外部用户访问 DMZ 上的 Web 服务器

下图显示了访问 DMZ Web 服务器的外部用户。

图 *27:* 外部到 *DMZ*



以下步骤介绍数据如何通过 ASA：

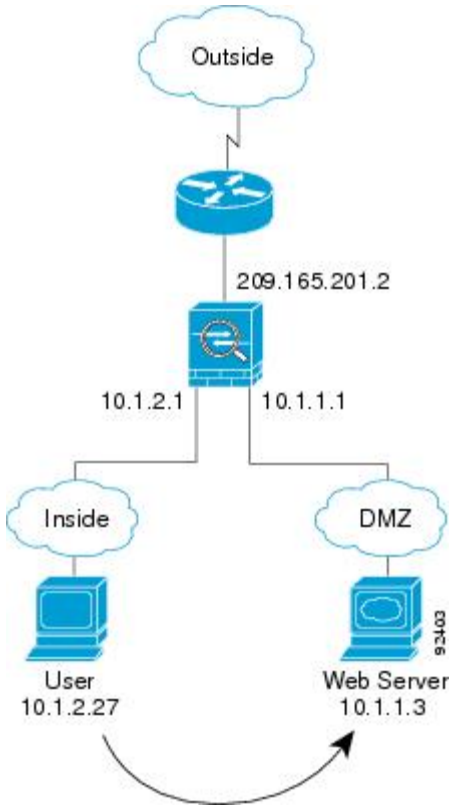
1. 外部网络上的用户使用映射地址 209.165.201.3（位于外部接口子网上）从 DMZ Web 服务器请求访问网页。
2. ASA 接收数据包并将映射的地址逆向转换为真实地址 10.1.1.3。
3. 由于是新会话，因此 ASA 会根据安全策略条款验证数据包是否获得允许。

   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
4. 然后，ASA 将会话条目添加到快速路径，并从 DMZ 接口转发数据包。
5. 当 DMZ Web 服务器响应请求时，数据包会通过 ASA，由于已建立会话，因此数据包会绕过许多与新连接关联的查找。ASA 通过将真实地址转换为 209.165.201.3 来执行 NAT。
6. ASA 将数据包转发给外部用户。

内部用户访问 DMZ 上的 Web 服务器

下图显示了显示访问 DMZ Web 服务器的内部用户。

图 *28:* 从内部到 *DMZ*



以下步骤介绍数据如何通过 ASA：

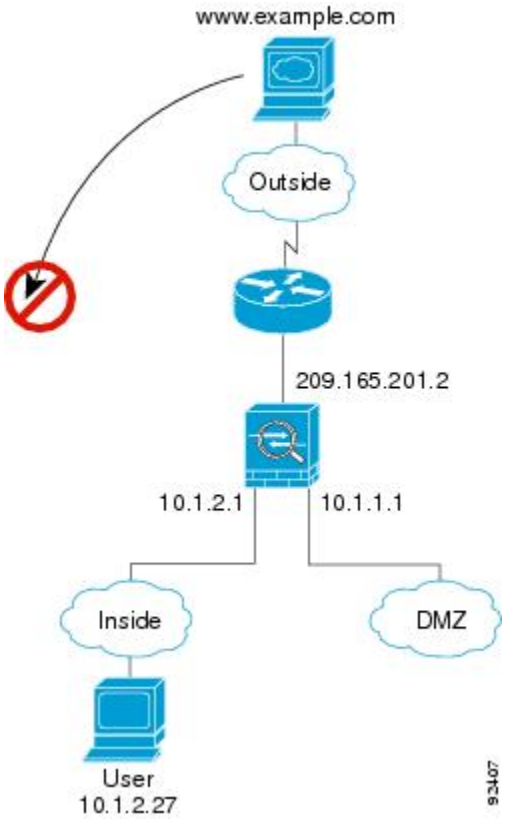
1. 内部网络上的用户使用目标地址 10.1.1.3 从 DMZ Web 服务器请求访问网页。
2. ASA 接收数据包，由于是新会话，因此 ASA 会根据安全策略条款验证数据包是否获得允许。

   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. 然后，ASA 会记录有关会话已建立的信息，并从 DMZ 接口将数据包转发出去。
4. 当 DMZ Web 服务器响应请求时，数据包会通过快速路径，这样可使数据包绕过许多与新连接关联的查找。
5. ASA 将数据包转发给内部用户。

外部用户尝试访问内部主机

下图显示外部用户尝试访问内部网络。

图 *29:* 从外部到内部



以下步骤介绍数据如何通过 ASA：

1. 外部网络上的用户尝试访问内部主机（假设主机具有可路由的 IP 地址）。

   如果内部网络使用专用地址，则外部用户在没有执行 NAT 的情况下无法访问内部网络。外部用户可能会通过使用现有 NAT 会话尝试访问内部用户。

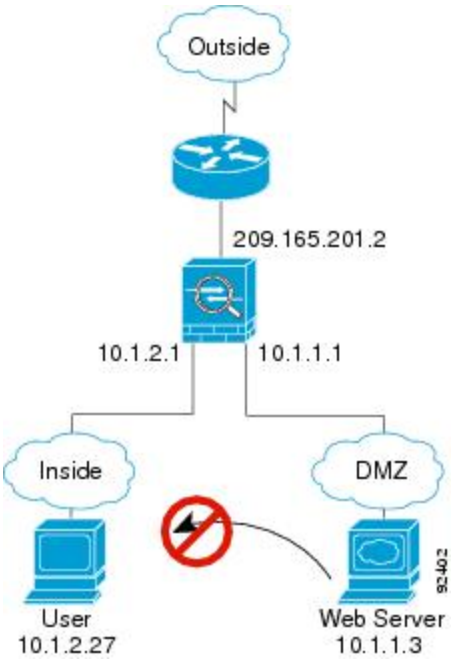
2. ASA 接收数据包；因为是新会话，因此它会根据安全策略验证是否允许该数据包。
3. 系统会拒绝数据包，而 ASA 则丢弃数据包并记录连接尝试情况。

   如果外部用户尝试攻击内部网络，则 ASA 会采用多种技术来确定数据包对于已建立的会话是否有效。

DMZ 用户尝试访问内部主机

下图显示了 DMZ 中的用户尝试访问内部网络。

图 *30:* 从 *DMZ* 到内部



以下步骤介绍数据如何通过 ASA：

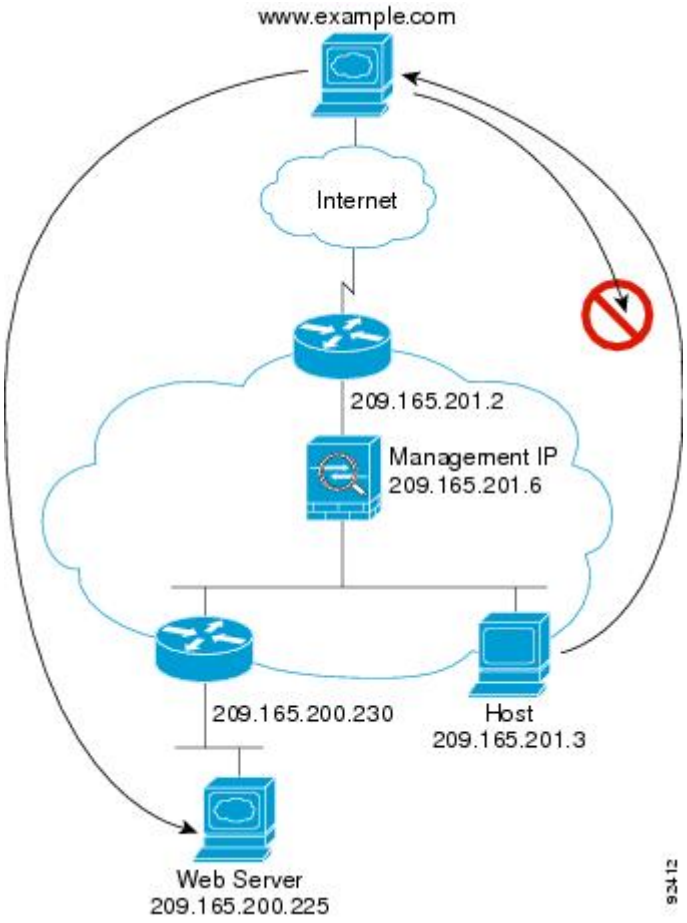
1. DMZ 网络上的用户尝试访问内部主机。由于 DMZ 不必路由互联网上的流量，因此专用寻址方案不会防止路由。
2. ASA 接收数据包；因为是新会话，因此它会根据安全策略验证是否允许该数据包。

   系统会拒绝数据包，而 ASA 则丢弃数据包并记录连接尝试情况。

数据如何通过透明防火墙

下图显示了包含公共Web服务器的内部网络上的典型透明防火墙实施。ASA具有访问规则以便内部用户可访问互联网资源。通过其他访问规则，外部用户只能访问内部网络上的 Web 服务器。

图 *31:* 典型透明防火墙数据路径

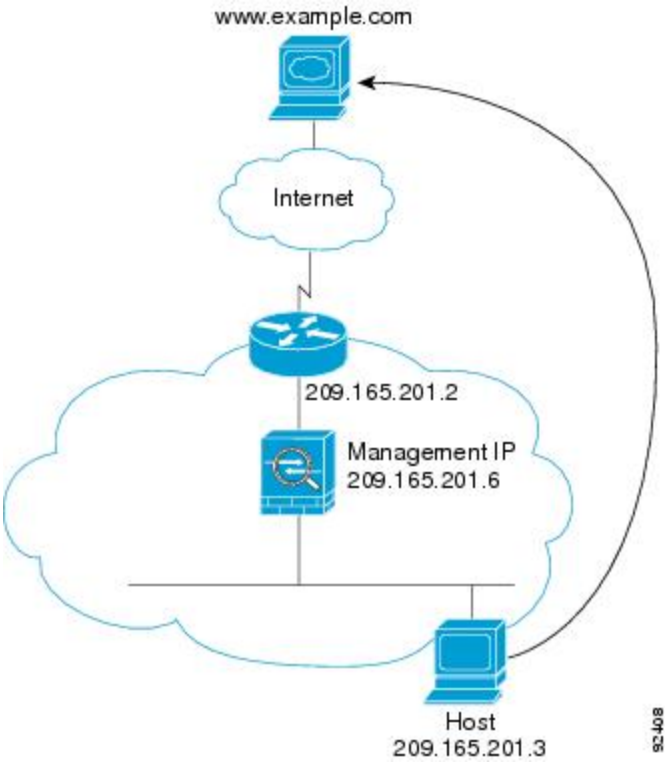


以下部分介绍数据如何通过 ASA。

内部用户访问 Web 服务器

下图显示了内部用户对外部 Web 服务器的访问。

图 *32:* 内部至外部



以下步骤介绍数据如何通过 ASA：

1. 内部网络中的用户从 www.example.com 请求访问网页。
2. ASA 接收数据包，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款验证数据包是否获得允许。

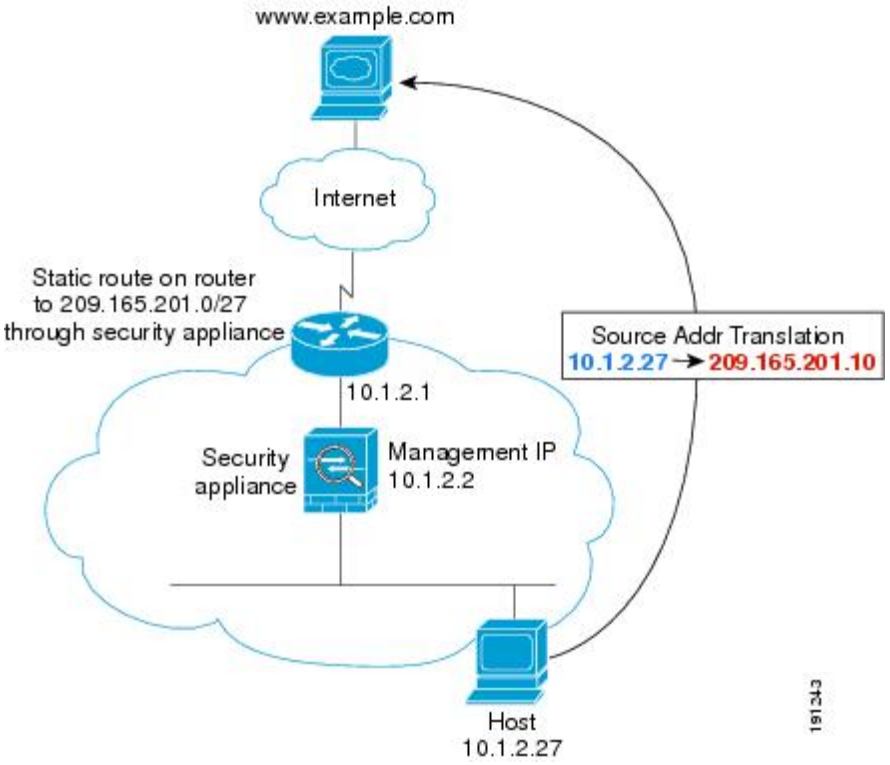
   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (209.165.201.2)。

   如果目标 MAC 地址不在 ASA 表中，则它会通过发送 ARP 请求或 ping 来尝试发现 MAC 地址。系统会丢弃第一个数据包。
5. Web 服务器响应请求；由于已建立会话，因此数据包会绕过许多与新连接关联的查找。
6. ASA 将数据包转发给内部用户。

内部用户使用 NAT 访问 Web 服务器

下图显示了内部用户对外部 Web 服务器的访问。

图 *33:* 使用 *NAT* 从内部到外部



以下步骤介绍数据如何通过 ASA：

1. 内部网络中的用户从 www.example.com 请求访问网页。
2. ASA 接收数据包，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款验证数据包是否获得允许。

   对于多情景模式，ASA 会首先根据唯一接口对数据包进行分类。
3. ASA 会将真实地址 (10.1.2.27) 转换为映射地址 209.165.201.10。

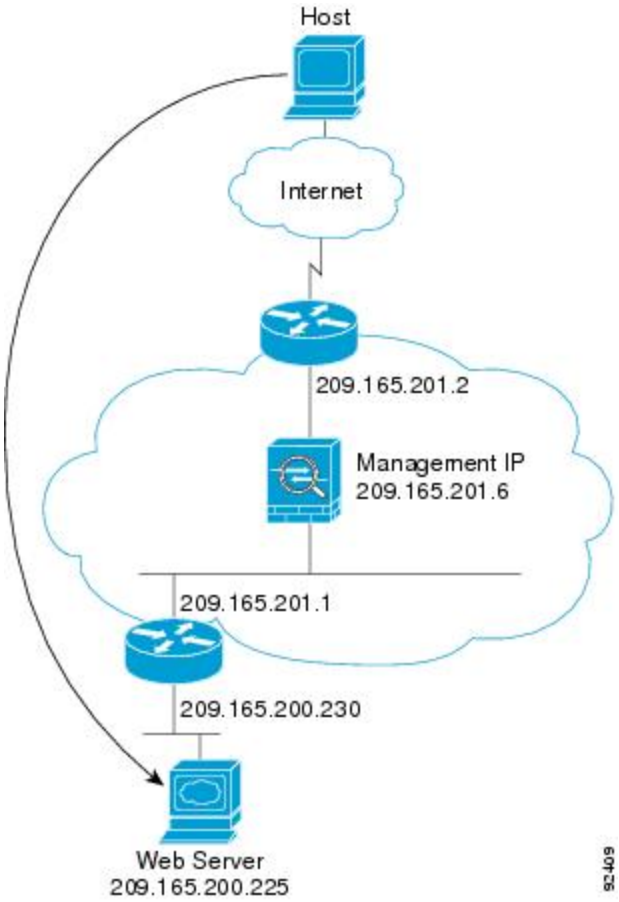
   由于映射地址与外部接口不在同一网络上，因此请确保上游路由器具有至映射网络（指向 ASA）的静态路由。
4. 然后，ASA 会记录有关会话已建立的信息，并从外部接口转发数据包。
5. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从外部接口转发出去。目标 MAC 地址是上游路由器的地址 (10.1.2.1)。

   如果目标 MAC 地址不在 ASA 表中，则它会通过发送 ARP 请求和 ping 来尝试发现 MAC 地址。系统会丢弃第一个数据包。
6. Web 服务器响应请求；由于已建立会话，因此数据包会绕过许多与新连接关联的查找。
7. ASA 通过将映射地址逆向转换为真实地址 10.1.2.27 来执行 NAT。

外部用户访问内部网络上的 Web 服务器

下图显示了访问内部 Web 服务器的外部用户。

图 *34:* 从外部到内部



以下步骤介绍数据如何通过 ASA：

1. 外部网络上的用户从内部 Web 服务器请求访问网页。
2. ASA 接收数据包，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款验证数据包是否获得允许。

   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. ASA 记录有关会话已建立的信息。
4. 如果目标 MAC 地址在其表中，则 ASA 会将数据包从内部接口转发出去。目标 MAC 地址是下游路由器的地址 (209.165.201.1)。

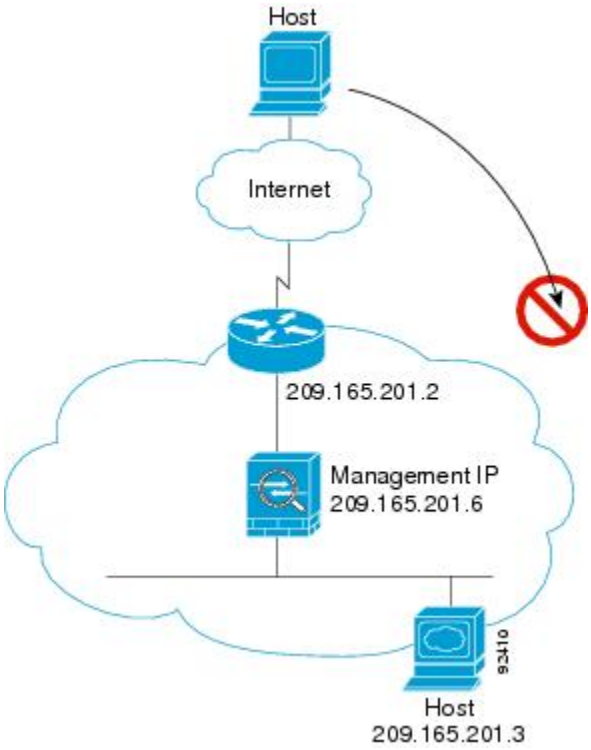
   如果目标 MAC 地址不在 ASA 表中，则它会通过发送 ARP 请求和 ping 来尝试发现 MAC 地址。系统会丢弃第一个数据包。
5. Web 服务器响应请求；由于已建立会话，因此数据包会绕过许多与新连接关联的查找。

6. ASA 将数据包转发给外部用户。

外部用户尝试访问内部主机

下图显示外部用户尝试访问内部网络上的主机。

图 *35:* 从外部到内部



以下步骤介绍数据如何通过 ASA：

1. 外部网络上的用户尝试访问内部主机。
2. ASA 接收数据包，并在需要时将源 MAC 地址添加到 MAC 地址表中。由于它是新会话，因此会根据安全策略条款验证数据包是否获得允许。

   对于多情景模式，ASA 会首先将数据包分类到一个情景中。
3. 由于没有允许外部主机的访问规则，因此会拒绝数据包，并且 ASA 会丢弃数据包。
4. 如果外部用户尝试攻击内部网络，则 ASA 会采用多种技术来确定数据包对于已建立的会话是否有效。

防火墙模式的历史记录

表 *6:* 防火墙模式的功能历史记录

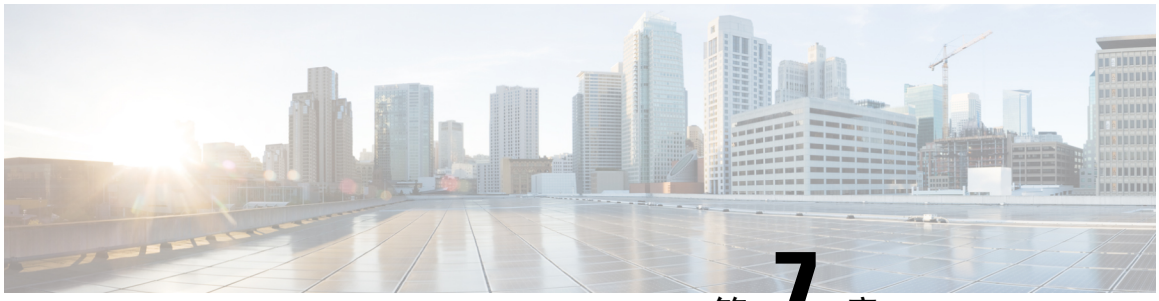
功能名称	平台版本	功能信息
透明防火墙模式	7.0(1)	透明防火墙是 2 层防火墙，充当“嵌入式防火墙”或“隐藏防火墙”，并且不会被视为所连接设备的路由器跃点。 引入了以下命令：**firewall transparent** 和 **show firewall**。
透明防火墙网桥组	8.4(1)	如果您不希望产生安全情景开销，或者希望最大限度地利用安全情景，则可以将接口一起集合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组流量相互分隔。在单情景模式和多情景模式的每个情景中，最多可配置 8 个网桥组，每组最多 4 个接口。 注释 尽管您可以在 ASA 5505 上配置多个网桥组，但在 ASA 5505 上的透明模式下数据接口数限制为两个意味着只能有效地使用 1 个网桥组。 引入了以下命令：**interface bvi**、**bridge-group** 和 **show bridge-group**。
在多情景模式下支持混合防火墙模式	8.5(1)/9.0(1)	可以在多情景模式下为每个情景独立设置防火墙模式，因此某些情景可在透明模式下运行，而另一些情景则可在路由模式中运行。 修改了以下命令：**firewall transparent**。
透明模式的网桥组最大数量增加到 250	9.3(1)	网桥组最大数量从 8 个增加到 250 个网桥组。在单情景模式和多情景模式的每个情景中，最多可配置 250 个网桥组，每组最多 4 个接口。 修改了以下命令：**interface bvi** 和 **bridge-group**。
每个桥接组的透明模式最大接口数增加到 64	9.6(2)	每个网桥组的最大接口数量已从 4 增加到 64。 未修改任何命令。

功能名称	平台版本	功能信息
集成的路由与桥接	9.7(1)	集成路由和桥接提供了在网桥组和路由接口之间路由的功能。网桥组指 ASA 桥接（而非路由）的接口组。ASA 并非真正的网桥，因为 ASA 仍继续充当防火墙：控制接口之间的访问控制，并执行所有常规防火墙检查。以前，您只能在透明防火墙模式下配置网桥组，而无法在网桥组之间路由。通过此功能，可以在路由防火墙模式下配置网桥组，并在网桥组之间以及网桥组与路由接口之间进行路由。网桥组使用网桥虚拟接口 (BVI) 作为网桥组的网关，由此参与路由。如果 ASA 上还有额外接口可分配给网桥组，集成路由和桥接可提供替代使用外部第 2 层交换机的其他方案。在路由模式下，BVI 可以是已命名接口，并可独立于成员接口参与某些功能，例如访问规则和 DHCP 服务器。 路由模式不支持透明模式下支持的以下功能：多情景模式、ASA 集群。以下功能在 BVI 上也不受支持：动态路由和组播路由。 修改了以下命令：**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn**
支持 Firepower 4100/9300 逻辑设备的透明模式部署	9.10(1)	您现在可以在 Firepower 4100/9300 上部署 ASA 时指定透明模式或路由模式。 新增/修改的 FXOS 命令：**enter bootstrap-key FIREWALL_MODE**、**set value routed** 和 **set value transparent**

第 II 部分

高可用性和可扩展性

- 多情景模式， 第 215 页
- 通过故障转移实现高可用性， 第 259 页
- 公共云中的高可用性故障转移， 第 311 页
- 为 Cisco Secure Firewall 3100/4200部署 ASA 集群， 第 333 页
- Firepower 4100/9300 的 ASA 集群， 第 427 页
- ASA 集群部署集群， 第 519 页
- 在公共云中为 ASA Virtual 部署 ASA 集群， 第 585 页



第 7 章

多情景模式

本章介绍如何在 ASA 上配置多个安全情景。

- 关于安全情景， 第 215 页
- 多情景模式许可， 第 225 页
- 多情景模式的先决条件， 第 226 页
- 多情景模式准则， 第 226 页
- 多情景模式默认设置， 第 228 页
- 配置多情景， 第 228 页
- 在情景和系统执行空间之间更改， 第 239 页
- 管理安全情景， 第 239 页
- 监控安全情景， 第 243 页
- 多情景模式示例， 第 254 页
- 多情景模式的历史记录， 第 255 页

关于安全情景

您可以将一台ASA设备分区成多个虚拟设备，这些虚拟设备被称为安全情景。每个情景都可以作为独立设备，拥有自己的安全策略、接口和管理员。多情景类似于拥有多台独立设备。有关在多情景模式下不支持的功能，请参阅多情景模式准则， 第 226 页。

本节提供安全情景的概述。

安全情景的公共用途

您可能希望在以下情况下使用多安全情景：

- 您作为运营商，希望向众多客户销售安全服务。通过在ASA上启用多个安全情景，可以实施具有成本效益且节约空间的解决方案，这样不仅可以确保所有客户流量的独立性和安全性，还可以简化配置。
- 您所在的组织是一家大型企业或大学校园，并且希望保持各部门完全分隔。
- 您所在的组织是一家企业，需要为不同部门提供不同的安全策略。

- 您有需要多个 ASA 的网络。

情景配置文件

本部分介绍 ASA 如何实施多情景模式配置。

情景配置

对于每个情景，ASA 都包括一项配置，用于确定安全策略、接口以及可以在独立设备中配置的所有选项。您可以在闪存中存储情景配置，也可以从 TFTP、FTP 或 HTTP(S) 服务器下载情景配置。

系统配置

系统管理员通过在系统配置（与单模式配置类似的启动配置）中配置每个情景配置位置、分配的接口以及其他情景运行参数，从而添加并管理情景。系统配置可标识ASA的基本设置。系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。系统配置中包含一个仅用于故障转移流量的专用故障转移接口。

管理情景配置

管理情景与任何其他情景一样，不同之处在于，当用户登录到管理情景时，该用户将具有系统管理员权限并可访问系统和所有其他情景。管理情景在任何情况下都不受限制，可用作常规情景。但是，由于登录到管理情景会授予用户针对所有情景的管理员权限，因此可能需要将对管理情景的访问限定于适当的用户。管理情景必须位于闪存中，而不是远程位置。

如果您的系统已处于多情景模式下，或者您从单模式进行转换，则管理情景会自动在内部闪存中创建名为 admin.cfg 的文件。此情景名为“admin”。如果您不希望将 admin.cfg 用作管理情景，则可以更改管理情景。

ASA 如何对数据包分类

必须对进入 ASA 的每个数据包进行分类，以便 ASA 能够确定将数据包发送到哪个情景。

注释 如果目标 MAC 地址为组播或广播 MAC 地址，则数据包会复制并传递到每个情景。

有效分类器条件

本节介绍分类器使用的条件。

注释 对于以接口为目标的管理流量，使用接口 IP 地址进行分类。

不使用路由表对数据包进行分类。

唯一接口

如果仅有一个情景与传入接口相关联，则ASA会将数据包分类至该情景。在透明防火墙模式下，要求情景具有唯一接口，因此总是使用此方法对数据包进行分类。

唯一 MAC 地址

如果多情景共享一个接口，则分类器在每个情景中使用分配给该接口的唯一 MAC 地址。上游路由器无法直接路由至不具有唯一MAC地址的情景。您可以启用MAC地址的自动生成。在配置每个接口时，您也可以手动设置 MAC 地址。

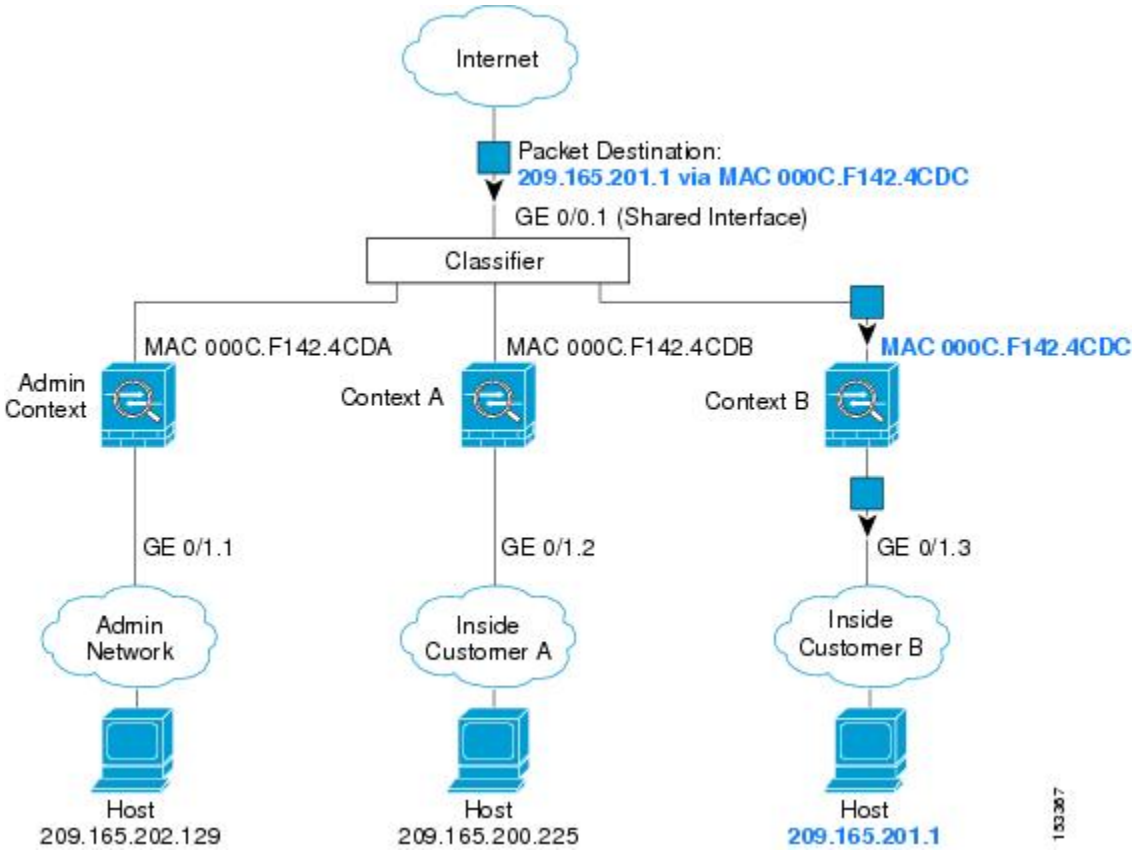
NAT 配置

如果不使用唯一 MAC 地址，ASA 将在您的 NAT 配置中使用映射地址对数据包进行分类。我们建议使用 MAC 地址而不是 NAT，这样，无论 NAT 配置的完整性如何，都可以进行流量分类。

分类示例

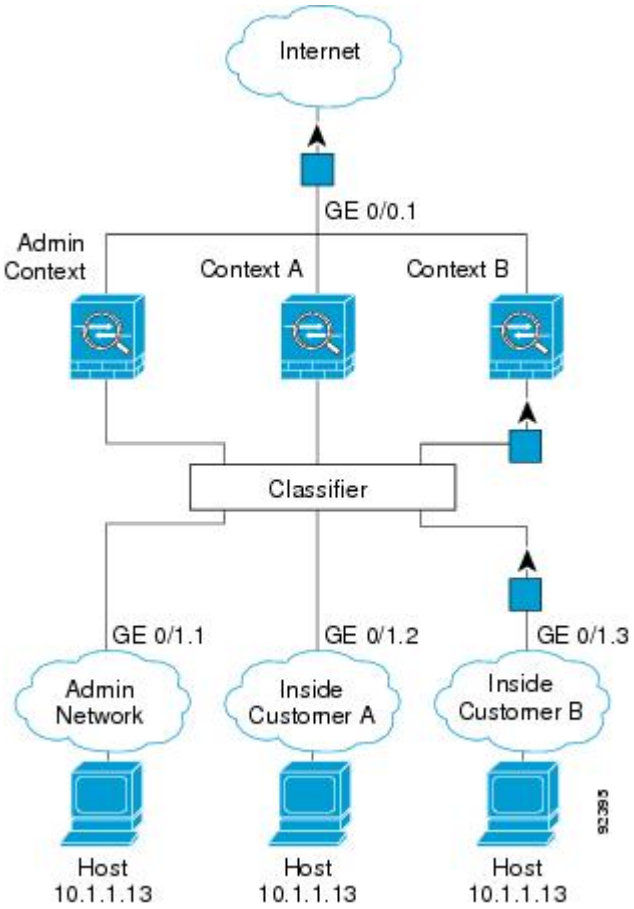
下图显示共享外部接口的多个情景。因为情景 B 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至情景 B。

图 *36:* 使用 ***MAC*** 地址通过共享接口进行数据包分类



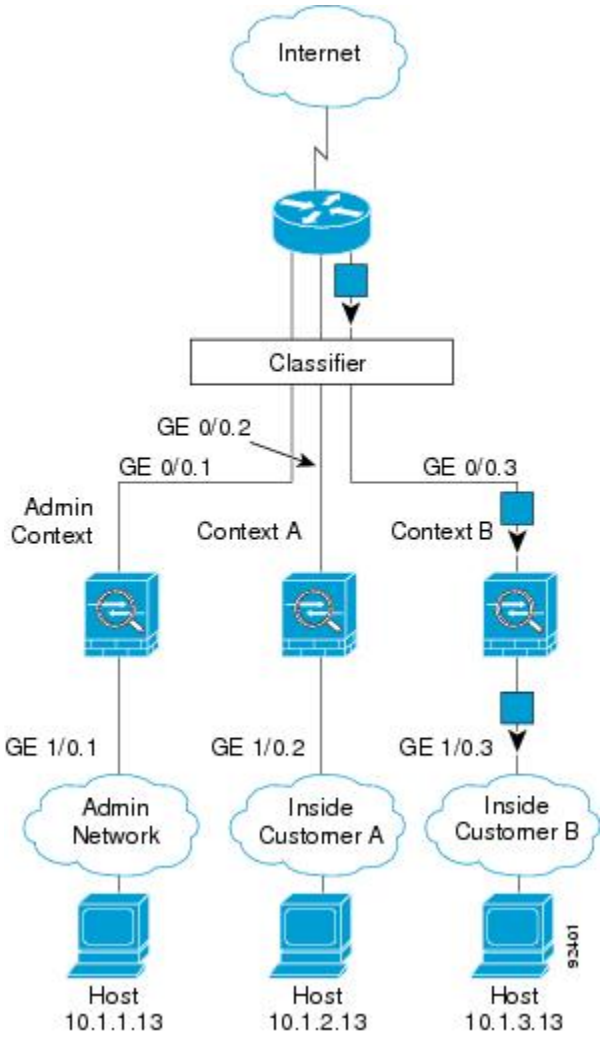
请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。下图展示了情景 B 内部网络上的主机访问互联网。由于传入接口是分配至情景 B 的千兆以太网 0/1.3，因此分类器会将数据包分配至情景 B。

图 *37:* 来自内部网络的传入流量



对于透明防火墙，您必须使用唯一接口。下图展示了来自互联网并以情景 B 内部网络上的主机为目标的数据包。由于传入接口是分配至情景 B 的千兆以太网 1/0.3，因此分类器会将数据包分配至情景 B。

图 *38:* 透明防火墙情景



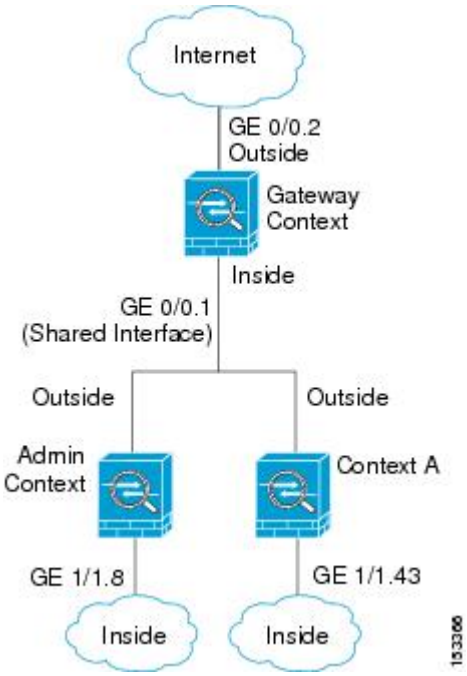
级联安全情景

将一个情景直接置于另一情景之前称为级联情景；一个情景的外部接口与另一个情景的内部接口是同一接口。如果您希望通过在顶级情景中配置共享参数，从而简化某些情景的配置，则可能要使用级联情景。

注释 级联情景要求每个情景接口具有唯一 MAC 地址。由于在不具有 MAC 地址的共享接口上对数据包进行分类存在限制，我们不建议在不具有唯一 MAC 地址的情况下使用级联情景。

下图显示了在网关后有两个情景的网关情景。

图 *39:* 级联情景



对安全情景的管理访问

ASA 提供了多情景模式下的系统管理员访问以及面向单个情景管理员的访问。

系统管理员访问

您可以通过两种方式以系统管理员身份访问 ASA：

- 访问 ASA 控制台。

  您可以从控制台访问系统执行空间，这意味着您输入的所有命令仅会影响系统配置或系统的运行（对于运行时命令而言）。

- 使用 Telnet、SSH 或 ASDM 访问管理情景。

作为系统管理员，您可以访问所有情景。

系统执行空间不支持任何 AAA 命令，但是，您可以在本地数据库中配置其自己的启用密码及用户名，以便提供单独的登录。

情景管理员访问

您可以使用 Telnet、SSH 或 ASDM 来访问情景。如果您登录到一个非管理情景，则只能访问该情景的配置。您可以提供该情景的单独登录。

管理接口使用情况

管理接口是一个仅用于管理流量的独立接口。

在路由防火墙模式下，您可以在所有情景中共享管理接口。

在透明防火墙模式下，管理接口是特殊的。除了允许的最大通过流量接口之外，您还可以将管理接口用作单独的仅管理接口。然而，在多情景模式下，您无法跨情景共享任何接口。您可以改为使用管理接口的子接口，并为每个情景分配一个子接口。但是，只有 Firepower 设备型号 允许管理接口上的子接口。ASA 5585-X，必须使用数据接口或数据接口的子接口，并将其添加到情景中的桥接组。

对于 Firepower 4100/9300 机箱 透明情景，管理接口和子接口都不会保留其特殊状态。在这种情况下，必须将其视为数据接口，并将其添加到桥接组。（请注意，在单情景模式下，管理接口会保留其特殊状态。）

有关透明模式的另一个注意事项：当您启用多情景模式时，所有配置的接口都会自动分配到管理情景。例如，如果您的默认配置包括管理接口，则该接口将分配给管理情景。一个选项是让主接口分配给管理情景，并使用本地 VLAN 对其进行管理，然后使用子接口管理每个情景。请记住，如果将管理情景设为透明，其 IP 地址将被删除；您必须将其分配给网桥组，并将 IP 地址分配给 BVI。

关于资源管理

默认情况下，除非为每个情景强制设置了最大限制，否则所有安全情景对ASA资源的访问都是不受限制的；但VPN资源是唯一一种例外情况，这些资源默认是禁用的。例如，如果您发现一个或者多个情景使用了过多资源，并且导致其他情景出现拒绝连接的情况，则您可以配置资源管理来限制每个情景对资源的使用。对于 VPN 资源，您必须将资源管理配置为允许任何 VPN 隧道。

资源类

ASA 通过向资源类分配情景来管理资源。每个情景使用由类设置的资源限制。要使用某个类的设置，请在定义情景时向该类分配情景。所有未分配给其他类的情景都属于默认类；您不必主动向默认类分配情景。只能将情景分配给一个资源类。此规则的例外是，在成员类中未定义的限制继承自默认类；因此，一个情景实际可能是默认类和另一个类的成员。

资源限制

您可以将单一资源的限制设置为百分比（如果存在硬性系统限制）或绝对值。

对于大多数资源，ASA 不会为分配至该类的每个情景预留部分资源，而是会由 ASA 为情景设置最大限制。如果您超订用资源或允许某些资源不受限制，则少数情景可能会“用尽”这些资源，从而潜在影响为其他情景提供服务。VPN 资源类型除外，您不能超订用此类资源，因此，分配给每个情景的资源量可以得到保证。为应对 VPN 会话数临时激增超过所分配数量的情况，ASA 会支持“突发”VPN 资源类型，其数量等于剩余的未分配 VPN 会话。突发会话可以超订用，并按照先到先得原则供情景使用。

默认类

所有未分配给其他类的情景都属于默认类；您不必主动向默认类分配情景。

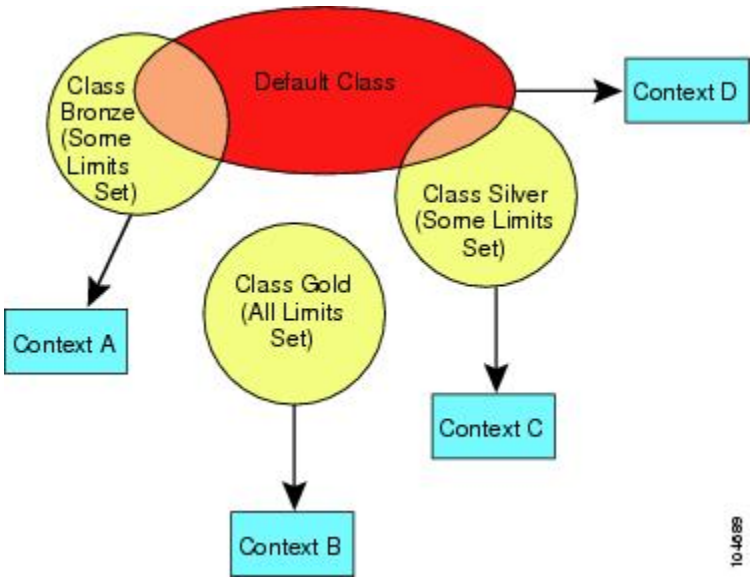
如果某个情景属于除默认类以外的类，则其类设置始终覆盖默认类设置。但是，如果另一个类具有任何未定义的设置，则成员情景为这些限制使用默认类。例如，如果创建的类对所有并发连接具有2%的限制，但没有任何其他限制，则所有其他限制都继承自默认类。相反，如果创建对所有资源都有限制的类，则该类不使用默认类中的任何设置。

对于大多数资源，默认类会为所有情景提供无限制的资源访问，但以下限制除外：

- Telnet 会话 - 5 个会话。（每个情景的最大值。）
- SSH 会话 - 5 个会话。（每个情景的最大值。）
- ASDM 会话 - 5 个会话。（每个情景的最大值。）
- MAC 地址 -（因型号而异）。（系统最大值。）
- Secure Client 对等体- 0 个会话。（您必须将该类手动配置为允许任何 Secure Client 对等体。）
- VPN 站点间隧道 - 0 个会话。（您必须将该类手动配置为允许任何 VPN 会话。）

下图显示了默认类与其他类之间的关系。情景 A 和 C 属于设置了某些限制的类；其他限制继承自默认类。情景 B 不会从默认类继承任何限制，因为所有限制都在其类（Gold 类）中进行设置。情景 D 未分配给某个类，因此会默认成为默认类的成员。

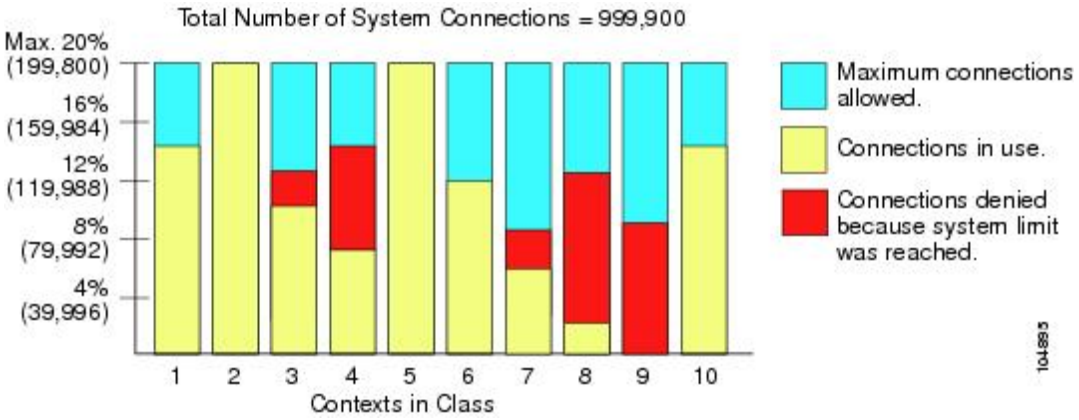
图 *40:* 资源类



使用超订用资源

您可以通过在所有情景范围内分配超过 100% 的资源（非突发 VPN 资源除外）来超订用 ASA。例如，您可以设置 Bronze 类，以便将连接限制为每个情景 20%，然后将 10 个情景分配给该类（总计 200%）。如果情景并发使用超过系统限制，则每个情景获得的数量少于您希望设置的 20%。

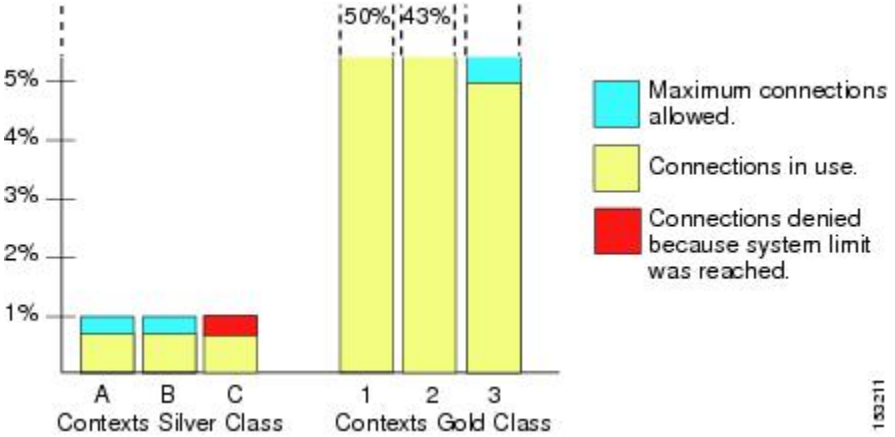
图 *41:* 资源超订用



使用不受限制的资源

通过 ASA，您可以分配对类中一个或多个资源的不受限制访问权限，而不是只分配一定的百分比或是一个绝对的数字。当资源不受限制时，情景可以使用系统可提供的所有资源。例如，情景 A、B 和 C 属于 Silver 类，该类限制每个类成员可使用 1% 的连接（总计 3%）；但是，三个情景当前仅在使用共计 2% 的连接。Gold 类不限制对连接的访问。Gold 类中的情景可使用超过 97% 的“未分配”连接；它们还可以使用情景 A、B 和 C 当前未使用的 1% 的连接，即使这意味着情景 A、B 和 C 无法达到其 3% 的合并限制。设置不受限制的访问权限类似于超额订用 ASA，只是对您超额订用系统的量不太好控制。

图 *42:* 不受限制的资源



关于 **MAC** 地址

您可以手动分配 MAC 地址以覆盖默认值。对于多情景模式，您可以自动生成唯一的 MAC 地址（适用于分配给情景的所有接口）和单情景模式（适用于子接口）。.

注释 您可能想要为 ASA 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。

多情景模式下的 MAC 地址

MAC 地址用于在情景中对数据包进行分类。如果您共享某个接口，但在每个情景中没有该接口的唯一 MAC 地址，则可尝试可能不会提供完全覆盖的其他分类方法。

为了允许情景共享接口，您应该为每个共享情景接口启用自动生成虚拟 MAC 地址的功能。

自动 MAC 地址

在多情景模式下，自动生成会为分配给情景的所有接口分配唯一的 MAC 地址。

如果您手动分配 MAC 地址，并且同时启用自动生成，则会使用手动分配的 MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址（如果已启用）。

在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，您可以为接口手动设置 MAC 地址。

由于自动生成的地址（使用前缀时）以 A2 开头，因此如果您同时希望使用自动生成，则不能使用以 A2 开头的手动 MAC 地址。

ASA 使用以下格式生成 MAC 地址：

A2*xx.yyzz.zzzz*

其中，*xx.yy* 是用户定义的前缀或根据接口 MAC 地址的最后两个字节自动生成的前缀，*zz.zzzz* 是由 ASA 生成的内部计数器。对于备用 MAC 地址，地址完全相同，但内部计数器会加 1。

如何使用前缀的示例如下：如果将前缀设置为 77，则 ASA 会将 77 转换为十六进制值 004D (*yyxx*)。在 MAC 地址中使用时，该前缀会反转 (*xxyy*)，以便与 ASA 的本地形式匹配：

A2**4D.00***zz.zzzz*

对于前缀 1009 (03F1)，MAC 地址为：

A2**F1.03***zz.zzzz*

注释 没有前缀的 MAC 地址格式是旧式版本。有关传统格式的详细信息，请参阅命令参考中的 **mac-address auto** 命令。

VPN 支持

对于 VPN 资源，您必须将资源管理配置为允许任何 VPN 隧道。

您可以在多情景模式下使用站点间 VPN。

对于远程访问 VPN，您必须使用 AnyConnect 3.x 及更高版本的 SSL VPN 和 IKEv2 协议。 您可以按情景自定义用于 Secure Client 映像和定制的闪存，以及跨所有情景使用共享闪存。有关不支持的功能，请参阅多情景模式准则，第 226 页。有关每个 ASA 版本支持的 VPN 功能的详细列表，请参阅多情景模式的历史记录，第 255 页。

注释 多情景模式下需要 Secure Client Premier Apex 许可证；您无法使用默认或传统许可证。

多情景模式许可

型号	许可证要求
Firepower 1010	不支持。
Firepower 1100	基础 许可证：2 个情景。 可选许可证，最多： *Firepower 1120：5* *Firepower 1140：10* *Firepower 1150：25*
Cisco Secure Firewall 1210/1220	不支持。
Cisco Secure Firewall 3100	基础 许可证：2 个情景。 可选许可证，最多： *Cisco Secure Firewall 3105: 100* *Cisco Secure Firewall 3110: 100* *Cisco Secure Firewall 3120: 100* *Cisco Secure Firewall 3130: 100* *Cisco Secure Firewall 3140: 100*
Firepower 4100	基础 许可证：10 个情景。 可选许可证：最多 *250* 个情景。

型号	许可证要求
Cisco Secure Firewall 4200	基础 许可证：2 个情景。 可选许可证，最多： *Cisco Secure Firewall 4215: 250* *Cisco Secure Firewall 4225: 250* *Cisco Secure Firewall 4245: 250*
Firepower 9300	基础 许可证：10 个情景。 可选许可证：最多 *250* 个情景。
ISA 3000	不支持。
ASA Virtual	不支持。

注释 如果管理情景仅包含仅管理接口，并且不包括直通流量的任何数据接口，则不计入限制。

注释 多情景模式下需要 Secure Client Premier Apex 许可证；您无法使用默认或传统许可证。

多情景模式的先决条件

在进入多情景模式后，请连接到系统或管理情景，以便访问系统配置。不能在非管理情景配置系统。默认情况下，在启用多情景模式之后，可以使用默认管理 IP 地址连接到管理情景。

多情景模式准则

故障转移

仅在多情景模式下支持主用/主用模式故障转移。

IPv6

跨情景 IPv6 路由不受支持。

不支持的功能

多情景模式不支持以下功能：

- RIP

- OSPFv3。（支持 OSPFv2。）
- 组播路由
- 威胁检测
- 统一通信
- QoS
- 虚拟隧道接口 (VTI)
- 静态路由跟踪

多情景模式当前不支持远程访问 VPN 的以下功能：

- AnyConnect 2.x 及更低版本
- IKEv1
- SAML
- WebLaunch
- VLAN Mapping
- HostScan
- VPN 负载均衡
- 可以定制
- L2TP

其他准则

- 情景模式（单情景或多情景）不会存储在配置文件中，即使该模式经过重新启动也是如此。如果您需要将配置复制到另一台设备，请将新设备设置为匹配的模式。
- 如果将情景配置存储在闪存的根目录中，则在某些型号上可能会用尽该目录中的空间，即使有可用内存也是如此。在这种情况下，请为配置文件创建子目录。背景：某些型号使用 FAT 16 文件系统的内部闪存，并且，如果您未使用兼容 8.3 格式的短名称，或使用大写字符，则只能存储少于 512 个的文件和文件夹，因为文件系统会用尽所有插槽来存储长文件名（请参阅 http://support.microsoft.com/kb/120138/en-us）。
- 在 ACI 中，使用所有枝叶上的相同 MAC 地址执行基于策略的重定向 (PBR) 运行状况检查（L2 ping）。这会导致 MAC 摆动。要解决 MAC 摆动问题，可以在内联集上配置分流模式选项。但是，如果 威胁防御 配置了高可用性，则必须在故障转移期间启用 MAC 获知以进行连接处理。因此，在 威胁防御 使用内联集接口的高可用性对的 ACI 环境中，为避免丢包，请在独立或集群中部署 威胁防御 。

多情景模式默认设置

- 默认情况下，ASA 处于单情景模式下。
- 请参阅默认类，第 221 页。

配置多情景

过程

步骤 1 启用或禁用多情景模式，第 228 页。

步骤 2 （可选）配置用于资源管理的类，第 230 页。

注释
要支持 VPN，必须在资源类中配置 VPN 资源；默认类不允许使用 VPN。

步骤 3 在系统执行空间中配置接口。

- Firepower 1100、Cisco Secure Firewall 3100/4200—基本接口配置，第 659 页。
- Firepower 4100/9300-逻辑设备 Firepower 4100/9300，第 167 页

步骤 4 配置安全情景，第 234 页。

步骤 5 （可选）自动为情景接口分配 MAC 地址，第 238 页。

步骤 6 完成情景中的接口配置。请参阅路由模式接口和透明模式接口，第 749 页。

启用或禁用多情景模式

根据您从思科订购 ASA 的方式，您的 ASA 可能以针对多个安全情景进行了配置。如果您需要从单模式转换为多模式，请遵循本节中的程序。

启用多情景模式

当您从单模式转换为多模式时，ASA 会将运行配置转换为两个文件：一个是包含系统配置的新启动配置，另一个是包含管理情景的 admin.cfg（位于内部闪存的根目录中）。原始运行配置另存为 old_running.cfg（位于内部闪存的根目录中）。系统不会保存原始启动配置。ASA 自动向系统配置中添加一个管理情景的条目，名称为“admin”。

开始之前

如果启动配置与运行配置不同，请备份启动配置。当您从单模式转换为多模式时，ASA 会将运行配置转换为两个文件。系统不会保存原始启动配置。请参阅备份和恢复配置或其他文件，第 1305 页。

过程

切换到多情景模式。

mode multiple

示例：

系统将提示您更改模式并转换配置，然后系统将会重新加载。

注释
您必须在管理情景中重新生成 RSA 密钥对，才能重新建立 SSH 连接。在控制台中，输入 **crypto key generate rsa modulus** 命令。有关详细信息，请参阅 配置 SSH 访问，第 1237 页。

示例：

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

Converting the configuration - this may take several minutes for a large configuration

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple
ciscoasa(config)#


***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   change mode
Shutting down isakmp
Shutting down webvpn
Shutting down License Controller
Shutting down File system



***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
```

```
***   change mode
```

恢复单情景模式

要将旧运行配置复制到启动配置，并将模式切换到单情景模式，请执行以下步骤：

开始之前

在系统执行空间中执行此程序。

过程

步骤 1 将原始运行配置的备份版本复制到当前启动配置：

copy disk0:old_running.cfg startup-config

示例：

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

步骤 2 将模式设置为单模式：

mode single

示例：

```
ciscoasa(config)# mode single
```

系统将提示您重新启动 ASA。

配置用于资源管理的类

要在系统配置中配置某个类，请执行下述步骤。您可以通过重新输入带有新值的命令来更改特定资源限制的值。

开始之前

- 在系统执行空间中执行此程序。
- 下表列出了资源类型和限制。另请参阅 **show resource types** 命令。

注释 如果系统限制为“不适用”，则无法设置该资源的百分比，因为该资源不存在硬性系统限制。

表 7: 资源名称和限制

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制	说明
asdm	并发	1（最小值） 5（最大值）	200	ASDM 管理会话。 ASDM 会话使用两个 HTTPS 连接：一个用于监控（始终存在），另一个用于进行配置更改（仅当进行更改时才存在）。例如，系统限制为 200 个 ASDM 会话表示 HTTPS 会话数限制为 400 。
conns	并发或速率	不适用	并发连接数：有关适用于您的型号的连接限制，请参阅每个型号的许可证，第 139 页。 速率：不适用	任意两台主机之间的 TCP 或 UDP 连接数，包括一台主机和多台其他主机之间的连接。 **注释** 对于值小于 xlates 或 conns 的任一限制，会生成相应的系统日志消息。例如，如果将 xlates 限制设置为 7 并将 conns 限制设置为 9，则 ASA 仅会生成系统日志消息 321001（“Resource 'xlates' limit of 7 reached for context 'ctx1'”），而不会生成 321002（“Resource 'conn rate' limit of 5 reached for context 'ctx1'”）。
主机	并发	不适用	不适用	可以通过 ASA 连接的主机数。
inspects	Rate	不适用	不适用	每秒应用检测数。
mac-addresses	并发	不适用	（因型号而异）	对于透明防火墙模式，表示 MAC 地址表中允许的 MAC 地址数量。
路由	并发	不适用	不适用	动态路由数。

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制	说明
vpn burst anyconnect	并发	不适用	您型号的 Secure Client 高级对等体数减去为 **vpn anyconnect** 向所有情景分配的会话总和。	所允许的 Secure Client 会话数超过了分配到某一包含 **vpn anyconnect** 的情景的会话数。例如，如果您的型号支持 5000 个对等体，而您为包含 **vpn anyconnect** 的所有情景共分配了 4000 个对等体，则剩余 1000 个对等体可用于 **vpn burst anyconnect**。不同于能保证情景会话的 **vpn anyconnect**，**vpn burst anyconnect** 有可能被超订用；突发池将根据先到先得的原则可用于所有情景。
vpn anyconnect	并发	不适用	有关适用于您的型号的 Secure Client 高级对等体数的信息，请参阅每个型号的许可证，第 139 页。	Secure Client 对等体。不能超订用此资源；所有情景分配的总和不得超过型号限制。为此资源分配的对等体数保证可供相应情景使用。
vpn burst other	并发	不适用	您型号的其他 VPN 会话数量减去为**vpn other** 向所有情景分配的会话总和。	所允许的站点间 VPN 会话数超过了分配到某一包含 **vpn other** 的情景的会话数。例如，如果您的产品型号支持 5000 个会话，您为具有 **vpn other** 的所有情景分配了 4000 个会话，其余 1000 个会话可用于 **vpn burst other**。不同于能保证情景会话的**vpn other**，**vpn burst other** 有可能被超订用；突发池将根据先到先得的原则可用于所有情景。
vpn other	并发	不适用	有关适用于您的型号的其他 VPN 会话数的信息，请参阅每个型号支持的功能许可证，第 62 页。	站点间 VPN 会话数。不能超订用此资源；所有情景分配的总和不得超过型号限制。为此资源分配的会话数保证可供相应情景使用。
ikev1 in-negotiation	并发（仅百分比）	不适用	分配到此情景的其他 VPN 会话的百分比。请参阅 **vpn other** 资源，为情景分配会话。	传入 IKEv1 SA 协商，占情景其他 VPN 限制的百分比。
ssh	并发	1（最小值） 5（最大值）	100	SSH 会话数。

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制	说明
storage	MB	最大值取决于您指定的闪存驱动器	最大值取决于您指定的闪存驱动器	情景目录的存储限制 (MB)。使用 **storage-url** 命令指定驱动器。
syslogs	Rate	不适用	不适用	每秒系统日志消息数。
telnet	并发	1（最小值） 5（最大值）	100	Telnet 会话数。
xlates	并发	不适用	不适用	网络地址转换数。

过程

步骤 1 指定类名并进入类配置模式：

class *name*

示例：

```
ciscoasa(config)# class gold
```

name 是最大长度为 20 个字符的字符串。要设置默认类的限制，请输入 **default** 作为名称。

步骤 2 设置资源类型的资源限制：

limit-resource [**rate**] *resource_name number*[**%**]

示例：

```
ciscoasa(config-class)# limit-resource rate inspects 10
```

- 有关资源类型列表，请参阅前面的表。如果指定 **all**，则会将所有资源都配置为相同的值。如果还指定了特定资源的值，则该限制会覆盖为 **all** 设置的限制。
- 输入 **rate** 参数以设置特定资源的每秒速率。
- 对于大多数资源，请将 *number* 指定为 **0**，从而将资源设置为不受限制或使用系统限制（如果适用）。对于 VPN 资源，**0** 表示将限制设置为无。
- 对于没有系统限制的资源，不能设置百分比 (**%**)；只能设置绝对值。
- 如果您还在情景中设置 **quota management-session** 命令以设置最大管理会话数（SSH 等），则将使用较小的值。

示例

例如，要将默认类的连接数限制设置为 10% 而非不受限制，并允许使用 5 个站点间 VPN 隧道（其中两个隧道预留用于 VPN 突发），请输入以下命令：

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 5
ciscoasa(config-class)# limit-resource vpn burst other 2
```

所有其他资源保持不受限制。

要添加名为 gold 的类，请输入以下命令：

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5
```

为情景配置了资源类时，会进行检查。如果在尝试 VPN 远程访问连接之前未安装适当的许可证，会生成安装警告。然后，管理员必须获取 Secure Client Premier 许可证。例如，可能显示如下警告：

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn anyconnect 10.0%
ciscoasa(config-class)# context test
Creating context 'text'...Done. (3)
ciscoasa(config-ctx)# member vpn
WARNING: Multi-mode remote access VPN support requires an AnyConnect Apex license.
Warning: An Access Context license is required for remote-access VPN support in multi-mode.
ciscoasa(config-ctx)#
```

配置安全情景

系统配置中的安全情景定义确定情景名称、配置文件 URL、情景可使用的接口以及其他设置。

开始之前

- 在系统执行空间中执行此程序。
- 配置接口。对于透明模式情景，您无法在情景之间共享接口，因此您可能需要使用子接口。要计划管理接口使用，请参阅 管理接口使用情况，第 221 页。
  - Firepower 1100、Cisco Secure Firewall 3100/4200—基本接口配置，第 659 页。

- Firepower 4100/9300-逻辑设备 Firepower 4100/9300 ，第 167 页

- 如果您没有管理情景（例如，如果清除了配置），则必须先通过输入以下命令指定管理情景名称：

```
ciscoasa(config)# admin-context name
```

虽然此情景在配置中尚不存在，但是可以随后输入 **context** *name* 命令来继续进行管理情景配置。

过程

步骤 1 添加或修改情景：

context *name*

示例：

```
ciscoasa(config)# context admin
```

name 是最大长度为 32 个字符的字符串。此名称区分大小写，因此您可以具有名为“customerA”和“CustomerA”的两个情景。您可以使用字母、数字或连字符，但名称不能以连字符开头或结尾。

注释
“System”或“Null”（采用大写或小写字母）是保留名称，因此不能使用。

步骤 2 （可选） 为此情景添加描述：

description 文本、

示例：

```
ciscoasa(config-ctx)# description Admin Context
```

步骤 3 指定您可以在此情景中使用的接口：

要分配接口，请执行以下操作：

allocate-interface *interface_id* [*mapped_name*] [**visible** | **invisible**]

要分配一个或多个子接口，请执行以下操作：

allocate-interface *interface_id.subinterface* [*-interface_id.subinterface*] [*mapped_name*[*-mapped_name*]] [**visible** | **invisible**]

示例：

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

注释
请勿在接口类型和端口号之间包含空格。

- 多次输入这些命令可指定不同的范围。如果使用此命令的**no**形式删除某项分配，则包括此接口的所有情景命令都将从运行的配置中删除。
- 如果需要，可以在路由模式下将相同接口分配给多情景。透明模式不允许使用共享接口。
- *Mapped_name* 是可在情景中使用的接口的字母数字别名，而不是接口 ID。如果不指定映射名称，则会在情景中使用接口 ID。出于安全目的，您可能不希望情景管理员知道情景使用的是哪些接口。映射名称必须以字母开头，以字母或数字结尾，并且内部字符只能是字母、数字或下划线。例如，您可以使用以下名称：**int0**、**inta**、**int_0**。
- 如果指定子接口的范围，则可以指定匹配的映射名称的范围。关于范围，请遵循以下准则：
  - 映射名称必须由后跟数字部分的字母部分组成。映射名称的字母部分必须与范围的两端均匹配。例如，可输入以下范围：**int0-int10**。例如，如果输入 gig0/1.1-gig0/1.5 **happy**1-**sad**5，则命令会失败。
  - 映射名称的数字部分必须与子接口范围包含相同的数字数量。例如，两个范围都包括 100 个接口：**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100**。例如，如果输入 gig0/0.**100**-gig0/0.**199** int**1**-int**15**，则命令会失败。
- 如果设置了映射的名称，则指定 **visible** 可在 **show interface** 命令中查看实际接口 ID。默认关键字 **invisible** 仅显示映射的名称。

步骤 4 标识系统从其下载情景配置的 URL。

config-url *url*

示例：

```
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
```

步骤 5 （可选） 允许每个情景使用闪存来存储 VPN 数据包（例如 Secure Client）以及为 Secure Client 和无客户端 SSL VPN 门户自定义提供存储。例如，如果使用多个情景模式来配置具有动态访问策略的 Secure Client 配置文件，则必须计划特定于情景的专用存储。每个情景可使用私有存储空间以及共享的只读存储空间。**注意**：请使用 **mkdir** 命令确保目标目录已存在于指定磁盘中。

storage-url {**private** | **shared**} [**disk***n***:/**]*path* [*context_label*]

示例：

```
ciscoasa(config)# mkdir disk1:/private-storage
ciscoasa(config)# mkdir disk1:/shared-storage
ciscoasa(config)# context admin
ciscoasa(config-ctx)# storage-url private disk1:/private-storage context
ciscoasa(config-ctx)# storage-url shared disk1:/shared-storage shared
```

您可以为每个情景指定一个**private**存储空间。您可以从情景中的此目录（以及从系统执行空间）执行读取/写入/删除操作。如果您不指定磁盘编号，则默认为 disk0。在指定的 *path* 下，ASA 将在情景后创建一个子目录。例如，对于 contextA，如果指定 **disk1:/private-storage** 作为路径，则 ASA 会在

disk1:/private-storage/contextA/ 为此情景创建一个子目录。或者，您也可以使用 *context_label* 在情景内为路径命名，这样文件系统不会暴露给情景管理员。例如，如果指定 *context_label* 作为 **context**，则此目录将在情景内称为 **context:**。要控制每个情景允许的磁盘空间量，请参阅配置用于资源管理的类，第 230 页。

您可以对每个情景指定一个只读**shared**存储空间，但可以创建多个共享目录。为了减少可以在所有情景之间共享的大型公共文件的副本，例如 Secure Client 包，可以使用共享存储空间。ASA 不会为此存储空间创建情景子目录，因为该存储空间是多个情景的共享空间。只有系统执行空间可以从共享目录写入和删除。

步骤 6 （可选） 将情景分配给资源类：

member *class_name*

示例：

```
ciscoasa(config-ctx)# member gold
```

如果不指定类，则情景属于默认类。只能将情景分配给一个资源类。

步骤 7 （可选） 将情景分配给主用/主用故障转移中的故障转移组：

join-failover-group {**1** | **2**}

示例：

```
ciscoasa(config-ctx)# join-failover-group 2
```

默认情况下，情景处于组 1 中。管理情景必须始终处于组 1 中。

步骤 8 （可选） 为此情景启用云网络安全：

scansafe [**license** *key*]

示例：

```
ciscoasa(config-ctx)# scansafe
```

如果不指定**license**，该情景会使用在系统配置中配置的许可证。ASA 将身份验证密钥发送到云网络安全代理服务器，以指明请求从哪个组织发出。身份验证密钥是一个 16 字节的十六进制数。

有关 ScanSafe 的详细信息，请参阅防火墙配置指南。

示例

以下示例将管理情景设置为“administrator”，在内部闪存中创建一个名为“administrator”的情景，然后从 FTP 服务器添加两个情景：

```
ciscoasa(config)# admin-context admin
ciscoasa(config)# context admin
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
```

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold


ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

自动为情景接口分配 MAC 地址

本节介绍如何配置 MAC 地址的自动生成。MAC 地址用于在情景中对数据包进行分类。

开始之前

- 当在情景中为接口配置 **nameif** 命令时，系统会立即生成新的 MAC 地址。如果在配置情景接口后启用此功能，则在启用之后，会立即为所有接口生成 MAC 地址。如果禁用此功能，则每个接口的 MAC 地址会恢复为默认 MAC 地址。例如，GigabitEthernet0/1 的子接口恢复为使用 GigabitEthernet0/1 的 MAC 地址。
- 在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，您可以在情景中为接口手动设置 MAC 地址。

过程

自动向每个情景接口分配专用 MAC 地址：

mac-address auto [**prefix** *prefix*]

示例：

```
ciscoasa(config)# mac-address auto prefix 19
```

如果未输入前缀，ASA 根据接口 (ASA 5500-X) 的最后两个字节自动生成前缀。

如果您手动输入前缀，则 *prefix* 是介于 0 和 65535 之间的十进制值。此前缀会转换为一个四位数的十六进制数字，并用作 MAC 地址的一部分。

在情景和系统执行空间之间更改

如果您登录到系统执行空间（或管理情景），则可以在情景之间切换，并在每个情景中执行配置和监控任务。您在配置模式下编辑或在 **copy** 或 **write** 命令中使用的运行配置取决于您的位置。当您处于系统执行空间时，运行配置仅包含系统配置；当您处于某个情景时，运行配置仅包含该情景。例如，您无法通过输入 **show running-config** 命令查看所有运行配置（系统配置以及所有情景配置）。系统仅显示当前配置。

过程

步骤 1 切换到情景：

changeto context *name*

提示符切换到 ciscoasa/*name*#

步骤 2 切换到系统执行空间：

changeto system

提示符切换到 ciscoasa#

管理安全情景

本部分介绍如何管理安全情景。

删除安全情景

除非您使用 **clear context** 命令删除所有情景，否则无法删除当前管理情景。

注释 如果使用故障转移，则从主用设备上删除情景到在备用设备上删除该情景之间存在一定延迟。您可能会看到错误消息，表明主用设备和备用设备上的接口数不一致；此错误是临时的，可以忽略。

开始之前

在系统执行空间中执行此程序。

过程

步骤 1 删除单个情景：

no context *name*

此外，还会删除所有情景命令。系统不会从配置 URL 位置中删除情景配置文件。

步骤 2 删除所有情景（包括管理情景）：

clear context

系统不会从配置 URL 位置中删除情景配置文件。

更改管理情景

系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。

管理情景与任何其他情景一样，不同之处在于，当用户登录到管理情景时，该用户将具有系统管理员权限并可访问系统和所有其他情景。管理情景在任何情况下都不受限制，可用作常规情景。但是，由于登录到管理情景会授予用户针对所有情景的管理员权限，因此可能需要将对管理情景的访问限定于适当的用户。

开始之前

- 可以将任何情景设置为管理情景，只要配置文件存储在内部闪存中即可。
- 在系统执行空间中执行此程序。

过程

设置管理情景：

admin-context *context_name*

示例：

```
ciscoasa(config)# admin-context administrator
```

连接到管理情景的所有远程管理会话（如 Telnet、SSH 或 HTTP）都会终止。必须重新连接到新的管理情景。

某些系统配置命令（包括 **ntp server**）会标识属于管理情景的接口名称。如果您更改管理情景，并且新的管理情景中不存在该接口名称，请务必更新引用该接口的所有系统命令。

更改安全情景 URL

本节介绍如何更改情景 URL。

开始之前

- 在没有通过新的 URL 重新加载配置的情况下，不能更改安全情景 URL。ASA 会将新的配置与当前的运行配置合并。
- 重新输入同一 URL 也可将已保存的配置与运行配置合并。
- 合并会将新配置中的所有新命令添加到运行配置中。
  - 如果配置相同，则不会发生任何更改。
  - 如果命令冲突或命令影响情景的运行，则合并的影响取决于命令。可能会发生错误，也可能出现意外结果。如果运行配置为空（例如，如果服务器不可用且从未下载配置），则使用新的配置。
- 如果您不想合并配置，可清除运行配置（该操作通过情景中断所有通信），然后从新的URL重新加载配置。
- 在系统执行空间中执行此程序。

过程

步骤 1 （可选，前提是您不需要执行合并）切换到情景并清除配置：

changeto context *name*

clear configure all

示例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(config)# clear configure all
```

如果要执行合并，请跳至步骤 2。

步骤 2 切换到系统执行空间：

changeto system

示例：

```
ciscoasa/ctx1(config)# changeto system
ciscoasa(config)#
```

步骤 3 进入要更改的情景的情景配置模式。

context *name*

示例：

```
ciscoasa(config)# context ctx1
```

步骤 4 输入新 URL。系统会立即加载情景，以便其正常运行。

config-url *new_url*

示例：

```
ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg
```

重新加载安全情景

您可以通过两种方式重新加载情景：

- 清除运行配置，然后导入启动配置。

  此操作会清除与情景关联的大多数属性，例如，连接和 NAT 表。

- 从系统配置中删除情景。

  此操作会清除其他属性，例如，可能有助于故障排除的内存分配。但是，将情景添加回系统要求重新指定 URL 和接口。

通过清除配置来重新加载

过程

步骤 1 切换到要重新加载的情景：

changeto context *name*

示例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(comfig)#
```

步骤 2 清除运行配置：

clear configure all

此命令会清除所有连接。

步骤 3 重新加载配置：

copy startup-config running-config

示例：

```
ciscoasa/ctx1(config)# copy startup-config running-config
```

ASA 会从系统配置中指定的 URL 中复制配置。不能在情景中更改此 URL。

通过删除和重新添加情景来重新加载

要通过删除情景再重新添加来重新加载情景，请执行以下步骤。

过程

步骤 1 删除安全情景，第 239 页。**同时从磁盘中删除配置 URL 文件**

步骤 2 配置安全情景，第 234 页

监控安全情景

本节介绍如何查看和监控情景信息。

查看情景信息

从系统执行空间中，您可以查看情景列表，包括名称、分配的接口和配置文件 URL。

过程

显示所有情景：

show context [*name* | **detail**| **count**]

如果要显示特定情景的信息，请指定 *name*。

detail 选项用于显示其他信息。有关详细信息，请参阅以下样本输出。

count 选项用于显示情景的总数。

示例

以下是 **show context** 命令的输出示例。以下样本输出显示三个情景：

```
ciscoasa# show context

Context Name      Interfaces                    URL
*admin            GigabitEthernet0/1.100        disk0:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200        disk0:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300        disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

下表显示了每个字段的说明。

表 *8: show context* 字段

字段	说明
Context Name	列出所有情景名称。名称中带有星号 (*) 的情景是管理情景。
Interfaces	分配给情景的接口。
URL	ASA 从中加载情景配置的 URL。

以下是 **show context detail** 命令的输出示例：

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257
```

```
Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

有关 **detail** 输出的详细信息，请参阅命令参考。

以下是 **show context count** 命令的输出示例：

```
ciscoasa# show context count
Total active contexts: 2
```

查看资源分配

从系统执行空间中，您可以查看每种资源跨所有类和类成员的分配情况。

过程

显示资源分配：

show resource allocation [**detail**]

此命令显示资源分配情况，但不显示实际正在使用的资源。有关实际资源使用情况的详细信息，请参阅查看资源使用情况，第 248 页。

detail 参数用于显示其他信息。有关详细信息，请参阅以下样本输出。

示例

以下样本输出以绝对值和可用系统资源百分比的形式，显示每个资源的总分配情况：

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Routes                      5000           N/A
 Telnet                        35           35.00%
 Xlates                     91749           N/A
 AnyConnect                  1000           10%
 AnyConnectBurst              200           2%
 Other VPN Sessions            20           2.66%
 Other VPN Burst               20           2.66%
 All                    unlimited
```

下表显示每个字段的说明。

表 *9: show resource allocation* 字段

字段	说明
Resource	可限制的资源的名称。
Total	跨所有情景分配的资源总量。此数量是每秒的并发实例或实例的绝对数量。如果在类定义中指定了百分比，则 ASA 会在显示该值时将百分比转换为绝对数量。
% of Avail	跨所有情景分配的总系统资源的百分比（如果资源有硬性系统限制）。如果资源没有系统限制，则此列将显示 N/A。

以下是 **show resource allocation detail** 命令的样本输出：

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A

SSH              default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Telnet           default          all       C          5
```

```
                gold                1       D          5          5      5.00%
                silver              1      CA         10         10     10.00%
                bronze              0      CA          5
                All Contexts:       3                             20     20.00%

Routes          default           all       C  unlimited                   N/A
                gold                1       D  unlimited          5       N/A
                silver              1      CA         10         10       N/A
                bronze              0      CA          5                   N/A
                All Contexts:       3                             20       N/A

Xlates          default           all      CA  unlimited
                gold                1      DA  unlimited
                silver              1      CA      23040      23040     N/A
                bronze              0      CA      11520
                All Contexts:       3                         23040     N/A

mac-addresses   default           all       C      65535
                gold                1       D      65535      65535    100.00%
                silver              1      CA       6553       6553      9.99%
                bronze              0      CA       3276
                All Contexts:       3                        137623    209.99%
```

下表显示每个字段的说明。

表 *10: show resource allocation detail* 字段

字段	说明
Resource	可限制的资源的名称。
Class	每个类（包括默认类）的名称。 All contexts 字段显示所有类的全部值。
Mmbrs	分配给每个类的情景数量。
Origin	资源限制的源，如下所示： • A - 使用 **all** 选项设置此限制，而不是将其设置为单独资源。 • C - 此限制派生自成员类。 • D - 此限制未在成员类中定义，而是派生自默认类。对于分配给默认类的情景，值将会是“C”而不是“D”。 ASA 可以将“A”和“C”或“D”结合使用。
Limit	每个情景的资源限制，显示为绝对数量。如果在类定义中指定了百分比，则ASA会在显示该值时将百分比转换为绝对数量。
Total	跨类中的所有情景分配的资源总量。此数量是每秒的并发实例或实例的绝对数量。如果资源不受限制，则显示为空白。
% of Avail	跨类中的所有情景分配的总系统资源的百分比。如果资源不受限制，则显示为空白。如果资源没有系统限制，则此列将显示 N/A。

查看资源使用情况

从系统执行空间中，您可以查看每个情景的资源使用情况，并显示系统资源使用情况。

过程

查看每个情景的资源使用情况：

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**] [**resource** {*resource_name* | **all**} | **detail**] [**counter** *counter_name* [*count_threshold*]]

- 默认情况下，系统会显示**所有**情景的使用情况；每个情景会单独列出。
- 输入 **top** *n* 关键字可显示对指定资源的使用排名前 *n* 的用户的情景。对于此选项，必须指定单个资源类型，而不能指定 **resource all**。
- **summary** 选项用于显示所有情景的综合使用情况。
- **system** 选项用于显示所有情景的综合使用情况，但显示的是资源的系统限制，而不是综合情景限制。
- 对于 **resource** *resource_name*，请参阅配置用于资源管理的类，第 230 页以获取可用资源名称。另请参阅 **show resource type** 命令。指定 **all**（默认值）表示所有类型。
- **detail** 选项用于显示所有资源的资源使用情况，包括无法管理的那些资源。例如，可以查看 TCP 拦截次数。
- **counter** *counter_name* 是以下关键字之一：
  - **current** - 显示活动并发实例数或资源的当前使用率。
  - **denied** - 显示由于超过 Limit 列中所示的资源限制而被拒绝的实例的数量。
  - **peak** - 显示自上一次清除统计信息（使用 **clear resource usage** 命令或由于设备重启）以来，峰值并发实例数或资源的峰值使用率。
  - **all** -（默认）显示所有统计信息。
- *count_threshold* 设置一个数值，如果超过此数值，则会显示资源。默认值为 1。如果资源的使用率低于所设置的数字，则不会显示资源。如果为计数器名称指定 **all**，则 *count_threshold* 适用于当前使用情况。
- 要显示所有资源，请将 *count_threshold* 设置为 **0**。

示例

以下是 **show resource usage context** 命令的样本输出，其中显示管理情景的资源使用情况：

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

以下是 **show resource usage summary** 命令的样本输出，其中显示所有情景和所有资源的资源使用情况。以下样本显示 6 个情景的限制。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      N/A            0 Summary
Conns                     584          763      280000(S)      0 Summary
Xlates                   8526         8966      N/A            0 Summary
Hosts                     254          254      N/A            0 Summary
Conns [rate]              270          535      N/A         1704 Summary
Inspects [rate]           270          535      N/A            0 Summary
AnyConnect                  2           25      1000           0 Summary
AnyConnectBurst             0            0      200            0 Summary
Other VPN Sessions          0           10      10           740 Summary
Other VPN Burst             0           10      10           730 Summary

S = System: Combined context limits exceed the system limit; the system limit is shown.
```

以下是 **show resource usage summary** 命令的样本输出，其中显示 25 种情景的限制：由于 Telnet 和 SSH 连接的情景限制是每个情景 5 个连接，因此总共限制为 125 个连接。系统限制仅为 100 个链接，因此会显示系统限制。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit    Denied   Context
Telnet                      1            1        100[S]      0   Summary
SSH                         2            2        100[S]      0   Summary
Conns                      56           90        130000(S)   0   Summary
Hosts                      89          102        N/A         0   Summary
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

以下内容是 **show resource usage system** 命令的样本输出，其中显示所有情景的资源使用情况，但是该命令显示的是系统限制，而不是综合情景限制。**counter all 0** 选项用于显示当前未使用的资源。Denied statistics 显示由于系统限制而拒绝资源的次数，如适用。

```
ciscoasa# show resource usage system counter all 0

Resource              Current         Peak      Limit          Denied    Context
Telnet                      0            0        100                0    System
SSH                         0            0        100                0    System
ASDM                        0            0         32                0    System
Routes                      0            0        N/A                0    System
IPSec                       0            0          5                0    System
Syslogs [rate]              1           18        N/A                0    System
Conns                       0            1     280000                0    System
Xlates                      0            0        N/A                0    System
Hosts                       0            2        N/A                0    System
Conns [rate]                1            1        N/A                0    System
```

```
Inspects [rate]              0           0        N/A             0    System
AnyConnect                   2          25      10000             0    System
AnyConnectBurst              0           0        200             0    System
Other VPN Sessions           0          10        750           740    System
Other VPN Burst              0          10        750           730    System
```

监控情景中的 SYN 攻击

ASA 使用 TCP 拦截防止 SYN 攻击。TCP 拦截使用 SYN cookie 算法防范 TCP SYN 泛洪攻击。SYN 泛洪攻击包含一系列通常源于欺骗性 IP 地址的 SYN 数据包。SYN 数据包的持续泛滥使服务器 SYN 队列始终保持充满状态，致使其无法处理连接请求。当超过初期连接阈值时，ASA 会充当服务器代理，并生成对客户端 SYN 请求的 SYN-ACK 响应。当 ASA 收到来自客户端的 ACK 后，即可对客户端进行身份验证，并且允许连接到服务器。

过程

步骤 1 监控各个情景的攻击速率：

show perfmon

步骤 2 监控 TCP 拦截对于各个情景使用的资源量：

show resource usage detail

步骤 3 监控 TCP 拦截对于整个系统使用的资源量：

show resource usage summary detail

示例

以下是 **show perfmon** 命令的样本输出，其中显示名为 admin 的情景的 TCP 拦截速率。

```
ciscoasa/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

```
TCP Intercept    322779/s      322779/s
```

以下是 **show resource usage detail** 命令的样本输出，其中显示 TCP 拦截对各个情景使用的资源量。（ **粗体**形式的样本文本显示 TCP 拦截信息。）

```
ciscoasa(config)# show resource usage detail
Resource              Current         Peak      Limit        Denied Context
memory                 843732       847288  unlimited             0 admin
chunk:channels             14           15  unlimited             0 admin
chunk:fixup                15           15  unlimited             0 admin
chunk:hole                  1            1  unlimited             0 admin
chunk:ip-users             10           10  unlimited             0 admin
chunk:list-elem            21           21  unlimited             0 admin
chunk:list-hdr              3            4  unlimited             0 admin
chunk:route                 2            2  unlimited             0 admin
chunk:static                1            1  unlimited             0 admin
tcp-intercepts         328787       803610  unlimited             0 admin
np-statics                  3            3  unlimited             0 admin
statics                     1            1  unlimited             0 admin
ace-rules                   1            1  unlimited             0 admin
console-access-rul          2            2  unlimited             0 admin
fixup-rules                14           15  unlimited             0 admin
memory                 959872       960000  unlimited             0 c1
chunk:channels             15           16  unlimited             0 c1
chunk:dbgtrace              1            1  unlimited             0 c1
chunk:fixup                15           15  unlimited             0 c1
chunk:global                1            1  unlimited             0 c1
chunk:hole                  2            2  unlimited             0 c1
chunk:ip-users             10           10  unlimited             0 c1
chunk:udp-ctrl-blk          1            1  unlimited             0 c1
chunk:list-elem            24           24  unlimited             0 c1
chunk:list-hdr              5            6  unlimited             0 c1
chunk:nat                   1            1  unlimited             0 c1
chunk:route                 2            2  unlimited             0 c1
chunk:static                1            1  unlimited             0 c1
tcp-intercept-rate      16056        16254  unlimited             0 c1
globals                     1            1  unlimited             0 c1
np-statics                  3            3  unlimited             0 c1
statics                     1            1  unlimited             0 c1
nats                        1            1  unlimited             0 c1
ace-rules                   2            2  unlimited             0 c1
console-access-rul          2            2  unlimited             0 c1
fixup-rules                14           15  unlimited             0 c1
memory              232695716    232020648  unlimited             0 system
chunk:channels             17           20  unlimited             0 system
chunk:dbgtrace              3            3  unlimited             0 system
chunk:fixup                15           15  unlimited             0 system
chunk:ip-users              4            4  unlimited             0 system
chunk:list-elem          1014         1014  unlimited             0 system
chunk:list-hdr              1            1  unlimited             0 system
chunk:route                 1            1  unlimited             0 system
block:16384               510          885  unlimited             0 system
block:2048                 32           34  unlimited             0 system
```

以下样本输出显示 TCP 拦截对整个系统使用的资源量。（**粗体**形式的样本文本显示 TCP 拦截信息。）

```
ciscoasa(config)# show resource usage summary detail
Resource              Current         Peak      Limit        Denied Context
memory              238421312    238434336  unlimited             0 Summary
```

```
chunk:channels              46          48  unlimited            0 Summary
chunk:dbgtrace               4           4  unlimited            0 Summary
chunk:fixup                 45          45  unlimited            0 Summary
chunk:global                 1           1  unlimited            0 Summary
chunk:hole                   3           3  unlimited            0 Summary
chunk:ip-users              24          24  unlimited            0 Summary
chunk:udp-ctrl-blk           1           1  unlimited            0 Summary
chunk:list-elem           1059        1059  unlimited            0 Summary
chunk:list-hdr              10          11  unlimited            0 Summary
chunk:nat                    1           1  unlimited            0 Summary
chunk:route                  5           5  unlimited            0 Summary
chunk:static                 2           2  unlimited            0 Summary
block:16384                510         885  unlimited            0 Summary
block:2048                  32          35  unlimited            0 Summary
tcp-intercept-rate      341306      811579  unlimited            0 Summary
globals                      1           1  unlimited            0 Summary
np-statics                   6           6  unlimited            0 Summary
statics                      2           2        N/A            0 Summary
nats                         1           1        N/A            0 Summary
ace-rules                    3           3        N/A            0 Summary
console-access-rul           4           4        N/A            0 Summary
fixup-rules                 43          44        N/A            0 Summary
```

查看分配的 MAC 地址

您可以查看系统配置或情景中的自动生成的 MAC 地址。

在系统配置中查看 MAC 地址

本节介绍如何查看系统配置中的 MAC 地址。

开始之前

如果您手动向接口分配MAC地址，但也启用了自动生成，则自动生成的地址会继续显示在配置中，即使正在使用的是手动MAC地址也如此。如果随后删除手动MAC地址，则会使用所显示的自动生成的地址。

过程

从系统执行空间显示分配的 MAC 地址：

show running-config all context [*name*]

查看分配的 MAC 地址必须使用 **all** 选项。虽然 **mac-address auto** 命令仅在全局配置模式下可由用户配置，但是该命令在情景配置模式下会与分配的 MAC 地址一起显示为只读条目。只有在情景中使用 **nameif** 命令配置的已分配接口会具有分配的 MAC 地址。

示例

show running-config all context admin 命令的以下输出显示了分配给 Management0/0 接口的主用 MAC 地址和备用 MAC 地址。

```
ciscoasa# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context 命令的以下输出显示了所有情景接口的所有 MAC 地址（主用 MAC 地址和备用 MAC 地址）。请注意，由于未在情景中使用 **nameif** 命令配置 GigabitEthernet0/0 和 GigabitEthernet0/1 主接口，因此没有为其生成 MAC 地址。

```
ciscoasa# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

查看情景中的 MAC 地址

本节介绍如何查看情景中的 MAC 地址。

过程

显示情景中的每个接口正在使用的 MAC 地址：

show interface | include (Interface)|(MAC)

示例

例如：

```
ciscoasa/context# show interface | include (Interface)|(MAC)

Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
        MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
        MAC address a201.0102.0600, MTU 1500
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
        MAC address a201.0103.0600, MTU 1500
...
```

注释 **show interface** 命令显示正在使用的 MAC 地址；如果您手动分配 MAC 地址，并且也启用了自动生成，则只能查看系统配置中未使用的自动生成地址。

多情景模式示例

以下示例：

- 使用自定义前缀自动设置情景中的 MAC 地址。
- 将默认类的连接数限制设置为 10% 而非不受限制，并将 VPN 其他会话连接数限制设置为 10 且 VPN 突发连接数限制为 5。
- 创建 gold 资源类。
- 将管理情景设置为“administrator”。
- 在内部闪存上创建一个名为“administrator”的情景，该情景将属于默认资源类。
- 从 FTP 服务器添加两个情景，作为 gold 资源类的一部分。

```
ciscoasa(config)# mac-address auto prefix 19

ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5

ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
ciscoasa(config-class)# limit-resource vpn other 100
ciscoasa(config-class)# limit-resource vpn burst other 50

ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member gold
```

多情景模式的历史记录

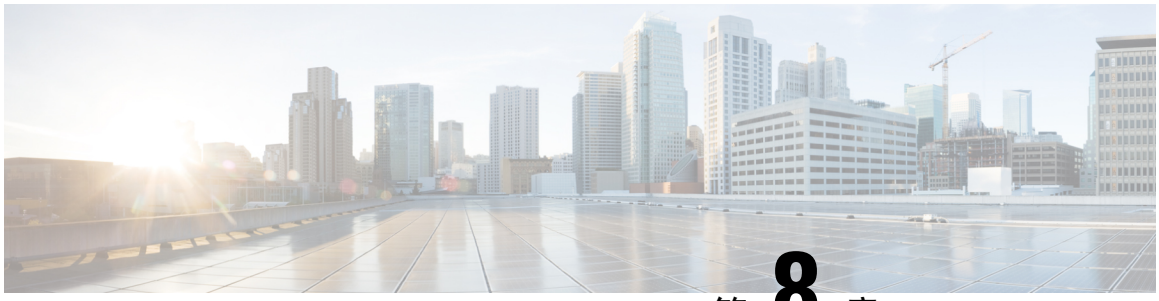
表 *11:* 多情景模式的历史记录

功能名称	平台版本	功能信息
多个安全情景	7.0(1)	引入了多情景模式。 引入了以下命令：**context**、**mode** 和 **class**。

功能名称	平台版本	功能信息
自动 MAC 地址分配	7.2(1)	引入了将 MAC 地址自动分配给情景接口的功能。 引入了以下命令：**mac-address auto**。
资源管理	7.2(1)	引入了资源管理。 引入了以下命令：**class**、**limit-resource** 和 **member**。
适用于 IPS 的虚拟传感器	8.0(2)	运行 IPS 软件版本 6.0 及更高版本的 AIP SSM 可以运行多个虚拟传感器，这意味着您可以在该 AIP SSM 上配置多个安全策略。您可以向一个或多个虚拟传感器分配每个情景或单模式 ASA，也可以向同一个虚拟传感器分配多个安全情景。 引入了以下命令：**allocate-ips**。
自动 MAC 地址分配增强功能	8.5(2) 8.6(2)	MAC 地址格式更改为使用前缀，以便使用固定起始值 (A2)，并在故障转移对中为主设备和辅助设备 MAC 地址使用不同方案。现在，MAC 地址在重新加载之后也会保持不变。现在，命令解析器会检查是否已启用自动生成；如果您还希望手动分配 MAC 地址，则手动 MAC 地址不能以 A2 开头。 修改了以下命令：**mac-address auto prefix**。
增加了 ASA 5550 和 5580 的最大情景数量。	8.4(1)	ASA 5550 的最大安全情景数量已从 50 增加到 100。ASA 5580 的最大安全情景数量已从 50 增加到 250。
默认情况下会启用自动 MAC 地址分配。	8.5(1)	现在，默认情况下会启用自动 MAC 地址分配。 修改了以下命令：**mac-address auto**。
自动生成 MAC 地址前缀	8.6(1)	在多情景模式下，ASA 现在支持将自动 MAC 地址生成配置转换为使用默认前缀。ASA 基于接口 (ASA 5500-X) 或背板 (ASASM) MAC 地址的最后两个字节自动生成前缀。当您重新加载或重新启用 MAC 地址生成时，系统自动执行此转换。前缀生成方法提供许多好处，包括更好地保证 MAC 地址在网段上的唯一性。您可以通过输入 **show running-config mac-address** 命令查看自动生成的前缀。如果要更改前缀，可以使用自定义前缀重新配置此功能。传统的 MAC 地址生成方法不再可用。 **注释** 为了保持故障转移对无中断升级，如果已启用故障转移，ASA 在重新加载时不会转变现有配置中的 MAC 地址方法。但是，我们强烈建议您在使用故障转移时手动更改前缀生成方法，特别是对于 ASASM。如果没有前缀方法，安装在不同插槽编号的 ASASM 在故障转移时会遇到 MAC 地址变更，并可能会遇到流量中断。升级后，要使用 MAC 地址生成的前缀方法，请重新启用 MAC 地址生成来使用前缀。 修改了以下命令：**mac-address auto**。

功能名称	平台版本	功能信息
默认所有型号（除 ASASM 之外）上均已禁用自动 MAC 地址分配	9.0(1)	现在，自动 MAC 地址分配默认处于禁用状态（除 ASASM 之外）。 修改了以下命令：**mac-address auto**。
安全情景中的动态路由	9.0(1)	现在，在多情景模式下支持 EIGRP 和 OSPFv2 动态路由协议。不支持 OSPFv3、RIP 和组播路由。
用于路由表条目的新资源类型	9.0(1)	系统创建了新的资源类型 routes，用于设置每个情景中的最大路由表条目数。 修改了以下命令：**limit-resource**、**show resource types**、**show resource usage** 和 **show resource allocation**。
多情景模式下的站点间 VPN	9.0(1)	现在，在多情景模式下支持站点间 VPN 隧道。
用于站点间 VPN 隧道的新资源类型	9.0(1)	系统创建了新的资源类型（即 vpn other 和 vpn burst other），用于设置每个情景中站点间 VPN 隧道的最大数量。 修改了以下命令：**limit-resource**、**show resource types**、**show resource usage** 和 **show resource allocation**。
SA IKEv1 SA 协商的新资源类型	9.1(2)	创建了新的资源类型 ikev1 in-negotiation，用于在每个情景中设置 IKEv1 SA 协商的最大百分比，以防 CPU 和加密引擎被淹没。在某些情况下（大型证书、CRL 检查），您可能希望限制此资源。 修改了以下命令：**limit-resource**、**show resource types**、**show resource usage** 和 **show resource allocation**。
支持多情景模式下的远程访问 VPN	9.5(2)	现在您可在多情景模式中使用以下远程访问功能： • AnyConnect 3.x 及更高版本（仅支持 SSL VPN；无 IKEv2 支持） • 集中 Secure Client 映像配置 • Secure Client 映像升级 • 对 Secure Client 连接进行情景资源管理 **注释** 多情景模式下需要 Secure Client Premier Apex 许可证；您无法使用默认或传统许可证。 引入了以下命令：**limit-resource vpn anyconnect**、**limit-resource vpn burst anyconnect**
多情景模式的 Pre-fill/Username-from-cert 功能	9.6(2)	Secure Client SSL 支持已扩展，允许 pre-fill/username-from-certificate 功能 CLI（以前其仅在单情景模式下可用）在多情景模式下也可启用。 未修改任何命令。

功能名称	平台版本	功能信息
使用闪存虚拟化实现远程访问VPN	9.6(2)	多情景模式下的远程访问 VPN 现在支持闪存虚拟化。每个情景都可以根据可用的总闪存拥有专用存储空间和共享存储位置： • 专用存储 - 仅存储与该用户关联且特定于您希望该用户具有的内容的文件。 • 共享存储 - 将文件上传到此空间，并且将其启用后，可供任何用户情景进行读/写访问。 引入了以下命令：**limit-resource storage**、**storage-url**
在多情景设备中支持Secure Client客户端配置文件	9.6(2)	在多情景设备中支持Secure Client 客户端配置文件要使用 ASDM 添加新配置文件，您必须要有 Secure Client 版本 4.2.00748 或 4.3.03013 及更高版本。
多情景模式下 Secure Client 连接的有状态故障转移	9.6(2)	现在，多情景模式下 Secure Client 连接支持有状态故障转移 未修改任何命令。
多情景模式下支持远程访问 VPN 动态访问策略 (DAP)	9.6(2)	现在，可以在多情景模式下按情景配置 DAP。 未修改任何命令。
多情景模式下支持远程访问 VPN CoA（授权更改）	9.6(2)	现在，可以在多情景模式下按情景配置 CoA。 未修改任何命令。
多情景模式下支持远程访问 VPN 本地化	9.6(2)	支持全局本地化。只有一组跨不同情景共享的本地化文件。 未修改任何命令。
支持多情景模式下的IKEv2远程访问 VPN	9.9(2)	您可以为 IKEv2 配置多情景模式的远程访问 VPN。
可配置管理会话限制	9.12(1)	现在，您可以配置汇聚管理会话数、每用户管理会话数和每协议管理会话数的最大值。以前，您只能配置汇聚会话数。此功能不会影响控制台会话。需要注意的是，在多情景模式下，如果最大 HTTPS 会话数固定为 5，则无法配置会话数。此外，系统配置中也不再接受 **quota management-session** 命令，您只能在情景配置中进行此设置。现在，最大汇聚会话数为 15。如果您已将其配置为 0（无限制）或大于 16 的值，在升级设备时，此值会自动更改为 15。 新增/修改的命令： **quota management-session**、**show quota management-session**
Firepower 1140 最大情景数从 5 增加到 10	9.16（1）	Firepower 1140 现在最多支持 10 个情景。



第 8 章

通过故障转移实现高可用性

本章介绍如何配置主用/备用或主用/主用故障转移来实现 ASA 的高可用性。

- 关于故障转移， 第 259 页
- 故障转移许可， 第 278 页
- 故障转移准则， 第 279 页
- 故障转移的默认设置， 第 282 页
- 配置主用/备用故障转移， 第 282 页
- 配置主用/主用故障转移， 第 287 页
- 配置可选故障转移参数， 第 293 页
- 管理故障转移， 第 301 页
- 监控 故障转移， 第 307 页
- 故障转移的历史记录， 第 308 页

关于故障转移

配置故障转移需要通过专用故障转移链路和状态链路（可选）相互连接的两台相同的 ASA。主用单元和接口的运行状况会受到监控，以便确定它们是否满足特定故障转移条件的时刻。如果符合这些条件，将执行故障转移。

故障转移模式

ASA 支持两种故障转移模式，主用/主用故障转移和主用/备用故障转移。每种故障转移模式都有自己确定和执行故障转移的方法。

- 如发生主用/备用故障转移，其中一个设备是主用设备，并传递流量。第二台设备指定为备用设备，不会主动传送流量。发生故障转移时，主用设备会故障转移到备用设备，后者随即变为主用状态。您可以在单情景模式或多情景模式下为 ASA 使用主用/备用故障转移。
- 在主用/主用故障转移配置中，两台 ASA 均可传递网络流量。主用/主用故障转移仅在多情景模式下适用于 ASA。在主用/主用故障转移中，将 ASA 上的安全情景划分为 2 个故障转移组。故障转移组就是一个或多个安全情景的逻辑组。一个组被指定为主 ASA 上的活动组，另一个组被指定为辅助 ASA 上的活动组。发生故障转移时，会在故障转移组级别进行。

两种故障转移模式都支持状态或无状态故障转移。

故障转移系统要求

本部分介绍在故障转移配置中对于 ASA 的硬件、软件和许可证要求。

硬件要求

故障转移配置中的两台设备必须：

- 型号相同。

  对于 Firepower 9300，高可用性仅在同种类型模块之间受支持；但是两个机箱可以包含混合模块。例如，每个机箱都设有 SM-56、SM-48 和 SM-40。可以在 SM-56 模块之间、SM-48 模块之间和 SM-40 模块之间创建高可用性对。

- 拥有相同数量和类型的接口。

  对于平台模式下的Firepower 4100/9300 机箱，在启用之前，所有接口都必须在 FXOS 中进行相同的预配置。故障转移如果您在启用故障转移后更改接口，请在备用设备上的 FXOS 中更改接口，然后在主用设备上进行相同更改。 如果在 FXOS 中删除一个接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中删除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

- 安装有相同的模块（如有）。

- 安装有相同的 RAM。

如果在故障转移配置中使用闪存大小不同的设备，请确保闪存较小的设备具有足够的空间来容纳软件映像文件和配置文件。如果闪存较小的设备没有足够的空间，从闪存较大的设备向闪存较小的设备进行配置同步将会失败。

软件要求

故障转移 配置中的两台设备必须：

- 处于相同的情景模式（单情景或多情景）。

- 单一模式下：处于相同的防火墙模式（路由或透明）。

  在多情景模式下，防火墙模式在情景级别设置，您可以使用混合模式。

- 具有相同的主要（第一个数字）和次要（第二个数字）软件版本。但是，您可以在升级过程中临时使用不同的软件版本；例如，可以将一台设备从 8.3(1) 版本升级到 8.3(2) 版本，并使故障转移保持主用状态。我们建议将两台设备都升级为相同版本，以便确保长期的兼容性。

- 具有相同的 Secure Client 映像。如果在执行无中断升级时，故障转移对具有不匹配的映像，则无客户端 SSL VPN 连接会在升级过程的最终重新启动步骤终止，数据库会显示一个孤立会话，并且 IP 池会显示分配给客户端的 IP 地址“正在使用中”。

- 处于相同的 FIPS 模式下。
- （Firepower 4100/9300）具有相同的流量分流模式，同时启用或禁用。

许可证要求

故障转移配置下的两台设备不需要具有相同的许可证；许可证将整合为故障转移集群许可证。

故障转移和状态故障转移链路

故障转移链路和可选的有状态故障转移链路是两台设备之间的专用连接。思科建议在故障转移链路或状态故障转移链路中的两台设备之间使用同一接口。例如，在故障转移链路中，如果您在设备 1 中使用的是 eth0，也要在设备 2 中使用相同的接口，即还是 eth0。

注意 除非您使用IPsec隧道或故障转移密钥保护通信，否则所有信息会以明文形式通过故障转移和状态链路发送。如果使用 ASA 端接 VPN 隧道，则此信息包括用于建立隧道的任何用户名、密码和预共享密钥。以明文发送此敏感数据可能会带来严重的安全风险。如果您使用 ASA 来端接 VPN 隧道，我们建议使用 IPsec 隧道或故障转移密钥来保护故障转移通信。

故障转移链路

故障转移对中的两台设备会不断地通过故障转移链路进行通信，以便确定每台设备的运行状态。

故障转移链路数据

以下信息将通过故障转移链路传输：

- 设备状态（主用或备用）
- Hello 消息 (keep-alives)
- 网络链路状态
- MAC 地址交换
- 配置复制和同步

故障转移链路接口

您可以使用未使用的数据接口（物理接口、子接口 EtherChannel 接口）作为故障转移链路；但不能指定当前已配置名称的接口。故障转移链路接口不会配置为常规网络接口；该接口仅会因为故障转移而存在。该接口只能用于故障转移链路（还用于状态链路）。大多数型号不能使用管理接口进行故障转移，除非明确作出如下说明。

ASA用户数据和故障转移链路之间共享接口。您也不能在同一父接口上使用单独的子接口用于故障转移链路和数据。

请参阅下列有关故障转移链路的准则：

- 5506-X 至 5555-X - 不能使用管理接口作为故障转移链路；您必须使用数据接口。5506H-X 是唯一的例外情况，您可以在其中将管理接口用作故障转移链路。
- 5506H-X - 您可以使用管理 1/1 接口作为故障转移链路。如果配置该接口作为故障转移接口，您必须重新加载设备，更改才能生效。在这种情况下，您也不能使用 ASA Firepower 模块，因为该模块需要使用管理接口实现管理目的。
- Firepower 4100/9300- 我们建议您将一个 10 GB 数据接口用于组合的故障转移和状态链路。 不能使用管理类型接口作为故障转移链路。
- 所有其他型号 - 1 GB 接口对于组合的故障转移和状态链路而言已足够大。

交替频率等于设备保持时间（**failover polltime unit** 命令）。

注释 如果配置较大且设备保持时间较短，则在成员接口之间交替可以防止辅助设备加入/重新加入。这种情况下，请禁用其中一个成员接口，直到辅助设备加入。

对于用作故障转移链路的 EtherChannel，要阻止无序数据包，仅使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作故障转移链路时对其进行修改。

连接故障转移链路

您可以使用以下两种方法之一连接故障转移链路：

- 使用不与任何其他设备处于相同网段（广播域或 VLAN）的交换机作为 ASA 的故障转移接口。
- 使用以太网电缆直接连接设备，无需外部交换机。

如果不在设备之间使用交换机，当接口出现故障时，两台对等体之间的链路将会断开。这种情况可能会妨碍故障排除工作，因为您无法轻松确定接口发生故障，导致链路断开的设备。

ASA在其铜缆以太网端口上支持自动 MDI/MDIX，因此您可以使用交叉电缆或直通电缆。如果使用的是直通电缆，接口会自动检测该电缆，并将其中一个发送/接收对交换为 MDIX。

状态故障转移链路

要使用有状态故障转移，必须配置有状态故障转移链路（也称为有状态链路），以便传送连接状态信息。

共享故障转移链路

共享故障转移链路是节约接口的最佳方式。但是，如果您有一个大型配置和高流量网络，必须考虑对状态链路和故障转移链路使用专用接口。

状态故障转移链路的专用接口

您可以将专用接口（物理或 EtherChannel）用于状态链路。有关专用状态链路的要求，请参阅故障转移链路接口，第 261 页，以及有关连接状态链路的信息，请参阅连接故障转移链路，第 262 页。

使用长距离故障转移时，为实现最佳性能，状态链路的延迟应低于 10 毫秒且不超过 250 毫秒。如果延迟超过 10 毫秒，重新传输故障转移消息会导致一些性能降级。

避免中断故障转移和数据链路

我们建议，让故障转移链路和数据接口使用不同的路径，以便降低所有接口同时发生故障的可能性。如果故障转移链路发生故障，ASA 可使用数据接口来确定是否需要进行故障转移。随后，故障转移操作会被暂停，直到故障转移链路恢复正常。

请参阅以下连接情景，以设计具有弹性的故障转移网络。

情景 1 - 不推荐

如果单台交换机或一组交换机用于连接两台 ASA 之间的故障转移和数据接口，则交换机或交换机间链路发生故障时，两台 ASA 都都将处于主用状态。因此，不推荐使用下图中显示的 2 种连接方法。

图 *43:* 使用单交换机连接 - 不推荐

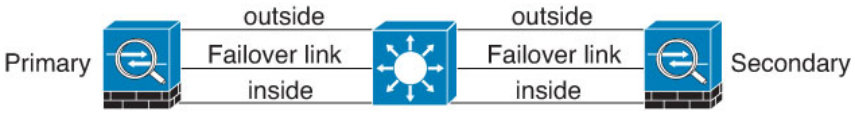
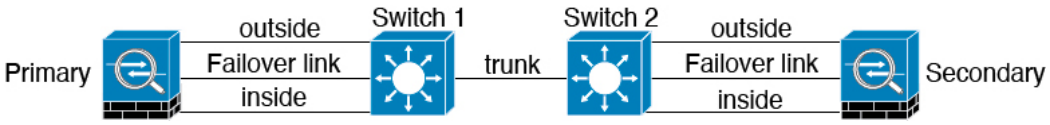


图 *44:* 使用双交换机连接 - 不推荐



情景 2 - 推荐

我们不推荐让故障转移链路和数据接口使用相同的交换机，而是应使用不同的交换机或使用直连电缆来连接故障转移链路，如下图所示。

图 *45:* 使用其他交换机连接

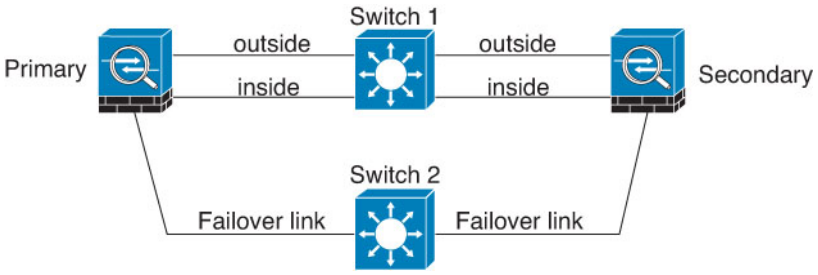
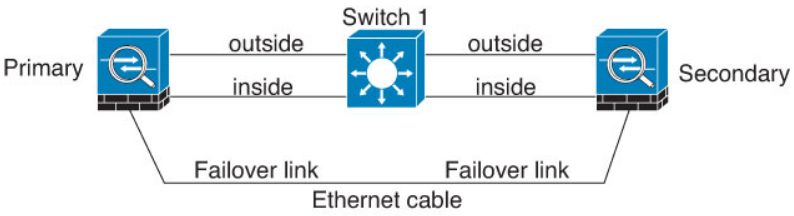


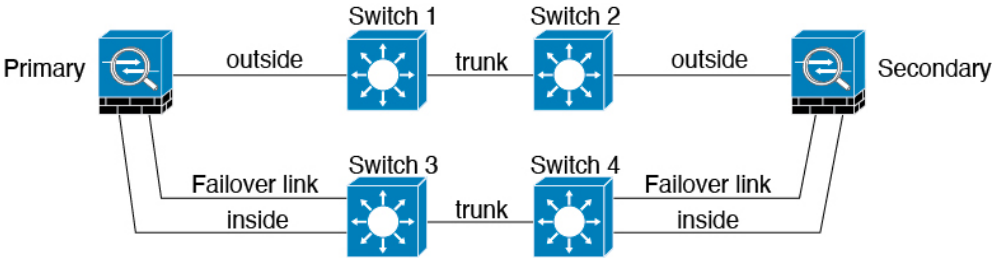
图 *46:* 通过缆线连接



情景 3 - 推荐

如果 ASA数据接口连接到多台交换机，则故障转移链路可以连接到其中一台交换机，最好是处于网络的安全一侧（内部）的交换机，如下图所示。

图 *47:* 使用安全交换机连接



故障转移中的 MAC 地址和 IP 地址

当您配置接口时，可以在相同网络上指定一个主用 IP 地址和一个备用 IP 地址。通常情况下，当发生故障转移时，新的主用设备会接管主用 IP 地址和 MAC 地址。由于网络设备不会发现 MAC 与 IP 地址配对的变化，网络上的任意位置都不会发生 ARP 条目变化或超时。

注释 虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。此外，您也无法出于管理目的，连接到该接口上的备用设备。

在发生故障转移时，状态链路的 IP 地址和 MAC 地址不会更改。

主用/备用 IP 地址和 MAC 地址

对于主用/备用故障转移，请参阅下文，了解故障转移事件期间 IP 地址和 MAC 地址的使用情况：

1. 主用设备始终使用主设备的 IP 地址和 MAC 地址。
2. 当主用设备进行故障转移时，备用设备会使用故障设备的 IP 地址和 MAC 地址，并开始传送流量。
3. 当故障设备恢复在线状态时，它现在处于备用状态，并且接管备用 IP 地址和 MAC 地址。

但如果辅助设备启动时未检测到主设备，辅助设备将成为主用设备，并使用其自己的 MAC 地址，因为它不知道主设备的 MAC 地址。当主设备变为可用时，辅助（主用）设备会将 MAC 地址更改为主设备的 MAC，这可能会导致网络流量中断。同样，如果您用新硬件替换主设备，将使用新 MAC 地址。

如果禁用故障转移并将故障转移配置设置为禁用状态，则需要手动恢复故障转移，或者重新启动设备。建议使用命令 **failover reset** 并恢复故障转移，而不是重新启动设备。如果在禁用故障转移配置的情况下重新加载备用设备，则备用设备将作为主用设备启动，并使用主设备的 IP 地址和 MAC 地址。这会导致 IP 地址重复并导致网络流量中断。使用命令 **failover reset** 启用故障转移并恢复流量。

使用虚拟 MAC 地址可防范这种中断，因为对于启动时的辅助设备，主用 MAC 地址是已知的，并在采用新的主设备硬件时保持不变。建议您在主设备和辅助设备上配置虚拟 MAC 地址，以确保辅助设备在作为主用设备时使用正确的 MAC 地址，即使它在主设备之前上线。如果您没有配置虚拟 MAC 地址，则可能需要清除连接的路由器上的 ARP 表，以便恢复流量。当 MAC 地址发生变化时，ASA 不会发送静态 NAT 地址的免费 ARP，因此连接的路由器不会知道这些地址的 MAC 地址发生变化。

主用/主用 IP 地址和 MAC 地址

对于主用/主用故障转移，请参阅下文，了解故障转移事件期间 IP 地址和 MAC 地址的使用情况：

1. 主设备为故障转移组 1 和 2 个情景中的所有接口自动生成主用和备用 MAC 地址。如有必要，例如 MAC 地址发生冲突时，您也可以手动配置 MAC 地址。
2. 每台设备将主用 IP 地址和 MAC 地址用于其主用故障转移组，并将备用地址用于其备用故障转移组。例如，主设备是故障转移组 1 的主用设备，因此它使用故障转移组 1 中情景的主用地址。它是故障转移组 2 中情景的备用设备，因此在其中使用备用地址。
3. 当设备进行故障转移时，另一个设备将会承担出现故障的故障转移组的主用 IP 地址和 MAC 地址，并开始传送流量。
4. 当故障设备恢复在线状态，并且您已启用抢占选项时，它将恢复故障转移组。

虚拟 MAC 地址

ASA 有多种方法配置虚拟 MAC 地址。我们建议仅使用一种方法。如果使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。手动方法包括接口模式 **mac-address** 命令、**failover mac address** 命令；对于主用/主用故障转移，除了以下所述的自动生成方法之外，还有故障转移组模式 **mac address** 命令。

在多情景模式下，您可以配置 ASA 自动为共享接口生成虚拟主用和备用 MAC 地址，然后将这些分配同步到辅助设备（请参阅 **mac-address auto** 命令）。对于非共享接口，您可以手动设置主用/备用模式的 MAC 地址（主用/主用模式会为所有接口自动生成 MAC 地址）。

对于主用/主用故障转移，始终将虚拟 MAC 地址与默认值或按接口设置的值一同使用。

故障转移中的 MAC 地址表更新

在故障转移期间，被指定为新活动设备的设备会为 MAC 表中的每个 MAC 地址条目生成组播数据包，并将其发送到所有桥接组接口。此操作会提示网桥组中的上游交换机使用新活动设备的接口更新路由表，以确保准确的流量转发。

生成组播数据包和更新上游交换机路由表所需的时间取决于 MAC 地址表的条目数量和桥接组接口的数量。使用 **show failover statistics state-switch-delay** 命令可显示与故障转移事件期间遇到的延迟相关的统计信息。

无状态故障转移和有状态故障转移

对于主用/备用和主用/主用模式，ASA 支持两种故障转移类型：无状态和状态故障转移。

注释 无客户端 SSL VPN 的某些配置元素（如书签和自定义）使用 VPN 故障转移子系统，该子系统是状态故障转移的一部分。您必须使用状态故障转移，在同步故障转移对中的成员之间同步这些元素。不推荐将无状态故障转移用于无客户端 SSL VPN。

无状态故障转移

发生故障转移时，所有活动连接将会被丢弃。在新的主用设备接管时，客户端需要重新建立连接。

注释 无客户端 SSL VPN 的某些配置元素（如书签和自定义）使用 VPN 故障转移子系统，该子系统是状态故障转移的一部分。您必须使用状态故障转移，在同步故障转移对中的成员之间同步这些元素。不推荐将无状态（常规）故障转移用于无客户端 SSL VPN。

状态故障转移

启用状态故障转移时，主用设备会不断将每个连接的状态信息发送至备用设备，在主用/主用故障转移期间，在主用和备用故障转移组之间发送。发生故障转移之后，相同的连接信息在新主用设备上可用。支持的最终用户应用不需要通过重新连接来保持同一通信会话。

支持的功能

对于状态故障转移，以下状态信息会传送至备用 ASA：

- NAT 转换表。
- TCP 和 UDP 连接和状态。其他类型的 IP 协议和 ICMP 不会通过主用设备解析，因为它们是在新数据包到达时在新的主用设备上建立的。
- HTTP 连接表（除非启用 HTTP 复制）。
- HTTP 连接状态（如果已启用 HTTP 复制）- 默认情况下，启用状态故障转移时，ASA 不会复制 HTTP 会话信息。建议启用 HTTP 复制。
- SCTP 连接状态。但是，SCTP 检测状态故障转移是尽力而为。在故障转移期间，如果任何 SACK 数据包丢失，新的主用设备将丢弃队列中其他所有无序的数据包，直到收到缺失的数据包为止。
- ARP 表

- 第 2 层网桥表（适用于桥接组）
- ISAKMP 和 IPsec SA 表
- GTP PDP 连接数据库
- SIP 信令会话和引脚。
- ICMP 连接状态 - 仅当相应的接口分配给非对称路由组时，才会启用 ICMP 连接复制。
- 静态和动态路由表 - 状态故障转移会参与动态路由协议（如 OSPF 和 EIGRP），因此通过主用设备上的动态路由协议获悉的路由，将会保留在备用设备的路由信息库 (RIB) 表中。发生故障转移事件时，数据包可以正常传输，并且只会对流量产生极小的影响，因为主用辅助设备一开始就具有镜像主设备的规则。进行故障转移后，新的主用设备上的重新融合计时器会立即启动。随后 RIB 表中的代编号将会增加。在重新融合期间，OSPF 和 EIGRP 路由将使用新的代编号进行更新。计时器到期后，过时的路由条目（由代编号确定）将从表中删除。于是 RIB 将包含新主用设备上的最新的路由协议转发信息。

注释 路由仅会因为主用设备上的链路打开或关闭事件而同步。如果备用设备上的链路打开或关闭，从主用设备发出的动态路由可能会丢失。这是预期的正常行为。

- DHCP 服务器 - 不会复制 DHCP 地址租用。但是，在接口上配置的 DHCP 服务器将发送 ping 命令，以确保在向 DHCP 客户端授予地址前不使用地址，使得服务不会受到影响。对于 DHCP 中继代理或 DDNS，状态信息不相关。
- 思科 IP SoftPhone 会话 - 如果在活动思科 IP SoftPhone 会话期间发生故障转移，呼叫将保持活动，因为呼叫会话状态信息已复制到备用设备。呼叫被终止时，IP SoftPhone 客户端将丢失与思科 Call Manager 的连接。发生此连接丢失是因为，没有备用设备上的 CTIQBE 挂机消息的会话信息。如果 IP SoftPhone 客户端在特定时间内未从 Call Manager 收到响应，则会认为 Call Manager 不可访问，并会取消注册自身。
- RA VPN - 故障转移后，远程访问 VPN 终端用户不必对 VPN 会话重新进行身份验证，也不必重新连接。但是，在 VPN 连接上运行的应用，在故障转移过程中可能会丢失数据包，并且无法从数据包丢失中恢复。
- 在所有连接中，只有已建立的连接会复制到备用 ASA 上。

不支持的功能

对于状态故障转移，以下状态信息不会传送至备用 ASA：

- 用户身份验证 (uauth) 表
- TCP 状态绕行连接
- 组播路由。
- 选定的无客户端 SSL VPN 功能：

- 智能隧道
- 端口转发
- 插件
- Java 小程序
- IPv6 无客户端或 Secure Client 会话
- Citrix 身份验证（Citrix 用户在故障转移后必须重新进行身份验证）

故障转移的网桥组要求

使用网桥组时，故障转移存在特殊的注意事项。

设备、ASAv 的网桥组要求

当主用设备故障转移到备用设备时，所连接的运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，会进入阻塞状态 30 秒至 50 秒。当端口处于阻塞状态时，为避免流量丢失，您可以根据交换机端口模式，配置以下任一变通方案：

- 访问模式 - 启用交换机上的 STP PortFast 功能：

  ```
  interface interface_id
    spanning-tree portfast
  ```

  链路打开时，PortFast 功能会立即使端口转换到 STP 转发模式。该端口仍会参与 STP。因此，如果端口是环路的一部分，则端口最终会转换为 STP 阻塞模式。

- Trunk 模式 - 使用 EtherType 访问规则阻止桥接组成员接口上 ASA 上的 BPDU。

  ```
  access-list id ethertype deny bpdu
  access-group id in interface name1
  access-group id in interface name2
  ```

  阻止 BPDU 会在交换机上禁用 STP。在您的网络布局中，确保没有任何环路涉及 ASA。

如果以上选项均不可行，则您可以使用以下任一不太理想的变通方案，这些方案可能会影响故障转移功能或 STP 稳定性。

- 禁用接口监控。
- 将接口保持时间增大到一个高值，这将允许 STP 在 ASA 进行故障转移之前收敛。
- 降低 STP 计时器的值，以 STP 在接口保持时间之内融合。

故障转移运行状态监控

ASA会监控每台设备的整体运行状态和接口运行状态。此部分包括有关 ASA如何执行测试以确定每台设备状态的信息。

设备运行状况监控

ASA 会通过 Hello 消息监控故障转移链路，进而确定其他设备的运行状况。当设备在故障转移链路上没有收到三条连续的 Hello 消息时，设备将在每个数据接口（包括故障转移链路）上发送接口 LANTEST 消息，来验证对等体是否响应。 对于 Firepower 9300 和 4100系列，您可以启用双向转发检测 (BFD) 监控，这比 Hello 消息更可靠。ASA 采取的操作取决于来自其他设备的响应。请参阅以下可以执行的操作：

- 如果 ASA 在故障转移链路上收到响应，则不会进行故障转移。
- 如果 ASA 在故障转移链路上未收到响应，但在数据接口上收到响应，则设备不会进行故障转移。故障转移链路会标记为发生故障。您应尽快恢复故障转移链路，因为当故障转移切换发生故障时，设备无法故障转移到备用设备。
- 如果ASA未在任何接口上收到响应，则备用设备会切换至主用模式，并会将另一台设备分类为故障设备。

心跳模块冗余

每个高可用性单位通过集群控制链路定期发送广播保持连接心跳数据包。如果控制平面忙于处理流量，有时心跳数据包无法到达对等体，或者对等体由于CPU过载而无法处理心跳数据包。当对等体无法在可配置的超时期限内传达保持连接状态时，会发生错误的故障转移或裂脑场景。

数据平面中的心跳模块有助于避免由于控制平面中的流量拥塞而发生错误的故障转移或裂脑。

- 附加心跳模块的工作原理与控制平面模块类似，但使用数据平面传输基础设施发送和接收心跳消息。
- 当对等体在数据平面中收到心跳数据包时，计数器会递增。
- 如果控制平面中的心跳传输失败，则节点会检查数据平面中的心跳计数器。如果计数器递增，则表示对等体处于活动状态，并且集群在这种情况下不会执行故障转移。

注释

- 每当启用 HA 时，都会默认启用额外的心跳模块。您不必为数据平面中的其他心跳模块设置轮询间隔。此模块使用您为控制平面设置的相同心跳间隔。
- 此功能在版本 7.3 中不可用。

接口监控

您最多可以监控1025个接口（在多情景模式下，会在所有情景之间进行分配）。您应监控重要的接口。例如，在多情景模式下，您可以配置一个用于监控共享接口的情景：因为接口是共享的，所有情景都可以从监控中受益。

当设备在 15 个秒 （默认值），未在受监控的接口上收到 hello 消息时，将运行接口测试。（要更改时间段，请参阅 **failover polltime interface** 命令，如果是主用/主用故障转移，请参阅 **polltime interface** 命令）如果对于某个接口，其中一个接口测试失败，但在另一设备上的此接口继续成功传送流量，则此接口会被视为发生故障，ASA 停止运行测试。

如果满足为故障接口数量定义的阈值（请参阅命令，或者对于主用/主用故障转移，请使用命令）（请参阅配置设备管理高可用性和可扩展性故障转移标准接口策略）（请参阅设备设备管理高可用性故障转移）触发条件（Trigger Criteria）），并且主用设备的故障接口比备用设备多，则发生故障转移。**failover interface-policyinterface-policy** 如果某个接口在两个单元上都失败，则这两个接口会进入“Unknown”状态，并且不会计入由故障转移接口政策制定的故障转移限制。

如果接口收到任何流量，则该接口会再次变为正常工作状态。如果不再满足接口故障阈值，发生故障的 ASA 会回到备用模式。

如果接口上配置了 IPv4 和 IPv6 地址，ASA 会使用 IPv4 地址执行运行状况监控。如果接口上仅配置了 IPv6 地址，则 ASA 会使用 IPv6 邻居发现，而不是 ARP 来执行运行状况监控测试。对于广播 Ping 测试，ASA 会使用所有的 IPv6 节点地址 (FE02::1)。

注释 如果故障设备未恢复，并且您认为其应未发生故障，则可通过输入 **failover reset** 命令重置状态。但是，如果故障转移条件仍然存在，设备将再次失败。

接口测试

ASA使用以下接口测试。默认情况下，每个测试的持续时间约为1.5秒，或故障转移接口保持时间的1/16（请参阅 **failover polltime interface** 命令，对于主用/主用故障转移，请参阅 **interface-policy** 命令）。

1. 链路打开/关闭测试 - 一种接口状态测试。如果链路打开/关闭测试指示接口关闭，则 ASA视为测试失败，然后测试停止。如果状态为打开，则 ASA执行 Network Activity 测试。
2. 网络活动测试 - 接收的网络活动测试。测试开始时，每台设备会清除其接口收到的数据包计数。在测试期间，一旦设备收到符合条件的数据包，则接口会被视为正常运行。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备均收到了流量，则 ASA开始进行 ARP 测试。
3. ARP 测试 - 用于测试成功的 ARP 回复。每台设备都向其 ARP 表中最新条目中的 IP 地址发送一个 ARP 请求。如果设备在测试期间收到 ARP 回复或其他网络流量，则认为该接口运行正常。如果设备未收到 ARP 回复，则 ASA会向 ARP 表中的下一个条目中的 IP 地址发送一次 ARP 请求。如果设备在测试期间收到 ARP 回复或其他网络流量，则认为该接口运行正常。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备均收到了流量，则 ASA开始进行广播 Ping 测试。

4. 广播 Ping 测试 - 测试成功的 Ping 回复。每台设备发送一个广播 Ping，然后对收到的所有数据包进行计数。在测试期间，当设备收到任何数据包，则接口会被视为正常运行。如果两台设备都收到流量，则测试会停止。如果一台设备收到测试流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果未收到任何流量，则测试将通过 ARP 测试再次开始。如果两台设备继续没有收到来自 ARP 和广播 Ping 测试的流量，则测试将会一直运行下去。

接口状态

受监控接口可以具有以下状态：

- Unknown - 初始状态。此状态也可能意味着状态无法确定。
- Normal - 接口正在接收流量。
- Testing - 接口上有 5 个轮询时间未收听到 Hello 消息。
- Link Down - 接口或 VLAN 通过管理方式关闭。
- No Link - 接口的物理链路关闭。
- Failed - 在接口上没有收到流量，但在对等体接口上收听到流量。

故障转移时间

以下事件会在 Firepower 高可用性对中触发故障转移：

- 主用设备上超过 50% 的 Snort 实例已关闭。
- 主用设备上使用的磁盘空间已超过 90%。
- 主用设备上运行的是 **no failover active** 命令，而备用设备上运行的是 **failover active** 命令。
- 主用设备的故障接口比备用设备更多。
- 主用设备上的接口故障超过配置的阈值。

  默认情况下，单个接口发生故障会导致故障转换。您可以通过配置接口数量的阈值或为发生故障转移而必须发生故障的受监控接口的百分比来更改默认值。如果在主用设备上达到阈值，则会发生故障转移。如果备用设备上的阈值超出阈值，则设备将进入“**故障**”状态。

  要更改默认故障转移条件，在全局配置模式下输入以下命令：

  表 12:

命令	目的
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	更改默认故障转移条件。 指定特定接口数时，*num* 参数可以介于 1 和 250 之间。 指定接口百分比时，*num* 参数可以介于 1 和 100 之间。

注释 如果使用 CLI 或 ASDM 手动进行故障转移，或者重新加载 ASA，则故障转移会立即开始，不受如下所列计时器的约束。

表 *13: ASA*

故障转移条件	最小	默认	最大
主用设备断电，硬件关闭或软件重新加载或崩溃。当出现这些情况时，受监控接口或故障转移链路不会收到任何 Hello 消息。	800 毫秒	15 秒	45 秒
主用设备主板接口链路发生故障。	500 毫秒	5 秒	15 秒
主用设备 4GE 模块接口链路发生故障。	2 秒	5 秒	15 秒
主用设备接口正常运行，但是连接问题导致接口测试。	5 秒	25 秒	75 秒

配置同步

故障转移包含各种类型的配置同步。

运行配置复制

当故障转移对中的任意一台或两台设备启动时，系统会执行运行配置复制。

在主用/备用故障转移中，配置始终会从主用设备同步到备用设备。

在主用/主用故障转移中，第二个启动的任何设备都会从第一个启动的设备获取正在运行的配置，无论指定的主或从属启动设备如何都是如此。在两个设备正常运行后，在系统执行空间中输入的命令会从其上的故障转移组 1 处于主用状态的设备复制。

备用/第二个设备完成其初始启动后，会清除其运行配置（需要与主用设备通信的**failover**命令除外），而主用设备则会向备用设备发送其完整配置。复制开始时，主用设备上的 ASA 控制台会显示消息“Beginning configuration replication: Sending to mate”；完成时，ASA 显示消息“End Configuration Replication to mate”。根据配置的大小，复制可能需要几秒到几分钟。

在接收配置的设备上，配置仅存在于运行内存中。您应该根据保存配置更改，第 35 页将配置保存到闪存。例如，在主用/主用故障转移中，请在故障转移组 1 处于主用状态的设备的系统执行空间中输入 **write memory all** 命令。该命令会复制到对等设备，该对等设备将继续将其配置写入到闪存。

注释 在复制时，在发送配置的设备上输入的命令可能无法正确地复制到对等设备，并且在接收配置的设备上输入的命令可能已被接受的配置覆盖。在配置复制过程中，应避免在故障转移对中的任一设备上输入命令。

文件复制

配置同步不复制以下文件和配置组件，因此您必须手动复制这些文件，以便它们匹配：

- Secure Client 映像
- CSD 映像
- Secure Client 配置文件

  ASA 使用存储在 cache:/stc/profiles 中的 Secure Client 配置文件的缓存文件，而不是存储在闪存文件系统中的文件。要将 Secure Client 配置文件复制到备用设备，请执行以下其中一项操作：

  - 在主用设备上输入 **write standby** 命令。
  - 在主用设备上重新应用配置文件。
  - 重新加载备用设备。

- 本地证书颁发机构 (CA)
- ASA 映像
- ASDM 映像

命令复制

启动后，您在主用设备上输入的命令会被立即复制到备用设备。 不必将主用配置保存到闪存才能复制命令。

在主用/主用故障转移中，在系统执行空间中输入的命令复制自其上的故障转移组 1 处于主用状态的设备。

未在要进行命令复制的相应设备上输入命令会导致配置不同步。在进行下一次初始配置同步时，这些更改可能会丢失。

以下命令会复制到备用 ASA：

- 除 **mode**、**firewall** 和 **failover lan unit** 之外的所有配置命令
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

以下命令不会复制到备用 ASA：

- 除 **copy** 命令外的所有形式的 **copy running-config startup-config** 命令

- 除 **write** 命令外的所有形式的 **write memory** 命令
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** 和 **pager**

config-sync 优化

当设备在暂停或恢复故障转移后重启或重新加入时，加入的设备会清除其运行配置。然后，主用设备将其整个配置发送到加入设备，以实现完全的配置同步。如果主用设备配置较大，则此过程可能需要几分钟时间。

配置同步优化功能可通过交换配置哈希值来比较加入设备和主用设备的配置。如果主用设备和加入设备上计算的哈希值匹配，加入设备就会跳过完全配置同步，重新加入故障转移配置。此功能可确保更快的对等互连，并缩短维护窗口和升级时间。

配置同步优化的准则和限制

- 配置同步优化功能默认已启用。
- ASA 多情景模式通过在完全配置同步期间共享情景顺序来支持配置同步优化，从而允许在后续节点重新加入期间比较情景顺序。
- 如果配置密码和故障转移 IPsec 密钥，则配置同步优化无效，因为主用设备和备用设备中计算的散列值不同。
- 如果使用动态 ACL 或 SNMPv3 配置设备，则配置同步优化无效。
- 主用设备将 LAN 链路摆动的完整配置作为默认行为进行同步。在主用设备和备用设备之间的故障转移摆动期间，不会触发配置同步优化，设备会执行完整的配置同步。
- 当故障转移配置从主用设备和备用设备之间的网络通信中断或丢失中恢复时，会触发配置同步优化。

监控配置同步优化

启用配置同步优化功能后，系统会生成系统日志消息，显示在主用设备和加入设备上计算的散列值是否匹配，或者操作超时是否已到期。系统日志消息还会显示从发送散列请求到获取并比较散列响应所经过的时间。

使用以下命令监控配置同步优化。

- **show failover config-sync checksum**

  显示有关设备状态和校验和的信息。

- **show failover config-sync configuration**

显示有关设备配置和校验和的信息。

- **show failover config-sync status**

  显示配置同步优化功能的状态。

关于主用/备用故障转移

主用/备用故障转移允许您使用备用ASA来接管故障设备的功能。当主用设备发生故障时，备用设备将变为主用设备。但在更换故障设备之前，必须将备用设备设置为主设备，以便保留辅助设备的配置。

注释 对于多情景模式，ASA 可以在整个设备（包括所有情景）上进行故障转移，但不能在单个情景上单独进行故障转移。

主/辅助角色和主用/备用状态

在故障转移对中这两台设备之间的主要区别是哪台是主用设备，哪台是备用设备，即要使用哪些 IP 地址以及哪台设备积极传递流量。

但是，设备之间还存在一些取决于哪一设备为主设备（在配置中指定），哪一设备为辅助设备的差别：

- 如果两台设备同一时间启动（并且运行状况相同），则主设备总是会成为主用设备。
- 主设备 MAC 地址始终与主用 IP 地址相匹配。此规则的例外是，当辅助设备成为主用设备并且无法通过故障转移链路获取主设备 MAC 时。在这种情况下，会使用辅助设备的 MAC 地址。

启动时的主用设备确定

主用设备按以下方式确定：

- 如果某台设备启动，并检测到对等体已作为主用设备运行，则该设备会成为备用设备。
- 如果某台设备启动，并且未检测到对等体，则该设备会成为主用设备。
- 如果两台设备同时启动，则主设备成为主用设备，辅助设备成为备用设备。

故障转移事件

在主用/备用故障转移中，故障转移会在设备级别进行。即使在多情景模式下运行的系统上，您也无法对个别情景或一组情景进行故障转移。

下表显示了每个故障事件的故障转移操作。对于每种故障事件，该表显示了故障转移策略（故障转移或禁用故障转移）、主用设备执行的操作、备用设备执行的操作，以及有关故障转移条件和操作的所有特别说明。

表 *14:* 故障转移事件

故障事件	策略	主用设备操作	备用设备操作	说明
主用设备发生故障（电源或硬件）	故障转移	不适用	成为主用设备 将主用设备标记为发生故障	在任何受监控接口或故障转移链路上，均未收到 Hello 消息。
以前的主用设备恢复	禁用故障转移	成为备用设备	无需操作	无。
备用设备发生故障（电源或硬件）	禁用故障转移	将备用设备标记为发生故障	不适用	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。
故障转移链路在运行过程中发生故障	禁用故障转移	将故障转移链路标记为发生故障	将故障转移链路标记为发生故障	您应尽快恢复故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。
故障转移链路在启动时发生故障	禁用故障转移	成为主用设备 将故障转移链路标记为发生故障	成为主用设备 将故障转移链路标记为发生故障	如果故障转移链路在启动时发生故障，则两台设备都会成为主用设备。
状态链路发生故障	禁用故障转移	无需操作	无需操作	如果发生故障转移，状态信息会过时，而且会话会被终止。
主用设备上的接口故障超过阈值	故障转移	将主用设备标记为发生故障	成为主用设备	无。
备用设备上的接口故障超过阈值	禁用故障转移	无需操作	将备用设备标记为发生故障	备用设备被标记为发生故障后，主用设备不会尝试进行故障转移，即使超过接口故障阈值也是如此。

关于主用/主用故障转移

本部分介绍主用/主用故障转移。

主用/主用故障转移概述

在主用/主用故障转移配置中，两台 ASA 均可传递网络流量。主用/主用故障转移仅在多情景模式下适用于 ASA。在主用/主用故障转移中，您可将 ASA 上的安全情景最多划分为 2 个故障转移组。

故障转移组就是一个或多个安全情景的逻辑组。您可以将故障转移组指定为在主ASA上处于主用状态，并将故障转移组 2 指定为在辅助 ASA 上处于主用状态。发生故障转移时，会在故障转移组级别进行。例如，根据接口故障模式，故障转移组 1 可能会故障转移到辅助 ASA，相应地，故障转移组 2 可能故障转移到主 ASA。在以下情况下可能发生此事件：故障转移组 1 中的接口在主 ASA 上发生

故障，但在辅助 ASA 上正常工作，而故障转移组 2 中的接口在辅助 ASA 上发生故障，但在主 ASA 上正常工作。

管理情景始终是故障转移组 1 的成员。默认情况下，所有未分配的安全情景也是故障转移组 1 的成员。如果希望使用主用/主用故障转移，但对多情景不感兴趣，最简单的配置是添加一个额外的情景并将其分配给故障转移组 2。

注释 配置主用/主用故障转移时，请确保两台设备的整合流量在每台设备的处理能力之内。

注释 需要时，可将两个故障转移组分配到一台 ASA，但您将无法利用具有两台主用 ASA 的优势。

故障转移组的主/辅助角色和主用/备用状态

与在主用/备用故障转移中一样，主用/主用故障转移对中的一台设备被指定为主设备，另一台指定为辅助设备。不同于主用/备用故障转移的是，当两台设备同时启动时，此指定不指示哪一台设备会成为主用设备。相反地，主设备/辅助设备指定会进行两个操作：

- 两台设备同时启动时，主设备会提供运行配置。
- 配置中的每个故障转移组都配置了主设备或辅助设备首选项。与抢占一起使用时，此首选项可确保故障转移组启动后在正确的设备上运行。如果不使用抢占，则两个组均在第一台要启动的设备上运行。

启动时的故障转移组主用设备确定

故障转移组在其上变为主用状态的的设备按以下方式确定：

- 一台设备启动时，如果对等设备不可用，则两个故障转移组都会在该设备上变为主用状态。
- 一台设备启动时，如果对等设备处于主用状态（而且两个故障转移组都处于主用状态），则故障转移组将在主用设备上保持主用状态，而无论故障转移组的主设备或辅助设备首选项如何，直到出现以下情形之一：
  - 发生故障转移。
  - 手动强制执行故障转移。
  - 为故障转移组配置了抢占，这导致故障转移组在设备变得可用时，自动在首选设备上变为主用状态。

故障转移事件

在主用/主用故障转移配置中，故障转移会在故障转移组级别，而不是系统级别进行。例如，如果您将两个故障转移组指定为主设备上的主用故障转移组，并且故障转移组 1 发生故障，则故障转移组 2 会在主设备上保持主用，而故障转移组 1 则会在辅助设备上变为主用状态。

由于故障转移组可以包含多个情景，并且每个情景可以包含多个接口，因此有可能单个情景中的所有接口都发生故障而不导致相关故障转移组发生故障。

下表显示了每个故障事件的故障转移操作。对于每种故障事件，给出了策略（是否发生故障转移）、主用故障转移组的操作和备用故障转移组的操作。

表 *15:* 故障转移事件

故障事件	策略	主用组操作	备用组操作	备注
设备发生电源或软件故障	故障转移	成为备用设备 标记为发生故障	成为主用设备 将主用设备标记为发生故障	故障转移对等体中的一台设备发生故障时，该设备上的所有主用故障转移组都会被标记为发生故障，并在对等设备上变为主用状态。
主用故障转移组上的接口故障超过阈值	故障转移	将主用组标记为发生故障	成为主用设备	无。
备用故障转移组上的接口故障超过阈值	禁用故障转移	无需操作	将备用组标记为发生故障	备用故障转移组标记为发生故障后，主用故障转移组不会尝试进行故障转移，即使超过接口故障阈值也是如此。
以前的主用故障转移组恢复	禁用故障转移	无需操作	无需操作	除非配置了故障转移组抢占，否则故障转移组会在其当前设备上保持主用状态。
故障转移链路在启动时发生故障	禁用故障转移	成为主用设备	成为主用设备	如果故障转移链路在启动时发生故障，则两台设备上的故障转移组都会变为主用状态。
状态链路发生故障	禁用故障转移	无需操作	无需操作	如果发生故障转移，状态信息会过时，而且会话会被终止。
故障转移链路在运行过程中发生故障	禁用故障转移	n/a	n/a	每台设备都会将故障转移链路标记为发生故障。您应尽快恢复故障转移链路，因为当故障转移链路发生故障时，设备无法故障转移到备用设备。

故障转移许可

对于绝大多数型号，故障转移设备不要求每个设备上具有同一许可证。如果您在两台设备上都有许可证，则这两个许可证会合并为一个运行故障转移集群许可证。此规则存在一些例外情况。有关故障转移的具体许可要求，请参阅下表。

型号	许可证要求
ASA Virtual	请参阅 ASAv 的故障转移许可证， 第 90 页。
Firepower 1010	两个设备上都有增强型安全许可证。请参阅Firepower 1010 的故障转移许可证， 第 90 页。
Firepower 1100	请参阅Firepower 1100 的故障转移许可证， 第 90 页。
Cisco Secure Firewall 1210/1220	请参阅Cisco Secure Firewall 1210/1220 的故障转移许可证， 第 92 页。
Cisco Secure Firewall 3100/4200	请参阅Cisco Secure Firewall 3100 的故障转移许可证， 第 93 页。
Firepower 4100/9300	请参阅适用于 Firepower 4100/9300 的故障转移许可证， 第 95 页。
ISA 3000	两个设备上都有增强型安全许可证。 注释 每台设备必须拥有相同的加密许可证。

注释 需要有效的永久密钥；在极少数情况下，在 ISA 3000 可以删除您的 PAK 身份验证密钥。如果密钥全部由 0 组成，则需要重新安装有效的身份验证密钥，然后才能启用故障转移。

故障转移准则

情景模式

- 仅多情景模式支持主用/主用模式。
- 对于多情景模式，请在系统执行空间中执行所有步骤，除非另外说明。

型号支持

- Firepower 1010 和 Cisco Secure Firewall 1210/1220：
  - 使用故障转移时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备 和备用设备上传输流量。故障转移旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常 故障转移网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN接口可通过故障转移监控，而交换机端口无法通过故障转移监控。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用 故障转移，但更简单的设置是改用物理防火墙接口。
  - 仅可使用防火墙接口作为故障转移链路。

- Firepower 9300 - 我们建议您使用机箱间故障转移以实现最佳冗余。
- 由于需要第 2 层的连接，因此不支持照常故障转移在公共云网络（如 Microsoft Azure 和 Amazon Web 服务）上使用 ASA virtual。另请参阅 公共云中的高可用性故障转移，第 311 页。

通过 ASA Virtual 故障转移实现高可用性

使用 ASA virtual 创建故障转移对时，需要按相同顺序将数据接口添加到每个 ASA virtual。如果完全相同的接口添加到每个 ASA virtual，但采用不同的顺序，在 ASA virtual控制台上会显示错误。故障转移功能可能也会受到影响

其他准则

- 当主用设备故障转移到备用设备时，所连接的运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，会进入阻塞状态 30 秒至 50 秒。当端口处于阻塞状态时，为避免流量丢失，您可以根据交换机启用 STP PortFast 功能：

  interface *interface_id* **spanning-tree portfast**

  此解决方法适用于连接到路由模式和桥接组接口的交换机。链路打开时，PortFast功能会立即使端口转换到 STP 转发模式。该端口仍会参与 STP。因此，如果端口是环路的一部分，则端口最终会转换为 STP 阻塞模式。
- 发生故障转移事件时，在连接到 ASA故障转移对的交换机上配置端口安全性，可能会导致通信问题。一个安全端口上配置或获悉的安全 MAC 地址移至另一安全端口，交换机端口安全功能标记违例时，会发生此问题。
- 您最多可以在一台设备上监控跨所有情景的 1025 个接口。
- 对于主用/备用 故障转移和 VPN IPSec 隧道，无法使用 SNMP 通过 VPN 隧道监控主用设备和备用设备。备用设备没有有效的 VPN 隧道，将丢弃发往 NMS 的流量。您可以改为使用具有加密功能的 SNMPv3，因此不需要 IPsec 隧道。
- 对于主用/主用故障转移，不应在相同 ASR 组中配置相同情景中的两个接口。
- 对于主用/主用故障转移，最多可以定义两个故障转移组。
- 对于主用/主用故障转移，删除故障转移组时，必须最后删除故障转移组 1。故障转移组 1 始终包含管理情景。未分配到故障转移组的所有情景将默认分配到故障转移组 1。不能删除已显式分配了情景的故障转移组。
- 故障转移后，系统日志消息的源地址将立即成为故障转移接口地址几秒钟。
- 为了更好地融合（在故障转移期间），您必须关闭 HA 对上未与任何配置或实例关联的接口。
- 如果您在评估模式下配置故障转移加密，系统将使用 DES 进行加密。如果随后您使用出口合规账户注册设备，则设备将在重新启动后使用 AES。因此，如果系统出于任何原因重新启动，包括安装升级后，对等体将无法通信，两台设备将变为主用设备。建议您在注册设备之前不要配置加密。如果您在评估模式下进行此配置，建议您在注册设备之前删除加密。
- 当使用具有故障转移功能的 SNMPv3 时，如果更换故障转移设备，则 SNMPv3 用户不会复制到新设备。您必须将 SNMPv3 用户重新添加到主用设备，以强制用户复制到新设备；或者，也可

以直接在新设备上添加用户。重新配置每个用户，方法是在控制/主用设备上输入 **snmp-server user** *username group-name* **v3** 命令，或者直接使用未加密形式的 *priv-password* 选项和 *auth-password* 选项直接连接到备用设备。

- 设备不再与其对等体共享 SNMP 客户端引擎数据。
- 如果您有大量访问控制和NAT规则，则配置的大小可能会阻止有效的配置复制，导致备用设备需要过长的时间才能达到备用就绪状态。这也会影响您在通过控制台或 SSH 会话进行复制期间连接到备用设备的能力。要提高配置复制性能，请使用 **asp rule-engine transactional-commit access-group** 和 **asp rule-engine transactional-commit nat** 命令为访问规则和 NAT 启用事务提交。
- 转换为备用角色的 故障转移 对中的设备可将其时钟与主用设备同步。

  示例：

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby               Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config                Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- 故障转移 中的设备不会动态同步时钟。以下是进行同步时的一些事件示例：
  - 将创建一个新的 故障转移 对。
  - 故障转移 已中断并已重新创建。
  - 故障转移链路上的通信中断并重新建立。
  - 使用 **no failover/failover** 或 **configure high-availability suspend/resume** （威胁防御）命令来在 CLI 。
- 启用 故障转移 会强制删除所有路由，并会在 故障转移 进程变为“活动”状态后重新添加这些路由。在此阶段，您可能会遇到连接丢失的情况。
- 如果在独立设备上启用故障转移，数据接口将在故障转移协商状态下关闭，从而中断流量。
- 在 故障转移 配置中，短期连接（通常使用端口 53）会快速关闭，并且永远不会从主用设备传输或同步到备用设备，因此两个 故障转移 设备上的连接数量可能存在差异。这是短期连接的预期行为。您可以尝试比较长期（例如，超过 30-60 秒）的连接。
- 在故障转移配置中，初期连接（尚未完成三次握手过程的连接请求）会快速关闭，并且不会在主用设备和备用设备之间同步。此设计可确保高可用性系统的效率和安全性。因此，两台 故障转移 设备上的连接数可能存在差异，这是预期行为。

- 如果故障转移LAN链路不是背靠背连接，而是通过一台或多台交换机连接，则中间路径内的故障可能会导致主用设备失去与备用设备的连接，从而导致主用/备用状态不一致。虽然这不会影响 故障转移 功能，但建议检查并恢复主用设备和备用设备之间的故障转移链路路径。

  当故障转移 LAN 链路发生故障时，不建议部署任何配置，因为它可能不会复制到对等设备。

- 在 ASA 的 OSPF 中，如果附近的交换机宕机，而 ASA 接口与同一交换机相连，则防火墙中的接口也会随着交换机故障而关闭。这是预期行为。这将按照设计触发高可用性故障转移。
- 如果备用 ASA 连接到不同的交换机，在这种情况下，当接口启动时，路由表将与活动 ASA 的路由表不同。这将导致短时间内（约 15-17 秒）中断，直至更新路由和邻接关系。

故障转移的默认设置

默认情况下，故障转移策略包含以下内容：

- 在状态故障转移中不进行 HTTP 复制。
- 单个接口故障导致故障转移。
- 接口轮询时间为 5 秒。
- 接口保持时间为 25 秒。
- 设备轮询时间为 1 秒。
- 设备保持时间为 15 秒。
- 在组播情景模式下。
- 监控所有物理接口。

配置主用/备用故障转移

要配置主用/备用故障转移，请在主设备和辅助设备上配置基本故障转移设置。其他所有配置仅在主设备上进行，然后这些设置会同步到辅助设备。

为主用/备用故障转移配置主设备

遵循本节介绍的步骤，配置主用/备用故障转移配置中的主设备。这些步骤提供了在主设备上启用故障转移所需的最小配置。

开始之前

- 我们建议您为除故障转移和状态链路外的所有接口配置备用IP地址。如果对于点对点连接使用 31 位子网掩码，请勿配置备用 IP 地址。如果为 DHCP 配置了任何接口，您将无法启用故障转移。

- 请勿为故障转移和状态链路配置 **nameif**。
- 对于多情景模式，请在系统执行空间中完成本程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。

过程

步骤 1 将此设备指定为主设备：

failover lan unit primary

步骤 2 指定要用作故障转移链路的接口：

failover lan interface *if_name interface_id*

示例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

此接口不可用于任何其他用途（但用于状态链路除外）。

if_name 参数可为接口指定名称。

interface_id 参数可以是数据物理接口、子接口、或 EtherChannel 接口 ID。在 Firepower 1010 和 Cisco Secure Firewall 1210/1220 上，该接口是防火墙接口 ID；不能指定交换机端口 ID 或 VLAN ID。Firepower 4100/9300 可以使用任何数据类型接口。

步骤 3 为故障转移链路分配主用和备用 IP 地址：

failover interface ip *failover_if_name* {*ip_address mask* | *ipv6_address* / *prefix*} **standby** *ip_address*

示例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

或：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

此地址应处于未使用的子网上。 此子网可以是 31 位 (255.255.255.254)，仅包含两个 IP 地址。169.254.0.0/16 和 fd00:0:0:*::/64 是内部使用的子网，不能用于故障转移或状态链路。

备用 IP 地址必须与主用 IP 地址位于同一子网。

步骤 4 启用故障转移链路：

interface *failover_interface_id*

no shutdown

示例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

步骤 5 （可选）如果想要使用状态链路的单独接口，指定此接口。

failover link *if_name interface_id*

示例：

```
ciscoasa(config)# failover link folink gigabitethernet0/4
```

如果不指定单独的接口，则故障转移链路将用于状态链路。

if_name 参数可为接口指定名称。

interface_id 参数可以是数据物理接口、子接口或 EtherChannel 接口 ID。在 Firepower 1010 和 Cisco Secure Firewall 1210/1220 上，该接口是防火墙接口 ID；不能指定交换机端口 ID 或 VLAN ID。

步骤 6 如果您指定了单独的状态链路，可以将主用和备用 IP 地址分配给状态链路：

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

示例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

或：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

此地址应处于不同于故障转移链路的未使用子网上。此子网可以是 31 位 (255.255.255.254)，仅包含两个 IP 地址。169.254.0.0/16 和 fd00:0:0:*::/64 是内部使用的子网，不能用于故障转移或状态链路。

备用 IP 地址必须与主用 IP 地址位于同一子网。

如果您将共享状态链路，请跳过此步骤。

步骤 7 如果您指定了单独的状态链路，请启用状态链路。

interface *state_interface_id*

no shutdown

示例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

如果您将共享状态链路，请跳过此步骤。

步骤 8 （可选）请执行以下任一操作，以加密故障转移和状态链路上的通信：

- （首选）在设备之间的故障转移和状态链路上建立 IPsec LAN 到 LAN 隧道，以加密所有的故障转移通信：

  failover ipsec pre-shared-key [**0** | **8**] 密钥

  示例：

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  该 *key* 的最大长度为 128 个字符。确定两台设备上的相同密钥。此密钥由 IKEv2 用于建立隧道。

  如果使用主密码（请参阅配置主密码，第 824 页），则该密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密密钥。默认情况下使用 **0**，表明未加密的密码。

  failover ipsec pre-shared-key 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。

  如果您未配置故障转移和状态链路加密，故障转移通信（包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

  不能同时使用 IPsec 加密和传统 **failover key** 加密。如果同时配置两种方法，将使用 IPsec。不过，如果使用主密码，则在配置 IPsec 加密之前必须首先使用 **no failover key** 命令删除故障转移密钥。

  故障转移 LAN 到 LAN 隧道不计入 IPsec（其他 VPN）许可证。

- （可选）对故障转移和状态链路上的故障转移通信进行加密：

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  示例：

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  使用 1 到 63 个字符的 *shared_secret*，或者 32 个字符的 **hex** *key*。对于 *shared_secret*，您可以任意组合使用数字、字母或标点符号。该共享密钥或十六进制密钥用于生成加密密钥。确定两台设备上的相同密钥。

  如果使用主密码（请参阅配置主密码，第 824 页），则共享密钥或十六进制密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密的共享密钥或十六进制密钥。默认情况下使用 **0**，表明未加密的密码。

  failover key 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。

  如果您未配置故障转移和状态链路加密，故障转移通信（包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

步骤 9 启用故障转移：

failover

步骤 10 将系统配置保存到闪存：

write memory

示例

以下示例配置主设备的故障转移参数：

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

为主用/备用故障转移配置辅设备

在辅助设备上只需要配置故障转移链路。最初辅助设备需要这些命令来与主设备进行通信。在主设备将其配置发送到辅助设备后，两个配置之间的唯一永久性差别是 **failover lan unit** 命令，该命令可确定每台设备是主设备，还是辅助设备。

开始之前

- 如果为 DHCP 配置了任何接口，您将无法启用故障转移。
- 请勿为故障转移和状态链路配置 **nameif**。
- 对于多情景模式，请在系统执行空间中完成本程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。

过程

步骤 1 在主设备上重新输入完全相同的命令，**failover lan unit primary** 命令除外。或者，您可以使用 **failover lan unit secondary** 命令代替该命令，但这并非必需，因为 **secondary** 是默认设置。请参阅为主用/备用故障转移配置主设备，第 282 页。

例如：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-ifc)# no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
```

```
ciscoasa(config)# failover
```

步骤 2 故障转移配置同步之后，会将配置保存到闪存：

```
ciscoasa(config)# write memory
```

配置主用/主用故障转移

本节介绍如何配置主用/主用故障转移。

为主用/主用故障转移配置主设备

遵循本节介绍的步骤，配置主用/主用故障转移配置中的主设备。这些步骤提供了在主设备上启用故障转移所需的最小配置。

开始之前

- 根据启用或禁用多情景模式，第 228 页启用多情景模式。
- 除故障转移和状态链路之外，我们建议您根据路由模式接口和透明模式接口，第 749 页为所有接口配置备用 IP 地址。 如果对于点对点连接使用 31 位子网掩码，请勿配置备用 IP 地址。如果为 DHCP 配置了任何接口，您将无法启用故障转移。
- 请勿为故障转移和状态链路配置 **nameif**。
- 在系统执行空间中完成本程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。

过程

步骤 1 将此设备指定为主设备：

failover lan unit primary

步骤 2 指定要用作故障转移链路的接口：

failover lan interface *if_name interface_id*

示例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

此接口不可用于任何其他用途（但用于状态链路除外）。

if_name 参数可为接口指定名称。

interface_id 参数可以是数据物理接口、子接口或 EtherChannel 接口 ID。Firepower 4100/9300 可以使用任何数据类型接口。

步骤 3 为故障转移链路分配主用和备用 IP 地址：

standby failover interface ip *if_name* {*ip_address mask* | *ipv6_address*/*prefix* } **standby** *ip_address*

示例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

或：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

此地址应处于未使用的子网上。 此子网可以是 31 位 (255.255.255.254)，仅包含两个 IP 地址。169.254.0.0/16 和 fd00:0:0:*::/64 是内部使用的子网，不能用于故障转移或状态链路。

备用 IP 地址必须与主用 IP 地址位于同一子网。

步骤 4 启用故障转移链路：

interface *failover_interface_id*

no shutdown

示例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

步骤 5 （可选）如果想要使用状态链路的单独接口，指定此接口。

failover link *if_name interface_id*

示例：

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

我们建议您使用故障转移链路中的一个单独状态链路。如果不指定单独的接口，则故障转移链路将用于状态链路。

if_name 参数可为接口指定名称。

interface_id 参数可以是数据物理接口、子接口或 EtherChannel 接口 ID。

步骤 6 如果您指定了单独的状态链路，可以将主用和备用 IP 地址分配给状态链路：

此地址应处于不同于故障转移链路的未使用子网上。 此子网可以是 31 位 (255.255.255.254)，仅包含两个 IP 地址。169.254.0.0/16 和 fd00:0:0:*::/64 是内部使用的子网，不能用于故障转移或状态链路。

备用 IP 地址必须与主用 IP 地址位于同一子网。

如果您将共享状态链路，请跳过此步骤。

failover interface ip state *if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

示例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

或：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

步骤 7 如果您指定了单独的状态链路，请启用状态链路：

interface *state_interface_id*

no shutdown

示例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

如果您将共享状态链路，请跳过此步骤。

步骤 8 （可选）请执行以下任一操作，以加密故障转移和状态链路上的通信：

- （首选）在设备之间的故障转移和状态链路上建立 IPsec LAN 到 LAN 隧道，以加密所有的故障转移通信：

  failover ipsec pre-shared-key [**0** | **8**] 密钥

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  该 *key* 的最大长度为 128 个字符。确定两台设备上的相同密钥。此密钥由 IKEv2 用于建立隧道。

  如果使用主密码（请参阅配置主密码，第 824 页），则该密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密密钥。默认情况下使用 **0**，表明未加密的密码。

  failover ipsec pre-shared-key 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。

  如果您未配置故障转移和状态链路加密，故障转移通信（包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

  不能同时使用 IPsec 加密和传统 **failover key** 加密。如果同时配置两种方法，将使用 IPsec。不过，如果使用主密码，则在配置 IPsec 加密之前必须首先使用 **no failover key** 命令删除故障转移密钥。

故障转移 LAN 到 LAN 隧道不计入 IPsec（其他 VPN）许可证。

- （可选）对故障转移和状态链路上的故障转移通信进行加密：

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  使用 *shared_secret*（1 到 63 个字符）或 32 个字符的 **十六进制** 密钥。

  对于 *shared_secret*，您可以任意组合使用数字、字母或标点符号。该共享密钥或十六进制密钥用于生成加密密钥。确定两台设备上的相同密钥。

  如果使用主密码（请参阅配置主密码，第 824 页），则共享密钥或十六进制密钥会在配置中加密。如果从配置复制（例如，从 **more system:running-config** 输出复制），则指定使用 **8** 关键字加密的共享密钥或十六进制密钥。默认情况下使用 **0**，表明未加密的密码。

  failover key 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。

  如果您未配置故障转移和状态链路加密，故障转移通信（包括在命令复制过程中发送的配置中的所有密码或密钥）将采用明文形式。

步骤 9 创建故障转移组 1：

failover group 1

primary

preempt [*delay*]

示例：

```
ciscoasa(config-fover-group)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 1200
```

通常，您可以将组 1 分配给主设备，将组 2 分配给辅助设备。两个故障转移组在首次启动的设备上都会变成主用状态（即使它们看似同时启动，但一台设备会首先变成主用状态），不考虑该组的主要或辅助设置。当指定设备变得可用时，**preempt** 命令会使故障转移组自动在该设备上变为主用状态。

您可以输入可选的 *delay* 值，该值指定故障转移组在指定设备上自动变为主用状态之前，在当前设备上保持主用状态的秒数。有效值范围为 1 至 1200。

如果启用状态故障转移，则抢占会延迟，直到连接从当前处于主用状态的故障转移组所在的设备中复制为止。

如果手动执行故障转移，则会忽略 **preempt** 命令。

步骤 10 创建故障转移组 2，并将其分配至辅助设备：

failover group 2

secondary

preempt [*delay*]

示例：

```
ciscoasa(config-fover-group)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 1200
```

步骤 11 进入给定情景的情景配置模式，然后将该情景分配给故障转移组：

context 名称

join-failover-group {**1** | **2**}

示例：

```
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

对每个情景重复此命令。

所有未分配的情景会自动分配到故障转移组 1。管理情景始终是故障转移组 1 的成员；您不能将其分配给组 2。

步骤 12 启用故障转移：

failover

步骤 13 将系统配置保存到闪存：

write memory

示例

以下示例配置主设备的故障转移参数：

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4

failover interface ip statelink 172.27.48.2 255.255.255.254 standby 172.27.48.3
interface gigabitethernet 0/4
  no shutdown
failover group 1
  primary
  preempt
failover group 2
  secondary
  preempt
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
```

```
failover
```

为主用/主用故障转移配置辅助设备

在辅助设备上只需要配置故障转移链路。最初辅助设备需要这些命令来与主设备进行通信。在主设备将其配置发送到辅助设备后，两个配置之间的唯一永久性差别是 **failover lan unit** 命令，该命令可确定每台设备是主设备，还是辅助设备。

开始之前

- 根据启用或禁用多情景模式，第 228 页启用多情景模式。
- 如果为 DHCP 配置了任何接口，您将无法启用故障转移。
- 请勿为故障转移和状态链路配置 **nameif**。
- 在系统执行空间中完成本程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。

过程

步骤 1 在主设备上重新输入完全相同的命令，**failover lan unit primary** 命令除外。或者，您可以使用 **failover lan unit secondary** 命令代替该命令，但这并非必需，因为 **secondary** 是默认设置。您也不需要输入 **failover group** 和 **join-failover-group** 命令，因为这些命令会从主设备复制。请参阅为主用/主用故障转移配置主设备，第 287 页。

例如：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

步骤 2 故障转移配置通过主设备同步后，将配置保存到闪存：

ciscoasa(config)# **write memory**

步骤 3 如果需要，可强行要求故障转移组 2 在辅助设备上处于主用状态：

failover active group 2

配置可选故障转移参数

您可以视需要自定义故障转移设置。

配置故障转移条件和其他设置

有关您可在本节中更改的许多参数的默认设置，请参阅故障转移的默认设置，第 282 页。对于主用/主用模式，您可以设置每个故障转移组的大多数条件。。

开始之前

- 在多情景模式下，可在系统执行空间中配置这些设置。
- 如需为设备运行状况监控配置双向转发检测 (BFD)，请参阅以下限制：
  - 仅限 Firepower 9300 和 4100。
  - 仅限主用/备用。
  - 仅限路由模式

过程

步骤 1 更改设备的轮询和保持时间：

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

示例：

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

polltime 范围介于 1 和 15 秒之间，或者 200 和 999 毫秒之间。**holdtime** 范围介于 1 到 45 秒之间或 800 到 999 毫秒之间。输入的保持时间值不能小于设备轮询时间的 3 倍。设置的轮询时间越快，ASA 便可越快检测到故障并触发故障转移。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。

如果设备在一个轮询周期内未收到故障转移通信的呼叫数据包，则会通过其余接口进行其他的测试。如果在保持时间内，仍未收到来自对等设备的响应，该设备会被视为发生故障，如果故障设备为主用设备，则备用设备会进行接管，成为主用设备。

在主用/主用模式下，您可以为系统设置此速率；但不能为每个故障转移组设置此速率。

步骤 2 为设备运行状况监控配置 BFD。

定期监控设备可能会在 CPU 使用率高时导致错误报警。BFD 方法是分布式的，所以高 CPU 不会影响其运行。

a) 定义要用于故障转移运行状况检测的 BFD 模板：

bfd-template single-hop *template_name*

bfd interval min-tx *milliseconds***min-rx** *milliseconds* **multiplier** *multiplier_value*

示例：

```
ciscoasa(config)# bfd template single-hop failover-temp
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
```

min-tx 指定 BFD 控制数据包被发送到故障转移对等体的速率。范围介于 50 到 999 毫秒之间。**min-rx** 指定预计收到来自故障转移对等体的 BFD 控制数据包的速率。范围介于 50 到 999 毫秒之间。**multiplier** 指定在 BFD 声明对等体不可用之前必须错过来自该故障转移对等体的连续 BFD 控制数据包数。范围为 3 到 50。

此外，还可以为此模板配置回应和身份验证；请参阅创建 BFD 模板，第 967 页。

b) 为运行状况监控启用 BFD：

failover health-check bfd *template_name*

示例：

```
ciscoasa(config)# failover health-check bfd failover-temp
```

步骤 3 更改接口链路状态轮询时间：

failover polltime link-state msec *poll_time*

示例：

```
ciscoasa(config)# failover polltime link-state msec 300
```

范围为 300 至 799 毫秒。默认情况下，故障转移对中的每个 ASA 每隔 500 毫秒检查一次其接口的链路状态。您可以自定义轮询时间；例如，如果将轮询时间设置为 300 毫秒，则 ASA 可以更快地检测接口故障并触发故障转移。

在主用/主用模式下，您可以为系统设置此速率；但不能为每个故障转移组设置此速率。

步骤 4 设置每秒连接中的会话复制速率：

failover replication rate *conns*

示例：

```
ciscoasa(config)# failover replication rate 20000
```

最小和最大速率取决于您的型号。默认值为最大速率。在主用/主用模式下，您可以为系统设置此速率；但不能为每个故障转移组设置此速率。

步骤 5 禁用在备用设备或情景中直接进行任何配置更改的功能：

failover standby config-lock

默认情况下，允许备用设备/情景上进行配置，但系统会显示一条警告消息。

步骤 6 （仅主用/主用模式）指定要自定义的故障转移组：

{| } **failover group1 2**

示例：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

步骤 7 启用 HTTP 状态复制：

- 对于主用/备用模式：

  failover replication http

- 对于主用/主用模式：

  replication http

要允许在状态信息复制中包含 HTTP 连接，您需要启用 HTTP 复制。我们建议启用HTTP状态复制。

注释
由于使用故障转移时从备用设备中删除 HTTP 数据流会产生延迟，所以 **show conn count** 输出在主用设备与备用设备上可能显示不同的数量；如果等待几秒钟再重新发出该命令，则会在两台设备上看到相同的数量。

步骤 8 设置接口发生故障时的故障转移阈值：

- 对于主用/备用模式：

  failover interface-policy *num* [%]

  示例：

  ```
  ciscoasa (config)# failover interface-policy 20%
  ```

- 对于主用/主用模式：

  interface-policy *num* [%]

  示例：

  ```
  ciscoasa(config-fover-group)# interface-policy 20%
  ```

默认情况下，一个接口故障会导致故障转移。

在指定接口的特定数量时，*num* 参数可介于 1 到 1025 之间。

在指定接口的百分比时，*num* 参数可介于 1 到 100 之间。

步骤 9 更改接口轮询和保持时间：

- 对于主用/备用模式：

  failover polltime interface [**msec**] *polltime* [**holdtime** *time*]

  示例：

  ```
  ciscoasa(config)# failover polltime interface msec 500 holdtime 5
  ```

- 对于主用/主用模式：

  polltime interface [**msec**] *polltime* [**holdtime***time*]

  示例：

  ```
  ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
  ```

- polltime-设置向对等体发送呼叫数据包之间的等待时间。轮询时间的有效值介于 1 到 15 秒之间；如果使用可选的 **msec** 关键字，则有效值介于 500 到 999 毫秒之间。默认值为 5 秒。
- **holdtime***time*-设置从对等体设备最后收到的*Hello*消息与开始接口测试以确定接口运行状况之间的时间（作为计算）。它还将每个接口测试的持续时间设置为holdtime / 16。有效值范围为 5 至 75 秒。默认值为轮询时间的5倍。输入的保持时间值不得短于设备轮询时间的 5 倍。

  要计算开始接口测试之前的时间（y），请执行以下操作：

  1. x =（*holdtime*/*polltime*）/ 2，四舍五入为最接近的整数。（.4 和向下四舍五入； 0.5 和向上四舍五入。）
  2. y = x**polltime*

  例如，如果使用默认保持时间25和轮询时间5，则y = 15秒。

步骤 10 配置接口的虚拟 MAC 地址：

- 对于主用/备用模式：

  failover mac address *phy_if active_mac standby_mac*

  示例：

  ```
  ciscoasa(config)# failover mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
  ```

- 对于主用/主用模式：

  mac address *phy_if active_mac standby_mac*

  示例：

  ```
  ciscoasa(config-fover-group)# mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
  ```

phy_if 参数是接口的物理名称，例如，gigabitethernet0/1。

active_mac 和 *standby_mac* 参数是 H.H.H 格式的 MAC 地址，其中 H 是 16 位十六进制数字。例如，MAC 地址 00-0C-F1-42-4C-DE 将需要输入 000C.F142.4CDE。

active_mac 地址与接口的活动 IP 地址相关联，而 *standby_mac* 与接口的备用 IP 地址相关联。

您也可以使用其他命令或方法设置 MAC 地址，但是我们建议只使用一种方法。如果使用多种方法设置 MAC 地址，所使用的 MAC 地址会取决于许多变量，可能会不可预测。

使用 **show interface** 命令可显示接口使用的 MAC 地址。

步骤 11 （仅限主用/主用模式）对于其他故障转移组重复此操作步骤。

配置接口监控

默认情况下，在所有物理接口上启用监控，或者对于 Firepower 1010，以及 Cisco Secure Firewall 1210/1220，则为所有 VLAN 接口。Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口无法进行接口监控。

您可能希望排除连接到非关键网络的接口，以免影响故障转移策略。

您最多可以在一台设备上监控 1025 个接口（跨多情景模式下的所有情景）。

开始之前

在多情景模式下，请在每个情景中配置接口。

过程

启用或禁用接口运行状况监控：

[**no**] **monitor-interface** {*if_name*}

示例：

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```

配置非对称路由数据包支持（主用/主用模式）

在主用/主用故障转移下运行时，设备可能会收到其对等设备发起的连接的一个返回数据包。由于收到该数据包的 ASA 没有该数据包的任何连接信息，该数据包会被丢弃。主用/主用故障转移对中的两台 ASA 连接到不同的运营商，并且出站连接不使用 NAT 地址时，最常发生此丢弃。

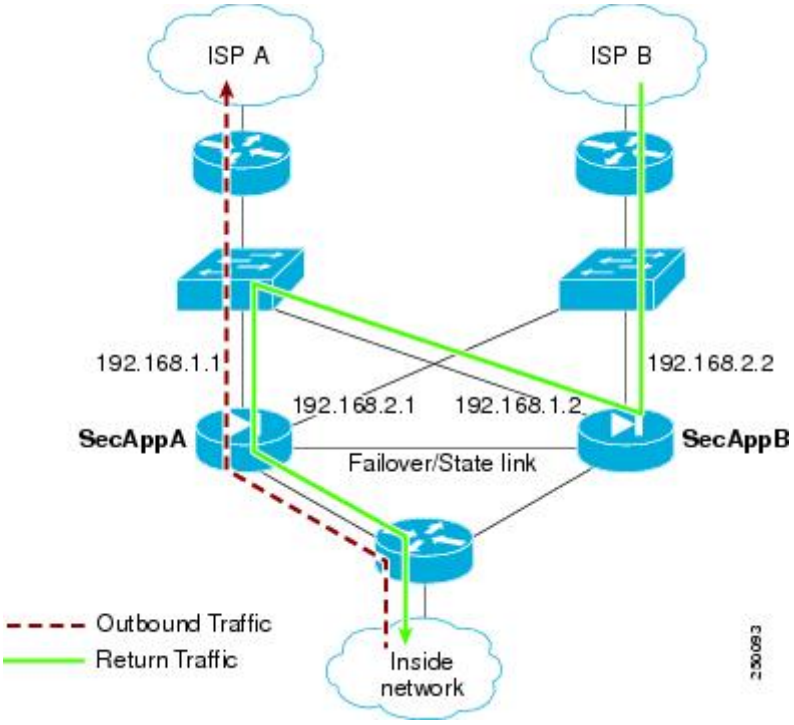
您可以通过允许非对称路由数据包来防止返回数据包。为此，您需要将每台ASA上的相似接口分配到同一个ASR组。例如，两台ASA的内部接口连接到内部网络，但外部接口连接到不同的ISP。在主设备上，将主用情景外部接口分配给 ASR 组 1；在辅助设备上，将主用情景外部接口分配给相同 ASR 组 1。当主设备外部接口收到没有其会话信息的数据包时，它会检查相同组中处于备用情景中的另一接口的会话信息；在此示例中，即 ASR 组 1。如果没有找到匹配项，数据包会被丢弃。如果找到匹配项，则会进行以下的操作：

- 如果传入流量来自对等设备，第 2 层报头的部分或全部内容会被重写，数据包会被重定向到另一设备。只要会话处于活动状态，此重定向即可继续。
- 如果传入流量来自相同设备上的不同接口，第 2 层报头的部分或全部内容会被重写，数据包会被重新注入数据流。

注释 此功能不提供非对称路由；它会将非对称路由数据包恢复到正确接口。

下图显示非对称路由数据包的示例。

图 *48: ASR* 示例



1. 出站会话使用主用 SecAppA 情景通过 ASA。该会话退出接口 outsideISP-A (192.168.1.1)。
2. 由于上游某处配置了非对称路由，返回流量会使用主用 SecAppA 情景通过 ASA 上的接口 outsideISP-B (192.168.2.2) 传回。
3. 由于没有接口 192.168.2.2 上的流量的会话信息，返回流量通常会被丢弃。但是，此接口被配置为 ASR 组 1 的一部分。设备会在配置为相同的 ASR 组 ID 的所有其他接口上查找该会话。

4. 会话信息会在接口 outsideISP-A (192.168.1.2) 上找到，该接口在使用 SecAppB 情景的设备上处于备用状态。状态故障转移会将会话信息从 SecAppA 复制到 SecAppB。
5. 第 2 层报头会使用接口 192.168.1.1 的信息重写，流量会被重定向，通过接口 192.168.1.2，在该接口上，流量随后会通过设备上的来源接口（SecAppA 上的 192.168.1.1）返回，而不是将流量丢弃。此转发会视需要继续，直到会话结束。

开始之前

- 状态故障转移 - 将主用故障转移组中的接口上的会话的状态信息，传送给备用故障转移组。
- 复制 HTTP - HTTP 会话状态信息不会传送给备用故障转移组，因此不存在于备用接口上。为了使 ASA 能够重新路由非对称路由的 HTTP 数据包，您需要复制 HTTP 状态信息。
- 请在主设备和辅助设备上的每个主用情景中，执行本程序。
- 您无法在一个情景中同时配置 ASR 组和流量区域。如果在情景中配置一个区域，任何情景接口都不能属于 ASR 组。

过程

步骤 1 在主设备上，指定要允许非对称路由数据包的接口：

interface *phy_if*

示例：

```
primary/admin(config)# interface gigabitethernet 0/0
```

步骤 2 设置接口的 ASR 组编号：

asr-group *num*

示例：

```
primary/admin(config-ifc)# asr-group 1
```

num 的有效值范围为 1 到 32。

步骤 3 在辅助设备上，指定要允许非对称路由数据包的类似接口：

interface *phy_if*

示例：

```
secondary/ctx1(config)# interface gigabitethernet 0/1
```

步骤 4 设置接口的 ASR 组编号，以匹配主设备接口：

asr-group *num*

示例：

```
secondary/ctx1(config-ifc)# asr-group 1
```

示例

两台设备具有以下配置（配置仅显示相关命令）。图中标记为 SecAppA 的设备是故障转移对中的主设备。

主设备系统配置

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
interface GigabitEthernet0/2
  no shutdown
interface GigabitEthernet0/3
  no shutdown
interface GigabitEthernet0/4
  no shutdown
interface GigabitEthernet0/5
  no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
  primary
failover group 2
  secondary
admin-context SecAppA
context admin
  allocate-interface GigabitEthernet0/2
  allocate-interface GigabitEthernet0/3
  config-url flash:/admin.cfg
  join-failover-group 1
context SecAppB
  allocate-interface GigabitEthernet0/4
  allocate-interface GigabitEthernet0/5
  config-url flash:/ctx1.cfg
  join-failover-group 2
```

SecAppA 情景配置

```
interface GigabitEthernet0/2
  nameif outsideISP-A
  security-level 0
  ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  asr-group 1
interface GigabitEthernet0/3
  nameif inside
  security-level 100
  ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
monitor-interface outside
```

SecAppB 情景配置

```
interface GigabitEthernet0/4
  nameif outsideISP-B
  security-level 0
  ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
  asr-group 1
interface GigabitEthernet0/5
  nameif inside
  security-level 100
  ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11
```

管理故障转移

本部分介绍您在启用故障转移后如何管理故障转移，包括如何更改故障转移设置以及如何强制从一台设备故障转移到另一台设备。

强制故障转移

要强制要求备用设备成为主用设备，请执行以下程序。

开始之前

在多情景模式下，请在系统执行空间中执行本程序。

过程

步骤 1 在备用设备上输入时，可以强制故障转移。备用设备将成为主用设备。

如果指定 **group** *group_id*，则在指定主用/主用故障转移组的备用设备上输入此命令时，将强制进行故障转移。备用设备将成为故障转移组的主用设备。

- 对于备用设备上的主用/备用模式：

  failover active

- 对于备用设备上的主用/主用模式：

  failover active [**group** *group_id*]

  示例：

  ```
  standby# failover active group 1
  ```

步骤 2 在主用设备上输入时，可以强制故障转移。主用设备将成为备用设备。

如果指定 **group** *group_id*，在指定故障转移组的主用设备上输入时，此命令将强制进行故障转移。主用设备将成为故障转移组的备用设备。

- 对于主用设备上的主用/备用模式：

  no failover active

- 对于主用设备上的主用/主用模式：

  no failover active [**group** *group_id*]

  示例：

```
active# no failover active group 1
```

禁用故障转移

在一台或两台设备上禁用故障转移，将会导致每台设备保持其主用和备用状态，直到您重新加载。对于主用/主用故障转移对，故障转移组在其处于主用状态的设备上保持主用状态，而无论它们被配置为首选哪一设备。

禁用故障转移时，请参阅以下特征：

- 备用设备/情景保持备用模式，以便两台设备都不开始传输流量（这称为假备用状态）。
- 备用设备/情景继续使用其备用 IP 地址，即使它不再连接到主用设备/情景也是如此。
- 备用设备/情景继续侦听故障转移链路上的连接。如果在主用设备/情景上重新启用故障转移，则备用设备/情景会在重新同步其他配置后恢复普通备用状态。
- 不要在备用设备上手动启用故障转移将其激活；请参阅强制故障转移，第 301 页。如果您在备用设备上启用故障转移，将看到可能会妨碍 IPv6 流量的 MAC 地址冲突。
- 要真正禁用故障转移，请将禁用故障转移配置保存到启动配置，然后重新加载。

开始之前

在多情景模式下，请在系统执行空间中执行本程序。

过程

步骤 1 禁用故障转移：

no failover

步骤 2 要完全禁用故障转移，请保存配置并重新加载：

write memory

reload

恢复故障设备

要将故障设备恢复到无故障状态，请执行以下程序。

开始之前

在多情景模式下，请在系统执行空间中执行本程序。

过程

步骤 1 将故障设备恢复为无故障状态：

- 对于主用/备用模式：

  failover reset

- 对于主用/主用模式：

  failover reset [**group** *group_id*]

  示例：

```
ciscoasa(config)# failover reset group 1
```

将故障设备恢复到无故障状态，不会自动使其成为主用设备；恢复后的设备将保持在备用状态，直到故障转移（强制或自然）使其变为主用状态。例外情况是，配置了故障转移抢占的故障转移组（仅主用/主用模式）。如果故障转移组之前处于主用状态且配置了抢占，并且它是在首选设备上发生故障的，则该故障转移组将变为主用状态。

如果指定 **group** *group_id*，此命令会将发生故障的主用/主用故障转移组恢复到无故障状态。

步骤 2 （仅主用/主用模式）要在故障转移组级别重置故障转移，请执行以下步骤：

a) 在 System 中，依次选择 **Monitoring > Failover > Failover Group #**，其中 # 是要控制的故障转移组的编号。

b) 点击 **Reset Failover**。

重新同步配置

如果在主用设备上输入 write standby 命令，备用设备将清除其运行配置（用于与主用设备进行通信的故障转移命令除外），并且，主用设备会将其完整配置发送到备用设备。

对于多情景模式，当您在系统执行空间中输入 **write standby** 命令时，系统将复制所有情景。如果在情景中输入 **write standby** 命令，该命令只会复制情景配置。

复制命令会存储在运行配置中。

测试故障转移功能

要测试故障转移功能，请执行以下程序。

过程

步骤 1 测试您的主用设备是否在通过使用 FTP（例如）来在不同接口上的主机之间发送文件，从而如预期传送流量。

步骤 2 在主用设备上输入以下命令，从而强制进行故障转移：

主用/备用模式：

ciscoasa(config)# **no failover active**

主用/主用模式：

ciscoasa(config)# **no failover active group** *group_id*

步骤 3 使用 FTP 在相同的两台主机之间发送另一个文件。

步骤 4 如果测试不成功，请输入 **show failover** 命令检查故障转移状态。

步骤 5 完成后，您可以在新的主用设备上输入以下命令，从而将设备恢复到主用状态：

主用/备用模式：

ciscoasa(config)# **no failover active**

主用/主用模式：

ciscoasa(config)# **failover active group** *group_id*

注释

ASA 接口关闭时，为了进行故障转移，该接口仍被视为是设备问题。如果 ASA 检测到接口关闭，会立即进行故障转移，而不等待接口保持时间。仅当 ASA 将接口状态视为 OK 时，接口保持时间才有用，但 ASA 并未从对等体接收呼叫数据包。要模拟接口保持时间，请关闭交换机上的 VLAN，以阻止对等体收到彼此的呼叫数据包。

远程命令执行

远程命令执行允许您将在命令行输入的命令发送到特定的故障转移对等体。

发送命令

由于配置命令会从主用设备或情景复制到备用设备或情景，所以无论您登录哪台设备，都可以使用 **failover exec** 命令在正确设备输入配置命令。例如，如果您登录到备用设备，可以使用 **failover exec active** 命令向主用设备发送配置更改。这些更改随后会复制到备用设备。不要使用 **failover exec** 命令向备用设备或情景发送配命令；这些配置更改不会被复制到主用设备，而且两种配置不会再进行同步。

configuration、exec 和 **show** 命令的输出显示在当前终端会话中，所以您可以使用 **failover exec** 命令在对等设备上发出 **show** 命令并在当前终端中查看结果。

您必须拥有足够在本地设备上执行命令的权限才能在对等设备上执行命令。

过程

步骤 1 如果您处于多情景模式下，请使用 **changeto context***name* 命令更改要配置的情景。无法使用 **failover exec** 命令在故障转移对等体上更改情景。

步骤 2 使用以下命令，将命令发送到指定的故障转移设备：

ciscoasa(config)# **failover exec** {**active** | **mate** | **standby**}

使用 **active** 或 **standby** 关键字可导致命令在指定设备上执行，即便该设备为当前设备。使用 **mate** 关键字可导致命令在故障转移对等体上执行。

导致命令模式更改的命令不会更改当前会话的提示。必须使用 **show failover exec** 命令来显示执行该命令的命令模式。有关详细信息，请参阅更改命令模式。

更改命令模式

failover exec 命令会保持独立于您的终端会话命令模式的命令模式状态。默认情况下，**failover exec** 命令在指定设备的全局配置模式下启动。您可以使用 **failover exec** 命令发送适当的命令（如 **interface** 命令）来更改该命令模式。当使用 **failover exec** 更改模式时，会话提示不会更改。

例如，如果您登录到故障转移对的主用设备的全局配置模式，然后使用 **failover exec active** 命令切换到接口配置模式，终端提示将保持处于全局配置模式，但使用 **failover exec** 输入的命令在接口配置模式下输入。

以下示例显示了终端会话模式和 **failover exec** 命令模式之间的差异。在此示例中，管理员将主用设备上的 **failover exec** 模式更改为 GigabitEthernet0/1 接口的接口配置模式。之后，使用 **failover exec active** 将输入的所有命令都会发送到接口 GigabitEthernet0/1的接口配置模式。然后，管理员使用 failover exec active 为该接口分配 IP 地址。虽然提示表明处于全局配置模式，**failover exec active** 模式实际上处于接口配置模式。

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# failover exec active ip address 192.168.1.1 255.255.255.0 standby
192.168.1.2
ciscoasa(config)# router rip
```

```
ciscoasa(config-router)#
```

更改设备当前会话的命令模式不会影响 **failover exec** 命令使用的命令模式。例如，如果您在主用设备上处于接口配置模式，并且您未更改**failover exec**命令模式，以下命令将在全局配置模式下执行。结果是您与设备的会话将保持处于接口配置模式，而使用 **failover exec active** 输入的命令将发送到指定的路由进程的路由器配置模式。

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

使用 **show failover exec** 命令可显示指定设备上的命令模式，通过 **failover exec** 命令发送的命令在该设备中执行。**show failover exec** 命令接受与 **failover exec** 命令相同的关键字：**active**、**mate** 或 **standby**。系统将单独跟踪每台设备的 **failover exec** 模式。

例如，以下内容是在备用设备上输入的 **show failover exec** 命令的示例输出：

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# sh failover exec active
Active unit Failover EXEC is at interface sub-command mode

ciscoasa(config)# sh failover exec standby
Standby unit Failover EXEC is at config mode

ciscoasa(config)# sh failover exec mate
Active unit Failover EXEC is at interface sub-command mode
```

安全注意事项

failover exec 命令使用故障转移链路向对等设备发送命令并接收对等设备的命令执行输出。您应在故障转移链路上启用加密，以防止窃听或中间人攻击。

远程命令执行的限制

当您使用远程命令时，会面临以下限制：

- 如果使用零停机升级程序升级一台设备，而不升级另一台设备，则两台设备正在运行的软件必须都支持 **failover exec** 命令。
- 命令完成和情景帮助对于 *cmd_string* 参数中的命令不可用。
- 在多情景模式下，只能向对等设备上的对等情景发送命令。要将命令发送到不同情景，必须在所登录的设备上切换到该情景。
- 不能将以下命令与 **failover exec** 命令配合使用：
  - **changeto**
  - **debug** (**undebug**)
- 备用设备处于故障状态时，如果这种故障是因服务卡故障引起，则该设备仍可以从**failover exec**命令接收命令；否则远程命令执行失败。

- 不能使用 **failover exec** 命令在故障转移对等体上从授权的 EXEC 模式切换到全局配置模式。例如，如果当前设备处于授权的 EXEC 模式下，并且您输入 **failover exec mate configure terminalfailover exec mate configure terminal**，则 **show failover exec mate** 输出将显示故障转移执行会话处于全局配置模式。但使用 **failover exec** 为对等体设备输入配置命令将会失败，直到您在当前设备上刚进入全局配置模式为止。
- 不能输入 recursive failover exec 命令，例如 **failover exec mate failover exec mate** 命令。
- 需要用户输入或确认的命令必须使用 **noconfirm** 选项。例如，要重新加载该伙伴，请输入：

  failover exec mate reload noconfirm

监控 故障转移

此部分用于监控故障转移状态。

故障转移消息

发生故障转移时，两台 ASA 都会发送系统消息。

故障转移系统日志消息

ASA 在优先级别 2 发出大量与故障转移有关的系统日志消息，级别 2 表示一种关键情况。要查看这些消息，请参阅系统日志消息指南。与故障转移关联的消息 ID 的范围是：101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx 和 727xxx。例如，105032 和 105043 表示故障转移链路存在问题。

注释 故障转移期间，ASA 按照逻辑先关闭接口，再启动接口，从而生成日志消息 411001 和 411002。这是正常活动。

故障转移调试消息

要查看调试消息，请输入 **debug fover** 命令。有关更多信息，请参阅命令参考。

注释 由于调试输出在 CPU 进程中分配的高优先级，它可能会极大地影响系统性能。为此，应仅在对特定问题进行故障排除或与思科 TAC 进行故障排除会话过程中使用 **debug fover** 命令。

SNMP 故障转移陷阱

要接收故障转移的 SNMP 系统日志陷阱，请将 SNMP 代理配置为发送 SNMP 陷阱到 SNMP 管理站、定义系统日志主机，并将思科系统日志 MIB 汇集到 SNMP 管理站中。

监控故障转移状态

要监控故障转移状态，请输入以下其中一个命令：

- **show failover**

  显示有关设备的故障转移状态的信息。

- **show failover group**

  显示有关故障转移组的故障转移状态的信息。显示的信息类似于 **show failover** 命令显示的信息，只不过前者限定于指定的组。

- **show monitor-interface**

  显示有关受监控接口的信息。

- **show running-config failover**

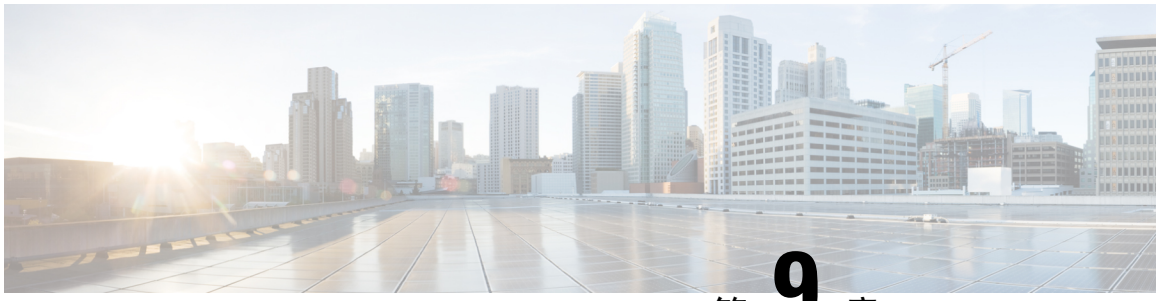
  显示运行配置中的故障转移命令。

故障转移的历史记录

功能名称	版本	功能信息
主用/备用故障转移	7.0(1)	引入了此功能。
主用/主用故障转移	7.0(1)	引入了此功能。
故障转移密钥支持使用十六进制值	7.0(4)	现在可以指定十六进制值用于故障转移链路加密。 修改了以下命令：**failover key hex**。
支持故障转移密钥的主密码	8.3(1)	故障转移密钥现在支持主密码，该密码用于加密运行配置和启动配置中的共享密钥。如果您在不同 ASA 之间复制共享密钥（例如通过 **more system:running-config** 命令），您可以成功复制和粘贴加密的共享密钥。 注释 **failover key** 在 **show running-config** 输出中显示为 ****；这种遮掩密钥无法复制。 修改了以下命令：**failover key** [**0** | **8**]。
添加了故障转移的 IPv6 支持。	8.2(2)	修改了以下命令：**failover interface ip**、**show failover**、**ipv6 address** 和 **show monitor-interface**。

功能名称	版本	功能信息
在“同时”启动过程中，更改为故障转移组设备首选项。	9.0(1)	较早的软件版本中允许“同时”启动，以便故障转移组无需 **preempt** 命令即可在首选设备上变为主用状态。但此功能现已更改，以使两个故障转移组在要启动的第一台设备上都变为主用状态。
支持 IPsec LAN 到 LAN 隧道加密故障转移和状态链路通信。	9.1(2)	现在可以将 IPSec LAN 到 LAN 隧道用于故障转移和状态链路加密，而不是对故障转移密钥使用专有加密（**failover key** 命令）。 注释 故障转移 LAN 到 LAN 隧道不计入 IPSec（其他 VPN）许可证。 引入或修改了以下命令：**failover ipsec pre-shared-key**、**show vpn-sessiondb**。
禁用硬件模块的运行状况监控	9.3(1)	默认情况下，ASA 会监控 ASA FirePOWER 模块等已安装硬件模块的运行状况。如果您不希望硬件模块故障触发故障转移，则可以禁用模块监控。 修改了以下命令：**monitor-interface service-module**
锁定故障转移对中的备用设备或备用情景上的配置更改	9.3(2)	现在可以锁定备用设备（主用/备用故障转移）或备用情景（主用/主用故障转移）上的配置更改，因此，除了正常的配置同步之外，将无法在备用设备上做出更改。 引入了以下命令：**failover standby config-lock**
在 ASA 5506H 上启用管理 1/1 接口作为故障转移链路	9.5(1)	现在您只能在 ASA 5506H 上将管理 1/1 接口配置为故障转移链路。此功能允许您使用设备上的所有其他接口作为数据接口。说明：如果您使用了此功能，便不能使用 ASA Firepower 模块，因为它要求管理 1/1 接口仍作为常规管理接口。 修改了以下命令：**failover lan interface**、**failover link**
现在支持在故障转移和 ASA 集群中增强运营商级 NAT	9.5(2)	对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。现在支持在故障转移和 ASA 集群部署中使用此功能。 修改了以下命令：**show local-host**

功能名称	版本	功能信息
缩短了使用主用/备用故障转移时从 Secure Client 进行动态 ACL 同步的时间	9.6(2)	当您在故障转移对上使用 Secure Client 时，将关联的动态 ACL (dACL) 同步到备用设备的时间现在已缩短。以前，对于大量 dACL，同步时间可能需要几小时，在此期间，备用设备会一直忙于同步而不是提供高度可用的备份。 未修改任何命令。
多情景模式下 Secure Client 连接的有状态故障转移	9.6(2)	现在，多情景模式下 Secure Client 连接支持有状态故障转移 未修改任何命令。
现在，可为故障转移配置接口链路状态监控轮询以加快检测速度	9.7(1)	默认情况下，故障转移对中的每个 ASA 都会每隔 500 毫秒检查一次其接口的链接状态。现在，您可以在 300 毫秒和 799 毫秒之间配置轮询间隔；例如，如果将轮询时间设置为 300 毫秒，ASA 则可以更快地检测接口故障并触发故障转移。 引入了以下命令：**failover polltime link-state**
Firepower 9300 和 4100 上支持使用双向转发检测 (BFD) 进行主用/备用故障转移运行状况监控	9.7(1)	您可以针对 Firepower 9300 和 4100 上主用/备用对两台设备之间的故障转移运行状况检查启用双向转发检测 (BFD)。将 BFD 用于运行状况检查比默认健康检查方法更可靠，并且 CPU 占用更少。 引入了以下命令：**failover health-check bfd**
禁用故障转移延迟	9.15（1）	当您使用网桥组或 IPv6 DAD 时，当发生故障转移时，新的主用设备会等待 3000 毫秒，等待备用设备完成网络任务并转换到备用状态。然后，主用设备便可以开始传输流量。要避免此类延迟，您可以禁用等待时间，主用设备将在备用设备转换之前开始传输流量。 新增/修改的命令：**failover wait-disable**
配置同步优化功能可实现更快的高可用性对	9.18(1)	配置同步优化功能通过交换配置散列值来比较加入设备和主用设备的配置。如果在主用设备和加入设备上计算的散列值匹配，则加入设备将跳过完全配置同步并重新加入 HA。此功能可实现更快的 HA 对等，并缩短维护窗口和升级时间。
心跳模块冗余	9.20(1)	在 ASA 高可用性的数据平面中引入了额外的心跳模块。该心跳模块有助于避免由于控制平面上的流量拥塞或 CPU 过载而可能发生的错误故障转移或裂脑情况。



第 9 章

公共云中的高可用性故障转移

本章介绍如何配置主用/备份故障转移，以在公共云环境（如 Microsoft Azure）中实现 ASA virtual 的高可用性。

- 关于公共云中的故障转移， 第 311 页
- 公共云中的故障转移许可， 第 315 页
- 公共云中的故障转移默认值， 第 316 页
- 关于 Microsoft Azure 中的 ASA Virtual 高可用性， 第 316 页
- 配置主用/备份故障转移， 第 319 页
- 配置可选故障转移参数， 第 320 页
- 启用主用/备份故障转移， 第 325 页
- 管理公共云中的故障转移， 第 327 页
- 监控公共云中的故障转移， 第 329 页
- 公共云中的故障转移历史记录， 第 331 页

关于公共云中的故障转移

为确保冗余，您可以在公共云环境中部署采用主用/备份高可用性 (HA) 配置的 ASA virtual 。公共云中的高可用性实施无状态主用/备份解决方案，允许主用 ASA virtual 故障触发系统自动执行故障转移以切换到备份 ASA virtual。

以下列表介绍高可用性公共云解决方案中的主要组件：

- **主用 ASA Virtual** - 高可用性对中设置为处理高可用性对等体的防火墙流量的 ASA virtual。
- **备份 ASA Virtual**- ASA virtual HA 对中未在处理防火墙流量并在主用 ASA virtual 发生故障的情况下接管作为主用 ASA virtual 的 。它之所以被称为备份而不是备用 ASAv，是因为它在发生故障转移时不会获取其对等体的身份。
- **HA 代理**- 在 ASA virtual 上运行并确定 ASA virtual的 HA 角色，检测其 HA 对等体的故障以及根据其 HA 角色执行操作的轻量级进程。

在物理 ASA 和非公共云虚拟 ASA 上，系统使用免费 ARP 请求处理故障转移条件，在此请求中，备份 ASA 发出免费 ARP，指示其现在与主用 IP 和 MAC 地址相关联。大多数公共云环境不允许此性质的广播流量。因此，公共云中的高可用性配置要求在发生故障转移时重新启动持续连接。

备份设备会对主用设备的运行状况进行监控，以便确定是否符合特定的故障转移条件。如果符合这些条件，将执行故障转移。故障转移时间可能在几秒到一分多钟之间变化，具体取决于公共云基础设施的响应能力。

关于主用/备份故障转移

在主用/备份故障转移中，一台设备是主用设备。它会传送流量。备份设备不会主动与主用设备传递流量或交换任何配置信息。主用/备份故障转移允许您使用备份 ASA virtual 设备接管故障设备的功能。主用设备出现故障时将变为备份状态，同时备份设备变为主用状态。

主/辅助角色和主用/备份状态

当设置主用/备份故障转移时，需要将一台设备配置为主设备，将另一台配置为辅助设备。此时，两台设备作为两个单独的设备，进行设备和策略配置，以及用于事件、控制面板、报告和运行状况监控。

故障转移对中两台设备之间的主要差别与哪一设备为主用设备，哪一设备为备份设备（即，哪一台设备会主动传送流量）有关。虽然两台设备都能传递流量，但只有主设备会响应负载均衡器的探测，并设定任何已配置的路由将其用作路由目标。备份设备的主要功能是监控主设备的运行状况。如果两台设备同一时间启动（并且运行状况相同），则主设备总是会成为主用设备。

故障转移连接

备份 ASA virtual 使用在 TCP 上建立的故障转移连接来监控主用 ASA virtual 的运行状况：

- 主用 ASA virtual 通过打开一个 侦听端口来充当连接服务器。
- 备份 ASA virtual 使用 连接端口连接到主用 ASA virtual 。
- 通常情况下， 侦听端口 和 连接端口 相同，除非您的配置要求在 ASA virtual 设备之间进行某种类型的网络地址转换。

故障转移连接的状态可用于检测主用 ASA virtual的故障。当备份 ASA virtual 看到故障转移连接断开时，它会将主用 ASA virtual 视为 出现故障。同样，如果备份 ASA virtual 没有收到发送至主用设备的保持连接消息的响应，它也会将主用 ASA virtual 视为 出现故障

相关主题

轮询和 **Hello** 消息

备份 ASA virtual 通过故障转移连接发送 Hello 消息到主用 ASA virtual ，并预期在回复中收到 Hello 响应。消息定时使用轮询间隔，即备份 ASA virtual 设备收到 Hello 响应与发送下一条 Hello 消息之

间的时段。接收响应由被称为保持时间的接收超时来执行。如果接收 Hello 响应发生超时，则主用 ASA virtual 被视为出现故障。

轮询间隔和保持时间间隔均为可配置参数；请参阅配置故障转移条件和其他设置，第 321 页。

启动时的主用设备确定

主用设备按以下方式确定：

- 如果某台设备启动，并检测到对等体已作为主用设备运行，则该设备将成为备份设备。
- 如果某台设备启动，并且未检测到对等体，则该设备会成为主用设备。
- 如果两台设备同时启动，则主设备成为主用设备，辅助设备成为备份设备。

故障转移事件

在主用/备份故障转移中，故障转移会在设备级别进行。下表显示了每个故障事件的故障转移操作。对于每种故障事件，该表显示了故障转移策略（故障转移或禁用故障转移）、主用设备执行的操作、备份设备执行的操作，以及有关故障转移条件和操作的所有特别说明。

表 *16:* 故障转移事件

故障事件	策略	主用设备操作	备份操作	说明
备份设备看到故障转移连接关闭	故障转移	不适用	成为主用设备 将主用设备标记为发生故障	这是标准的故障转移使用案例。
主用设备看到故障转移连接关闭	禁用故障转移	将备份设备标记为发生故障	n/a	到非主用设备的故障转移永远不会发生。
主用设备在故障转移链路上看到 TCP 超时	禁用故障转移	将备份设备标记为发生故障	无需操作	如果主用设备未从备份设备获取响应，则不应发生故障转移。
备份设备在故障转移链路上看到 TCP 超时	故障转移	不适用	成为主用设备 将主用设备标记为发生故障 尝试向主用设备发送故障转移命令	备份设备假定主用设备无法继续操作并接管控制权。 如果主用设备仍处于正常运行状态，但无法及时发送响应，备份设备将会发送故障转移命令到主用设备。

故障事件	策略	主用设备操作	备份操作	说明
主用身份验证失败	禁用故障转移	无需操作	无需操作	由于备份设备正在更改路由表，因此它是唯一需要向 Azure 进行身份验证的设备。 主用设备是否已向 Azure 进行身份验证无关紧要。
备份身份验证失败	禁用故障转移	将备份设备标记为未进行身份验证	无需操作	如果备份设备未向 Azure 进行身份验证，则无法进行故障转移。
主用设备有意启动故障转移	故障转移	变为备份设备	成为主用设备	主用设备通过关闭故障转移链路连接来启动故障转移。 备份设备看到连接关闭，并成为主用设备。
备份设备有意启动故障转移	故障转移	变为备份设备	成为主用设备	备份设备通过发送故障转移消息到主用设备来启动故障转移。 当主用设备看到此消息时关闭连接并将成为备份设备。 备份设备看到连接关闭，并成为主用设备。
以前的主用设备恢复	禁用故障转移	变为备份设备	将伙伴设备标记为备份设备	除非绝对必要，否则不应发生故障转移。
主用设备看到发自备份设备的故障转移消息	故障转移	变为备份设备	成为主用设备	由用户启动手动故障转移时，或者当备份设备看到TCP超时，但主用设备能够从备份设备接收消息时可能发生。

准则和限制

本节包括此功能的准则和限制。

公共云中的高可用性ASA Virtual 故障转移

为确保冗余，您可以在公共云环境中部署采用主用/备份高可用性 (HA) 配置的 ASA virtual 。

- 仅在 Microsoft Azure 公共云上受支持；配置 ASA virtual VM 时，支持的最大数量 Vcpu 为 8；支持的最大内存为 64GB RAM。有关受支持实例的详细列表，请参阅 ASA virtual 入门指南。
- 实施无状态主用/备份解决方案，允许主用 ASA virtual 故障触发系统自动执行故障转移以切换到备份 ASA virtual。

限制

- 故障转移按秒级别而不是毫秒级别执行。
- 高可用性角色的确定和以高可用性设备角色参与部署的能力取决于高可用性对等体之间以及高可用性设备与 Azure 基础设施之间的 TCP 连接。有几种情况下， ASA virtual 将无法以高可用性设备角色参与部署：
  - 无法建立到其高可用性对等体的故障转移连接。
  - 无法从 Azure 检索身份验证令牌。
  - 无法与 Azure 进行身份验证。
- 没有从主用设备到备份设备的配置同步。每台设备必须单独配置相似的配置，用于处理故障转移流量。
- 故障转移路由表限制

  关于公共云中 HA 的路由表：
  - 您最多可以配置 16 个路由表。
  - 在路由表中，最多可以配置 64 个路由。

  在每种情况下，系统都会在达到限制时向您发出警报，并建议删除路由表或路由并重试。
- 无 ASDM 支持
- 没有 IPSec 远程访问 VPN 支持。

注释 有关公共云中受支持的 VPN 拓扑的信息，请参阅《思科自适应安全虚拟设备 (ASAv) 快速入门指南 》。

- ASA Virtual 虚拟机实例必须在同一可用性集中。如果您是 Azure 中的当前 ASA virtual 用户，您将无法从现有部署升级到高可用性部署。您必须删除您的实例，然后部署 Azure 市场提供的 ASA virtual 4 NIC 高可用性产品。

公共云中的故障转移许可

ASA virtual 使用思科智能软件许可。需要安装智能许可证才能正常运行。每个 ASA virtual 必须使用 ASA virtual 平台许可证单独进行许可。在安装许可证之前，吞吐量限制为 100 kbps，以便您可以执行初步连接测试。请参阅 思科 ASA 系列功能许可证 页面，查找 ASA virtual的精确许可要求。

公共云中的故障转移默认值

默认情况下，故障转移策略包含以下内容：

- 仅无状态故障转移。
- 每台设备必须单独配置相似的配置，用于处理故障转移流量。
- 故障转移 TCP 控制端口号是 44442。
- Azure 负载均衡器运行状况探测端口号是 44441。
- 设备轮询时间为 5 秒。
- 设备保持时间为 15 秒。
- ASA virtual 响应主接口 (Management 0/0) 上的运行状况探测。
- 在主接口 (Management 0/0) 上执行 Azure 服务主体 ASA virtual 身份验证。

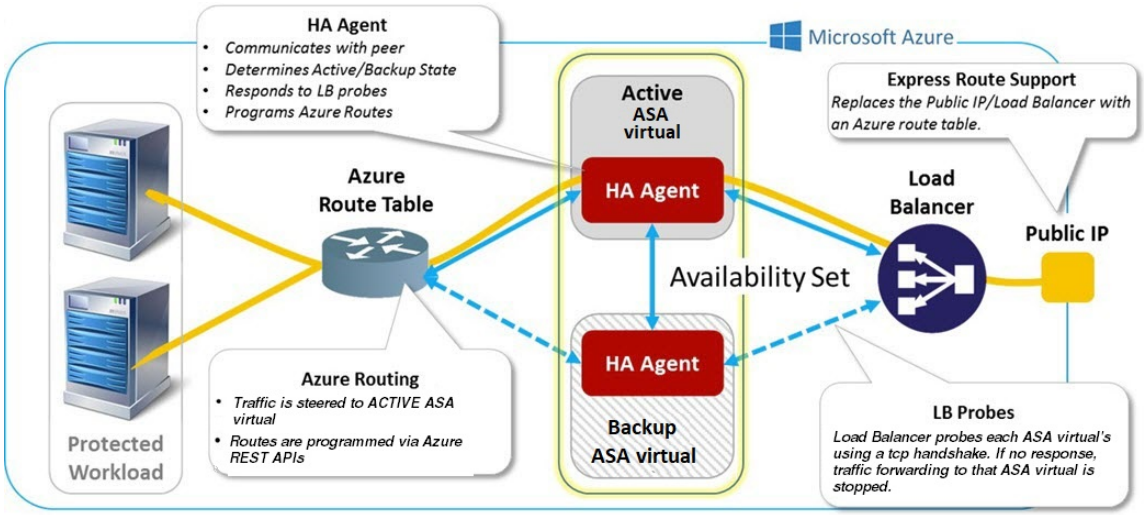
注释　如需获取更改故障转移端口号、运行状况探测端口号、轮询时间和主接口的选项，请参阅配置可选故障转移参数，第 320 页。

关于 Microsoft Azure 中的 ASA Virtual 高可用性

下图简要显示了 Azure 中的 ASA virtual 高可用性部署的情况。受保护的工作负载位于主用/备份故障转移配置中的两个 ASA virtual 实例后面。Azure 负载均衡器使用三次 TCP 握手来探测这两个 ASA virtual 设备。主用 ASA virtual 完成三次握手，指示其处于正常运行状态，而备份 ASA virtual 则特意不响应。由于未对负载均衡器做出响应，在负载均衡器看来，备份 ASA virtual 处于非正常运行状况，进而导致负载均衡器不会向其发送流量。

发生故障转移时，主用 ASA virtual 停止响应负载均衡器探测，备份 ASA virtual 则开始响应，从而导致所有新连接被发送到备份 ASA virtual。备份 ASA virtual 发送 API 请求至 Azure 交换矩阵以修改路由表，将流量从主用设备重定向至备份设备。此时，备份 ASA virtual 成为主用设备，主用设备则成为备份设备或离线，具体取决于发生故障转移的原因。

图 *49: Azure* 中的*ASA Virtual* 高可用性部署



为了能够自动进行 API 调用以修改 Azure 路由表， ASA virtual 高可用性设备需要具有 Azure Active Directory 凭证。Azure 采用服务主体的概念，简单来说，就是服务帐户。服务主体允许您调配帐户，前提是该帐户仅具有在预定义的 Azure 资源集内运行任务所需的足够权限和范围。

通过两个步骤可启用 ASA virtual 高可用性部署，以使用服务主体管理您的 Azure 订用：

1. 创建 Azure Active Directory 应用和服务主体；请参阅关于 Azure 服务主体 ，第 317 页。
2. 配置 ASA virtual 实例以使用服务主体向 Azure 进行身份验证；请参阅 配置 Azure 服务主体的身份验证凭证 ，第 322 页。

相关主题

有关负载均衡器的更多信息，请参阅 Azure 文档。

关于 Azure 服务主体

当您的应用需要访问或修改 Azure 资源，例如路由表时，您必须设置 Azure Active Directory (AD) 应用并为其分配所需的权限。这是在您自己的凭证下运行应用的首选方法，因为：

- 您可以向应用身份分配不同于您自己权限的其他权限。通常，这些权限严格局限于应用需要执行的任务。
- 如果您的责任发生变化，您无需更改应用的凭证。
- 您可以使用证书，在执行无人值守的脚本时自动进行身份验证。

在 Azure 门户注册 Azure AD 应用时，将在您的 Azure AD 租户中创建两个对象：一个应用对象和一个服务主体对象。

- **应用对象** - Azure AD 应用由其仅有的一个应用对象定义，该应用对象位于在其中注册应用的 Azure AD 租户中，此租户也称为应用的“主”租户。

- **服务主体对象** - 服务主体对象定义在特定租户中使用应用的策略和权限，从而为安全主体在运行时代表该应用提供基础。

Azure 在 *Azure* 资源管理器文档中提供了关于如何创建 Azure AD 应用和服务主体的说明。有关完整的说明，请参阅以下主题：

- 使用门户创建可以访问资源的 Azure Active Directory 应用和服务主体
- 使用 Azure PowerShell 创建服务主体以访问资源

注释 设置服务主体后，获取**目录 ID**、**应用 ID** 和**密钥** 。配置 Azure 身份验证需要这些信息；请参阅配置 Azure 服务主体的身份验证凭证 ， 第 322 页。

Azure 中的 ASA Virtual 高可用性配置要求

要部署与#unique_411 unique_411_Connect_42_fig_cgx_dlh_h1b中所述配置相似的配置，您需要以下信息：

- Azure 身份验证信息（请参阅关于 Azure 服务主体 ， 第 317 页）：
  - 目录 ID
  - 应用 ID
  - 秘密密钥
- Azure 路由信息（请参阅配置 Azure 路由表 ， 第 324 页）：
  - Azure 订用 ID
  - 路由表资源组
  - 表名称
  - 地址前缀
  - 下一跳地址
- ASA 配置（请参阅配置主用/备份故障转移 ， 第 319 页、公共云中的故障转移默认值 ， 第 316 页）：
  - 主用/备份 IP 地址
  - 高可用性代理通信端口
  - 负载均衡器探测端口
  - 轮询间隔

注释 在主设备和辅助设备上配置基本故障转移设置。没有主设备到辅助设备的配置同步。每台设备必须单独配置相似的配置，用于处理故障转移流量。

配置主用/备份故障转移

要配置主用/备份故障转移，请在主设备和辅助设备上配置基本故障转移设置。没有主设备到辅助设备的配置同步。每台设备必须单独配置相似的配置，用于处理故障转移流量。

开始之前

- 在 Azure 可用性集中部署您的 ASA virtual 高可用性对。
- 提供您的 Azure 环境信息，包括您的 Azure 订用 ID 和服务主体的 Azure 身份验证凭证。

配置主用/备份故障转移的主设备

遵循本节介绍的步骤，配置主用/备份故障转移配置中的主设备。这些步骤提供了在主设备上启用故障转移所需的最小配置。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。

示例

以下示例显示如何配置主/主用设备的故障转移参数：

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.5 port 4444
ciscoasa(config)#
```

下一步做什么

根据需要配置其他参数：

- 配置备份设备；请参阅配置主用/备份故障转移的辅助设备，第 320 页。
- 配置 Azure 身份验证；请参阅配置 Azure 服务主体的身份验证凭证，第 322 页。
- 配置 Azure 路由信息；请参阅配置 Azure 路由表，第 324 页。
- 查看其他参数；请参阅配置故障转移条件和其他设置，第 321 页。

配置主用/备份故障转移的辅助设备

遵循本节介绍的步骤，配置主用/备份故障转移配置中的辅助设备。这些步骤提供了启用故障转移到辅助设备所需的最小配置。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。

过程

步骤 1 将此设备指定为备份设备：

failover cloud unit secondary

步骤 2 为故障转移链路分配主用 IP 地址：

failover cloud peer ip *ip-address* [**port** *port-number*]

此 IP 地址用于建立到高可用性对等体的 TCP 故障转移控制连接。尝试打开到高可用性对等体（可能已经是主用设备）的故障转移连接时使用此端口。如果在高可用性对等体之间部署了 NAT，则可能需要在此处配置该端口。大多数情况下不需要配置该端口。

示例

以下示例显示如何配置辅助/备份设备的故障转移参数：

```
failover cloud unit secondary
failover cloud peer ip 10.4.3.4 port 4444
```

下一步做什么

根据需要配置其他参数：

- 配置 Azure 身份验证；请参阅配置 Azure 服务主体的身份验证凭证，第 322 页。
- 配置 Azure 路由信息；请参阅配置 Azure 路由表，第 324 页。
- 查看其他参数；请参阅配置故障转移条件和其他设置，第 321 页。

配置可选故障转移参数

您可以在必要时自定义故障转移设置。

配置故障转移条件和其他设置

有关您可在本节中更改的许多参数的默认设置，请参阅公共云中的故障转移默认值，第 316 页。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。
- 在主设备和辅助设备上配置这些设置。配置未从主设备同步到辅助设备。

过程

步骤 1 指定 TCP 端口以用于与高可用性对等体的通信：

failover cloud port control *port-number*

示例：

```
ciscoasa(config)# failover cloud port control 4444
```

port-number 参数为用于对等通信的 TCP 端口分配编号。

这将配置处于主用设备角色时，在其上接受连接的故障转移连接 TCP 端口。这是在备份 ASA virtual 连接到的主用 ASA virtual 上开放的端口。

注释
我们建议您保持默认值 44442，它是两个高可用性对等体的默认值。如果您更改了其中一个高可用性对等体的默认值，则最佳做法是对另一个高可用性设备进行相同的更改。

步骤 2 更改设备的轮询和保持时间：

failover cloud polltime *poll_time* [**holdtime** *time*]

示例：

```
ciscoasa(config)# failover cloud polltime 10 holdtime 30
```

polltime 的范围为 1 至 15 秒。保持时间用于确定从一个呼叫数据包丢失到将设备标记为发生故障之间的时长。**holdtime** 的范围介于 3 到 60 秒之间。输入的保持时间值不能小于设备轮询时间的 3 倍。设置的轮询时间越快，ASA 便可越快检测到故障并触发故障转移。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。

步骤 3 指定用于 Azure 负载均衡器运行状况探测的 TCP 端口：

failover cloud port probe *port-number*

示例：

```
ciscoasa(config)# failover cloud port probe 4443
```

如果您的部署使用 Azure 负载均衡器，则主用 ASA virtual 必须响应来自负载均衡器的 TCP 探测，以便将传入连接定向至主用设备。

步骤 4 指定 Azure 负载均衡器运行状况探测器的辅助接口：

failover cloud port probe *port-number* **interface** *if-name*

示例：

```
ciscoasa(config)# failover cloud port probe 4443 interface inside
```

云 HA 中使用的 TCP 探测的源 IP 地址为 168.63.129.16。此地址是 Azure 的虚拟公共 IP 地址。此地址既是 Azure DHCP 数据包的源地址，也是 Azure 中 DNS 名称服务器的地址。

默认情况下，根据 ASA 路由表， ASA virtual 响应可到达 168.63.129.16 的探测。由于存在默认路由，这最终成为主接口 (Management0/0)。

要在除 Management0/0 以外的接口上支持负载均衡器，请为端口探测器配置另一个接口。您还需要配置两条静态路由：一条用于主接口，一条用于为负载均衡器探测器配置的接口。

步骤 5 为主接口和为负载均衡器探测器配置的接口添加静态路由：

route *if-name dest_ip mask gateway_ip* **[distance]**

示例：

```
ciscoasa(config)# route outside 168.63.129.16 255.255.255.255 10.22.0.1 1
ciscoasa(config)# route inside 168.63.129.16 255.255.255.255 10.22.1.1 2
```

distance 参数是路由的管理距离。如果未指定值，则默认值为 **1**。管理距离是用于比较不同路由协议之间路由的参数。当存在通向同一目标 (168.63.129.16) 的多个路由时，路由的管理距离即可确定优先级。

管理距离为 1 的主接口（外部）的静态路由将主接口设定为发往 168.63.129.16 的数据包的首选接口，但也允许为负载均衡器探测器配置的接口将数据包发送到 168.63.129.16。

注释
响应探测的机制是在接口上创建 TCP 套接字。云 HA 使用 168.63.129.16 的路由查找来决定要在哪个接口上创建套接字。由于存在默认路由，这最终成为主接口。如果没有为探测配置接口的静态路由，ASA 将不会响应负载均衡器发送的 TCP 数据包。

配置 Azure 服务主体的身份验证凭证

您可以使 ASA virtual 高可用性对等体使用 Azure 服务主体来访问或修改 Azure 资源，例如路由表。您必须设置一个 Azure Active Directory (AD) 应用，并为其分配所需的权限。以下命令允许 ASA virtual 使用服务主体向 Azure 进行身份验证。有关 Azure 服务主体的详细信息，请参阅《 ASA virtual 快速入门指南》的 Azure 一章。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。
- 在主设备和辅助设备上配置这些设置。配置未从主设备同步到辅助设备。

过程

步骤 1 配置 Azure 服务主体的 Azure 订用 ID：

failover cloud subscription-id *subscription-id*

示例：

```
(config)# failover cloud subscription-id ab2fe6b2-c2bd-44
```

修改Azure路由表需要Azure订用ID，例如，当云高可用性用户想要将内部路由定向至主用设备时。

步骤 2 配置 Azure 服务主体的凭证信息：

failover cloud authentication {**application-id** | **directory-id** | **key**}

要在故障转移期间更改 Azure 路由表，您需要从 Azure 基础设施获取访问密钥，才能访问路由表。您可以使用应用 ID、目录 ID 以及控制高可用性对的 Azure 服务主体的密钥来获取访问密钥。

步骤 3 配置 Azure 服务主体的应用 ID：

failover cloud authentication application-id *appl-id*

示例：

```
(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-6931704e4201
```

当您从 Azure 基础设施请求访问密钥时，需要此应用 ID。

步骤 4 配置 Azure 服务主体的目录 ID：

failover cloud authentication directory-id *dir-id*

示例：

```
(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138b77ae9
```

当您从 Azure 基础设施请求访问密钥时，需要此目录 ID。

步骤 5 配置 Azure 服务主体的密钥 ID：

failover cloud authentication key *secret-key* [**encrypt**]

示例：

```
(config)# failover cloud authentication key 5yOhH593dtD/O8gzAlWgulrkWz5dH02d2STk3LDbI4c=
```

当您从 Azure 基础设施请求访问密钥时，需要此密钥。如果 **encrypt** 关键字存在，密钥将在 **running-config** 中加密。

配置 Azure 路由表

路由表配置包含在 ASA virtual 承担主用角色时需要更新的用户定义的 Azure 路由的相关信息。在故障转移时，您需要将内部路由定向至主用设备，主用设备则使用配置的路由表信息将路由自动定向至自身。

注释 您需要同时在主用和备份设备上配置任何 Azure 路由表信息。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。
- 在主设备和辅助设备上配置这些设置。配置未从主设备同步到辅助设备。
- 提供您的 Azure 环境信息，包括您的 Azure 订用 ID 和服务主体的 Azure 身份验证凭证。

过程

步骤 1 配置在故障转移期间需要更新的 Azure 路由表：

failover cloud route-table *table-name* [**subscription-id** *sub-id*]

示例：

```
ciscoasa(config)# failover cloud route-table inside-rt
```

（可选）要更新多个 Azure 订用中用户定义的路由，请包括 **subscription-id** 参数。

示例：

```
ciscoasa(config)# failover cloud route-table inside-rt subscription-id cd5fe6b4-d2ed-45
```

route-table 命令级别的 **subscription-id** 参数将会覆盖在全局级别指定的 Azure 订用 ID。如果您输入 **route-table** 命令，而未指定 Azure 订用 ID，则将使用全局 **subscription-id** 参数。有关 Azure 订用 ID 的信息，请参阅 配置 Azure 服务主体的身份验证凭证，第 322 页。

注释
当您输入 **route-table** 命令时， ASA virtual 将会切换到 **cfg-fover-cloud-rt** 模式。

步骤 2 配置路由表的 Azure 资源组：

rg *resource-group*

示例：

```
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
```

Azure 中的路由表更新请求需要一个资源组。

步骤 3 配置在故障转移期间需要更新的路由：

route name *route-name* **prefix** *address-prefix* **nexthop** *ip-address*

示例：

```
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
```

地址前缀配置为 IP 地址前缀、斜线 (‘/’) 和数字网络掩码。例如 *192.120.0.0/16*。

示例

完整的配置示例：

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4
```

启用主用/备份故障转移

在主设备和辅助设备上配置设置后，启用主用/备份故障转移。没有主设备到辅助设备的配置同步。每台设备必须单独配置相似的配置，用于处理故障转移流量。

启用主用/备份故障转移的主设备

遵循本节介绍的步骤，启用主用/备份故障转移配置中的主设备。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。

过程

步骤 1 启用故障转移：

ciscoasa(config)# failover

步骤 2 将系统配置保存到闪存：

ciscoasa(config)# write memory

示例

以下示例显示了主设备的完整配置：

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.4

ciscoasa(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44

ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

ciscoasa(config)# failover
ciscoasa(config)# write memory
```

下一步做什么

启用辅助设备。

启用主用/备份故障转移的辅助设备

遵循本节介绍的步骤，启用主用/备份故障转移配置中的辅助设备。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。

过程

步骤 1 启用故障转移：

ciscoasa(config)# **failover**

步骤 2 将系统配置保存到闪存：

ciscoasa(config)# **write memory**

示例

以下示例显示了辅助设备的完整配置：

```
ciscoasa(config)# failover cloud unit secondary
ciscoasa(config)# failover cloud peer ip 10.4.3.5

ciscoasa(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44

ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

ciscoasa(config)# failover
ciscoasa(config)# write memory
```

管理公共云中的故障转移

本节介绍在启用故障转移后，如何管理云中的故障转移设备，包括如何更改为强制从一台设备故障转移到另一台设备。

强制故障转移

要强制要求备用设备成为主用设备，请执行以下命令。

开始之前

在单情景模式下的系统执行空间中使用此命令。

过程

步骤 1 在备用设备上输入时强制进行故障转移：

failover active

示例：

```
ciscoasa# failover active
```

备用设备将成为主用设备。

步骤 2 在主用设备上输入时强制进行故障转移：

no failover active

示例：

```
ciscoasa# no failover active
```

主用设备将成为备用设备。

更新路由

如果 Azure 中的路由状态与处于 主用 角色的 ASA virtual 状态不一致，您可以使用以下 EXEC 命令在 ASA virtual 上强制进行路由更新：

开始之前

在单情景模式下的系统执行空间中使用此命令。

过程

更新主用设备上的路由：

failover cloud update routes

示例：

```
ciscoasa# failover cloud update routes
Beginning route-table updates
Routes changed
```

此命令仅在处于 主用 角色的 ASA virtual 上有效。如果身份验证失败，命令输出将是 `Route changes failed`。

验证 Azure 身份验证

要在 Azure 中成功完成 ASA virtual 高可用性部署，服务主体配置必须完整、准确。没有适当的 Azure 授权， ASA virtual 设备将无法访问处理故障转移和执行路由更新的资源。您可以测试您的故障转移配置，以检测与以下 Azure 服务主体元素相关的错误：

- 目录 ID
- 应用 ID
- 身份验证密钥

开始之前

在单情景模式下的系统执行空间中使用此命令。

过程

测试 ASA virtual 高可用性配置中的 Azure 身份验证元素：

test failover cloud authentication

示例：

```
ciscoasa(config)# test failover cloud authentication
Checking authentication to cloud provider
Authentication Succeeded
```

如果身份验证失败，命令输出将是 `Authentication Failed`。

如果未正确配置目录 ID 或应用 ID，Azure 将无法识别 REST 请求中所述的资源，以获取身份验证令牌。此条件条目的事件历史记录将显示：

```
Error Connection - Unexpected status in response to access token request: Bad Request
```

如果目录 ID 或应用 ID 正确，但未正确配置身份验证密钥，Azure 将不会授予生成身份验证令牌的权限。此条件条目的事件历史记录将显示：

```
Error Connection - Unexpected status in response to access token request: Unauthorized
```

监控公共云中的故障转移

本节介绍如何监控故障转移状态。

故障转移状态

要监控故障转移状态，请输入以下其中一个命令：

- **show failover**

  显示有关设备的故障转移状态的信息。尚未配置的配置元素的值将显示未配置 。

  仅显示主用设备的路由更新信息。

- **show failover history**

  显示故障转移事件历史记录与时间戳、严重性级别、事件类型和事件文本。

故障转移消息

故障转移系统日志消息

ASA 在优先级别 2 发出大量与故障转移有关的系统日志消息，级别 2 表示一种关键情况。要查看这些消息，请参阅系统日志消息指南。系统日志消息的范围是 1045xx 到 1055xx 之间。

注释 故障转移期间，ASA 按照逻辑先关闭接口，再启动接口，从而生成系统日志消息。这是正常活动。

以下是在切换期间生成的系统日志示例：

```
%ASA-3-105509: (Primary) Error sending Hello message to peer unit 10.22.3.5, error: Unknown
 error
%ASA-1-104500: (Primary) Switching to ACTIVE - switch reason: Unable to send message to
Active unit
%ASA-5-105522: (Primary) Updating route-table wc-rt-inside
%ASA-5-105523: (Primary) Updated route-table wc-rt-inside
%ASA-5-105522: (Primary) Updating route-table wc-rt-outside
%ASA-5-105523: (Primary) Updated route-table wc-rt-outside
%ASA-5-105542: (Primary) Enabling load balancer probe responses
%ASA-5-105503: (Primary) Internal state changed from Backup to Active no peer
%ASA-5-105520: (Primary) Responding to Azure Load Balancer probes
```

每个与公共云部署相关的系统日志均以设备角色：(Primary) 或 (Secondary) 作为前缀。

故障转移调试消息

要查看调试消息，请输入 **debug fover** 命令。有关更多信息，请参阅命令参考。

注释 由于调试输出在CPU进程中分配的高优先级，它可能会极大地影响系统性能。为此，应仅在对特定问题进行故障排除或与思科 TAC 进行故障排除会话过程中使用 **debug fover** 命令。

SNMP 故障转移陷阱

要接收故障转移的 SNMP 系统日志陷阱，请将 SNMP 代理配置为发送 SNMP 陷阱到 SNMP 管理站、定义系统日志主机，并将思科系统日志 MIB 汇集到 SNMP 管理站中。

公共云中的故障转移历史记录

功能名称	版本	功能信息
Microsoft Azure 上的主用/备份故障转移	9.8(200)	引入了此功能。

第 10 章

为 Cisco Secure Firewall 3100/4200部署 ASA 集群

集群允许您将多个ASA作为单一逻辑设备组合到一起。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。

注释 使用集群时，有些功能不受支持。请参阅集群不支持的功能，第 409 页。

- 关于 ASA 集群，第 333 页
- ASA 集群许可证，第 337 页
- ASA 集群要求和前提条件，第 338 页
- ASA 集群准则，第 340 页
- 配置 ASA 集群，第 345 页
- 管理集群节点，第 378 页
- 监控 ASA 集群，第 383 页
- ASA 集群示例，第 395 页
- 集群参考，第 409 页
- Cisco Secure Firewall 3100/4200 的 ASA 集群的历史记录，第 425 页

关于 ASA 集群

本节介绍集群架构及其工作原理。

集群如何融入网络中

集群包含多台防火墙，作为单一设备工作。要用作集群，该防火墙需要以下基础设施：

- 独立的高速背板网络（称为集群控制链路）用于集群内的通信。
- 对每台防火墙的管理访问权限，用于进行配置和监控。

将集群接入网络中时，上游和下游路由器需要能够使用 以下方法之一使出入集群的数据实现负载均衡：

- 跨网络 EtherChannel（推荐）- 将多个集群成员上的接口分组为一个 EtherChannel；EtherChannel 在设备之间执行负载均衡。
- 基于策略的路由（仅适用于路由防火墙模式）- 上游和下游路由器使用路由映射和 ACL 在设备之间执行负载均衡。
- 等价多路径路由（仅适用于路由防火墙模式）- 上游和下游路由器使用等价静态或动态路由在设备之间执行负载均衡。

集群成员

集群成员协调工作来实现安全策略和流量的共享。本节介绍每种成员角色的性质。

引导程序配置

您要在每台设备上配置最低的引导程序配置，包括集群名称、集群控制链路接口和其他集群设置。启用集群的第一个节点通常成为控制节点。在后续节点上启用集群时，这些设备将作为数据节点加入集群。

控制和数据节点角色

一个集群成员是控制节点。如果多个集群节点同时上线，则控制节点由引导程序配置中的优先级设置决定；优先级可设置为 1 到 100，其中 1 为最高优先级。所有其他成员都是数据节点。 通常，当您首次创建集群时，您添加的第一个节点会成为控制节点，因为它是到目前为止集群中的唯一节点。

必须只能在控制节点上执行所有配置（引导程序配置除外）；然后配置将被复制到数据节点中。如果是接口等物理资产，控制节点的配置将被镜像到所有数据节点。例如，如果将以太网接口 1/2 配置为内部接口，将以太网接口 1/1 配置为外部接口，则这些接口也将在数据节点上用作内部和外部接口。

有些功能在集群中无法扩展，控制节点将处理这些功能的所有流量。

集群接口

您可以将数据接口配置为 或 跨区以太网通道 或独立接口。集群中的所有数据接口只能。有关详细信息，请参阅关于集群接口 ，第 346 页。

集群控制链路

每台设备至少必须将一个硬件接口专门用作集群控制链路。有关详细信息，请参阅集群控制链路 ，第 346 页。

配置复制

集群中的所有节点共享一个配置。您只能在控制节点上进行配置更改（引导程序配置除外），这些更改会自动同步到集群中的所有其他节点。

ASA 集群管理

使用 ASA 集群的优势之一是易于管理。本节介绍如何管理集群。

管理网络

我们建议将所有设备都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理接口

对于管理接口，我们建议使用一个专用管理接口。您可以将管理接口配置为独立接口（适用于路由和透明模式）或跨区以太网通道接口。

即便使用跨区以太网通道作为数据接口。独立接口可以根据需要直接连接到每台设备，而跨区以太网通道接口则只允许远程连接到当前的控制单元。

注释 如果使用跨区以太网通道接口模式并将管理接口配置为独立接口，您无法为管理接口启用动态路由。您必须使用静态路由。

对于单个接口，主集群 IP 地址是集群的固定地址，始终属于当前的控制设备。您还要为每个接口配置一个地址范围，以便包括当前控制设备在内的每台设备都可以使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问；当主设备更改时，主集群 IP 地址将转移到新的主设备，使集群的管理得以无缝继续。本地 IP 地址用于路由，在排除故障时也非常有用。

例如，您可以连接到主集群 IP 地址来管理集群，该地址始终属于当前的控制设备。要管理单个成员，您可以连接到本地 IP 地址。

注释 传入设备的流量必须指向节点的管理 IP 地址；传入设备的流量不会通过群集控制链路转发到任何其他节点。

对于 TFTP 或系统日志等出站管理流量，包括控制设备在内的每台设备都使用本地 IP 地址连接到服务器。

对于跨区以太网通道接口，您只能配置一个 IP 地址，该 IP 地址始终属于控制设备。您无法使用 EtherChannel 接口直接连接到数据单元；我们建议将管理接口配置为独立接口，以便您连接到每台设备。请注意，您可以使用设备本地 EtherChannel 进行管理。

控制设备管理与数据设备管理

所有管理和监控均可在控制节点上进行。从控制节点中，您可以检查所有节点的运行时统计信息、资源使用情况或其他监控信息。您也可以向集群中的所有节点发出命令，并将控制台消息从数据节点复制到控制节点。

如果需要，您可以直接监控数据节点。虽然在控制节点上可以执行文件管理，但在数据节点上也可以如此（包括备份配置和更新映像）。以下功能在控制节点上不可用：

- 监控每个节点的集群特定统计信息。
- 监控每个节点的系统日志（控制台复制启用时发送至控制台的系统日志除外）。
- SNMP
- NetFlow

加密密钥复制

当您在控制节点上创建加密密钥时，该密钥将复制到所有数据节点。如果您有连接到主集群 IP 地址的 SSH 会话，则控制节点发生故障时连接将断开。新控制节点对 SSH 连接使用相同的密钥，这样当您重新连接到新的控制节点时，无需更新缓存的 SSH 主机密钥。

ASDM 连接证书 IP 地址不匹配

默认情况下，ASDM 连接将根据本地 IP 地址使用自签名证书。如果使用 ASDM 连接到主集群 IP 地址，则可能会因证书使用的是本地 IP 地址而不是主集群 IP 地址，系统会显示一则警告消息，指出 IP 地址不匹配。您可以忽略该消息并建立 ASDM 连接。但是，为了避免此类警告，您也可以注册一个包含主集群 IP 地址和 IP 地址池中所有本地 IP 地址的证书。然后，您可将此证书用于每个集群成员。有关详细信息，请参阅 https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html。

站点间集群

对于站点间安装，您只要遵循建议的准则即可充分发挥 ASA 集群的优势。

您可以将每个集群机箱配置为属于单独的站点 ID。

站点 ID 与站点特定的 MAC 地址和 IP 地址配合使用。集群发出的数据包使用站点特定的 MAC 地址和 IP 地址，而集群接收的数据包使用全局 MAC 地址和 IP 地址。此功能可防止交换机从两个不同端口上的两个站点获知相同全局 MAC 地址，导致 MAC 地址摆动；相反，它们仅获知站点 MAC 地址。只有使用跨区以太网通道的路由模式支持站点特定的 MAC 地址和 IP 地址。

站点 ID 还用于使用 LISP 检查、导向器本地化来实现流量移动，以提高性能、减少数据中心的站点间集群的往返时间延迟以及连接的站点冗余，其中流量流的备用所有者始终位于与所有者不同的站点上。

有关站点间集群的详细信息，请参阅以下各节：

- 调整数据中心互联的规模 - ASA 集群要求和前提条件，第 338 页

- 站点间准则 - ASA 集群准则， 第 340 页
- 配置集群流移动性 -配置集群流移动性， 第 374 页
- 启用导向器本地化 - 启用导向器本地化， 第 372 页
- 启用站点冗余 - 启用导向器本地化， 第 372 页
- 站点间示例：站点间集群示例， 第 405 页

ASA 集群许可证

智能软件管理器常规版和本地版

每台设备需要基础许可证（默认启用）和相同的加密许可证。我们建议在启用集群之前使用许可服务器对每台设备进行许可，避免出现许可不匹配的问题，并在使用强加密许可证时出现集群控制链路加密问题。

集群功能本身不需要任何许可证。数据设备上的情景许可证不会产生额外成本。

当您应用注册令牌时，系统会自动为符合条件的用户启用强加密许可证。对于在ASA配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在ASA许可证配置中，默认情况下，始终在所有设备上启用基础许可证。您只能在控制设备上配置智能许可。该配置会复制到数据设备，但某些许可证不使用该配置；它仍处于缓存状态，只有控制设备才会请求许可证。这些许可证将聚合成一个由集群设备共享的集群许可证，此聚合许可证也会缓存在数据设备上，以便将来某个从属设备变为控制设备时使用。各个许可证类型将按以下方式进行管理：

- 基础 — 每台设备都会向服务器请求一个基础许可证。
- 情景 - 只有控制设备从服务器请求情景许可证。默认情况下，基础许可证包括 2 个情景，并且位于所有集群成员上。每台设备的基础许可证的值加上控制设备上的情景许可证的值共同形成了聚合集群许可证中的平台限制。例如：
  - 您在集群中有 6 个 Cisco Secure Firewall 3100。基础许可证包括 2 个情景；因为有 6 台设备，因此这些许可证加起来总共包括 12 个情景。您在控制设备上额外配置一个包含 20 个情景的许可证。因此，聚合的集群许可证包括32个情景。由于一台机箱的平台限制为100，因此合并许可证最多允许 100 个情景；32 个情景在该限制范围内。因此，您可以在控制设备上配置最多 32 个情景；每台数据设备通过配置复制也将拥有 32 个情景。
  - 您在集群中有 3 个 Cisco Secure Firewall 3100。基础许可证包括 2 个情景；因为有 3 台设备，因此这些许可证加起来总共包括 6 个情景。您在控制设备上额外配置一个包含 100 个情景的许可证。因此，聚合的集群许可证包括 106 个情景。由于一台设备的平台限制为 100，因此合并许可证最多允许 100 个情景；106 个情景超出限制范围。因此，您仅可以在控制设备上配置最多 100 个情景；每台数据设备通过配置复制也将拥有 100 个情景。在此情况下，只能将控制设备情景许可证配置为 94 个情景。

- 强加密 (3DES) - 如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。只有控制设备需要请求此许可证，并且由于许可证聚合，两台设备均可使用它。

如果选择了新的控制设备，新的控制设备继续使用聚合的许可证。它还会使用缓存的许可证配置再次请求控制设备许可证。当旧的控制设备作为数据设备重新加入集群后，它会释放控制设备许可证授权。在数据设备释放该许可证之前，如果帐户中没有可用的许可证，则控制设备的许可证可能处于一个非合规状态。保留的许可证的有效期为30天，但如果它在此宽限期过后仍处于非合规状态，您将无法对需要特殊许可证的功能进行配置更改；否则操作将不受影响。新主用设备会每隔35秒发送一次权限授权续约请求，直到许可证合规为止。在对许可证请求进行完整的处理之前，应避免进行配置更改。如果某台设备退出集群，缓存的控制配置将被删除，而按设备进行的授权将会保留。尤其是，您需要在非集群设备上重新请求情景许可证。

永久许可证预留

对于永久许可证预留，必须在配置集群之前为每个机箱单独购买许可证并启用。

ASA 集群要求和前提条件

型号要求

- Cisco Secure Firewall 3100 - 最多 16 台设备
- Cisco Secure Firewall 4200 - 最多 16 台设备

ASA 硬件和软件要求

集群中的所有设备：

- 必须为相同型号且 DRAM 相同。闪存的大小不必相同。
- 除在映像升级时以外，必须运行完全相同的软件。支持无中断升级。不匹配的软件版本可能会导致性能不佳，因此请务必在同一维护窗口中升级所有节点。
- 必须处于相同的安全情景模式下，无论是单情景模式还是多情景模式。
- （单情景模式）必须处于相同的防火墙模式下，无论是路由模式还是透明模式。
- 在配置复制之前，新的集群成员对初始集群控制链路通信必须使用与控制单元相同的 SSL 加密设置（**ssl encryption** 命令）。

交换机要求

- 请务必先完成交换机配置，然后再对 ASA 配置集群。
- 有关受支持的交换机的列表，请参阅思科 ASA 兼容性。

ASA 要求

- 将设备加入管理网络之前，为每台设备提供唯一的 IP 地址。
  - 有关连接到 ASA 并设置管理 IP 地址的详细信息，请参阅“入门”一章。
  - 除用作控制单元（通常为添加到集群中的第一台设备）使用的 IP 地址外，这些管理 IP 地址仅供临时使用。
  - 数据单元加入集群后，其管理接口配置将替换为从控制单元复制的配置。

调整站点间集群的数据中心互联

您应在数据中心互联 (DCI) 上为集群控制链路流量保留等同于以下计算结果的带宽：

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

如果各站点的成员数不同，请使用较大的数量进行计算。DCI 的最低带宽不得低于一个成员的集群控制链路的流量大小。

例如：

- 位于 4 个站点的 2 个成员：
  - 总共 4 个集群成员
  - 每个站点 2 个成员
  - 每个成员 5 Gbps 集群控制链路

  保留的 DCI 带宽 = 5 Gbps (2/2 x 5 Gbps)。
- 对位于 3 个站点的 6 个成员而言，规格加大：
  - 总共 6 个集群成员
  - 站点 1 有 3 个成员，站点 2 有 2 个成员，站点 3 有 1 个成员
  - 每个成员 10 Gbps 集群控制链路

  保留的 DCI 带宽 = 15 Gbps (3/2 x 10 Gbps)。
- 位于 2 个站点的 2 个成员：
  - 总共 2 个集群成员
  - 每个站点 1 个成员
  - 每个成员 10 Gbps 集群控制链路

  保留的 DCI 带宽 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps；但最低带宽不得低于集群控制链路的流量大小 (10 Gbps)）。

其他要求

我们建议使用终端服务器访问所有集群成员设备的控制台端口。为了进行初始设置和持续管理（例如在设备发生故障时），终端服务器对于远程管理非常有用。

ASA 集群准则

情景模式

每台成员设备上的模式必须匹配。

防火墙模式

对于单情景模式，所有设备上的防火墙模式必须匹配。

故障转移

集群不支持故障转移。

IPv6

集群控制链路只有在使用 IPv4 时才受支持。

交换机

- 确保连接的交换机与集群数据接口和集群控制链路接口的 MTU 匹配。您应将集群控制链路接口 MTU 配置为比数据接口 MTU 至少高 100 字节，因此请确保适当配置集群控制链路连接的交换机。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销。此外，我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。
- 对于 Cisco IOS XR 系统，如果要设置非默认 MTU，请将 IOS XR 接口 MTU 设置为比集群设备 MTU 高 14 字节。除非使用 **mtu-ignore** 选项，否则 OSPF 邻近对等尝试可能会失败。请注意，集群设备 MTU 应与 IOS XR *IPv4* MTU 匹配。Cisco Catalyst 和 Cisco Nexus 交换机不需要进行这种调整。
- 在用于集群控制链路接口的交换机上，您可以选择在连接到集群设备的交换机端口上启用生成树 PortFast 来加快新设备加入集群的过程。
- 在交换机上，我们建议使用以下其中一种 EtherChannel 负载均衡算法：**source-dest-ip** 或 **source-dest-ip-port** （请参阅思科 Nexus OS 和思科 IOS-XE **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中的设备的流量分摊不均。请勿 更改集群设备上默认的负载均衡算法。
- 如果在交换机上更改 EtherChannel 的负载均衡算法，则交换机上的 EtherChannel 接口将暂时停止转发流量，生成树协议重新启动。在流量再次开始传输之前会存在延迟。
- 集群控制链路路径上的交换机不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。

- 端口通道绑定中断时间不得超过配置的 keepalive 间隔。
- 在 Supervisor 2T EtherChannel 上，默认的散列值分配算法是自适应算法。为了避免 VSS 设计中的非对称流量，请将连接到集群设备的端口通道上的散列算法更改为固定：

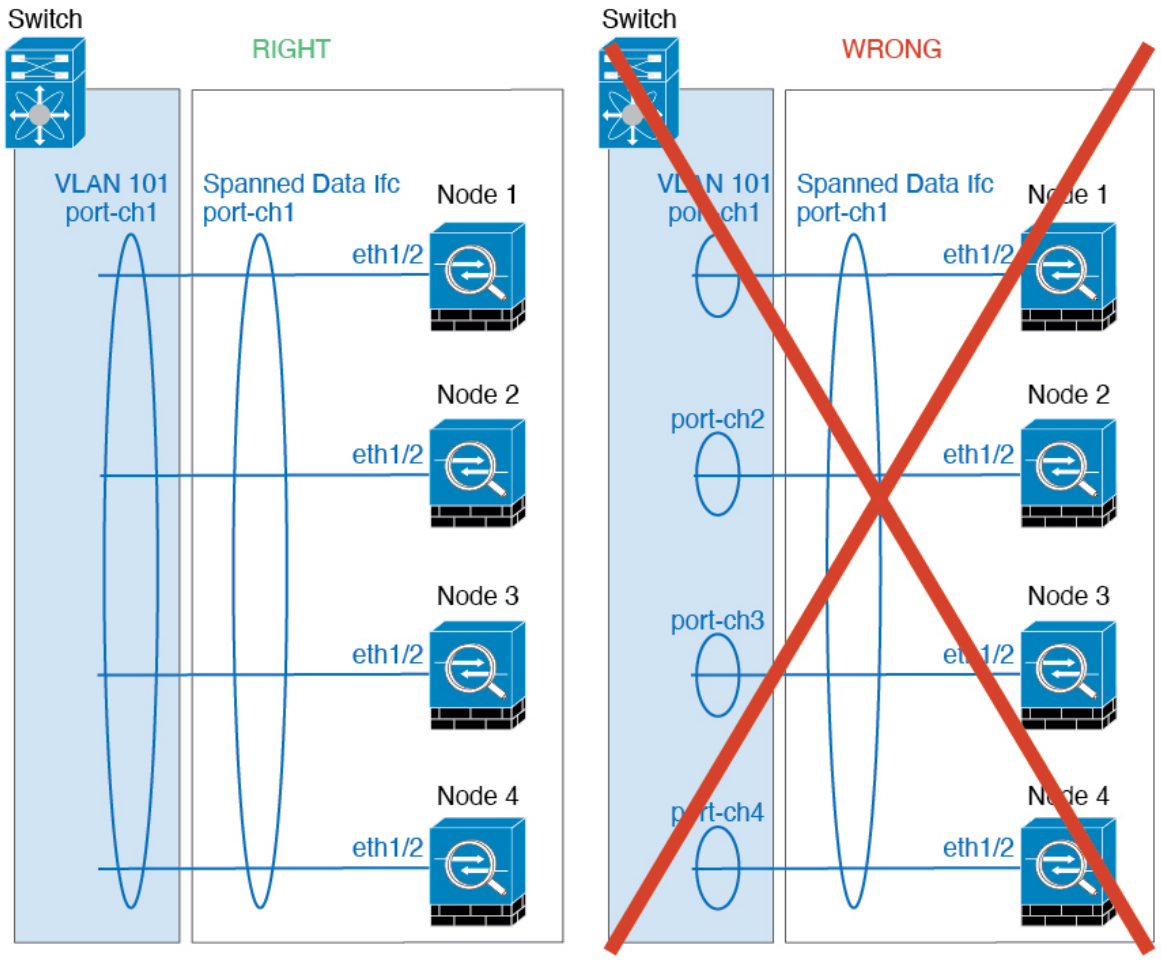
  router(config)# **port-channel** *id* **hash-distribution fixed**

  请勿全局更改算法；您可能需要对 VSS 对等链路使用自适应算法。

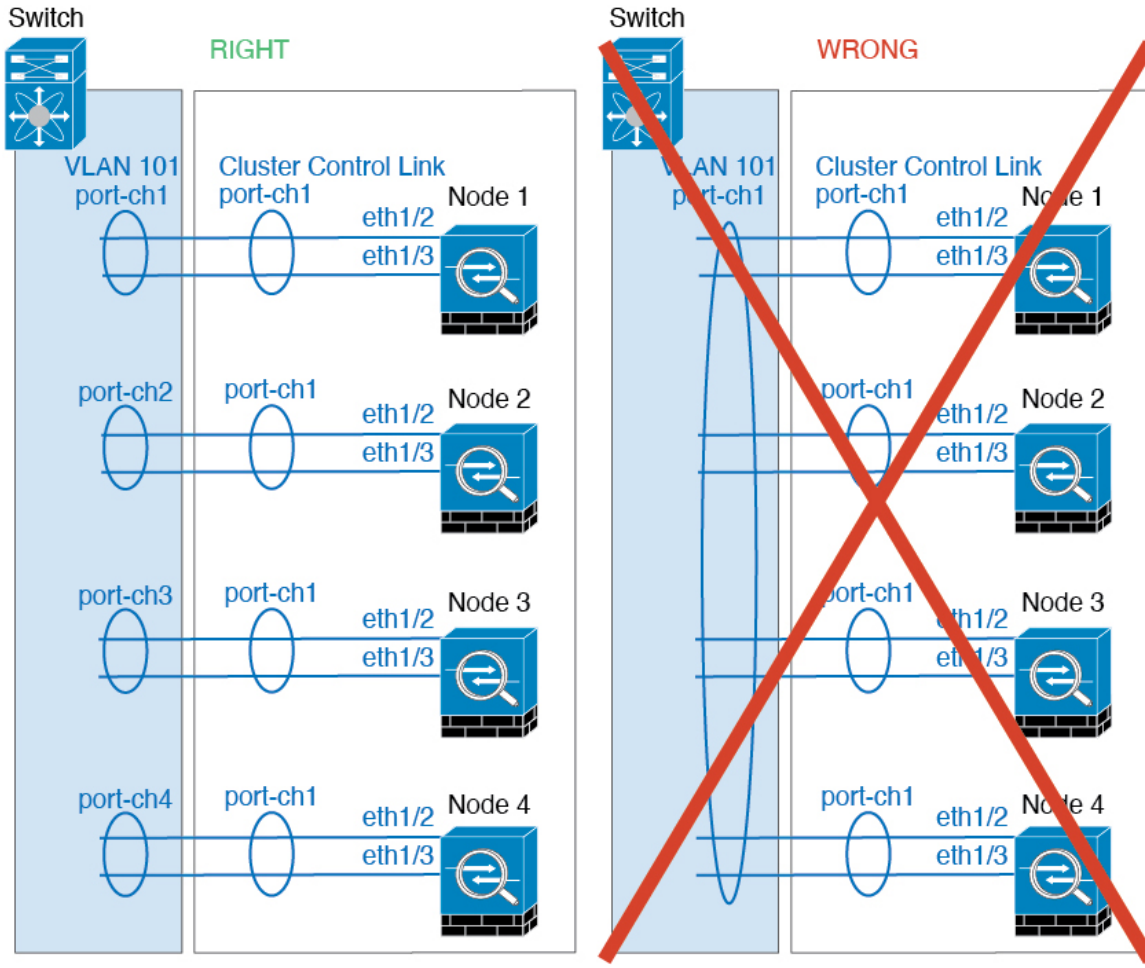
- 您应在所有面向集群的 EtherChannel 接口上为思科 Nexus 交换机禁用 LACP Graceful Convergence 功能。

EtherChannel

- 在低于 15.1(1)S2 的 Catalyst 3750-X 思科 IOS 软件版本中，此集群设备不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆栈连接集群设备 EtherChannel，则当控制设备交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。
- 跨网络与设备本地 EtherChannel 配置 - 请务必为跨区以太网通道和设备本地 EtherChannel 适当地配置交换机。
  - 跨区以太网通道 - 对于跨越所有集群成员的集群设备跨网络 EtherChannel，所有接口在交换机上合并为一个 EtherChannel。请确保每个接口都属于交换机上的同一个通道组。



- 设备本地 EtherChannel - 对于集群设备本地 EtherChannels，包括为集群控制链路配置的任何 EtherChannel，请务必在交换机上配置分散的 EtherChannel；请勿在交换机上将多个集群设备 EtherChannel 合并为一个 EtherChannel。



站点间准则

请参阅有关站点间集群的以下准则：

- 在以下接口和防火墙模式下，支持站点间集群：

接口模式	防火墙模式	
	路由	透明
独立接口	是	不适用
跨区以太网通道	是	是

- 对于单个接口模式，在对组播交汇点 (RP) 使用 ECMP 时，我们建议您将静态路由用于 RP IP 地址，使用主集群 IP 地址作为下一跳。此静态路由会阻止将单播 PIM 注册数据包发送到数据单元。如果数据单元收到了 PIM 注册数据包，将丢弃该数据包，并且无法注册组播流。

- 集群控制链路的延迟必须小于 20 微秒往返时间 (RTT)。

- 集群控制链路必须可靠，没有数据包无序或丢弃数据包的情况；例如，您应使用专用链路。
- 请勿配置连接再均衡；您不需要将连接再均衡到位于不同站点的集群成员。
- ASA 不会加密集群控制链路上转发的数据流量，因为它是专用链接，即使在数据中心互连 (DCI) 上使用也是如此。如果您使用重叠传输虚拟化 (OTV) 或将集群控制链路扩展到本地管理域外部，可以在边界路由器（例如基于 OTV 的 802.1AE MacSec）上配置加密。
- 对于传入连接而言，位于多个站点的成员之间的集群实施没有区别；因此，给定连接的连接角色可以跨越所有站点。这是预期行为。但是，如果您启用导向器本地化，系统将始终从连接所有者所在同一站点选择本地导向器角色（根据站点 ID）。此外，如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者（注意：如果不同站点间的流量非对称，且原始所有者发生故障后远程站点继续发出流量，则远程站点节点可能成为新的所有者，但条件是该设备在重新托管期间接收到数据包。）。
- 对于导向器本地化，以下流量类型不支持本地化：NAT 或 PAT 流量；SCTP 检查的流量；分段所有者查询。
- 对于透明模式，如果集群布置于内部和外部路由器对之间（AKA 南北插入），您必须确保两个内部路由器共享一个 MAC 地址，两个外部路由器共享一个 MAC 地址。当位于站点 1 的集群成员将连接转发到位于站点 2 的成员时，目标 MAC 地址会被保留。如果该 MAC 地址与位于站点 1 的路由器相同，则数据包只会到达位于站点 2 的路由器。
- 对于透明模式，如果集群布置于每个站点上的数据网络和网关路由器之间，用作内部网络之间的防火墙（AKA 东西插入），则每个网关路由器都应使用 HSRP 等第一跳冗余协议 (FHRP) 在每个站点提供相同的虚拟 IP 和 MAC 地址目标。数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术扩展到多个站点。您需要创建过滤器，阻止发往本地网关路由器的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的网关路由器，则您需要删除所有过滤器，使流量能够成功到达另一站点的网关。
- 对于透明模式，如果集群连接到 HSRP 路由器，则必须在 ASA 上将路由器 HSRP MAC 地址添加为静态 MAC 地址表条目（请参阅 为网桥组添加静态 MAC 地址，第 909 页）。当邻接路由器使用 HSRP 时，发往 HSRP IP 地址的流量将发送到 HSRP MAC 地址，但返回流量将来自 HSRP 对中特定路由器接口的 MAC 地址。因此，ASA MAC 地址表通常仅在 HSRP IP 地址的 ASA ARP 表条目到期时更新，并且 ASA 发送 ARP 请求并接收应答。由于 ASA 的 ARP 表条目默认在 14400 秒后到期，但 MAC 地址表条目默认在 300 秒后到期，因此需要添加静态 MAC 地址条目来避免 MAC 地址表到期流量丢弃。
- 对于使用跨区以太网通道的路由模式，请配置站点特定的 MAC 地址。使用 OTV 或类似技术跨站点扩展数据 VLAN 。您需要创建过滤器，阻止发往全局 MAC 地址的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的集群，则您需要删除所有过滤器，使流量能够成功到达另一站点的集群节点。当站点间集群作为扩展网段的第一跳路由器时，不支持动态路由。

其他准则

- 当拓扑发生重大更改时（例如添加或删除 EtherChannel 接口、启用或禁用 ASA 或交换机上的接口、添加额外的交换机形成 VSS、vPC、StackWise 或 StackWise Virtual），您应禁用运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑更改完成且配置更改已同步到所有设备后，您可以重新启用接口运行状态检查功能。

- 将设备添加到现有集群时或重新加载设备时，会有限地暂时丢弃数据包/断开连接；这是预期行为。有些时候，丢弃的数据包会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包将使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 如果使用连接到跨网络 EtherChannel 的 Windows 2003 服务器，当系统日志服务器端口关闭且服务器没有限制 ICMP 错误信息时，将会有大量 ICMP 消息被发送回 ASA 集群。这些消息会导致 ASA 集群的某些设备 CPU 使用率极高，进而影响性能。因此，我们建议您限制 ICMP 错误信息。
- 我们不支持独立接口模式下的 VXLAN。仅跨区以太网通道模式支持 VXLAN。
- 我们不支持跨区以太网通道模式下的 IS-IS。仅独立接口模式支持 IS-IS。
- 将更改复制到集群中的所有设备需要时间。如果进行较大的更改，例如，添加使用对象组的访问控制规则（在部署时会拆分为多个规则），完成更改所需的时间可能会超过集群设备响应的超时时间与成功消息。如果发生这种情况，您可能会看到“无法复制命令”消息。您可以忽略此消息。

ASA 集群的默认设置

- 使用跨区以太网通道时，将自动生成 cLACP 系统 ID 且系统优先级默认为 1。
- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。
- 用于发生故障的集群控制链路的集群自动重新加入功能为每 5 分钟尝试无限次。
- 用于发生故障的数据接口的集群自动重新加入功能为每 5 分钟尝试 3 次，增量间隔设置为 2。
- 默认情况下，连接再均衡处于禁用状态。如果启用连接再均衡，交换负载信息的默认间隔时间为 5 秒。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

配置 ASA 集群

要配置集群，请执行以下任务。

注释 要启用或禁用集群，您必须使用控制台连接（适用于 CLI）或 ASDM 连接。

使用电缆连接设备并配置接口

在配置集群之前，需要先使用电缆连接集群控制链路网络、管理网络和数据网络。然后，配置您的接口。

关于集群接口

您可以将数据接口配置为 或跨区以太网通道或独立接口。集群中的所有数据接口只能是一种类型。不能将以太网 1/1 配置为跨区以太网通道，也不能将以太网 1/2 配置为同一集群内的独立接口，例如。

每台设备还必须至少将一个硬件接口专门用作集群控制链路。

集群控制链路

每台设备至少必须将一个硬件接口专门用作集群控制链路。我们建议将 EtherChannel 用于集群控制链路（如果可用）。

集群控制链路流量概述

集群控制链路流量包括控制流量和数据流量。

控制流量包括：

- 控制节点选举。
- 配置复制。
- 运行状况监控。

数据流量包括：

- 状态复制。
- 连接所有权查询和数据包转发。

集群控制链路接口和网络

您可以将任何数据接口用于集群控制链路，但以下情况除外：

- VLAN 子接口不能用作集群控制链路。
- 管理 *x*/*x* 接口（无论是作为独立接口还是作为 EtherChannel），都不能用作集群控制链路。

您可以使用 EtherChannel 。

每条集群控制链路都有一个属于同一子网的 IP 地址。此子网应与所有其他流量隔离，并且只包括 ASA 集群控制链路接口。

对于有 2 个成员的集群，请勿将集群控制链路从一台 ASA 直接连接到另一台 ASA。如果直接连接两个接口，则当一台设备发生故障时，集群控制链路失效，会导致剩下的那台正常设备也发生故障。而如果通过交换机连接集群控制链路，则集群控制链路仍会对正常设备打开。

确定集群控制链路规格

如果可能，应将集群控制链路的大小设定为与每个机箱的预期吞吐量匹配，以使集群控制链路可以处理最坏情况。

集群控制链路流量主要由状态更新和转发的数据包组成。集群控制链路在任一给定时间的流量大小不尽相同。转发流量的大小取决于负载均衡的效率或是否存在大量用于集中功能的流量。例如：

- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 用于网络访问的 AAA 是集中功能，因此所有流量都会转发到控制设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

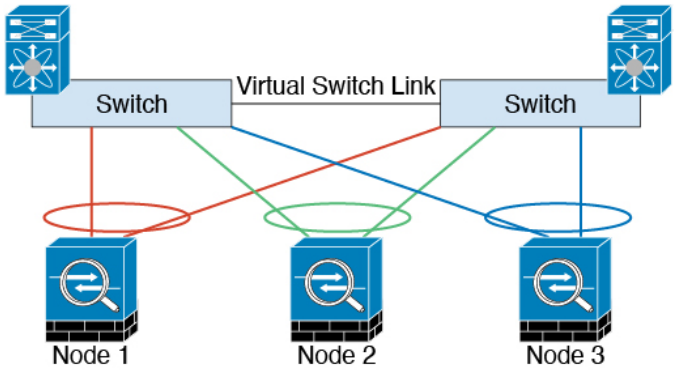
带宽较高的集群控制链路可以帮助集群在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。

注释 如果集群中存在大量不对称（再均衡）流量，应增加集群控制链路的吞吐量大小。

集群控制链路冗余

我们建议将 EtherChannel 用于集群控制链路，以便在 EtherChannel 中的多条链路上传输流量，同时又仍能实现冗余。

下图显示了如何在虚拟交换系统 (VSS)、虚拟端口通道 (vPC)、StackWise 或 StackWise Virtual 环境中使用 EtherChannel 作为集群控制链路。EtherChannel 中的所有链路都是活动链路。如果交换机是冗余系统的一部分，则您可以将同一个 EtherChannel 中的防火墙接口连接到冗余系统中单独的交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台不同的交换机的行为就像一台交换机一样。请注意，此 EtherChannel 是设备本地的，而非跨网络 EtherChannel。



集群控制链路可靠性

为了确保集群控制链路的功能，设备之间的往返时间 (RTT) 务必要小于 20 毫秒。此最大延迟能够增强与不同地理位置安装的集群成员的兼容性。要检查延迟，请在设备之间的集群控制链路上执行 ping 操作。

集群控制链路必须可靠，没有数据包无序或丢弃数据包的情况；例如，站点间部署应使用专用链路。

集群控制链路故障

如果某台设备的集群控制链路线路协议关闭，则集群将被禁用；数据接口关闭。当您修复集群控制链路之后，必须通过重新启用集群来手动重新加入集群。

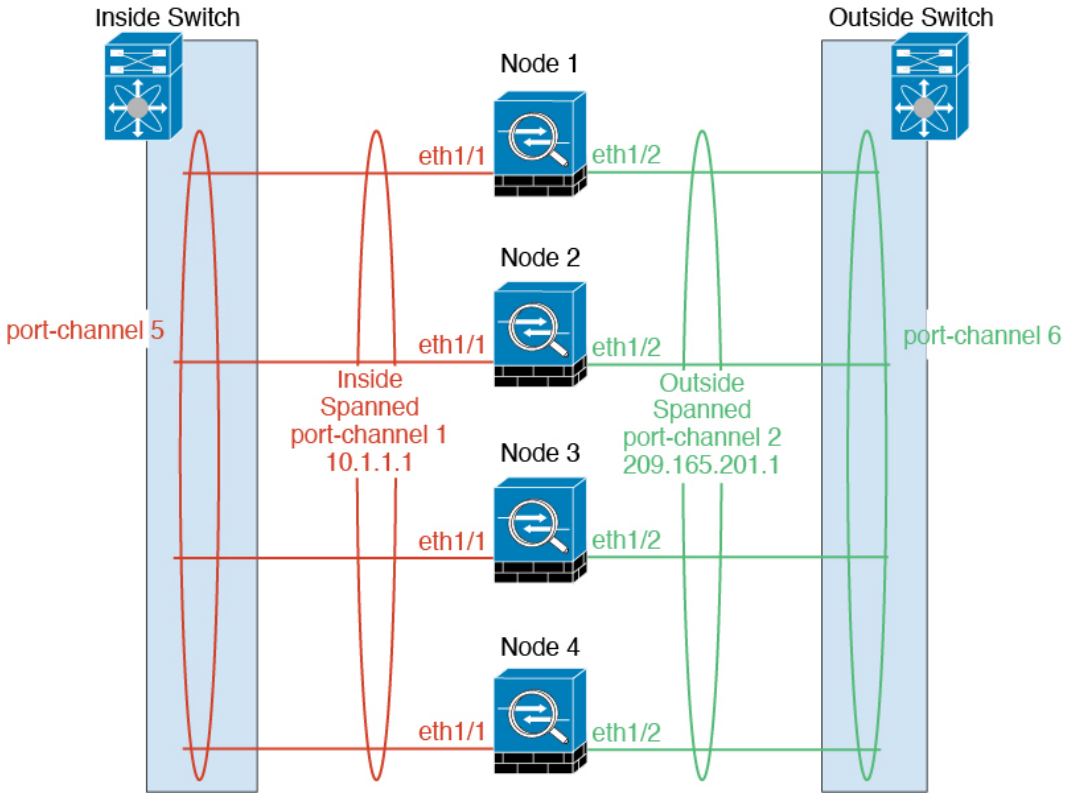
注释 当ASA处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。管理接口将保持打开，使用设备从集群 IP 池接收的 IP 地址。但是，如果您重新加载而设备在集群中仍然处于非活动状态，管理接口将无法访问（因为它届时将使用与控制设备相同的主 IP 地址）。您必须使用控制台端口来进行任何进一步配置。

跨网络 EtherChannel（推荐）

您可以将每个机箱的一个或多个接口组成跨集群中所有机箱的 EtherChannel。EtherChannel 汇聚通道中所有可用活动接口上的流量。

在路由模式和透明防火墙模式下均可配置跨区以太网通道。在路由模式下，EtherChannel 配置为具有单个 IP 地址的路由接口。在透明模式下，IP 地址分配到 BVI 而非网桥组成员接口。

负载均衡属于 EtherChannel 固有的基本操作。



跨区以太网通道优势

我们优先推荐 EtherChannel 负载均衡方法，因其具有以下优势：

- 发现故障的速度更快。
- 收敛速度更快。独立接口依靠路由协议来实现流量的负载均衡，而路由协议在链路发生故障时通常收敛速度缓慢。

- 易于配置。

最大吞吐量准则

要实现最大吞吐量，我们建议采取以下措施：

- 使用“对称”的负载均衡散列算法，亦即来自两个方向的数据包具有相同的散列值，并将在跨网络 EtherChannel 中发送到同一台 ASA。我们建议将源和目标 IP 地址（默认设置）或源和目标端口用作散列算法。
- 将 ASA 连接到交换机时使用相同类型的线路卡，以使应用于所有数据包的散列算法都相同。

负载均衡

EtherChannel 链路使用专有散列算法并且根据源或目标 IP 地址以及 TCP 和 UDP 端口号进行选择。

注释 在交换机上，我们建议使用以下其中一种算法：**source-dest-ip** 或 **source-dest-ip-port**（请参阅思科 Nexus OS 或思科 IOS **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中的 ASA 的流量分摊不均。

EtherChannel 中的链路数量会影响负载均衡。

对称的负载均衡有时并不能够实现。如果您配置了 NAT，则转发和返回数据包具有不同的 IP 地址和/或端口。返回流量将根据散列值被发送到不同的设备，因此集群不得不将大部分返回流量重定向到正确的设备。

EtherChannel 冗余

EtherChannel 有内置冗余。它监控所有链路的线路协议状态。如果一条链路发生故障，将在其余链路之间再均衡流量。如果 EtherChannel 中的所有链路在特定设备上发生故障，但其他设备仍然处于活动状态，则会从集群中删除该设备。

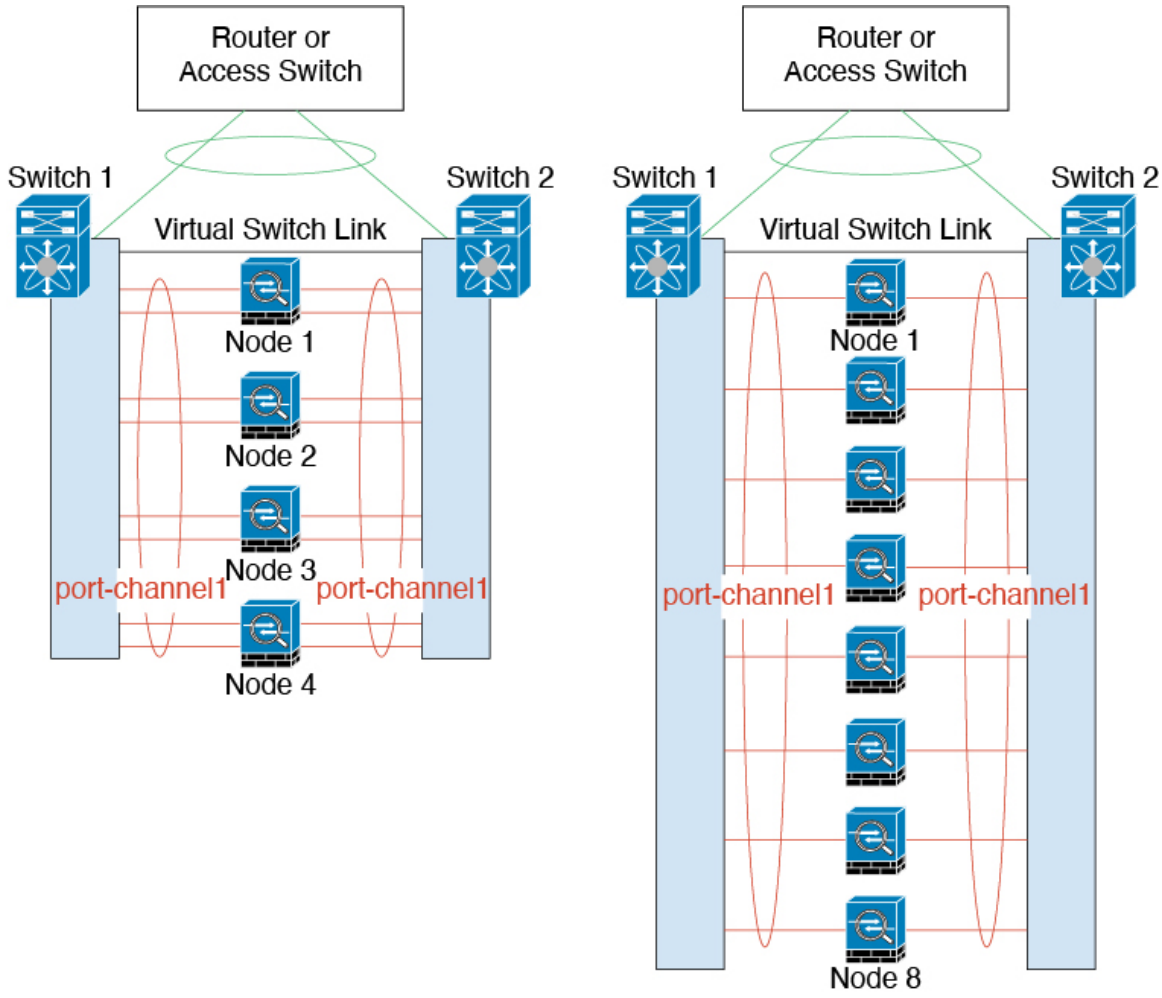
连接到冗余交换机系统

您可以在跨网络 EtherChannel 中包含每台 ASA 的多个接口。每台 ASA 有多个接口，对于连接到 VSS、vPC、StackWise 或 StackWise Virtual 中两台交换机的情况特别有用。

根据交换机的不同，最多可在跨网络 EtherChannel 中配置 32 条活动链路。此功能需要 vPC 中的两台交换机都支持各有 16 条活动链路的 EtherChannel（例如带 F2 系列 10 千兆以太网模块的思科 Nexus 7000）。

对于支持 EtherChannel 中有 8 条活动链路的交换机，在连接到冗余系统中的两台交换机时，最多可在跨区以太网通道 中配置 16 条活动链路。

下图所示为 4 节点集群和 8 节点集群中有 16 条活动链路的跨区以太网通道。

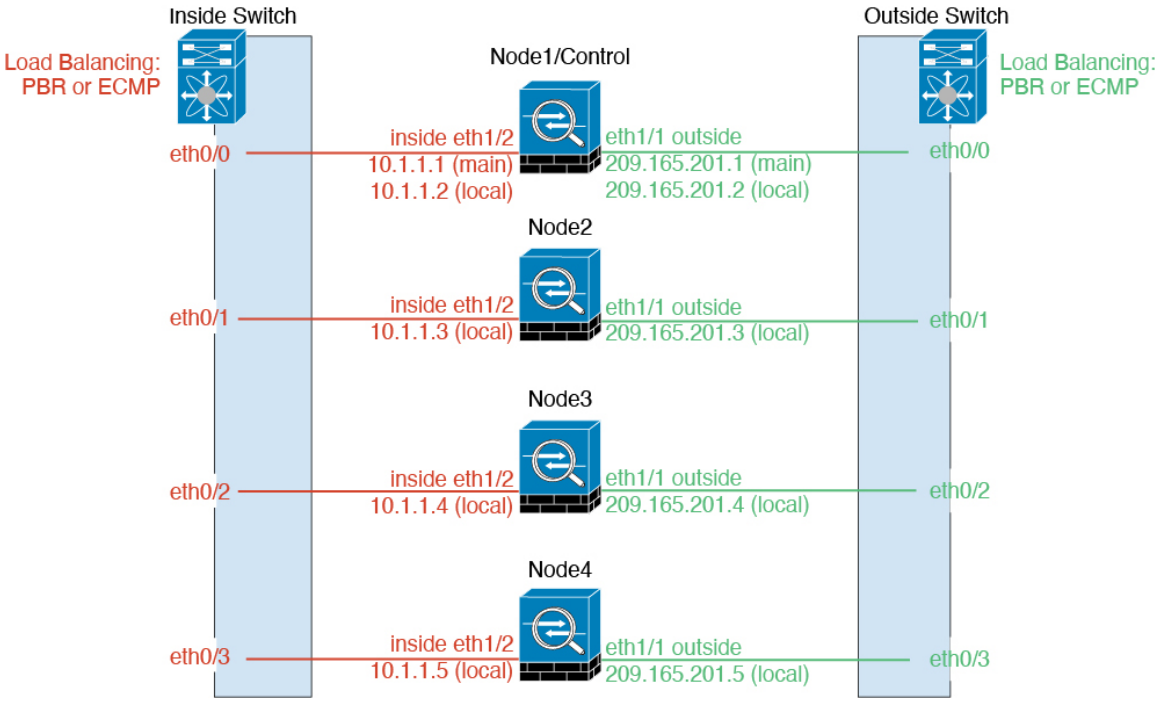


独立接口（仅适用于路由防火墙模式）

独立接口是正常的路由接口，每个接口都有自己的 本地 *IP* 地址 用于路由。每个接口的 主集群 *IP* 地址 是固定地址，始终属于控制节点。当控制节点更改时，主集群IP地址将转移到新的控制节点，使集群的管理得以无缝继续。

由于接口配置只能在控制节点上配置，因此您可以通过接口配置设置一个 IP 地址池，供集群节点上的给定接口（包括控制节点上的一个接口）使用。

必须在上游交换机上分别配置负载均衡。



基于策略的路由

使用独立接口时，每个 ASA 接口都会保留自己的 IP 地址和 MAC 地址。基于策略的路由 (PBR) 是一种负载均衡方法。

如果已经在使用 PBR 并希望充分利用现有的基础设施，我们建议使用此方法。

PBR 根据路由映射和 ACL 作出路由决定。您必须在集群中的所有 ASA 之间手动划分流量。由于 PBR 是静态路由，因此可能有时候无法实现最佳的负载均衡效果。为了获得最佳性能，建议您配置 PBR 策略，以便连接的转发数据包和返回数据包定向到同一个 ASA。例如，如果您有一台思科路由器，使用带对象跟踪的思科 IOS PBR 即可实现冗余。思科 IOS 对象跟踪使用 ICMP ping 监控每台 ASA。然后，PBR 可根据特定 ASA 的可访问性来启用或禁用路由映射。有关详细信息，请参阅以下 URL：

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

同等成本的多路径路由

使用独立接口时，每个 ASA 接口都会保留自己的 IP 地址和 MAC 地址。等价多路径 (ECMP) 路由是一种负载均衡方法。

如果已经在使用 ECMP 并希望充分利用现有的基础设施，我们建议使用此方法。

ECMP 路由可以通过路由指标并列最优的多条“最佳路径”转发数据包。它与 EtherChannel 一样，也可以使用源和目标 IP 地址及/或源和目标端口的散列值将数据包发送到下一跃点。如果将静态路由用于 ECMP 路由，则 ASA 故障会导致问题；如果继续使用该路由，发往故障 ASA 的流量将丢失。因此，如果使用静态路由，请务必要使用静态路由监控功能，例如对象跟踪。我们还建议使用动态路由协议来添加和删除路由，在这种情况下，您必须配置每台 ASA 使之加入动态路由。

思科智能流量导向器（仅路由防火墙模式）

使用独立接口时，每个 ASA 接口都会保留自己的 IP 地址和 MAC 地址。智能流量导向器 (ITD) 是适用于 Nexus 5000、6000、7000 和 9000 交换机系列的高速硬件负载均衡解决方案。除了完全恢复传统 PBR 的功能以外，它还可以提供简化配置工作流和多种附加功能，以实现更精细的负载分布。

ITD 支持 IP 粘性、面向双向流对称的一致散列处理、虚拟 IP 寻址、运行状态监控、具有 N+M 冗余的复杂故障处理策略、加权负载均衡，以及应用 IP SLA 探测（包括 DNS）。由于负载均衡的动态性质，它可在所有集群节点上实现比 PBR 更均匀的流量分布。为了实现双向流对称，我们建议配置 ITD，以便将连接的数据包转发和返回定向到同一 ASA。有关详细信息，请参阅以下 URL：

https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/sw/design/itd_deployment/ITD_ASA_Deployment_Guide.pdf

使用电缆连接集群设备并配置上游和下游设备

在配置集群之前，需要先使用电缆连接集群控制链路网络、管理网络和数据网络。

过程

步骤 1 使用电缆连接集群控制链路网络、管理网络和数据网络。

注释
在配置要加入集群的节点之前，至少需要有一个活动的集群控制链路网络。

步骤 2 此外，还应配置上游和下游设备。例如，如果使用 EtherChannel，则应为上游和下游设备进行 EtherChannel 配置。

上在每个设备上配置集群接口模式

您只能为集群配置一种类型的接口：跨网络 EtherChannel 或独立接口；不能在集群中混合使用不同的接口类型。

开始之前

- 您必须在要添加到集群中的每台 ASA 上分别设置模式。
- 您始终可以将管理专用接口配置为独立接口（推荐），即使是在跨区以太网通道模式下亦如此。即使是在透明防火墙模式下，管理接口也可以是独立接口。
- 在跨区以太网通道模式下，，如果将管理接口配置为独立接口，您将无法为管理接口启用动态路由。您必须使用静态路由。
- 在多情景模式下，您必须为所有情景选择一种接口类型。例如，如果使用透明和路由模式的混合情景，则必须将跨区以太网通道模式用于所有情景，因为这是透明模式允许的唯一接口类型。

过程

步骤 1 显示任何不兼容的配置，以便稍后强制设置接口模式并修复配置；该模式不会随以下命令而更改：

cluster interface-mode {**individual** | **spanned**} **check-details**

示例：

```
ciscoasa(config)# cluster interface-mode spanned check-details
```

步骤 2 为集群设置接口模式：

cluster interface-mode {**individual** | **spanned**} **force**

示例：

```
ciscoasa(config)# cluster interface-mode spanned force
```

不存在默认设置；您必须明确选择模式。如果尚未设置模式，则无法启用集群。

force 选项可直接更改模式而无需检查配置中是否存在不兼容的设置。更改模式后，您需要手动修复任何配置问题。由于任何接口配置都只能在设置完模式后修复，因此我们建议使用 **force** 选项，这样您至少可以从现有配置着手。设置模式后，您可以重新运行 **check-details** 选项来获得更多参考信息。

如果不使用 **force** 选项，当存在任何不兼容的配置时，系统将提示您清除配置并重新加载，从而需要您连接到控制台端口来重新配置管理访问。如果您的配置兼容（极为罕见），则会更改模式并保留配置。如果您不想清除配置，则可以键入 **n** 退出命令。

要删除接口模式，请输入 **no cluster interface-mode** 命令。

在控制节点上配置接口

启用集群之前，您必须修改所有当前配置了 IP 地址的接口，使其准备好加入集群。至于其他接口，您可以在启用集群之前或之后配置；我们建议预配置所有接口，以便将完整的配置同步到新的集群成员。

本节介绍如何将接口配置为与集群兼容。您可以将数据接口配置跨区以太网通道或独立接口。每种方法使用的负载均衡机制不同。在同一个配置中不能配置两种接口类型，只有管理接口除外，它即使在跨区以太网通道模式下也可以是独立接口。您可以将数据接口配置跨区以太网通道或独立接口。每种方法使用的负载均衡机制不同。在同一个配置中不能配置两种接口类型，只有管理接口除外，它即使在跨区以太网通道模式下也可以是独立接口。

配置独立接口（推荐为管理接口）

独立接口是正常的路由接口，每个接口都从 IP 地址池获取自己的 IP 地址。集群的主集群 IP 地址是集群的固定地址，始终属于控制节点。

在跨区以太网通道模式下， 建议将管理接口配置为独立接口。独立接口可以根据需要直接连接到每台设备，而跨区以太网通道接口则只允许连接到控制节点。

开始之前

- 除管理专用接口之外，您必须处于独立接口模式下。
- 对于多情景模式，请在每个情景下执行本程序。如果您尚未进入情景配置模式，请输入**changeto context** *name* 命令。
- 独立接口要求在邻居设备上配置负载均衡。管理接口不需要外部负载均衡。
- （可选）将接口配置为设备本地 EtherChannel 接口和/或配置子接口。
  - 如果配置为 EtherChannel，则此 EtherChannel 是设备本地的，而非跨区以太网通道。

过程

步骤 1 配置本地 IP 地址池（IPv4 和/或 IPv6），其中一个地址将被分配到每个集群设备作为接口地址：

(IPv4)

ip local pool *poolname first-address* — *last-address* [**mask** *mask*]

(IPv6)

ipv6 local pool *poolname ipv6-address*/*prefix-length number_of_addresses*

示例：

```
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8:45:1002/64 8
```

至少包含与集群中的设备数量相同的地址。如果计划扩展集群，则应包含更多地址。属于当前主设备的主集群 IP 地址不在此地址池中；请务必在同一个网络中为主集群 IP 地址保留一个 IP 地址。

您无法预先确定分配到每台设备的确切本地地址；要查看每台设备上使用的地址，请输入**show ip**[**v6**] **local pool** *poolname* 命令。每个集群成员在加入集群时都会分配到一个成员 ID。此 ID 决定了所用的来自地址池中的本地 IP。

步骤 2 进入接口配置模式：

interface *interface_id*

示例：

```
ciscoasa(config)# interface management 1/1
```

步骤 3 （仅适用于管理接口）将一个接口设置为管理专用模式，确保不会有流量流经该接口：

management-only

默认情况下，管理类型的接口被配置为管理专用。在透明模式下，此命令对管理类型的接口始终启用。

如果集群接口模式为跨网络，则必须配置此设置。

步骤 4 为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif management
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。

步骤 5 设置主集群 IP 地址并确定集群池：

(IPv4)

ip address *ip_address* [*mask*] **cluster-pool** *poolname*

(IPv6)

ipv6 address *ipv6-address*/*prefix-length* **cluster-pool** *poolname*

示例：

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8:45:1002::99/64 cluster-pool insipv6
```

此 IP 地址必须与集群池地址属于同一个网络，但不在地址池中。您可以配置 IPv4 和/或 IPv6 地址。

不支持 DHCP、PPPoE 和 IPv6 自动配置；您必须手动配置 IP 地址。也不支持手动配置链路本地地址。

步骤 6 设置安全级别，其中 *number* 为 0（最低）到 100（最高）之间的整数：

security-level 编号

示例：

```
ciscoasa(config-if)# security-level 100
```

步骤 7 启用接口：

no shutdown

示例

以下示例将以太网 1/3 和以太网 1/4 接口配置为设备本地 EtherChannel，然后将 EtherChannel 配置为独立接口：

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface ethernet 1/3
channel-group 1 mode active
no shutdown

interface ethernet 1/4
channel-group 1 mode active
no shutdown

interface port-channel 1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8:45:1002::99/64 cluster-pool mgmtipv6
security-level 100
management-only
```

配置跨区以太网通道

跨网络 EtherChannel 跨越集群中的所有 ASA，并在 EtherChannel 操作的过程中提供负载均衡。

开始之前

- 您必须处于跨网络 EtherChannel 接口模式下。
- 对于多情景模式，请在系统执行空间中开始本程序。如果尚未进入系统配置模式，请输入**changeto system** 命令。
- 对于透明模式，请配置网桥组。请参阅配置网桥虚拟接口 (BVI)，第 757 页。
- 使用跨网络 EtherChannel 时，端口通道接口在集群完全启用之前不会进入工作状态。此要求可防止将流量转发到集群中并非处于活动状态的设备。

过程

步骤 1 指定要添加到通道组的接口：

interface *physical_interface*

示例：

```
ciscoasa(config)# interface ethernet 1/1
```

The *physical_interface* ID includes the type, slot, and port number as type slot/port. 通道组中的第一个接口决定了该组中所有其他接口的类型和速度。

步骤 2 将此接口分配到 EtherChannel：

channel-group *channel_id* **mode active**

示例：

```
ciscoasa(config-if)# channel-group 1 mode active
```

channel_id 的值为 1 到 48。如果配置中尚没有此通道 ID 的端口通道接口，将自动添加一个接口：

interface port-channel *channel_id*

跨网络 EtherChannel 只支持 **active** 模式。

步骤 3 启用接口：

no shutdown

步骤 4 （可选）通过重复该过程，将更多接口添加到 EtherChannel。

示例：

```
ciscoasa(config)# interface ethernet 1/2
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# no shutdown
```

每台设备在 EtherChannel 中有多个接口，对于连接到 VSS、vPC、StackWise 或 StackWise Virtual 中交换机的情况非常有用。

步骤 5 指定端口通道接口：

interface port-channel *channel_id*

示例：

```
ciscoasa(config)# interface port-channel 1
```

在将接口添加到通道组时，将自动创建此接口。

步骤 6 （可选）如果准备在此 EtherChannel 上创建 VLAN 子接口，请立即执行此操作。

示例：

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

本程序的其余部分适用于子接口。

步骤 7 （多情景模式）将接口分配到情景。然后输入：

changeto context *name*
interface port-channel *channel_id*

示例：

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

对于多情景模式，其余的接口配置将在每个情景中完成。

步骤 8 为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。

步骤 9 根据防火墙模式，执行以下其中一项操作。

- 路由模式 - 设置 IPv4 和/或 IPv6 地址：

  (IPv4)

  ip address *ip_address* [*mask*]

  (IPv6)

  ipv6 address *ipv6-prefix*/*prefix-length*

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
  ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
  ```

  不支持 DHCP、PPPoE 和 IPv6 自动配置。对于点对点连接，可以指定 31 位子网掩码 (255.255.255.254)。在此情况下，不会为网络或广播地址保留 IP 地址。也不支持手动配置链路本地地址。

- 透明模式 - 将接口分配到网桥组：

  bridge-group *number*

  示例：

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  number 为 1 到 100 之间的整数。最多可将 64 个接口分配到网桥组。您不能将同一接口分配至多个网桥组。请注意，BVI 配置包含 IP 地址。

步骤 10 设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 为 0（最低）到 100（最高）之间的整数。

步骤 11 为跨网络 EtherChannel 配置全局 MAC 地址，以避免潜在的网络连接问题：

mac-address *mac_address*

示例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

如果是手动配置的 MAC 地址，该 MAC 地址将始终属于当前的控制设备。如果不配置 MAC 地址，则如果控制设备发生更改，新的控制设备会将新的 MAC 地址用于该接口，而这可能导致临时网络故障。

在多情景模式下，如果您在情景之间共享接口，则应改为启用自动生成 MAC 地址，这样就无需手动设置 MAC 地址。请注意，您必须使用此命令为非共享 接口手动配置 MAC 地址。

mac_address 的格式为 H.H.H，其中 H 是 16 位十六进制数字。例如， MAC 地址 00-0C-F1-42-4C-DE 以 000C.F142.4CDE 的形式输入。

如果您还要使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。

步骤 12 （路由模式）对于站点间集群，为每个站点配置一个站点特定的 MAC 地址和 IP 地址：

mac-address *mac_address* **site-id** *number* **site-ip** *ip_address*

示例：

```
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.9.9.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.9.9.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.9.9.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.9.9.4
```

站点特定的 IP 地址必须与全局 IP 地址位于同一子网。供设备使用的站点特定的 MAC 地址和 IP 地址取决于您在每台设备的引导程序配置中指定的站点 ID。

创建引导程序配置

集群中的每个节点都需要有引导程序配置才能加入集群。

配置控制节点引导程序设置

集群中的每个节点都需要有引导程序配置才能加入集群。通常，您配置为加入集群的第一个节点将是控制节点。启用集群后，集群会在选举时间结束后选举出一个控制节点。最初只有一个节点在集群中，该节点将成为控制节点。添加到集群的后续节点将是数据节点。

开始之前

- 请备份配置，以防稍后要退出集群而需要恢复配置。

- 对于多情景模式，请在系统执行空间中完成这些程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。
- 您必须使用控制台端口来启用或禁用集群。您不能使用 Telnet 或 SSH。
- 除集群控制链路外，配置中的任何接口都必须根据接口模式使用集群 IP 池进行配置，或者配置为跨区以太网通道，然后才能启用集群。如果有以前就存在的接口配置，您可以清除该接口配置 (**clear configure interface**)，也可以将接口转换为集群接口后再启用集群。
- 将节点添加到正在运行的集群时，可能会有限地暂时丢弃数据包/断开连接；这是预期行为。
- 预先确定集群控制链路的吞吐量大小。请参阅确定集群控制链路规格，第 346 页。

过程

步骤 1 加入集群之前，先启用集群控制链路接口。

稍后，您要在启用集群时将此接口确定为集群控制链路。

如果您有足够的接口，我们建议您将多个集群控制链路接口合并到 EtherChannel 中。此 EtherChannel 是 ASA 本地的，而非跨区以太网通道。

集群控制链路接口配置不会从控制节点复制到数据节点；但是，必须在每个节点上使用相同的配置。由于此配置不会复制，您必须在每个节点上分别配置集群控制链路接口。

- VLAN 子接口不能用作集群控制链路。
- 管理 *x*/*x* 接口（无论是作为独立接口还是作为 EtherChannel），都不能用作集群控制链路。

a) 进入接口配置模式：

interface *interface_id*

示例：

```
ciscoasa(config)# interface ethernet 1/6
```

b) （可选，适用于 EtherChannel）将此物理接口分配到 EtherChannel：

channel-group *channel_id* **mode on**

示例：

```
ciscoasa(config-if)# channel-group 1 mode on
```

channel_id 的值为 1 到 48。如果配置中尚没有此通道 ID 的端口通道接口，将自动添加一个接口：

interface port-channel *channel_id*

我们建议对集群控制链路成员接口使用 ON 模式来减少集群控制链路上不必要的流量。由于集群控制链路是单独、稳定的网络，因此无需 LACP 流量开销。**注意**：我们建议将数据 EtherChannel 设置为 Active 模式。

c) 启用接口：

no shutdown

您只需要启用接口；不要为接口配置名称或任何其他参数。

d) （适用于 EtherChannel）对每个要添加到 EtherChannel 的其他接口重复此操作：

示例：

```
ciscoasa(config)# interface ethernet 1/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

步骤 2 指定集群控制链路接口的最大传输节点至少比数据接口的最高 MTU 高 100 字节。

mtu cluster 字节

示例：

```
ciscoasa(config)# mtu cluster 9198
```

将 MTU 设置为介于 1400 和 9198 字节之间的，但不在 2561 和 8362 字节之间。由于块池处理，此 MTU 大小不是系统运行的最佳值。默认 MTU 为 1500 字节。我们建议将集群控制链路 MTU 设置为最大 。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销。

例如，由于最大 MTU 为 9198 字节，因此最高的数据接口 MTU 可以是 9098，而集群控制链路则可以设置为 9198。

此命令是全局配置命令，但是也属于不会在节点之间复制的引导程序配置。

步骤 3 为集群命名并进入集群配置模式：

cluster group 名称

示例：

```
ciscoasa(config)# cluster group pod1
```

名称必须是长度为 1 到 38 个字符的 ASCII 字符串。每个节点只能配置一个集群组。集群的所有成员必须使用同一名称。

步骤 4 为此集群成员命名：

local-unit *unit_name*

使用唯一的 ASCII 字符串，长度必须为 1 到 38 个字符。每个节点必须具有唯一的名称。集群中不允许存在名称重复的节点。

示例：

```
ciscoasa(cfg-cluster)# local-unit node1
```

步骤 5 指定集群控制链路接口，最好是 EtherChannel：

cluster-interface *interface_id* **ip** *ip_address mask*

示例：

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

不允许子接口和管理接口。

指定 IP 地址的 IPv4 地址；此接口不支持 IPv6。此接口不能配置 **nameif**。

对于每个节点，在同一网络上指定不同的 IP 地址。

步骤 6 （路由模式；跨区以太网通道模式）如果您使用站点间集群，则请为此节点设置站点 ID，以使其能使用站点特定的 MAC 地址。

site-id 编号

示例：

```
ciscoasa(cfg-cluster)# site-id 1
```

编号介于 1 到 8 之间。

步骤 7 设置控制节点选择的此节点的优先级：

priority *priority_number*

示例：

```
ciscoasa(cfg-cluster)# priority 1
```

优先级的值为 1 到 100，其中 1 为最高优先级。

步骤 8 （可选）设置身份验证密钥以便控制集群控制链路上的流量：

key *shared_secret*

示例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

共享密钥是长度介于 1 和 63 个字符之间的 ASCII 字符串。共享密钥用于生成密钥。此命令不会影响数据路径流量，包括始终以明文发送的连接状态更新和转发数据包。

步骤 9 （可选）手动指定 cLACP 系统 ID 和系统优先级：

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

示例：

```
ciscoasa(cfg-cluster)# clacp system-mac 000a.0000.aaaa
```

使用跨区以太网通道时，ASA 使用 cLACP 与邻居交换机协商 EtherChannel。集群中的 ASA 在 cLACP 协商中协作，使其在交换机看来就好似一台（虚拟）设备。cLACP 协商中的一个参数是 MAC 地址格式的系统 ID。该集群中的所有 ASA 都使用同一个系统 ID：由控制单元（默认）自动生成并复制到所有辅助设备；也可以使用此命令，按照*H.H.H*的格式手动指定，其中 H 是 16 位十六进制数字。（例如，MAC 地址 00-0A-00-00-AA-AA 输入为 000A.0000.AAAA。）例如，您可能出于排除故障的目的而要手动配置 MAC 地址，以便使用易于识别的 MAC 地址。通常情况下，您会使用自动生成的 MAC 地址。

系统优先级的值为 1 到 65535，用于确定哪个节点负责作出绑定决定。默认情况下，ASA 使用优先级 1，即最高优先级。该优先级需要高于交换机上的优先级。

此命令并非引导程序配置的一部分，而是从控制节点复制到数据节点上的。但是，在启用集群后无法更改此值。

步骤 10 启用集群：

enable [**noconfirm**]

示例：

```
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands? [Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

输入 **enable** 命令时，ASA 将扫描正在运行的配置，查找集群不支持的功能的不兼容命令，包括默认配置中可能存在的命令。系统会提示您删除不兼容命令。如果您选择 **No**，则不会启用集群。使用 **noconfirm** 关键字可绕过确认步骤并自动删除不兼容命令。

对于启用的第一个节点，会进行控制节点选择。由于到目前为止第一个节点应该是集群的唯一成员，因此它将成为控制节点。请勿在此期间执行任何配置更改。

要禁用集群，请输入 **no enable** 命令。

注释
如果禁用集群，所有数据接口都将关闭；只有管理专用接口处于活动状态。

示例

以下示例先配置管理接口，再为集群控制链路配置设备本地 EtherChannel，然后为名为“node1”的 ASA 启用集群，由于该设备是第一台添加到集群的设备，因此将成为控制节点。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8
interface management 1/1
   nameif management
   ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
   ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
   security-level 100
   management-only
   no shutdown

interface ethernet 1/6
   channel-group 1 mode on
   no shutdown

interface ethernet 1/7
   channel-group 1 mode on
   no shutdown

cluster group pod1
   local-unit node1
   cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
   priority 1
   key chuntheunavoidable
   enable noconfirm
```

配置数据节点引导程序设置

执行以下程序配置数据节点。

开始之前

- 您必须使用控制台端口来启用或禁用集群。您不能使用 Telnet 或 SSH。
- 请备份配置，以防稍后要退出集群而需要恢复配置。
- 对于多情景模式，请在系统执行空间中完成本程序。要从该情景切换到系统执行空间，请输入 **changeto system** 命令。
- 如果配置中有任何接口未被配置用于集群（例如，默认配置管理 1/1 接口），可以作为数据节点加入集群（在当前选择下不可能变成控制节点）。
- 将节点添加到正在运行的集群时，可能会有限地暂时丢弃数据包/断开连接；这是预期行为。

过程

步骤 1 配置集群控制链路接口，其必须与您为控制节点配置的接口相同。

示例：

```
ciscoasa(config)# interface ethernet 1/6
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
ciscoasa(config)# interface ethernet 1/7
```

```
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

步骤 2 指定您为控制节点配置的同一 MTU：

示例：

```
ciscoasa(config)# mtu cluster 9198
```

步骤 3 确定集群名称，其必须与您为控制节点配置的集群名称相同：

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 4 用唯一的字符串为此集群成员命名：

local-unit *unit_name*

示例：

```
ciscoasa(cfg-cluster)# local-unit node2
```

指定长度为 1 到 38 个字符的 ASCII 字符串。

每个节点必须具有唯一的名称。集群中不允许存在名称重复的节点。

步骤 5 指定您为控制节点配置的同一集群控制链路接口，但在每个节点的相同网络上指定不同的 IP 地址：

cluster-interface *interface_id* **ip** *ip_address mask*

示例：

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.2 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

指定 IP 地址的 IPv4 地址；此接口不支持 IPv6。此接口不能配置 **nameif**。

步骤 6 （路由模式；跨区以太网通道模式）如果您使用站点间集群，则请为此节点设置站点 ID，以使其能使用站点特定的 MAC 地址。

site-id 编号

示例：

```
ciscoasa(cfg-cluster)# site-id 1
```

number介于 1 到 8 之间。

步骤 7 设置此节点在控制节点选择的优先级，通常设置为高于控制节点的值：

priority *priority_number*

示例：

```
ciscoasa(cfg-cluster)# priority 2
```

设置值为 1 到 100 的优先级，其中 1 为最高优先级。

步骤 8 设置一个身份验证密钥，使其与您为控制节点设置的密钥相同：

示例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

步骤 9 启用集群：

enable as-data-node

使用 **enable as-data-node** 命令可避免任何配置不兼容（主要是任何尚未进行集群配置的接口的存在）。此命令可确保加入集群的数据节点不可能在任何当前选举中成为控制节点。从属设备的配置将被同步自控制节点的配置覆盖。

要禁用集群，请输入 **no enable** 命令。

注释
如果禁用集群，所有数据接口将关闭，只有管理接口会处于活动状态。

示例

以下示例包括数据节点 node2 的配置：

```
interface ethernet 1/6

channel-group 1 mode on
no shutdown

interface ethernet 1/7

channel-group 1 mode on
no shutdown

cluster group pod1

local-unit node2
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-data-node
```

自定义集群操作

您可以自定义集群运行状况监控、TCP 连接复制延迟、流移动性和其他优化。

在控制节点上执行这些程序。

配置基本 ASA 集群参数

您可以在控制节点上自定义集群设置。

开始之前

- 对于多情景模式，请在控制节点的系统执行空间中完成本程序。要从情景更改到系统执行空间，请输入 **changeto system** 命令。

过程

步骤 1 进入集群配置模式：

cluster group *name*

步骤 2 （可选） 启用数据节点到控制节点的控制台复制：

console-replicate

默认情况下会禁用此功能。对于特定的重要事件，ASA 可将某些消息直接打印输出到控制台。如果启用了控制台复制，数据节点会将控制台消息发送到控制节点，因此您只需要监控集群的一个控制台端口。

步骤 3 设置集群事件的最低跟踪级别：

trace-level 级别

根据需要设置最低级别：

- **critical** - 重要事件（严重性=1）
- **warning** - 警告（严重性 = 2）
- **informational** - 信息事件（严重性=3）
- **debug** - 调试事件（严重性=4）

步骤 4 设置从流所有者到导向器和备份所有者的流状态刷新消息（clu_keepalive 和 clu_update 消息）的保持连接间隔。

clu-keepalive-interval 秒

- 秒 - 15 到 55。默认值为 15。

您可能想将间隔设置为比默认值更长的时间，以减少集群控制链路上的流量。

配置运行状态监控并自动重新加入设置

此程序可以配置节点和接口运行状态监控。

您可能想禁用不重要的接口（例如管理接口）的运行状况检查。可以监控任何端口通道ID、冗余ID或单一物理接口ID。运行状况监控不在VLAN子接口或虚拟接口（例如，VNI或BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

步骤 2 自定义集群节点运行状况检查功能。

health-check [**holdtime** *timeout*] [**vss-enabled**]

为了确定节点运行状况，ASA集群节点会在集群控制链路上将heartbeat消息发送到其他节点。如果节点在保持期内未接收到来自对等节点的任何heartbeat消息，则对等节点被视为无响应或无法工作。

- **holdtime**-用于确定两次设备keepalive状态消息之间的时间间隔，其值介于0.8到45秒；默认值为3秒。
- **vss-enabled** - 将所有 EtherChannel 接口上的 heartbeat 消息泛洪到集群控制链路，以确保至少其中一个交换机可收到它们。如果将集群控制链路配置为EtherChannel（推荐）且它连接到VSS、vPC、StackWise 或 StackWise Virtual 对，则您可能需要启用 **vss-enabled** 选项。对于某些交换机，当冗余系统中的一个节点关闭或启动时，连接到该交换机的 EtherChannel 成员接口可能看似依赖于 ASA，但它们在交换机端不传输流量。如果您将 ASA 保持时间超时设置为一个较低值（如 0.8 秒），则可将 ASA 从集群中匿名删除，ASA 会将 keepalive 消息发送到这些 EtherChannel 接口之一。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用ASA、或交换机上的接口、或者添加额外的交换机形成VSS、vPC、StackWise 或 StackWise Virtual），您应禁用运行状态检查功能(**no health-check monitor-interface**)，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

步骤 3 在接口上禁用接口运行状况检查。

no health-check monitor-interface *interface_id*

接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。ASA在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定成员还是正在加入集群的设备。默认情况下，为

所有接口启用运行状况检查。您可以使用此命令的**no**形式逐个接口将其禁用。您可能想禁用不重要的接口（例如管理接口）的运行状况检查。

- *interface_id* - 禁用任何端口通道 ID、冗余 ID 或单一物理接口 ID 的监控。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用 ASA、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC、StackWise 或 StackWise Virtual），您应禁用运行状态检查功能 (**no health-check**)，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management1/1
```

步骤 4 自定义在运行状况检查发生故障后的自动重新加入集群设置。

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**- 指定内部错误的自动重新加入设置。内部故障包括：应用程序同步超时、不一致的应用程序状态等。
- **unlimited** —（**cluster-interface** 的默认值）不限制重新加入尝试的次数。
- *auto-rejoin-max* — 设置重新加入尝试次数，介于 0 和 65535 之间。**0** 禁用自动重新加入。**data-interface** 和 **system** 的默认值为 3。
- *auto_rejoin_interval* - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。节点尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- *Auto_rejoin_interval_variation* - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。对于集群接口，默认值为 **1**；对于数据接口和系统，默认值为 **2**。

示例：

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

步骤 5 配置 ASA 将接口视为发生故障并将节点从集群中删除之前经过的防反跳时间。

health-check monitor-interface debounce-time *ms*

示例：

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，ASA 会等待指定的毫秒数，然后才将接口标记为发生故障，并将节点从集群中删除。 对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群节点上的接口仅仅因为另一个集群节点在绑定端口时的速度更快便显示为故障状态。

步骤 6 （可选） 配置流量负载监控。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds* — 设置监控消息之间的时间（以秒为单位），范围介于 10 到 360 秒之间。默认值为 20 秒。
- **intervals** *intervals* — 设置 ASA 维护数据的间隔的数量，该值介于 1 到 60 之间。默认值为 30。

您可以监控集群成员的流量负载，包括总连接计数、CPU 和内存使用情况以及缓冲区丢弃。如果负载过高，且剩余的节点可以处理负载，您可以选择在节点上手动禁用集群，或调整外部交换机上的负载均衡。默认情况下启用此功能。例如，对于每个机箱中具有 3 个安全模块的 Firepower 9300 上的机箱间集群，如果机箱中的 2 个安全模块离开集群，则与该机箱的相同数量的流量将被发送到剩余的模块，并可能压垮它。您可以定期监控流量负载。如果负载过高，您可以选择手动禁用节点上的集群。

使用 **show cluster info load-monitor** 命令查看流量负载。

示例：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
   1           0            0            13              27
```

示例

以下示例将 health-check holdtime 配置为 0.3 秒；启用 VSS；禁用以太网 1/2 接口（用于管理）的监控；将数据接口的 auto-rejoin 设置为从 2 分钟开始的 4 次尝试，将 duration 增至上一次间隔的 3 倍；以及将集群控制链路的 auto-rejoin 设为 6 次尝试，每隔 2 分钟一次。

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3 vss-enabled
ciscoasa(cfg-cluster)# no health-check monitor-interface ethernet1/2
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
```

```
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1
```

配置连接再均衡和集群 TCP 复制延迟

可以配置连接再均衡。有关详细信息，请参阅跨集群实现新 TCP 连接再均衡，第 424 页

为 TCP 连接启用集群复制延迟有助于延迟创建导向器/备份数据流，从而消除与短期数据流相关的“非必要工作”。请注意，如果某个节点在创建导向器/备份数据流前出现故障，则无法恢复这些数据流。同样，如果流量在创建数据流前再均衡到其他节点，则无法恢复该数据流。不应为已对其禁用 TCP 随机化的流量启用 TCP 复制延迟。

过程

步骤 1 为 TCP 连接启用集群复制延迟：

cluster replication delay *seconds* { **http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] { **host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

示例：

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

将 *seconds* 设置为介于 1 到 15 之间的值。默认启用 **http** 延迟，时间为 5 秒。

在多情景模式下，请在相应情景中配置此设置。

步骤 2 进入集群配置模式：

cluster group *name*

步骤 3 （可选）为 TCP 流量启用连接再均衡：

conn-rebalance [**frequency** *seconds*]

示例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

此命令默认禁用。如果启用，ASA 会定期交换有关每秒连接数的信息，并将新连接从每秒连接数较多的设备分流到负载较低的设备。现有连接永远不会移动。此外，由于此命令仅基于每秒的连接数进行重新平衡，因此不会考虑每个节点上已建立的连接总数，并且连接总数可能并不相等。此频率的值为 1 到 360 秒，用于指定多长时间交换一次负载信息。默认值为 5 秒。

将连接分流到其他节点后，它将成为不对称连接。

请勿为站点间拓扑结构配置连接再均衡；您不需要将连接再均衡到位于不同站点的集群成员。

配置站点间功能

对于站点间集群，您可以自定义配置，以提高冗余性和稳定性。

启用导向器本地化

为了提高性能并缩短数据中心的站点间集群的往返时间延迟，您可以启用导向器本地化。新的连接通常实现了负载均衡，并且由特定站点中的集群成员拥有。但是，ASA会向任意站点的成员分配导向器角色。导向器本地化支持其他导向器角色：与所有者同一站点的本地导向器和可位于任意站点的全局导向器。将所有者和导向器保留在同一站点可以提高性能。此外，如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者。当集群成员收到属于其他站点的连接的数据包时，使用全局导向器。

开始之前

- 在引导程序配置中为集群成员设置站点 ID。
- 以下流量类型不支持本地化：NAT 或 PAT 流量；SCTP 检查的流量；分段所有者查询。

过程

步骤 1 进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 启用导向器本地化。

director-localization

启用站点冗余

为保护流量免受站点故障的影响，您可以启用站点冗余。如果连接的备份所有者与所有者位于同一站点，则将从另一个站点选择一个额外的备份所有者来保护流量免受站点故障的影响。

开始之前

- 在引导程序配置中为集群成员设置站点 ID。

过程

步骤 1 进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 启用站点冗余。

site-redundancy

配置每站点免费 ARP

现在，ASA 可以生成免费 ARP (GARP) 数据包，以确保交换基础设施始终处于最新状态：它将作为每个站点优先级最高的成员，定期生成流向全局 MAC/IP 地址的 GARP 流量。

当使用来自集群的各站点 MAC 和 IP 地址数据包使用站点特定的 MAC 地址和 IP 地址时，集群接收的数据包使用全局 MAC 地址和 IP 地址。如果流量不是定期从全局 MAC 地址生成的，您的全局 MAC 地址交换机上可能会出现 MAC 地址超时。发生超时后，以全局 MAC 地址为目标的流量将在整个交换基础设施中进行泛洪，这有可能造成性能和安全问题。

当您为每台设备设置站点 ID 和为每个跨区以太网通道设置站点 MAC 地址时，默认情况下会启用 GARP。您可以自定义 GARP 间隔，也可以禁用 GARP。

开始之前

- 在引导程序配置中为集群成员设置站点 ID。
- 在控制设备配置中为跨区以太网通道设置每站点 MAC 地址。

过程

步骤 1 进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 自定义 GARP 间隔。

site-periodic-garp interval 秒

- *seconds* — 设置 GARP 生成之间的时间（以秒为单位），介于 1 到 1000000 秒之间。默认值为 290 秒。

要禁用 GARP，请输入 **no site-periodic-garp interval**。

配置集群流移动性

当服务器在站点之间移动时，您可以检查 LISP 流量以启用流移动性。

关于 *LISP* 检测

可以检查 LISP 流量，以便在站点间启用流移动性。

关于 LISP

利用数据中心的虚拟机移动性（例如，VMware VMotion），服务器可以在数据中心之间迁移，同时维持与客户端的连接。为了支持此类数据中心服务器移动性，路由器需要能够在服务器移动时更新通往服务器的入口路由。思科定位/ID 分离协议 (LISP) 架构将设备身份或终端标识符 (EID) 与设备位置或路由定位符 (RLOC) 分离开，并分隔到两个不同的编号空间，实现服务器迁移对客户端的透明化。例如，当服务器迁移到新的站点并且客户端向服务器发送流量时，路由器会将流量重定向到新位置。

LISP 需要充当特定角色的路由器和服务器，例如 LISP 出口隧道路由器 (ETR)、入口隧道路由器 (ITR)、第一跳路由器、映射解析器 (MR) 和映射服务器 (MS)。当服务器的第一跳路由器检测到服务器连接了其他路由器时，它会更新所有其他路由器和数据库，以便连接到客户端的 ITR 可以拦截、封装流量并将流量发送到新的服务器位置。

ASA LISP 支持

ASA 本身不运行 LISP；但是，它可以通过检查 LISP 流量确定位置更改，然后使用此信息进行无缝集群操作。如果不使用 LISP 集成，当服务器移动到新站点时，流量将到达位于新站点的 ASA 集群成员，而不是原始的流所有者。新 ASA将流量转发到旧站点的 ASA，然后旧 ASA必须将流量发回新站点，才能到达服务器。此类流量流并未处于最佳状态，称为“长号”或“发夹”。

如果使用 LISP 集成，ASA 集群成员可以检查第一跳路由器与 ETR 或 ITR 之间的 LISP 流量，然后将流所有者位置更改为新站点。

LISP 准则

- ASA 集群成员必须位于第一跳路由器和该站点的 ITR 或 ETR 之间。ASA 集群本身不能作为扩展网段的第一跳路由器。
- 仅支持全分布数据流；集中数据流、半分布数据流或属于单个节点的数据流不会移动到新的所有者。半分布数据流包括应用（例如 SIP），其中作为父数据流所有者的同一 ASA 拥有所有子数据流。
- 集群仅移动第 3 和第 4 层流状态；一些应用数据可能丢失。

- 对于持续时间极短的数据流或非关键业务数据流，移动所有者可能并非最佳选择。在配置检查策略时，您可以控制该功能支持的流量类型，并应只对必要流量限制流移动性。

ASA LISP 实施

此功能包含多种相互关联的配置（本章将逐一说明）：

1. （可选）基于主机或服务器 IP 地址限制检查的 EID - 第一跳路由器可能会向与 ASA 集群无关的主机或网络发送 EID 通知消息，因此，您可以限制只向与您的集群有关的服务器或网络发送 EID。例如，如果集群仅涉及 2 个站点，但是 LISP 在 3 个站点上运行，应只包括集群涉及的 2 个站点的 EID。
2. LISP 流量检查 - ASA 检查 UDP 端口 4342 上的 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个将 EID 和站点 ID 相关联的 EID 表。例如，您应检查包含第一跳路由器源 IP 地址以及 ITR 或 ETR 目标地址的 LISP 流量。请注意，没有为 LISP 流量分配导向器，并且 LISP 流量本身不参与集群状态共享。
3. 用于启用指定流量的流移动性的服务策略 - 您应对关键业务流量启用流移动性。例如，您可以只对 HTTPS 流量和/或发送到特定服务器的流量启用流移动性。
4. 站点 ID - ASA 使用集群中每个节点的站点 ID 确定新的所有者。
5. 用于启用流移动性的集群级别配置 - 您还必须在集群级别启用流移动性。此开/关切换器允许您轻松地启用或禁用特定流量类或应用类的流移动性。

配置 *LISP* 检测

当服务器在站点之间移动时，您可以检查 LISP 流量以启用流移动性。

开始之前

- 根据配置控制节点引导程序设置，第 359 页和配置数据节点引导程序设置，第 364 页，为每个集群设备分配一个站点 ID。
- LISP 流量未包含在 default-inspection-traffic 类中，因此，您在此过程中必须为 LISP 流量配置单独的类。

过程

步骤 1 （可选） 配置 LISP 检测映射以根据 IP 地址限制检测的 EID，并配置 LISP 预共享密钥：

a) 创建扩展 ACL；仅目标 IP 地址与 EID 嵌入式地址匹配：

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。

b) 创建 LISP 检测映射，并进入参数模式：

policy-map type inspect lisp *inspect_map_name*

parameters

c) 通过识别您创建的 ACL 定义允许的 EID：

allowed-eid access-list *eid_acl_name*

第一跳路由器或 ITR/ETR 可能会向与 ASA 集群无关的主机或网络发送 EID 通知消息，因此，您可以限制只向与您的集群有关的服务器或网络发送 EID。例如，如果集群仅涉及 2 个站点，但是 LISP 在 3 个站点上运行，应只包括集群涉及的 2 个站点的 EID。

d) 如果需要，请输入预共享密钥：

validate-key 密钥

示例：

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

步骤 2 在端口 4342 上为第一跳路由器与 ITR 或ETR 之间的 UDP 流量配置 LISP检测：

a) 配置扩展 ACL 以识别 LISP 流量：

access list *eid_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

您必须 指定 UDP 端口 4342。接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。

b) 为 ACL 创建类映射：

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) 使用可选 LISP 检测映射指定策略映射、类映射以及启用检测，然后将服务策略应用于接口（如果为新接口）：

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

如果您有现有服务策略，请指定现有策略映射名称。默认情况下，ASA 包括称为 **global_policy** 的全局策略，因此对于全局策略，请指定该名称。如果您希望全局应用该策略，还可以为每个接口创建一个服务策略。LISP 检测会双向应用于流量，因此您无需在源接口和目标接口上应用服务策略；如果流量与两个方向的类映射都匹配，则进入或退出您应用策略映射的接口的所有流量都受影响。

示例：

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
```

```
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

ASA 会检测 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个关联 EID 和站点 ID 的 EID 表。

步骤 3 为流量类启用流移动性：

a) 配置扩展 ACL 以在服务器更改站点时确定要重新分配至最佳站点的业务关键流量：

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。您应对业务关键流量启用流移动性。例如，您可以只对HTTPS流量和/或发送到特定服务器的流量启用流移动性。

b) 为 ACL 创建类映射：

class-map *flow_map_name*

match access-list *flow_acl_name*

c) 指定在其上启用了 LISP 检测的同一策略映射，再指定流类映射，然后启用流移动性：

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

示例：

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0
 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

步骤 4 进入集群组配置模式，并为集群启用流移动性：

cluster group *name*

flow-mobility lisp

此开/关使您可以轻松地启用或禁用流移动性。

示例

以下示例：

- 将 EID 限制为 10.10.10.0/24 网络上的 EID
- 检查位于 192.168.50.89 的 LISP 路由器（内部）与位于 192.168.10.8 的 ITR 或 ETR 路由器（在另一个 ASA 接口上）之间的 LISP 流量 (UDP 4342)
- 为使用 HTTPS 在 10.10.10.0/24 上进入服务器的所有内部流量启用流移动性。
- 为集群启用流移动性。

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

管理集群节点

部署集群后，您可以更改配置和管理集群节点。

成为非活动节点

要成为集群的非活动成员，请在节点上禁用集群，同时保持集群配置不变。

注释 当ASA处于非活动状态（以手动方式或因运行状况检查失败）时，所有数据接口都将关闭；只有管理专用接口可以发送和接收流量。要恢复流量传输，请重新启用集群；或者，您也可以从集群中完全删除该节点。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，您保存了已禁用集群的配置），则管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

开始之前

- 您必须使用控制台端口；不能通过远程 CLI 连接启用或禁用集群。
- 对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入**changeto system** 命令。

过程

步骤 1 进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 禁用集群：

no enable

如果此节点是控制节点，则会进行新的控制选择，并且其他成员将成为控制节点。

集群配置保持不变，因此您可于稍后再次启用集群。

停用节点

要禁用您登录的节点以外的成员，请执行以下步骤。

注释 当ASA处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。要恢复流量流，请重新启用集群。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，假设您保存了已禁用集群的配置），管理接口将被禁用。您必须使用控制台端口来进行任何进一步的配置。

开始之前

对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入 **changeto system** 命令。

过程

从集群中删除该节点：

cluster remove unit *node_name*

引导程序配置保持不变，从控制节点同步的最新配置也保持不变，因此您可于稍后重新添加该节点而不会丢失配置。如果在数据节点上输入此命令来删除控制节点，则会选择新的控制节点。

要查看成员名称，请输入 **cluster remove unit ?**，或者输入 **show cluster info** 命令。

示例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

重新加入集群

如果从集群中删除了某个节点（例如针对出现故障的接口），或者如果您手动停用了某个成员，那么您必须手动重新加入集群。

开始之前

- 您必须使用控制台端口来重新启用集群。其他接口已关闭。
- 对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入**changeto system** 命令。
- 确保故障已解决，再尝试重新加入集群。

过程

步骤 1 在控制台中，进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 启用集群。

enable

离开集群

要完全退出集群，需要删除整个集群引导程序配置。由于每个节点上的当前配置相同（从主用设备同步），因此退出集群就意味着要么从备份恢复集群前的配置，要么清除现有配置并重新开始配置以免 IP 地址冲突。

开始之前

您必须使用控制台端口；删除集群配置时，所有接口都会关闭，包括管理接口和集群控制链路。而且，您不能通过远程 CLI 连接启用或禁用集群。

过程

步骤 1 对于数据节点，禁用集群：

cluster group *cluster_name* **no enable**

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

在数据节点上启用集群时，您无法进行配置更改。

步骤 2 清除集群配置：

clear configure cluster

ASA 将关闭所有接口，包括管理接口和集群控制链路。

步骤 3 禁用集群接口模式：

no cluster interface-mode

模式并非存储于配置中，因此必须手动重置。

步骤 4 如果有备份配置，可将备份配置复制到正在运行的配置中：

copy *backup_cfg* **running-config**

示例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

步骤 5 将配置保存到启动配置：

write memory

步骤 6 如果没有备份配置，请重新配置管理访问。例如，确保更改接口 IP 地址，并恢复正确的主机名。

更改控制节点

⚠

注意 要更改控制节点，最好的方法是在控制节点上禁用集群，等到新的控制选举后再重新启用集群。如果必须指定要成为控制节点的具体节点，请使用本节中的程序。但是请注意，对集中功能而言，如果使用本程序强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

要更改控制节点，请执行以下步骤：

开始之前

对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入 **changeto system** 命令。

过程

将新节点设置为控制节点：

cluster control-node unit*node_name*

示例：

```
ciscoasa(config)# cluster control-node unit asa2
```

您需要重新连接到主集群 IP 地址。

要查看成员名称，请输入 **cluster control-node unit ?**（可查阅除当前节点之外的所有名称），或输入 **show cluster info** 命令。

在整个集群范围内执行命令

要向集群中的所有节点或某个特定节点发送命令，请执行以下步骤。向所有节点发送 **show** 命令以收集所有输出并将其显示在当前节点的控制台上。也可在整个集群范围内执行其他命令（如 **capture** 和 **copy**）。

过程

发送命令到所有节点，或者如果指定了节点名称，则发送到特定节点：

cluster exec [**unit** *node_name*] *command*

示例：

```
ciscoasa# cluster exec show xlate
```

要查看节点名称，请输入 **cluster exec unit ?**（可查阅除当前节点之外的所有名称），或输入 **show cluster info** 命令。

示例

要同时将同一捕获文件从集群中的所有节点复制到TFTP服务器，请在控制节点上输入以下命令：

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

多个 PCAP 文件（一个文件来自一个节点）将复制到 TFTP 服务器。目标捕获文件名会自动附加节点名称，例如 capture1_asa1.pcap、capture1_asa2.pcap 等。在本例中，asa1和asa2是集群节点名称。

以下是 **cluster exec show port-channel** 汇总命令的输出示例，显示了集群内每个节点的 EtherChannel 信息：

```
ciscoasa# cluster exec show port-channel summary
control node(LOCAL):**********************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 slave:************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

监控 ASA 集群

您可以监控集群状态和连接并排除故障。

监控集群状态

请参阅以下命令来监控集群状态：

- **show cluster info** [**health** [**details**]]

如果没有关键字，**show cluster info** 命令将显示所有集群成员的状态。

show cluster info health 命令将显示接口、节点和整个集群的当前运行状况。**details** 关键字显示心跳消息失败的次数。

请参阅 **show cluster info** 命令的以下输出：

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state CONTROL_NODE
      ID        : 2
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state DATA_NODE
      ID        : 3
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info auto-join**

  显示集群节点是否将在一段延迟后自动重新加入集群，以及是否已清除故障条件（例如等待许可证、机箱运行状况检查失败，等等）。如果节点已永久禁用，或节点已在集群中，则此命令将不会显示任何输出。

  请参阅 **show cluster info auto-join** 命令的以下输出：

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
```

```
Unit will try to join cluster when quit reason is cleared.
Quit reason: Control node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport**{**asp** |**cp** [**detail**]}

  显示以下项目传输相关的统计信息：

  - **asp** — 数据平面传输统计信息。
  - **cp** — 控制平面传输统计信息。

    如果您输入 **detail** 关键字，您可以查看集群可靠传输协议的使用情况，以便确定控制平面中的缓冲区已满时的丢包问题。请参阅 **show cluster info transport cp detail** 命令的以下输出：

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
--------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
```

```
  UE    0          0          0          0
  SN    1656a4ce   acb26fe    5f839f76   7b680831
  R     733840     1042168    852285     867311
  RE    0          0          0          0
  RDC   699789     934969     740874     756490
  RA    385525     281198     204021     205384
  RFR   27626      56397      0          0
  RTR   34051      107199     111411     110821
  RDP   0          0          0          0
  RDPR  0          0          0          0

This unit as a receiver of broadcast messages
----------------------------------------------
        0          2          3
  U     111847     121862     120029
  R     7503       665700     749288
  ESN   5d75b4b3   6d81d23    365ddd50
  RI    630        34278      40291
  RO    0          582        850
  ROW   0          566        850
  ROB   0          16         0
  RAS   1571       123289     142256

This unit as a receiver of unicast messages
-------------------------------------------
        0          2          3
  U     1          3308122    4370233
  R     513846     879979     1009492
  ESN   4458903a   6d841a84   7b4e7fa7
  RI    66024      108924     102114
  RO    0          0          0
  ROW   0          0          0
  ROB   0          0          0
  RAS   130258     218924     228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  -----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%
```

```
Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  显示集群历史记录，以及有关集群节点加入失败的原因或节点离开集群的原因的错误消息。

捕获整个集群范围内的数据包

有关在集群中捕获数据包的信息，请参阅以下命令：

cluster exec capture

要支持集群范围的故障排除，您可以使用 **cluster exec capture** 命令在控制节点上启用捕获集群特定流量的功能，随后集群中的所有数据节点上将自动启用此功能。

监控集群资源

请参阅以下命令以监控集群资源：

show cluster {**cpu** | **memory** | **resource**} [*options*]

显示整个集群的聚合数据。可用 *options* 取决于数据类型。

监控集群流量

请参阅以下命令以监控集群流量：

- **show conn [detail], cluster exec show conn**

  show conn 命令显示一个传输是导向者、备用还是转发者传输。在任意节点上使用 **cluster exec show conn** 命令可查看所有连接。此命令可以显示单个流的流量到达集群中不同 ASA 的方式。集群的吞吐量取决于负载均衡的效率和配置。此命令可以让您很方便地查看某个连接的流量如何流经集群，也可以帮助您了解负载均衡器对传输的性能有何影响。

  show conn detail 命令还显示哪些流应 遵守流移动性。

  以下是 **show conn detail** 命令的输出示例：

```
ciscoasa/ASA2/data node# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
```

```
uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic received
 at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface NP
Identity
Ifc Locally received: 716 (8 byte/s)
```

要对连接流进行故障排除，请先在任意节点上输入 **cluster exec show conn** 命令查看所有节点上的连接。寻找具有以下标志的流：导向者 (Y)、备用 (y) 和转发者 (z)。下例显示了三台 ASA 上的一条从 172.18.124.187:22 到 192.168.103.131:44727 的 SSH 连接；ASA 1 带有 z 标志，表示其是该连接的转发者；ASA3 带有 Y 标志，表示其是该连接的导向者；而 ASA2 则没有特殊的标志，表示其是所有者。在出站方向，此连接的数据包进入 ASA2 上的内部接口并从外部接口流出。在入站方向，此连接的数据包进入 ASA 1 和 ASA3 上的外部接口，通过集群控制链路被转发到 ASA2，然后流出 ASA2 上的内部接口。

```
ciscoasa/ASA1/control node# cluster exec show conn
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**********************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:**********************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0,
flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance** | **flow-mobility counters**]

  show cluster info conn-distribution 和 **show cluster info packet-distribution** 命令显示流量在所有集群节点上的分布。这些命令可以帮助您评估和调整外部负载均衡器。

  show cluster info loadbalance 命令显示连接再均衡统计信息。

  The **show cluster info flow-mobility counters** 命令显示 EID 移动和流所有者移动信息。请参阅 **show cluster info flow-mobility counters** 的以下输出：

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 4
EID movement notification processed : 4
Flow owner moving requested         : 2
```

- **show cluster info load-monitor** [**details**]

  show cluster info load-monitor 命令显示最后一个间隔的集群成员的流量负载，以及已配置的总间隔数（默认情况下为 30）。使用 **details** 关键字查看每个时间间隔的每个度量值。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 30 interval:
   0           0            0            12              28
   1           0            0            13              27


ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval



Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Buffer drops captured over 30 intervals:

Unit ID  0
```

```
          0          0          0          0          0          0
          0          0          0          0          0          0
          0          0          0          0          0          0
          0          0          0          0          0          0
          0          0          0          0          0          0
Unit ID  1
          0          0          0          0          0          0
          0          0          0          0          0          0
          0          0          0          0          0          0
          0          0          0          0          0          0
          0          0          0          0          0          0

Memory usage(%) captured over 30 intervals:
Unit ID  0
         25         25         30         30         30         35
         25         25         35         30         30         30
         25         25         30         25         25         35
         30         30         30         25         25         25
         25         20         30         30         30         30
Unit ID  1
         30         25         35         25         30         30
         25         25         35         25         30         35
         30         30         35         30         30         30
         25         20         30         25         25         30
         20         30         35         30         30         35

CPU usage(%) captured over 30 intervals:
Unit ID  0
         25         25         30         30         30         35
         25         25         35         30         30         30
         25         25         30         25         25         35
         30         30         30         25         25         25
```

```
        25          20          30          30          30          30

Unit ID  1

        30          25          35          25          30          30

        25          25          35          25          30          35

        30          30          35          30          30          30

        25          20          30          25          25          30

        20          30          35          30          30          35
```

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  显示整个集群的聚合数据。可用 *options* 取决于数据类型。

  请参阅 **show cluster access-list** 命令的以下输出：

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

  要显示所有节点在用连接的汇聚计数，请输入：

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):**************************************************************
  100 in use, 100 most used

  cl1:*********************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  此命令对于数据路径故障排除非常有用。

监控集群路由

有关集群路由的信息，请参阅以下命令：

- **show route cluster**
- **debug route cluster**

  显示集群的路由信息。

- **show lisp eid**

  显示 ASA EID 表，表中显示了 EID 和站点 ID。

  请参阅 **cluster exec show lisp eid** 命令的以下输出。

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):***************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:**************************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  该命令对于故障排除非常有用。

配置集群日志记录

有关为集群配置日志记录的信息，请参阅以下命令：

logging device-id

集群中的每个节点将独立生成系统日志消息。您可以使用 **logging device-id** 命令来生成具有相同或不同设备 ID 的系统日志消息，以使消息看上去是来自集群中的相同或不同节点。

监控集群接口

请参阅以下用于监控集群接口的命令：

- **show cluster interface-mode**

  显示集群接口模式。

- **show port-channel**

  包括有关端口通道是否跨网络的信息。

- **show lacp cluster {system-mac | system-id}**

  显示 cLACP 系统 ID 和优先级。

- **debug lacp cluster [all | ccp | misc | protocol]**

  显示 cLACP 的调试消息。

- **show interface**

  显示使用中的站点 MAC 地址的使用情况：

```
ciscoasa# show interface port-channel1.3151
Interface Port-channel1.3151 "inside", is up, line protocol is up
Hardware is EtherChannel/LACP, BW 1000 Mbps, DLY 10 usec
VLAN identifier 3151
MAC address aaaa.1111.1234, MTU 1500
Site Specific MAC address aaaa.1111.aaaa
IP address 10.3.1.1, subnet mask 255.255.255.0
Traffic Statistics for "inside":
132269 packets input, 6483425 bytes
1062 packets output, 110448 bytes
98530 packets dropped
```

调试集群

请参阅以下用于调试集群的命令：

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  显示集群的调试消息。

- **debug cluster flow-mobility**

  显示与集群流移动性相关的事件。

- **debug lisp eid-notify-intercept**

  当 eid-notify 被拦截时显示事件。

- **show cluster info trace**

  show cluster info trace 命令显示调试信息，供进一步排除故障之用。

  请参阅 **show cluster info trace** 命令的以下输出：

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

  例如，如果您看到以下消息显示两个具有相同**local-unit**名称的节点充当控制节点，这可能意味着两个节点具有相同的**local-unit**名称（请检查您的配置），或者某个节点正在接收自己的广播消息（请检查您的网络）。

```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node
 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

ASA 集群示例

这些示例包括典型部署中所有与集群相关的 ASA 配置。

ASA 和交换机配置示例

以下配置示例连接 ASA 与交换机之间的下列接口：

ASA 接口	交换机接口
以太网 1/2	GigabitEthernet 1/0/15
以太网 1/3	GigabitEthernet 1/0/16
以太网 1/4	GigabitEthernet 1/0/17
以太网1/5	GigabitEthernet 1/0/18

ASA 配置

每台设备上的接口模式

```
cluster interface-mode spanned force
```

ASA1 控制单元引导程序配置

```
interface Ethernet1/6
 channel-group 1 mode on
 no shutdown
!
interface Ethernet1/7
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit A
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
 priority 10
 key emphyri0
 enable noconfirm
```

ASA2 数据单元引导程序配置

```
interface Ethernet1/6
 channel-group 1 mode on
 no shutdown
!
interface Ethernet1/7
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
 key emphyri0
 enable as-data-node
```

控制单元接口配置

```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface Ethernet1/2
 channel-group 10 mode active
 no shutdown
!
```

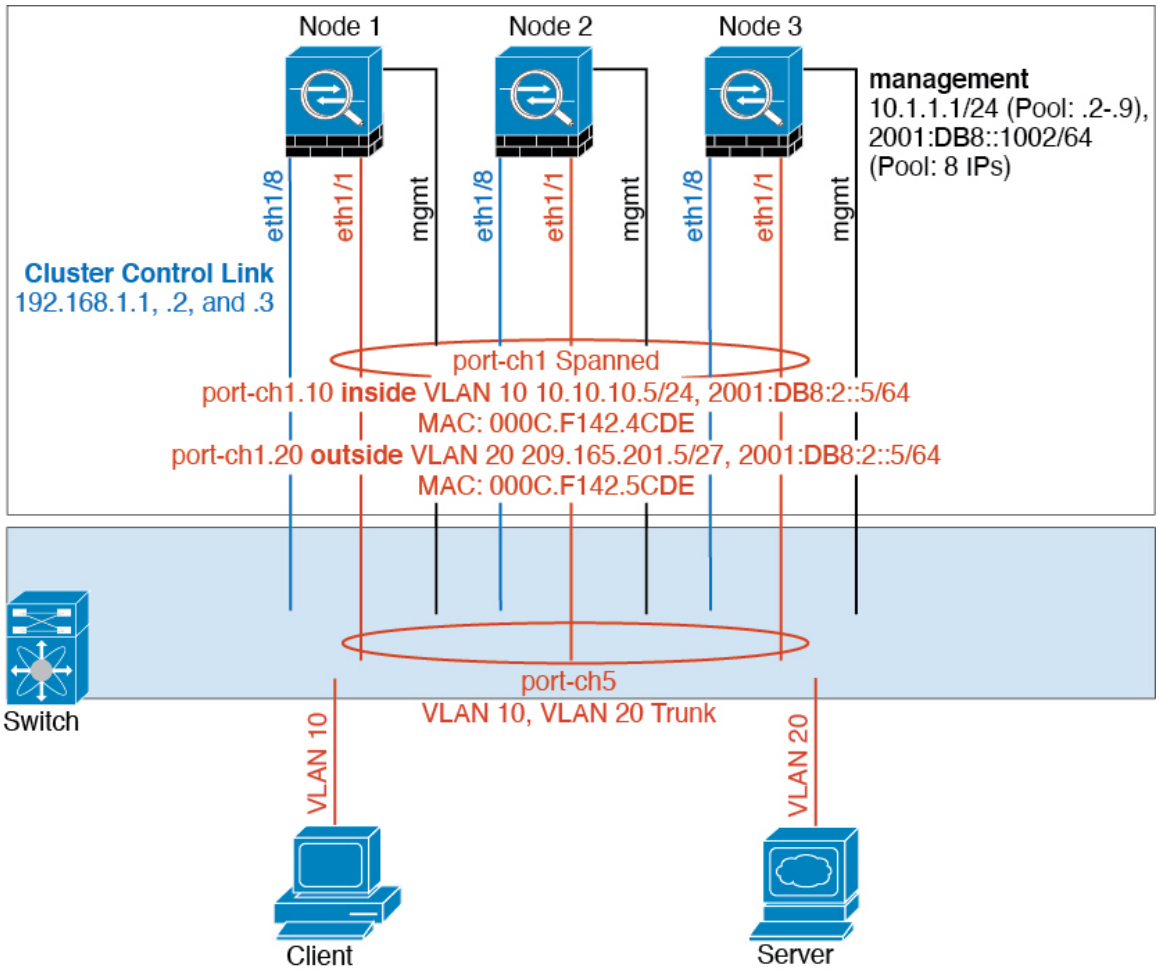
```
interface Ethernet1/3
 channel-group 10 mode active
 no shutdown
!
interface Ethernet1/4
 channel-group 11 mode active
 no shutdown
!
interface Ethernet1/5
 channel-group 11 mode active
 no shutdown
!
interface Management1/1
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
 no shutdown
!
interface Port-channel10
 mac-address aaaa.bbbb.cccc
 nameif inside
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 mac-address aaaa.dddd.cccc
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

思科 IOS 交换机配置

```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

interface Port-channel10
 switchport access vlan 201
 switchport mode access

interface Port-channel11
```

```
switchport access vlan 401
switchport mode access
```

单臂防火墙



来自不同安全域的数据流量与不同的 VLAN 关联，例如，VLAN 10 用于内部网络，而 VLAN 20 用于外部网络。每台ASA都有一个连接到外部交换机或路由器的物理端口。启用中继使物理链路上的所有数据包都采用 802.1q 封装。ASA 是 VLAN 10 与 VLAN 20 之间的防火墙。

使用跨网络 EtherChannel 时，所有数据链路在交换机侧分组为一个 EtherChannel。如果一台 ASA 变得不可用，交换机将在其余设备之间再均衡流量。

每台设备上的接口模式

```
cluster interface-mode spanned force
```

设备 1 控制单元引导程序配置

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa1
cluster-interface ethernet1/8 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

设备 2 数据单元引导程序配置

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa2
cluster-interface ethernet1/8 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-data-node
```

单元 3 数据单元引导程序配置

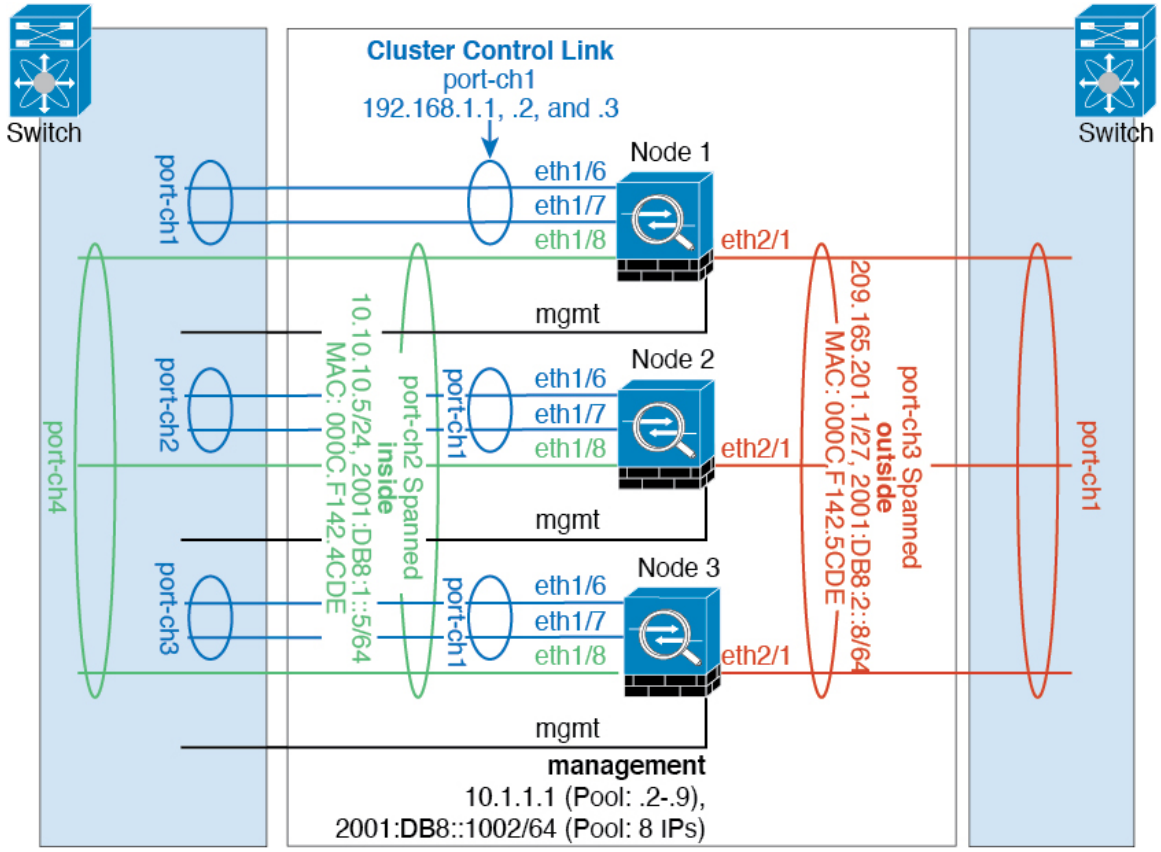
```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa3
cluster-interface ethernet1/8 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-data-node
```

控制单元接口配置

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
no shutdown

interface ethernet1/1
channel-group 1 mode active
no shutdown
```

```
interface port-channel 1

interface port-channel 1.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE

interface port-channel 1.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

流量分隔



您可能更愿意在内部和外部网络之间采用物理方式分离流量。

如上图所示，左侧有一个跨网络 EtherChannel 连接到内部交换机，而右侧的另一个跨网络 EtherChannel 连接到外部交换机。如果需要，您还可以在每个 EtherChannel 上创建 VLAN 子接口。

每台设备上的接口模式

```
cluster interface-mode spanned force
```

设备 1 控制单元引导程序配置

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa1
 cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
 priority 1
 key chuntheunavoidable
 enable noconfirm
```

设备 2 数据单元引导程序配置

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa2
 cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
 priority 2
 key chuntheunavoidable
 enable as-data-node
```

单元 3 数据单元引导程序配置

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL
```

```
cluster group cluster1
 local-unit asa3
 cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
 priority 3
 key chuntheunavoidable
 enable as-data-node
```

控制单元接口配置

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
 nameif management
 ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
 ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
 security-level 100
 management-only
 no shutdown

interface ethernet 1/8
 channel-group 2 mode active
 no shutdown

interface port-channel 2
 nameif inside
 ip address 10.10.10.5 255.255.255.0
 ipv6 address 2001:DB8:1::5/64
 mac-address 000C.F142.4CDE

interface ethernet 2/1
 channel-group 3 mode active
 no shutdown

interface port-channel 3
 nameif outside
 ip address 209.165.201.1 255.255.255.224
 ipv6 address 2001:DB8:2::8/64
 mac-address 000C.F142.5CDE
```

路由模式站点间集群的 OTV 配置

使用跨区以太网通道的路由模式的站点间集群能否成功，取决于OTV的配置和监控是否适当。OTV 通过在 DCI 上转发数据包来发挥重要作用。仅当在其转发表中获知 MAC 地址时，OTV 才会通过 DCI 转发单播数据包。如果在 OTV 转发表中未获知 MAC 地址，它将丢弃单播数据包。

OTV 配置示例

```
//Sample OTV config:
//3151 - Inside VLAN, 3152 - Outside VLAN, 202 - CCL VLAN
//aaaa.1111.1234 - ASA inside interface global vMAC
//0050.56A8.3D22 - Server MAC

feature ospf
```

```
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
```

```
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

因站点故障需要修改 OTV 过滤器

如果站点断开，需要删除 OTV 的过滤器，因为无需再阻止全局 MAC 地址。还需要一些其他配置。

您需要在正常工作的站点中的 OTV 交换机上添加 ASA 全局 MAC 地址的静态条目。此条目将允许另一端的 OTV 在重叠接口上添加这些条目。之所以需要此步骤，是因为如果服务器和客户端已有 ASA 的 ARP 条目（对于现有连接即是如此），它们将不再发送该 ARP。因此，OTV 将不会有机会在其转发表中获知 ASA 全局 MAC 地址。由于 OTV 的转发表中没有该全局 MAC 地址，并且根据 OTV 设计，它不会通过重叠接口泛洪发送单播数据包，则它将丢弃从服务器到全局 MAC 地址的单播数据包，现有连接将中断。

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

当另一个站点恢复时，您需要重新添加过滤器，并删除 OTV 上的此静态条目。清除两个 OTV 上的动态 MAC 地址表，从而清除全局 MAC 地址的重叠条目，这一点非常重要。

MAC 地址表清除

当站点断开并且全局 MAC 地址的静态条目已添加到 OTV 时，您需要让另一个 OTV 获知重叠接口上的全局MAC地址。在另一个站点恢复后，应清除这些条目。务必清除MAC地址表，以确保OTV 的转发表中没有这些条目。

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
```

```
O 3151 0050.5660.9412 dynamic -  F F Overlay1
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

OTV ARP 缓存监控

OTV 为代理 ARP 维护通过 OTV 接口获知的 IP 地址的 ARP 缓存。

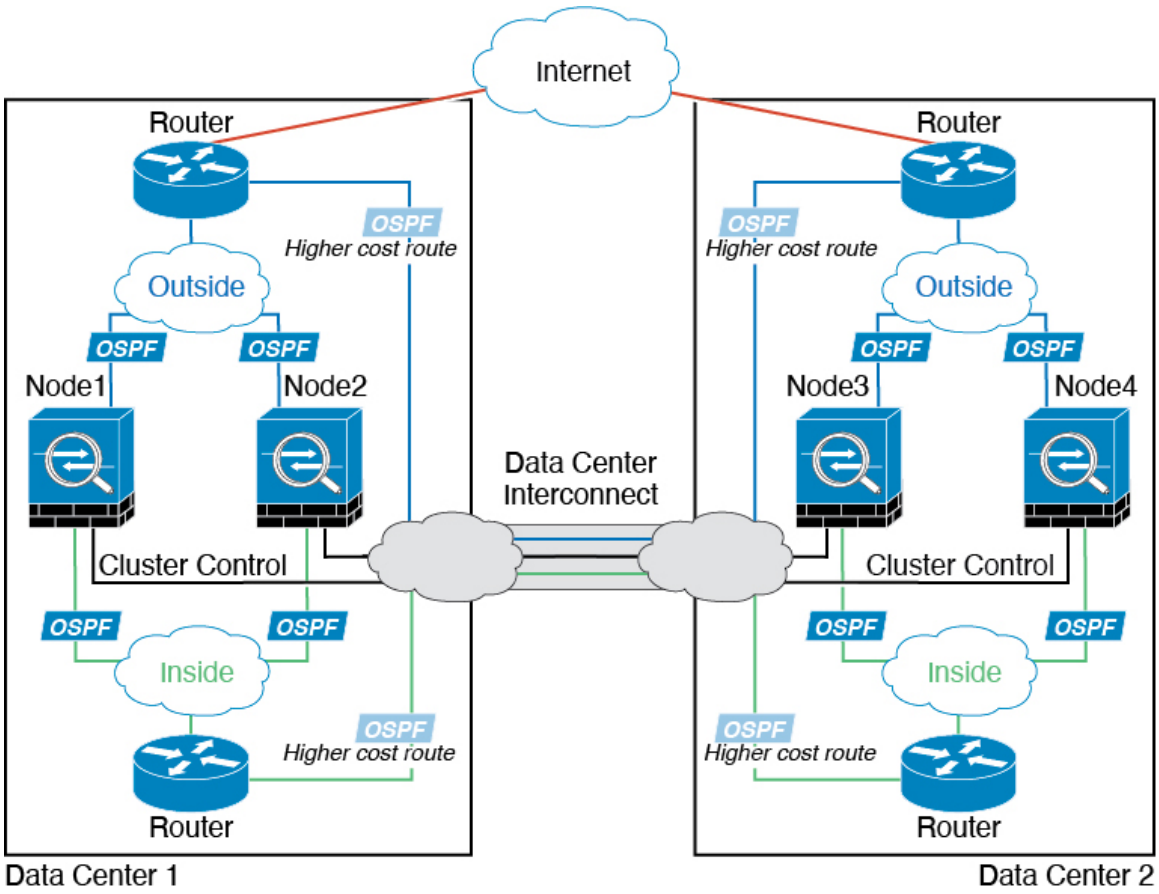
```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

站点间集群示例

以下示例显示支持的集群部署。

独立接口路由模式南北站点间集群示例

以下示例显示的 2 个 ASA 集群节点分别位于 2 个部署在内部和外部路由器之间（南北插入）的数据中心。集群节点由集群控制链路通过 DCI 连接。位于每个数据中心的内部和外部路由器使用 OSPF 和 PBR 或 ECMP 在集群成员之间对流量执行负载均衡。通过指定 DCI 中开销较高的路由可将流量保持在每个数据中心内（除非给定站点上的所有 ASA 集群节点都中断连接）。如果一个站点上的所有集群节点都发生故障，流量将从每台路由器通过 DCI 发往另一个站点上的 ASA 集群节点。



具有站点特定的 MAC 和 IP 地址的跨区以太网通道路由模式示例

以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在每个站点上的网关路由器和内部网络之间（东西插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部网络的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

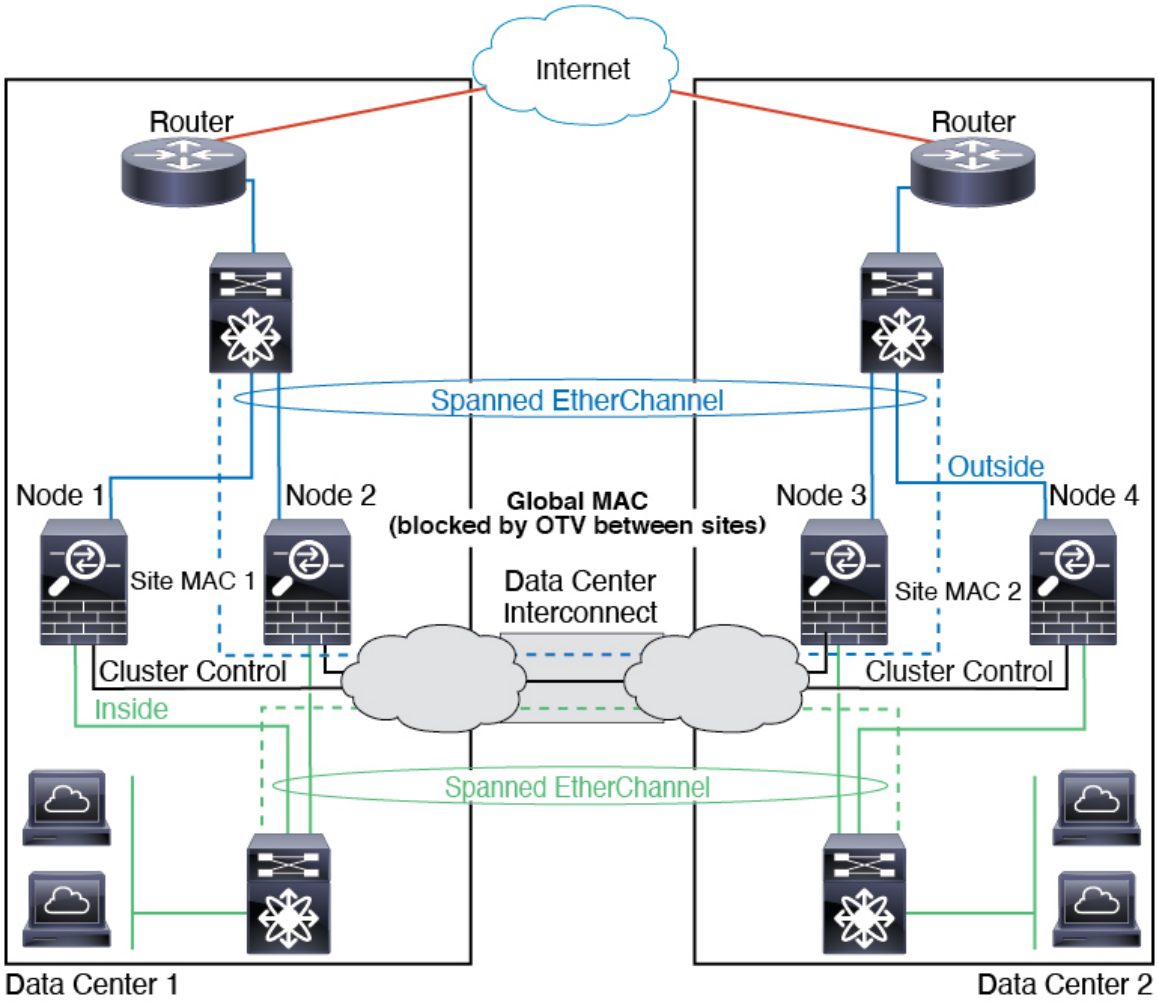
数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术在站点之间扩展。您必须添加阻止全局 MAC 地址的过滤器，防止发往集群的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的集群节点，则您必须删除过滤器，使流量能够发送到另一站点的集群节点。您应使用 VACL 来过滤全局 MAC 地址。对于某些交换机（例如具有 F3 系列线卡的 Nexus），您还必须使用 ARP 检查屏蔽来自全局 MAC 地址的 ARP 数据包。ARP 检查要求您在 ASA 上设置站点 MAC 地址和站点 IP 地址。如果仅配置站点 MAC 地址，请禁用 ARP 检查。

集群相当于内部网络的网关。所有集群节点共享的全局虚拟 MAC 仅用于接收数据包。传出数据包使用来自每个 DC 集群的站点特定的 MAC 地址。此功能可防止交换机从两个不同端口上的两个站点获知相同全局 MAC 地址，导致 MAC 地址摆动；相反，它们仅获知站点 MAC 地址。

在此场景中：

- 从集群发送的所有出口数据包使用站点 MAC 地址，并在数据中心进行本地化。

- 发送到集群的所有入口数据包使用全局MAC地址发送，因此可以被两个站点的任何节点接收；OTV 的过滤器将数据中心内的流量本地化。



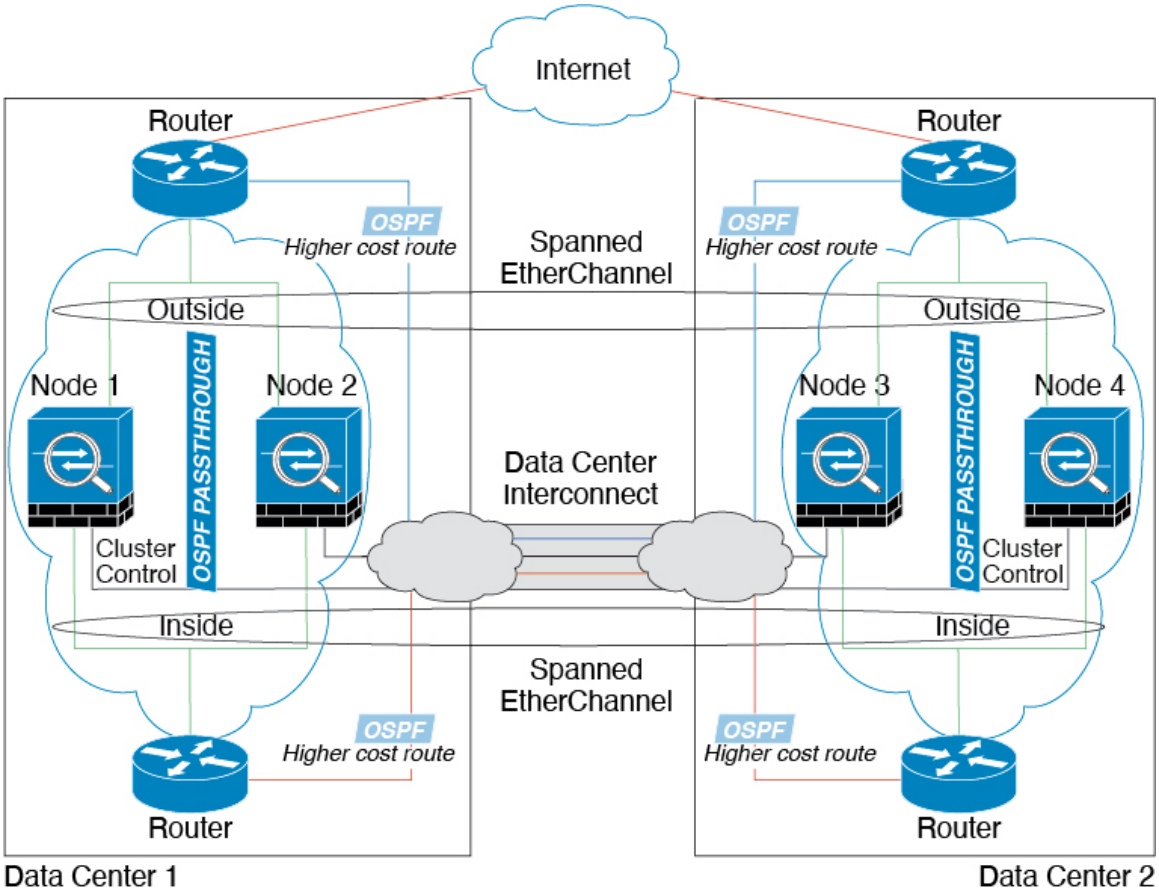
跨区以太网通道透明模式南北站点间集群示例

以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在内部和外部路由器之间（南北插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

位于每个数据中心的内部和外部路由器均使用OSPF（可通过透明的ASA）。与MAC地址不同，路由器IP地址在所有路由器上都是唯一的。通过指定DCI中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有集群成员都中断连接。通过ASA的开销较低的路由必须经过位于每个站点的同一网桥组才能使集群维持非对称连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的集群成员。

位于每个站点的交换机的实施可包括：

- 站点间 VSS、vPC、StackWise 或 StackWise Virtual - 在此情景中，一台交换机安装在数据中心 1，另一台交换机安装在数据中心 2。一个方案是将位于每个数据中心的集群节点只连接到本地交换机，而冗余交换机流量通过 DCI 传输。在此情况下，连接多半会保持在每个数据中心本地。如果 DCI 可以处理额外的流量，您也可以选择将每个节点通过 DCI 连接到两台交换机。在此情况下，流量跨数据中心分摊，因此 DCI 必须非常强健稳定。
- 位于每个站点的本地 VSS、vPC、StackWise 或 StackWise Virtual - 为了获得更高的交换机冗余能力，您可以在每个站点安装 2 对单独的冗余交换机。在此情况下，尽管集群节点仍然有一个跨区以太网通道将数据中心 1 的机箱仅连接到两台本地交换机，将数据中心 2 的机箱连接到本地交换机，但跨区以太网通道本质上是“分离的”。每个本地冗余交换机系统都会将跨区以太网通道视作站点本地的 EtherChannel。

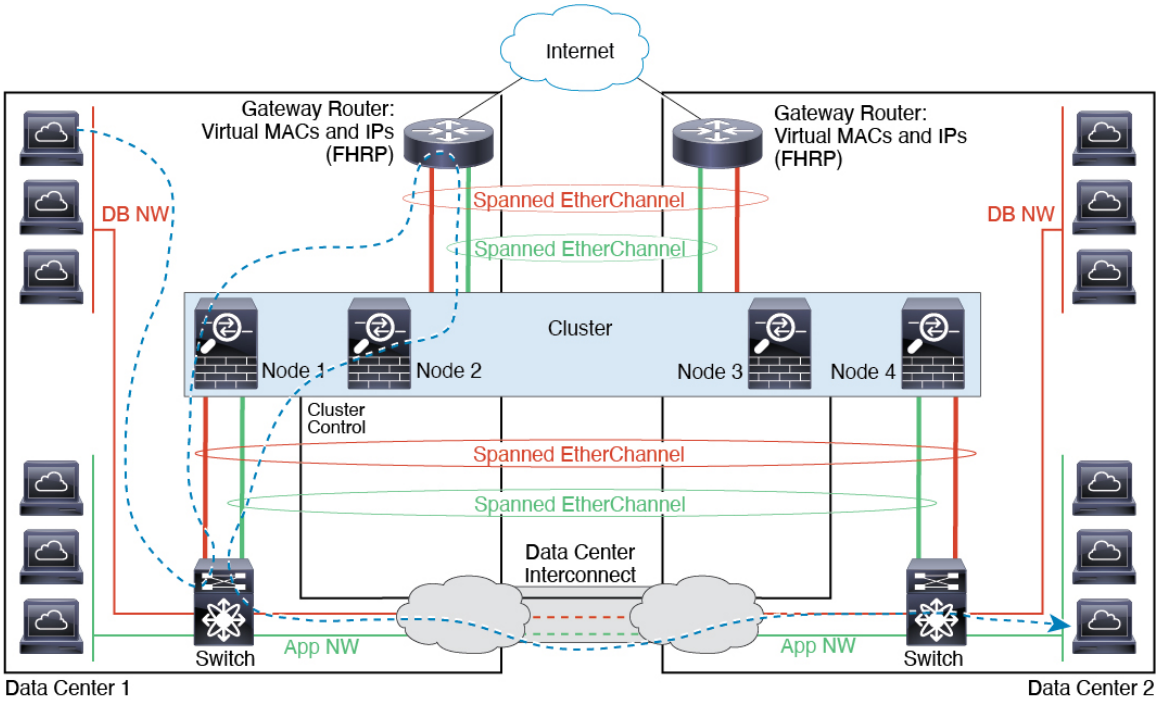


跨区以太网通道 透明模式东西站点间集群示例

以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在每个站点上的网关路由器和两个内部网络（应用网络和数据库网络）之间（东西插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。每个站点上的集群成员使用面向内部与外部应用网络和数据库网络的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

每个站点上的网关路由器使用 FHRP（例如 HSRP）在每个站点上提供相同的目标虚拟 MAC 和 IP 地址。要避免 MAC 地址意外摆动，最好使用使用 **mac-address-table static** *outside_interface mac_address*

命令将网关路由器实际 MAC 地址静态添加到 ASA MAC 地址表。如果没有这些条目，当位于站点 1 的网关与位于站点 2 的网关通信时，流量可能通过 ASA 并尝试从内部接口到达站点 2，从而导致出现问题。数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术在站点之间扩展。您必须添加过滤器，阻止发往网关路由器的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的网关路由器，则您必须删除过滤器，使流量能够发送到另一站点的网关路由器。



集群参考

本部分包括有关集群工作原理的详细信息。

ASA 功能和集群

部分 ASA 功能不受 ASA 集群支持，还有部分功能仅在控制节点上受支持。其他功能可能对如何正确使用规定了注意事项。

集群不支持的功能

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

- 依靠 TLS 代理实现的统一通信功能
- 远程访问 VPN（SSL VPN 和 IPsec VPN）
- 虚拟隧道接口 (VTI)
- 以下应用检查：

- CTIQBE
- H323、H225 和 RAS
- IPsec 穿透
- MGCP
- MMP
- RTSP
- SCCP（瘦客户端）
- WAAS
- WCCP

- 僵尸网络流量过滤器
- 自动更新服务器
- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- VPN 负载均衡
- Azure 上的故障转移
- 集成路由和桥接
- FIPS 型号

集群集中化功能

以下功能只有在控制节点上才受支持，且无法为集群扩展。

注释 集中功能的流量从成员节点通过集群控制链路转发到控制节点。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非控制节点的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回控制节点。

对集中功能而言，如果控制节点发生故障，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

- 以下应用检查：
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS

- PPTP
- RADIUS
- RSH
- SNMP
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- 静态路由监控
- 网络访问的身份验证和授权。记帐被分散。
- 筛选服务
- 站点间 VPN
- IGMP 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- PIM 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- 动态路由（仅适用于跨网络 EtherChannel 模式）

应用到单个节点的功能

这些功能将应用到每个 ASA 节点而非整个集群或控制节点。

- QoS - QoS 策略将于配置复制过程中在集群中同步。但是，该策略是在每个节点上独立执行。例如，如果对输出配置管制，则要对流出特定 ASA 的流量应用符合规则的速率和符合规则的突发量值。在包含 3 个节点且流量均衡分布的集群中，符合规则的速率实际上变成了集群速率的 3 倍。
- 威胁检测 - 威胁检测在各节点上独立工作；例如，排名统计信息就要视具体节点而定。以端口扫描检测为例，由于扫描的流量将在所有节点间进行负载均衡，而一个节点无法看到所有流量，因此端口扫描检测无法工作。
- 资源管理 - 多情景模式下的资源管理根据本地使用情况在每个节点上分别执行。
- LISP 流量 - UDP 端口 4342 上的 LISP 流量由每个接收节点进行检查，但是没有为其分配导向器。每个节点都会添加到集群共享的 EID 表，但是 LISP 流量本身并不参与集群状态共享。

用于网络访问的 **AAA** 和集群

用于网络访问的 AAA 由三部分组成：身份验证、授权和记账。身份验证和授权作为集中功能在集群控制节点上实施，且数据结构复制到集群数据节点。如果选举出控制节点，新的控制节点将拥有所

需的所有信息，以继续不间断运行经过验证的既有用户及其相关授权。当控制节点发生变化时，用户身份验证的空闲和绝对超时将保留。

记账作为分散的功能在集群中实施。记账按每次流量完成，因此在为流量配置记账时，作为流量所有者的集群节点会将记账开始和停止消息发送到 AAA 服务器。

连接设置和集群

连接限制在集群范围强制实施（请参阅 **set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max** 和 **set connection per-client-max** 命令）。每个节点都有根据广播消息估计的集群范围的计数器值。出于效率考虑，在集群中配置的连接限制可能不会严格按限制数量实施。每个节点在任何指定时间都可能高估或低估集群范围内的计数器值。不过，在负载均衡的集群中，该信息将随时间而更新。

FTP 和集群

- 如果 FTP 数据通道和控制通道流量由不同的集群成员所有，则数据通道所有者会将空闲超时更新定期发送到控制通道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父/子流量关系；控制流量空闲超时不会更新。
- 如果您将 AAA 用于 FTP 访问，则控制通道流集中在控制节点上。

ICMP检测和集群

ICMP 和 ICMP 错误数据包通过集群的流取决于是否启用 ICMP/ICMP 错误检查。不启用 ICMP 检查时，ICMP 是单向流，并且不支持导向器流。启用 ICMP 检查时，ICMP 流变为双向流，并由导向器/备份流支持。被检查的 ICMP 流的一个不同之处在于导向器对转发数据包的处理：导向器会将 ICMP 回应应答数据包转发给流所有者，而不是将数据包返回给转发器。

组播路由和集群

组播路由的行为因接口模式而异。

跨区以太网通道模式下的组播路由

在跨区以太网通道模式下：控制单元负责处理所有组播路由数据包和数据包，直到建立快速路径转发为止。在连接建立之后，每台数据设备都可以转发组播数据包。

独立接口模式下的组播路由

在独立接口模式下，设备并不单独处理组播。所有数据和路由数据包都由控制设备进行处理和转发，从而避免数据包复制。

NAT 和集群

NAT 可能会影响集群的总吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 ASA，因为负载均衡算法取决于 IP 地址和端口，NAT 会导致入站和出站数据包具有不同的 IP 地址和/或端口。当数据包到达并非 NAT 所有者的 ASA时，会通过集群控制链路转发到所有者，导致集群控制链路上

存在大量流量。请注意，接收节点不会创建流向所有者的转发流量，因为NAT所有者最终可能不会根据安全和策略检查结果为数据包创建连接。

如果您仍想在集群中使用 NAT，请考虑以下准则：

- 不使用代理 ARP - 对于独立接口，切勿为映射的地址发送代理 ARP 回复。这可以防止邻接路由器与可能已经不在集群中的 ASA 保持对等关系。对于指向主集群 IP 地址的映射地址，上游路由器需要静态路由或带对象跟踪的 PBR。这对跨网络 EtherChannel 来说不是问题，因为只有一个 IP 地址与集群接口关联。
- 不对独立接口使用接口 PAT - 独立接口不支持接口 PAT。
- PAT 采用端口块分配 - 请参阅该功能的以下准则：
  - 每主机最大流量限制并不针对整个集群，而是单独应用于每个节点。因此，在每主机最大流量限制配置为 1 的包含 3 个节点的集群中，如果在全部 3 个节点上对来自主机的流量实行负载均衡，则可以分配 3 个端口块，每个节点 1 个。
  - 在执行每主机最大流量限制时，在备份池中的备份节点上创建的端口块不计算在内。
  - 如果进行即时 PAT 规则修改（对 PAT 池改用全新的 IP 地址范围），会导致在新的池生效时仍在传输的转换项备份请求的转换项备份创建失败。此行为并非端口块分配功能所特有，它是一个暂时性 PAT 池问题，只发现于在集群节点之间分配池并执行流量负载均衡的集群部署。
  - 在集群中操作时，不能直接更改块分配大小。只有在集群中重新加载每个设备后，新的大小才会生效。为避免重新加载每个设备，我们建议您删除所有块分配规则并清除与这些规则相关的所有转换。然后，您可以更改块大小并重新创建块分配规则。
- 对动态 PAT 使用 NAT 池地址分配 - 配置 PAT 池时，集群将池中的每个 IP 地址划分为端口块。默认情况下，每个块都是 512 个端口，但如果配置端口块分配规则，则使用块设置。这些块在集群中的各个节点之间均匀分配，因此每个节点都有一个或多个块对应 PAT 池中的每个 IP 地址。因此，在一个集群的 PAT 池中可以最少拥有一个 IP 地址，只要这足以支持您预期的 PAT 连接数即可。端口块覆盖的端口范围为 1024-65535，除非您在 PAT 池 NAT 规则中配置该选项以包含保留的端口 1-1023。
- 在多个规则中重复使用 PAT 池 - 要在多条规则中使用同一 PAT 池，必须注意规则中的接口选择。必须在所有规则中使用特定接口，或者在所有规则中使用“任意”接口。不能在规则中混合使用特定接口和“任意”接口，否则系统可能无法将返回流量与集群中的正确节点进行匹配。每条规则使用唯一的 PAT 池是最可靠的方案。
- 不使用轮询 - 集群不支持 PAT 池轮询。
- 无扩展 PAT - 集群不支持扩展 PAT。
- 控制节点管理的动态 NAT 转换 - 控制节点保留转换表并复制到数据节点。当数据节点收到需要动态 NAT 的连接并且转换不在表中时，它将请求从控制节点转换。数据节点拥有该连接。
- 过时 xlate - 连接所有者上的 xlate 空闲时间不会更新。因此，空闲时间值可能会超过空闲超时值。如果空闲计时器值高于配置的超时值（refcnt 为 0），则表示 xlate 过时。

- 每会话 PAT 功能 - 每会话 PAT 功能并非集群专用功能，但它能提高 PAT 的可扩展性，而且对集群而言，它允许每个数据节点成为 PAT 连接的所有者；相比之下，多会话 PAT 连接则必须转发到控制节点并由控制节点所有。默认情况下，所有 TCP 流量和 UDP DNS 流量均使用每会话 PAT 转换，而 ICMP 和所有其他 UDP 流量均使用多会话。您可以为 TCP 和 UDP 配置每会话 NAT 规则以更改这些默认设置，但是，您不能为 ICMP 配置每会话 PAT。对于使用多会话 PAT 的流量（例如 H.323、SIP 或 Skinny），您可以禁用关联 TCP 端口的每会话 PAT（这些 H.323 和 SIP 的 UDP 端口已默认为多会话）。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。
- 对以下检查不使用静态 PAT：
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 如果您有大量 NAT 规则（超过一万条），则应使用设备 CLI 中的 **asp rule-engine transactional-commit nat** 命令启用事务提交模型。否则，节点可能无法加入集群。

动态路由和集群

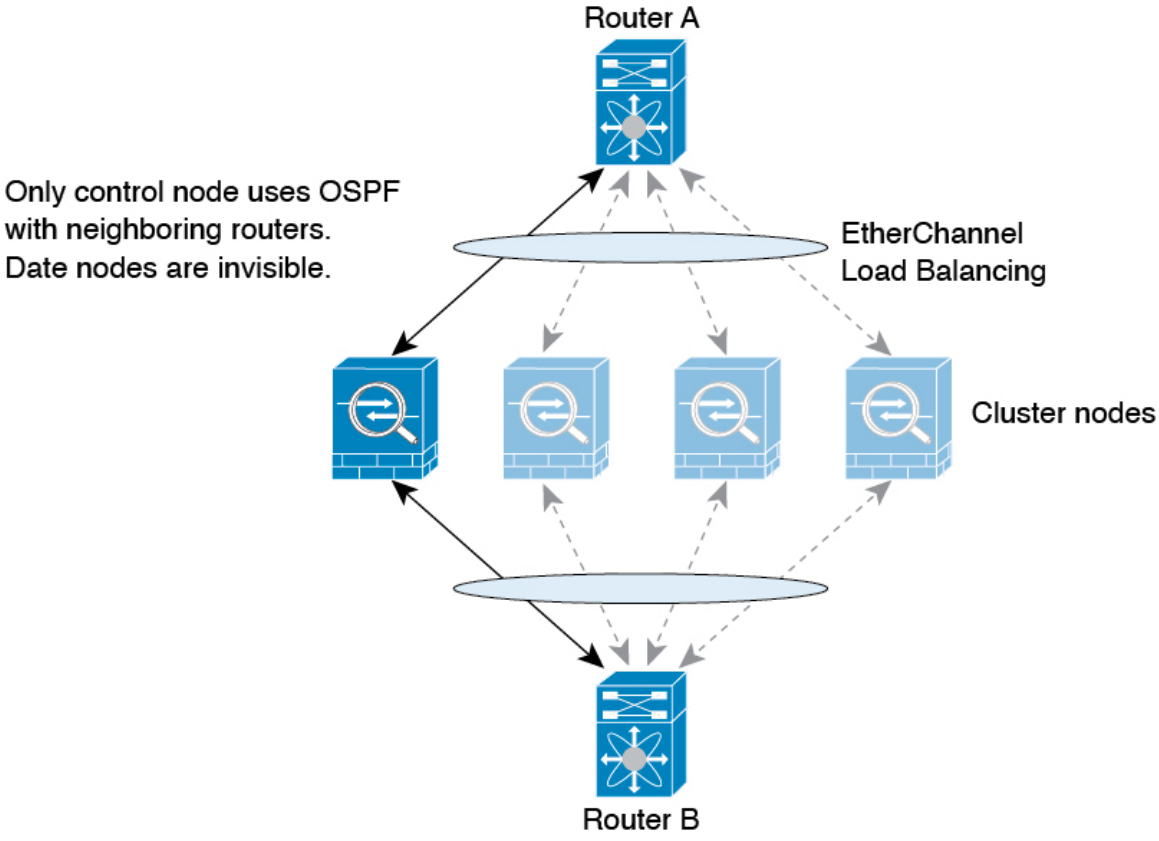
本部分介绍如何使用动态路由和集群。

跨区以太网通道模式下的动态路由

注释 跨区以太网通道模式不支持 IS-IS。

路由过程仅在控制节点上运行，并且通过控制节点学习路线后复制到数据节点。如果路由数据包到达数据节点，它将重定向到控制节点。

图 *50:* 跨区以太网通道模式下的动态路由



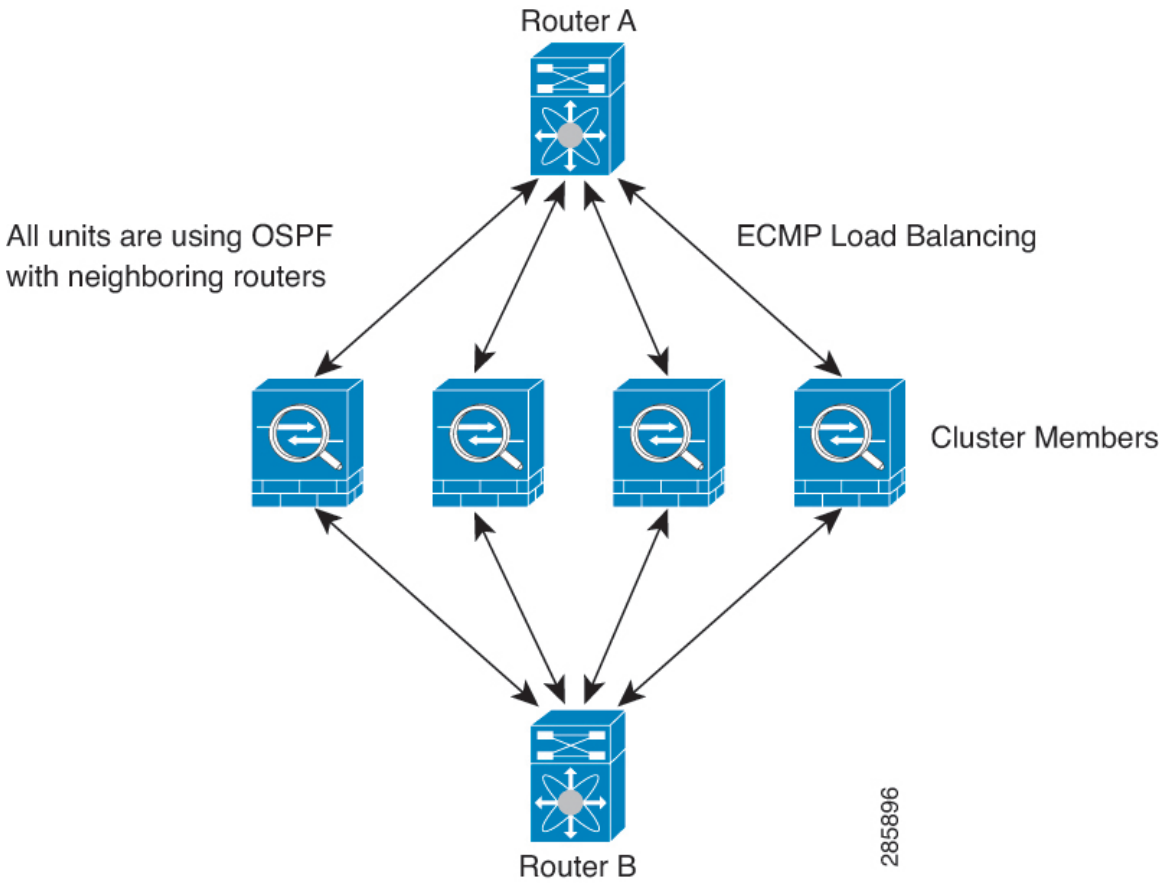
在数据节点向控制节点学习路线后，每个节点将单独做出转发决策。

OSPF LSA 数据库不会从控制节点同步到数据节点。如果切换了控制节点，邻近路由器将检测到重新启动；切换是不透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。请参阅 OSPF 无间断转发功能，解决中断问题。

独立接口模式下的动态路由

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *51:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一个节点。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每个节点在与外部路由器通信时，都会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

EIGRP 与单个接口模式下的集群对等体不构成邻居关系。

注释 如果该集群为实现冗余有多个设备与同一个路由器相邻，则非对称路由可能会造成不可接受的流量损失。要避免非对称路由，请将所有这些节点接口分组到同一流量区域中。请参阅配置流量区域，第 806 页。

SCTP 和集群

SCTP 关联可以在任何节点上创建（由于负载均衡），但其多宿主连接必须位于同一节点上。

SIP 检测和集群

控制流可以在任何节点上创建（由于负载均衡），但其子数据流必须位于同一节点上。

不支持 TLS 代理配置。

SNMP 和集群

SNMP 代理按照本地 IP 地址轮询每一个ASA。您无法轮询集群的合并数据。

您应始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的控制节点时，对新控制节点的轮询将失败。

当使用 SNMPv3 进行集群时，如果您在初始集群形成后添加新的集群节点，则 SNMPv3 用户不会复制到新节点。您必须在控制节点上重新添加它们以强制用户复制到新节点，或者直接在数据节点上复制。

STUN 和集群

故障转移和集群模式支持STUN检查，因为针孔被复制。但是，节点之间不进行事务ID的复制。如果节点在收到 STUN 请求后发生故障，并且另一个节点收到 STUN 响应，则该 STUN 响应将被丢弃。

系统日志与 NetFlow 和集群

- 系统日志 - 集群中的每个节点都会生成自己的系统日志消息。您可以配置日志记录，使每个节点在系统日志消息的报头字段中使用相同或不同的设备ID。例如，集群中的所有节点都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备ID，则所有节点生成的系统日志消息都会看似来自一个节点。如果将日志记录配置为使用集群引导程序配置中指定的本地节点名称作为设备 ID，系统日志消息就会看似来自不同节点。
- NetFlow - 集群中的每个节点都会生成自己的 NetFlow 数据流。NetFlow 收集器只能将每台 ASA 视为单独的 NetFlow 导出器。

思科 TrustSec 和集群

只有控制节点学习安全组标记 (SGT) 信息。然后，控制节点将 SGT 填充到数据节点，数据节点可以根据安全策略对 SGT 做出匹配决策。

VPN 和集群

站点间 VPN 是集中功能；只有控制节点支持 VPN 连接。

注释 集群不支持远程访问 VPN。

VPN 功能仅限控制节点使用，且不能利用集群的高可用性功能。如果控制节点发生故障，所有现有的 VPN 连接都将断开，VPN 用户将遇到服务中断。选择新的控制节点后，必须重新建立 VPN 连接。

将 VPN 隧道连接到跨网络 EtherChannel 地址时，连接会自动转移到控制节点。 对于使用 PBR 或 ECMP 时与独立接口的连接，您必须始终连接到主集群 IP 地址而非本地地址。

与 VPN 相关的密钥和证书将被复制到所有节点。

性能换算系数

将多台设备组成一个集群时，预计可以达到近似 80% 最大组合吞吐量的集群总体性能。

例如，如果您的型号在单独运行时可以处理大约 10 Gbps 的流量，则对于 8 台设备的集群，最大组合吞吐量约为 80 Gbps（8 台设备 x 10 Gbps）的 80%：64 Gbps。

控制节点选择

集群节点通过集群控制链路通信，如下选举控制节点：

1. 当为节点启用集群（或当节点首次启动时已启用集群）时，设备会每 3 秒广播一个选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级设置在 1 和 100 之间，其中 1 为最高优先级。
3. 如果某节点在 45 秒后未收到另一个具有较高优先级的节点的响应，则该设备会成为控制节点。

注释 如果多个节点并列获得最高优先级，则使用集群节点名称和序列号确定控制节点。

4. 如果节点稍后加入具有更高优先级的集群，它不会自动成为控制节点；现有控制节点始终保持为控制节点，除非它停止响应，此时会选择新的控制节点。
5. 在“裂脑”场景中，当临时存在多个控制节点时，具有最高优先级的节点将会保留角色，而其他节点则恢复为数据节点角色。

注释 您可以手动强制节点成为控制节点。对集中功能而言，如果强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

集群中的高可用性

集群通过监控节点和接口的运行状况并在节点之间复制连接状态来提供高可用性。

节点运行状况监控

每个节点通过集群控制链路定期发送广播保持连接心跳数据包。如果控制节点在可配置的超时期限内未从数据节点接收任何keepalive心跳数据包或其他数据包，则控制节点会从集群中删除该数据节点。如果数据节点未从控制节点接收数据包，则从其余节点中选择新的控制节点。

如果节点因为网络故障而不是因为节点实际故障而无法通过集群控制链路相互访问，则集群可能会进入“裂脑”场景，其中隔离的数据节点将选择自己的控制节点。例如，如果路由器在两个集群位置之间发生故障，则位于位置1的原始控制节点将从集群中删除位置2数据节点。同时，位置2的节点将选择自己的控制节点并形成自己的集群。请注意，在这种情况下，非对称流量可能会失败。恢复集群控制链路后，优先级较高的控制节点将保留控制节点的角色。

有关详细信息，请参阅控制节点选择，第 418 页。

接口监控

每个节点都会监控使用中的所有已命名的硬件接口的链路状态，并向控制节点报告状态更改。

- 跨网络 EtherChannel - 使用集群链路聚合控制协议 (cLACP)。每个节点都会监控链路状态和 cLACP 协议消息，以便确定 EtherChannel 中的端口是否仍处于活动状态。状态会报告给控制节点。
- 独立接口（仅适用于路由模式）- 每个节点都会监控自己的接口并向控制节点报告接口状态。

当您启用运行状况监控时，默认情况下会监控所有物理接口（包括主要的 EtherChannel）；您可以选择按接口禁用监控。只能监控已命名接口。例如，已命名的 EtherChannel 必须发生故障，才能将其视为发生故障，这意味着 EtherChannel 的所有成员端口必须发生故障才能触发集群删除（具体取决于您的最小端口绑定设置）。

如果某个节点被监控的接口发生故障，则将从集群中删除该设备。ASA 在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定成员还是正在加入集群的设备。对于 EtherChannel（无论是否跨网络）：如果既定成员上的接口关闭，ASA 将在 9 秒后删除该成员。ASA 在节点加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 ASA从集群中删除。如果是非 EtherChannel，则无论节点的成员状态如何，都会在 500 毫秒后删除设备。

发生故障后的状态

当集群中的节点发生故障时，该节点承载的连接将无缝转移到其他节点；流量的状态信息将通过控制节点的集群控制链路共享。

如果控制节点发生故障，则优先级最高（数字最小）的另一个集群成员将成为控制节点。

ASA将自动尝试重新加入集群，具体取决于故障事件。

注释 当ASA变成不活动状态且无法自动重新加入集群时，所有数据接口都会关闭，仅管理专用接口可以发送和接收流量。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但是，如果您重新加载而节点在集群中仍然处于非活动状态，管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

重新加入集群

当集群节点从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路在 最初加入时出现故障 - 在解决集群控制链路存在的问题后，您必须通过在控制台端口输入 **cluster group** *name*，然后输入 **enable**重新启用集群 ，以手动重新加入集群。
- 加入集群后出现故障的集群控制链路 - ASA 无限期地每 5 分钟自动尝试重新加入。此行为是可配置的。
- 出现故障的数据接口 - ASA 尝试在 5 分钟时、然后在 10 分钟时、最后在 20 分钟时重新加入。如果 20 分钟后仍加入失败，ASA 将禁用集群。解决数据接口问题之后，您必须在控制台端口上通过输入**cluster group** *name*，然后输入**enable** 来手动启用集群。此行为是可配置的。
- 节点存在故障 - 如果节点因节点运行状况检查失败而从集群中删除，则如何重新加入集群取决于失败的原因。例如，临时电源故障意味节点将在重新启动时重新加入集群，只要集群控制链路打开并且仍然使用 **enable** 命令启用集群。ASA 每 5 秒钟尝试重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。 节点将尝试以下列间隔自动重新加入集群：5 分钟，10 分钟，然后是 20 分钟。此行为是可配置的。

请参阅配置控制节点引导程序设置 ， 第 359 页。

数据路径连接状态复制

每个连接在集群中都有一个所有者和至少一个备用所有者。备用所有者在发生故障时不会接管连接；而是存储 TCP/UDP 状态信息，使连接在发生故障时可以无缝转移到新的所有者。备用所有者通常也是导向器。

有些流量需要 TCP 或 UDP 层以上的状态信息。请参阅下表了解支持或不支持此类流量的集群。

表 *17:* 在集群中复制的功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	-
MAC 地址表	是	-
用户标识	是	包括 AAA 规则 (uauth) 。
IPv6 邻居数据库	是	—
动态路由	是	—
SNMP 引擎 ID	否	-
适用于 Firepower 4100/9300的分布式 VPN（站点间）	是	备用会话成为主用会话，并创建一个新的备用会话。

集群管理连接的方式

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

连接角色

请参阅为每个连接定义的下列角色：

- 所有者 - 通常为最初接收连接的节点。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。如果原始所有者发生故障，则当新节点从连接接收到数据包时，导向器会从这些节点中选择新的所有者。
- 备用所有者 - 存储从所有者接收的 TCP/UDP 状态信息的节点，以便在出现故障时可以无缝地将连接转移到新的所有者。在发生故障时，备用所有者不会接管连接。如果所有者处于不可用状态，从该连接接收数据包的第一个节点（根据负载均衡而定）联系备用所有者获取相关的状态信息，以便成为新的所有者。

  只要导向器（见下文）与所有者不是同一节点，导向器也可以是备用所有者。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  对于 Firepower 9300 上的在一个机箱中包括多达 3 个集群节点的集群，如果备用所有者与所有者在同一机箱上，则将从另一个机箱中选择一个额外的备用所有者来保护流量免受机箱故障的影响。

  如果您对站点间集群启用导向器本地化，则有两个备用所有者角色：本地备用和全局备用。所有者始终选择与自身位于同一站点（基于站点 ID）的本地备用。全局备用可以位于任何站点，甚至可以与本地备用是同一个节点。所有者向两个备用所有者发送连接状态信息。

  如果启用站点冗余，并且备用所有者与所有者位于同一站点，则将从另一个站点选择一个额外的备用所有者来保护流量免受站点故障的影响。机箱备份和站点备份是独立的，因此流量在某些情况将同时具有机箱备份和站点备份。

- 导向器 - 处理来自转发器的所有者查找请求的节点。当所有者收到新连接时，会根据源/目的 IP 地址和端口的散列值（有关 ICMP 散列详细信息，请参见下文）选择导向器，然后向导向器发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他节点，该节点会向导向器查询哪一个节点是所有者，以便转发数据包。一个连接只有一个导向器。如果导向器发生故障，所有者会选择一个新的导向器。

  只要导向器与所有者不是同一节点，导向器也可以是备用所有者（见上文）。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  如果您对站点间集群启用导向器本地化，则有两个导向器角色：本地导向器和全局导向器。所有者始终选择与它自身位于同一站点（基于站点 ID）的本地导向器。全局导向器可以位于任何站点，甚至可以与本地导向器是同一节点。如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者。

  ICMP/ICMPv6 散列详细信息：

  - 对于 Echo 数据包，源端口为 ICMP 标识符，目的端口为 0。
  - 对于 Reply 数据包，源端口为 0，目的端口为 ICMP 标识符。

- 对于其他数据包，源端口和目的端口均为 0。

- 转发器 - 向所有者转发数据包的节点。如果转发者收到并非其所有的连接的数据包，则会向导向器查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向器也可以是转发者。如果启用导向器本地化，转发器将始终向本地导向器查询。如果本地导向器未获知所有者，例如，当集群成员收到所有者位于其他站点上的连接的数据包时，转发者将仅查询全局导向器。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN Cookie 直接获知所有者，因此无需向导向器查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向器查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。一个连接了可以有多个转发器；采用良好的负载均衡方法可以做到没有转发器，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。

注释 不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

当连接使用端口地址转换 (PAT) 时，PAT 类型（每会话或多会话）会对哪个集群成员将成为新连接的所有者产生影响：

- 每会话 PAT - 所有者是接收连接中的初始数据包的节点。

  默认情况下，TCP 和 DNS UDP 流量均使用每会话 PAT。

- 多会话 PAT - 所有者始终是控制节点。如果多会话 PAT 连接最初由数据节点接收，则数据节点会将连接转发给控制节点。

  默认情况下，UDP（DNS UDP 除外）和 ICMP 流量使用多会话 PAT，因此这些连接始终归控制节点所有。

您可以更改 TCP 和 UDP 的每会话 PAT 默认设置，以便根据配置按每会话或多会话处理这些协议的连接。对于 ICMP，您不能更改默认的多会话 PAT。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。

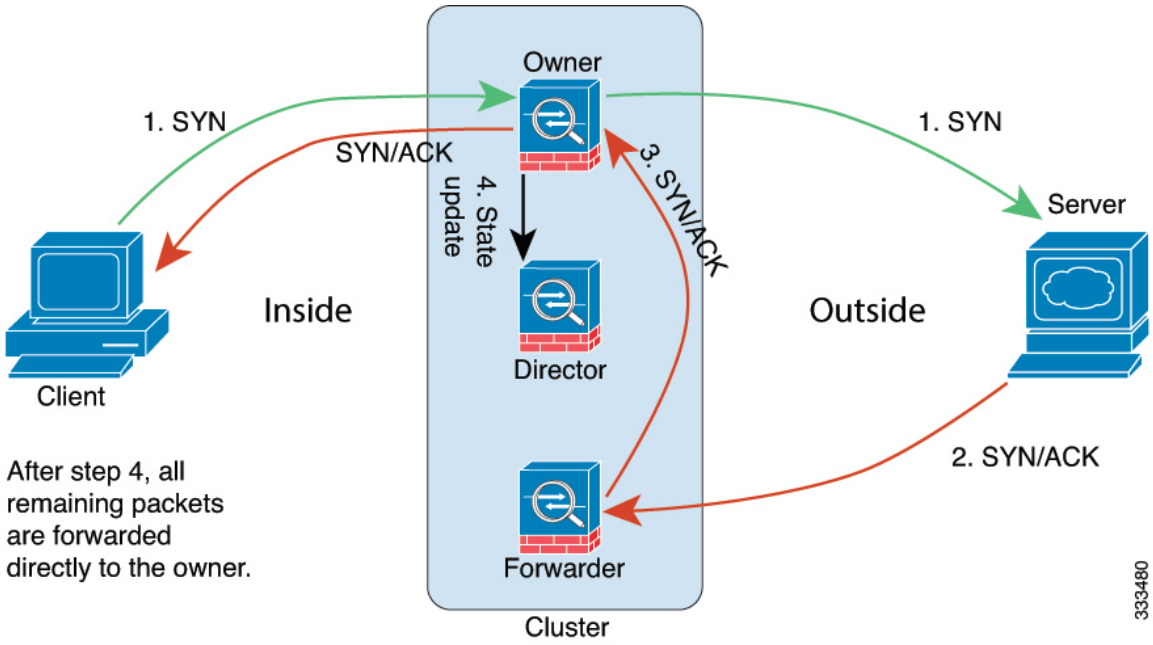
新连接所有权

通过负载均衡将新连接定向到集群节点时，该连接的两个方向都由此节点所有。如果该连接有任何数据包到达其他节点，这些数据包都会通过集群控制链路被转发到所有者节点。为了获得最佳性能，

对于要到达同一个节点的流量的两个方向以及要在节点之间均摊的流量，都需要执行适当的外部负载均衡。如果反向流量到达其他节点，会被重定向回原始节点。

TCP 的数据流示例

以下图例显示了新连接的建立。

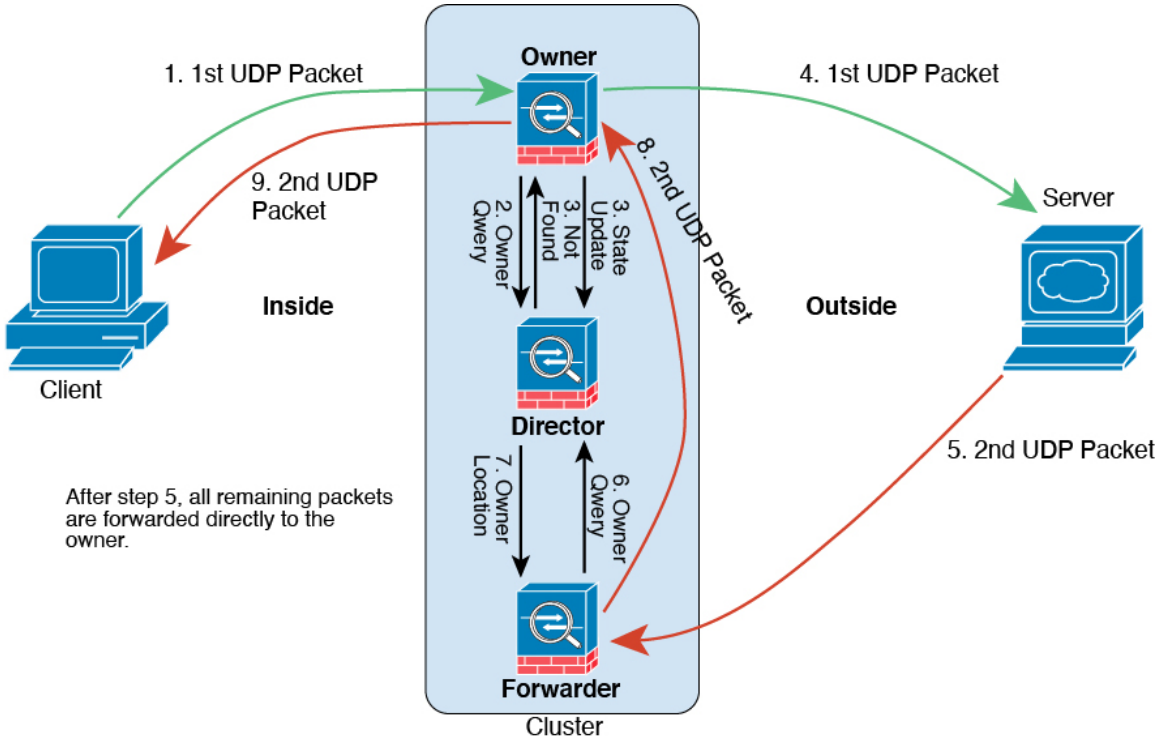


1. SYN 数据包从客户端发出，被传送到一台 ASA（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 ASA（基于负载均衡方法）。此 ASA是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，并记录TCP状态信息以及所有者。导向器将充当该连接的备用所有者。
6. 传送到转发器的任何后续数据包都会被转发到所有者。
7. 如果数据包被传送到任何其他节点，它将向导向器查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向器发送状态更新。

ICMP 和 UDP 的数据流示例

以下图例显示了新连接的建立。

1. 图 *52: ICMP* 和 *UDP* 数据流



第一个 UDP 数据包从客户端发出，被传送到一个ASA（基于负载均衡方法）。

2. 收到第一个数据包的节点查询基于源/目的 IP 地址和端口的散列值选择的导向器节点。
3. 导向器找不到现有流，创建导向器流并将数据包转发回前一个节点。换句话说，导向器已为此流选择了所有者。
4. 所有者创建流，向导向器发送状态更新，然后将数据包转发到服务器。
5. 第二个 UDP 数据包从服务器发出，并被传送到转发器。
6. 转发器向导向器查询所有权信息。对于 DNS 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。
7. 导向器向转发器回复所有权信息。
8. 转发器创建转发流以记录所有者信息，并将数据包转发给所有者。
9. 所有者将数据包转发到客户端。

跨集群实现新 TCP 连接再均衡

如果上游或下游路由器的负载平衡功能导致流量分布不平衡，则可以配置新的连接再平衡，这样每秒新连接数较高的节点就会将新 TCP 流量重定向到其他节点。现有流量将不会移至其他节点。

由于此命令仅基于每秒的连接数进行重新平衡，因此不会考虑每个节点上已建立的连接总数，并且连接总数可能并不相等。

将连接分流到其他节点后，它将成为不对称连接。

请勿为站点间拓扑结构配置连接再均衡；您不需要将新的连接再均衡到位于不同站点的集群成员。

Cisco Secure Firewall 3100/4200 的 ASA 集群的历史记录

功能名称	版本	功能信息
通过 Cisco Secure Firewall 4200 上的集群支持分布式站点间VPN	9.23(1)	Cisco Secure Firewall 4200 上的 ASA 集群在分布式模式下支持站点间 VPN。使用分布式模式能够在 ASA 集群的成员之间分布多个站点间 IPsec IKEv2 VPN 连接，而不仅分布在控制节点上（如集中模式一样）。这将在集中式 VPN 功能的基础上大幅扩展 VPN 支持，并提供高可用性。 新增或修改的命令：**cluster redistribute vpn-sessiondb**、 **show cluster vpn-sessiondb**、**vpn-mode**、**show cluster resource usage**、**show vpn-sessiondb**、**show conn detail**、**show crypto ikev2 stats**
最大集群节点数增加到 16	9.22(1)	最大节点数从 8 个增加到 16 个。
独立接口模式	9.22(1)	独立接口是正常的路由接口，每个接口都有自己的 本地 *IP* 地址 用于路由。每个接口的主集群 *IP* 地址 是固定地址，始终属于控制节点。当控制节点更改时，主集群 IP 地址将转移到新的控制节点，使集群的管理得以无缝继续。 必须在上游交换机上分别配置负载均衡。 新增/修改的命令：**cluster interface-mode individual**
流状态的可配置集群保持连接间隔	9.20(1)	流所有者向导向器和备份所有者发送保持连接（clu_keepalive 消息）和更新（clu_update 消息），以刷新流状态。您现在可以设置保持连接的间隔。默认值为 15 秒，您也可以将间隔设为 15 到 55 秒。您可能想将间隔设置得更长，以减少集群控制链路上的流量。 新增/修改的命令：**clu-keepalive-interval**
引入了对 Cisco Secure Firewall 4200上的集群的支持	9.20(1)	在跨区以太网通道模式下，您最多可以对 8 台 Cisco Secure Firewall 4200 节点进行集群。
删除偏差语言	9.19(1)	包含术语“主”和“从”的命令、命令输出和系统日志消息已被更改为“控制”和“数据”。 新增/修改的命令：**cluster control-node**、**enable as-data-node**、**prompt**、**show cluster history**、**show cluster info**
引入了对 Cisco Secure Firewall 3100上的集群的支持	9.17(1)	在跨区以太网通道模式下，您最多可以对 8 台 Cisco Secure Firewall 3100 节点进行集群。

第 11 章

Firepower 4100/9300 的 ASA 集群

通过集群，您可以将多台Firepower 4100/9300 机箱 ASA 组合成单个逻辑设备。Firepower 4100/9300 机箱 系列包括 Firepower 9300 和 Firepower 4100 系列。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。

注释 使用集群时，有些功能不受支持。请参阅集群不支持的功能，第 499 页。

- 关于 Firepower 4100/9300 机箱上的集群，第 427 页
- Firepower 4100/9300 机箱上的集群要求和前提条件，第 433 页
- 集群许可证 Firepower 4100/9300 机箱，第 435 页
- 集群准则和限制，第 436 页
- 在 Firepower 4100/9300 机箱上配置集群，第 441 页
- FXOS：删除集群设备，第 474 页
- ASA：管理集群成员，第 476 页
- ASA：监控 Firepower 4100/9300 机箱上的 ASA 集群，第 480 页
- 分布式站点间 VPN 故障排除，第 491 页
- ASA 集群示例，第 492 页
- 集群参考，第 499 页
- Firepower 4100/9300上 ASA 集群的历史记录，第 513 页

关于 Firepower 4100/9300 机箱上的集群

在 Firepower 4100/9300 机箱 上部署集群时，它执行以下操作：

- 为设备间通信创建 集群控制链路 （默认情况下，使用端口通道 48）。

  对于同一个 Firepower 9300 机箱内的安全模块隔离的集群，此链路利用 Firepower 9300 背板进行集群通信。

  对于多机箱集群，需要手动将物理接口分配到此 EtherChannel 以进行机箱间通信。

- 在应用中创建集群引导程序配置。

在部署集群时，机箱管理引擎将最低引导程序配置推送到包含集群名称、集群控制链路接口及其他集群设置的每个设备。 如果您需要自定义集群环境，可以在应用内对引导程序配置的某些用户可配置部分进行配置。

- 将数据接口作为跨网络 接口分配给集群。

  对于同一个 Firepower 9300 机箱内的安全模块隔离的集群，跨网络接口不限于 EtherChannel，就像用于多个机箱的集群一样。 Firepower 9300 管理引擎在内部利用 EtherChannel 技术，将流量负载均衡到共享接口上的多个模块，使任何数据接口类型都可用于跨网络模式。 对于多机箱集群，必须对所有数据接口使用跨网络 EtherChannel。

注释 除管理接口以外，不支持独立接口。

- 向集群中的所有设备分配管理接口。

有关集群的详细信息，请参阅以下各节：

引导程序配置

在部署集群时，Firepower 4100/9300 机箱管理引擎将最低引导程序配置推送到包含集群名称、集群控制链路接口及其他集群设置的每个设备。 如果您需要自定义集群环境，则用户可以配置引导程序配置的某些部分。

集群成员

集群成员协调工作来实现安全策略和流量的共享。

一个集群成员是**控制**设备。系统自动确定控制设备。所有其他成员都是**数据**设备。

您必须仅在控制设备上执行所有配置；然后，配置将复制到数据设备。

有些功能在集群中无法扩展，控制设备将处理这些功能的所有流量。请参阅集群集中化功能，第 500 页。

集群控制链路

集群控制链路是用于设备到设备通信的 EtherChannel（端口通道 48）。对于机箱内集群，此链路利用 Firepower 9300 背板进行集群通信。对于机箱间集群，需要手动将物理接口分配到 Firepower 4100/9300 机箱 上的此 EtherChannel 以进行机箱间通信。

对于有 2 个机箱的机箱间集群，请勿将集群控制链路从一机箱直接连接至另一机箱。如果直接连接两个接口，则当一台设备发生故障时，集群控制链路失效，会导致剩下的那台正常设备也发生故障。而如果通过交换机连接集群控制链路，则集群控制链路仍会对正常设备打开。

集群控制链路流量包括控制流量和数据流量。

控制流量包括：

- 控制节点选举。
- 配置复制。
- 运行状况监控。

数据流量包括：

- 状态复制。
- 连接所有权查询和数据包转发。

有关集群控制链路的详细信息，请参阅以下部分。

确定集群控制链路规格

如果可能，应将集群控制链路的大小设定为与每个机箱的预期吞吐量匹配，以使集群控制链路可以处理最坏情况。

集群控制链路流量主要由状态更新和转发的数据包组成。集群控制链路在任一给定时间的流量大小不尽相同。转发流量的大小取决于负载均衡的效率或是否存在大量用于集中功能的流量。例如：

- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 用于网络访问的 AAA 是集中功能，因此所有流量都会转发到控制设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

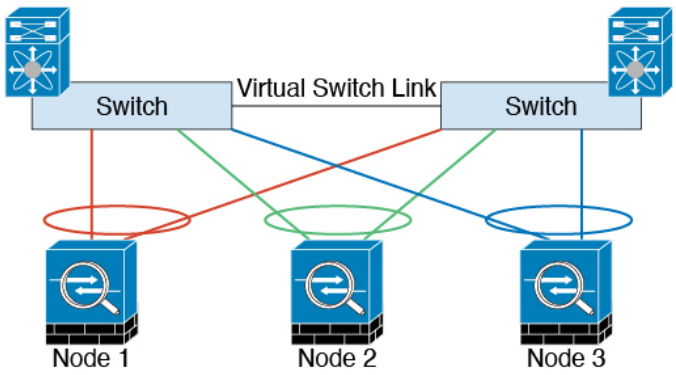
带宽较高的集群控制链路可以帮助集群在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。

注释 如果集群中存在大量不对称（再均衡）流量，应增加集群控制链路的吞吐量大小。

集群控制链路冗余

我们建议将 EtherChannel 用于集群控制链路，以便在 EtherChannel 中的多条链路上传输流量，同时又仍能实现冗余。

下图显示了如何在虚拟交换系统 (VSS)、虚拟端口通道 (vPC)、StackWise 或 StackWise Virtual 环境中使用 EtherChannel 作为集群控制链路。EtherChannel 中的所有链路都是活动链路。如果交换机是冗余系统的一部分，则您可以将同一个 EtherChannel 中的防火墙接口连接到冗余系统中单独的交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台不同的交换机的行为就像一台交换机一样。请注意，此 EtherChannel 是设备本地的，而非跨网络 EtherChannel。



机箱间集群的集群控制链路可靠性

为了确保集群控制链路的功能，设备之间的往返时间 (RTT) 务必要小于 20 毫秒。此最大延迟能够增强与不同地理位置安装的集群成员的兼容性。要检查延迟，请在设备之间的集群控制链路上执行 ping 操作。

集群控制链路必须可靠，没有数据包无序或丢弃数据包的情况；例如，站点间部署应使用专用链路。

集群控制链路网络

Firepower 4100/9300 机箱基于机箱 ID 和插槽 ID 自动为每个设备生成集群控制链路接口 IP 地址：127.2.*chassis_id*.*slot_id*。当您部署集群时，您可以自定义此 IP 地址。集群控制链路网络不能包括设备之间的任何路由器；仅可执行第 2 层交换。 对于站点间流量，思科建议使用重叠传输虚拟化 (OTV)。

集群接口

对于同一个 Firepower 9300 机箱内的安全模块隔离的集群，可以为集群分配物理接口或 EtherChannel 接口（也称为端口通道）。分配给集群的接口是对集群各个成员间的流量进行负载均衡的跨网络接口。

对于多机箱集群，只能为集群分配数据 EtherChannel 接口。这些跨网络 EtherChannel 在每个机箱上都包括相同的成员接口；在上游交换机上，所有这些接口都包括在一个 EtherChannel 内，因此交换机不知道它连接到多台设备。

除管理接口以外，不支持独立接口。

连接到冗余交换机系统

我们建议将 EtherChannel 连接到冗余交换机系统（例如 VSS、vPC、StackWise 或 StackWise Virtual 系统），以便为接口提供冗余。

配置复制

集群中的所有节点共享一个配置。您只能在控制节点上进行配置更改（引导程序配置除外），这些更改会自动同步到集群中的所有其他节点。

Cisco Secure Firewall ASA集群管理

使用 ASA集群的一个好处可以简化管理。本节介绍如何管理集群。

管理网络

我们建议将所有设备都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理接口

必须为集群分配管理类型的接口。此接口是与跨网络接口相对立的一种特殊接口。通过管理接口，可以直接连接到每个设备。

集群的主集群 IP 地址是集群的固定地址，始终属于当前的控制单元。您也可以配置一个地址范围，使每个设备（包括当前控制单元在内）都能使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问；当主设备更改时，主集群 IP 地址将转移到新的主设备，使集群的管理得以无缝继续。

例如，您可以连接到主集群 IP 地址来管理集群，该地址始终属于当前的控制设备。要管理单个成员，您可以连接到本地 IP 地址。

注释 传入设备的流量必须指向节点的管理 IP 地址；传入设备的流量不会通过群集控制链路转发到任何其他节点。

对于 TFTP 或系统日志等出站管理流量，包括控制设备在内的每台设备都使用本地 IP 地址连接到服务器。

控制设备管理与数据设备管理

所有管理和监控均可在控制节点上进行。从控制节点中，您可以检查所有节点的运行时统计信息、资源使用情况或其他监控信息。您也可以向集群中的所有节点发出命令，并将控制台消息从数据节点复制到控制节点。

如果需要，您可以直接监控数据节点。虽然在控制节点上可以执行文件管理，但在数据节点上也可以如此（包括备份配置和更新映像）。以下功能在控制节点上不可用：

- 监控每个节点的集群特定统计信息。
- 监控每个节点的系统日志（控制台复制启用时发送至控制台的系统日志除外）。
- SNMP
- NetFlow

加密密钥复制

当您在控制节点上创建加密密钥时，该密钥将复制到所有数据节点。如果您有连接到主集群 IP 地址的 SSH 会话，则控制节点发生故障时连接将断开。新控制节点对 SSH 连接使用相同的密钥，这样当您重新连接到新的控制节点时，无需更新缓存的 SSH 主机密钥。

ASDM 连接证书 IP 地址不匹配

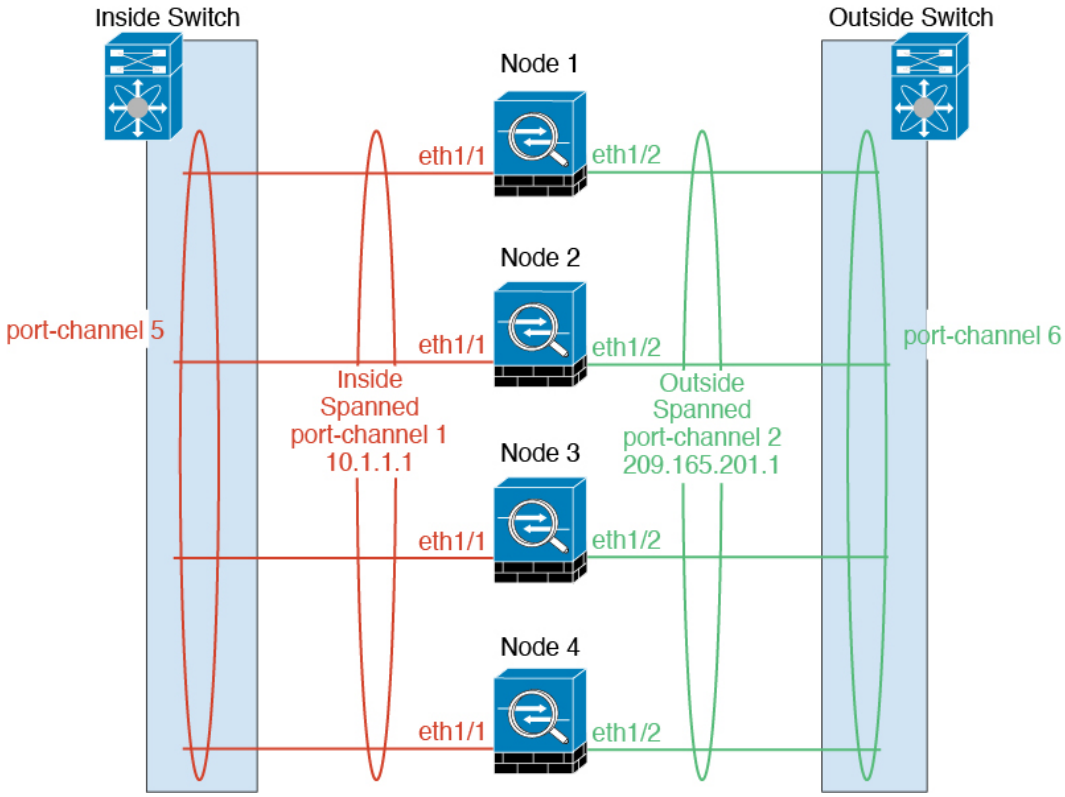
默认情况下，ASDM 连接将根据本地 IP 地址使用自签名证书。如果使用 ASDM 连接到主集群 IP 地址，则可能会因证书使用的是本地 IP 地址而不是主集群 IP 地址，系统会显示一则警告消息，指出 IP 地址不匹配。您可以忽略该消息并建立 ASDM 连接。但是，为了避免此类警告，您也可以注册一个包含主集群 IP 地址和 IP 地址池中所有本地 IP 地址的证书。然后，您可将此证书用于每个集群成员。有关详细信息，请参阅 https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html。

跨网络 EtherChannel（推荐）

您可以将每个机箱的一个或多个接口组成跨集群中所有机箱的 EtherChannel。EtherChannel 汇聚通道中所有可用活动接口上的流量。

在路由模式和透明防火墙模式下均可配置跨区以太网通道。在路由模式下，EtherChannel 配置为具有单个 IP 地址的路由接口。在透明模式下，IP 地址分配到 BVI 而非网桥组成员接口。

负载均衡属于 EtherChannel 固有的基本操作。



站点间集群

对于站点间安装，您只要遵循建议的准则即可充分发挥 ASA 集群的优势。

您可以将每个集群机箱配置为属于单独的站点 ID。

站点 ID 与站点特定的 MAC 地址和 IP 地址配合使用。集群发出的数据包使用站点特定的 MAC 地址和 IP 地址，而集群接收的数据包使用全局 MAC 地址和 IP 地址。此功能可防止交换机从两个不同端口上的两个站点获知相同全局 MAC 地址，导致 MAC 地址摆动；相反，它们仅获知站点 MAC 地址。只有使用跨区以太网通道的路由模式支持站点特定的 MAC 地址和 IP 地址。

站点 ID 还用于使用 LISP 检查、导向器本地化来实现流量移动，以提高性能、减少数据中心的站点间集群的往返时间延迟以及连接的站点冗余，其中流量流的备用所有者始终位于与所有者不同的站点上。

有关站点间集群的详细信息，请参阅以下各节：

- 调整数据中心互联的规模 - Firepower 4100/9300 机箱上的集群要求和前提条件， 第 433 页
- 站点间准则 - 集群准则和限制， 第 436 页
- 配置集群流移动性 -配置集群流移动性， 第 464 页
- 启用导向器本地化 - 启用导向器本地化， 第 462 页
- 启用站点冗余 - 启用导向器本地化， 第 462 页

Firepower 4100/9300 机箱上的集群要求和前提条件

每个模型的最大集群单位

- Firepower 4100 机箱 — 16 机箱
- Firepower 9300 — 16 个模块。例如，您可以在 16 个机箱中使用 1 个模块，或者在 8 个机箱中使用 2 个模块，也可以使用最多提供 16 个模块的任意组合。

机箱间集群的硬件和软件要求

集群中的所有机箱：

- 对于 Firepower 4100：所有机箱必须为同一型号。对于 Firepower 9300：所有安全模块必须为同一类型。例如，如果使用集群，则 Firepower 9300 中的所有模块都必须是 SM-40s。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。
- 除进行映像升级外，必须运行完全相同的 FXOS 和应用程序软件。不匹配的软件版本可能会导致性能不佳，因此请务必在同一维护窗口中升级所有节点。
- 对于分配给集群的接口，必须采用相同的接口配置，例如：相同的管理接口、EtherChannel、主用接口、速度和复用等。您可在机箱中使用不同的网络模块类型，但必须满足以下条件：对于相同接口 ID，容量必须匹配，且接口可成功捆绑于同一跨区以太网通道中。请注意，所有数据

接口必须是具有多个机箱的集群中的 EtherChannel。如果您要在启用集群（例如，通过添加或删除接口模块，或配置 Etherchannel）后更改 FXOS 中的接口，则请对每个机箱执行相同更改，从数据节点开始，到控制节点结束。请注意，如果您要删除 FXOS 中的接口，ASA 配置将保留相关命令，以便您可以进行任何必要的调整；从配置中删除接口可能具有广泛影响。您可以手动删除旧的接口配置。

- 必须使用同一台 NTP 服务器。请勿手动设置时间。
- ASA：每个 FXOS 机箱都必须注册到许可证颁发机构或卫星服务器。数据节点没有额外的成本。对于预留永久许可证，必须为每个机箱购买单独的许可证。对于威胁防御，所有许可由管理中心处理。

交换机要求

- 请务必先完成交换机配置并将机箱中的所有 EtherChannel 成功连接至交换机后，再在 Firepower 4100/9300 机箱 上配置集群。
- 有关受支持的交换机的特性，请参阅思科 FXOS 兼容性。

调整站点间集群的数据中心互联

您应在数据中心互联 (DCI) 上为集群控制链路流量保留等同于以下计算结果的带宽：

$$\frac{\#\text{ of cluster members per site}}{2} \times \text{cluster control link size per member}$$

如果各站点的成员数不同，请使用较大的数量进行计算。DCI 的最低带宽不得低于一个成员的集群控制链路的流量大小。

例如：

- 位于 4 个站点的 2 个成员：
  - 总共 4 个集群成员
  - 每个站点 2 个成员
  - 每个成员 5 Gbps 集群控制链路

  保留的 DCI 带宽 = 5 Gbps (2/2 x 5 Gbps)。
- 对位于 3 个站点的 6 个成员而言，规格加大：
  - 总共 6 个集群成员
  - 站点 1 有 3 个成员，站点 2 有 2 个成员，站点 3 有 1 个成员
  - 每个成员 10 Gbps 集群控制链路

  保留的 DCI 带宽 = 15 Gbps (3/2 x 10 Gbps)。
- 位于 2 个站点的 2 个成员：

- 总共 2 个集群成员
- 每个站点 1 个成员
- 每个成员 10 Gbps 集群控制链路

保留的 DCI 带宽 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps；但最低带宽不得低于集群控制链路的流量大小 (10 Gbps)）。

集群许可证 Firepower 4100/9300 机箱

智能软件管理器常规版和本地版

集群功能本身不需要任何许可证。要使用强加密和其他可选许可证，每个 Firepower 4100/9300 机箱都必须注册到许可证颁发机构或智能软件管理器常规版和本地版中。数据设备不会产生额外成本。

当您应用注册令牌时，对于符合条件的用户，系统会自动启用强加密许可证。使用令牌时，每个机箱必须具有相同的加密许可证。对于在 ASA 配置中启用的可选强加密 (3DES/AES) 功能许可证，请参阅下文。

在ASA许可证配置中，只能在控制设备上配置智能许可。该配置会复制到数据设备，但某些许可证不使用该配置；它仍处于缓存状态，只有控制设备才会请求许可证。这些许可证将聚合成一个由集群设备共享的集群许可证，此聚合许可证也会缓存在数据设备上，以便将来某个从属设备变为控制设备时使用。各个许可证类型将按以下方式进行管理：

- 基础 - 只有控制设备从服务器请求基础许可证，并且由于许可证汇聚，两个设备都可以使用标准许可证。
- 情景 - 只有控制设备从服务器请求情景许可证。默认情况下，基础许可证包括 10 个情景，并且位于所有集群成员上。每台设备的基础许可证的值加上控制设备上的情景许可证的值共同形成了聚合集群许可证中的平台限制。例如：
  - 集群中有 6 个 Firepower 9300 模块。基础许可证包括 10 个情景；对于 6 台设备，这些许可证相加之和为 60 个情景。您在控制设备上额外配置一个包含 20 个情景的许可证。因此，聚合的集群许可证包括 80 个情景。由于一个模块的平台限制为 250，因此聚合后的许可证最多允许 250 个情景；80 个情景没有超出此限制。因此，您可以在控制设备上配置最多 80 个情景；每台数据设备通过配置复制也将拥有 80 个情景。
  - 集群中有 3 台 Firepower 4112 设备。基础许可证包括 10 个情景；对于 3 台设备，这些许可证相加之和为 30 个情景。您在控制设备上额外配置一个包含 250 个情景的许可证。因此，聚合的集群许可证包括 280 个情景。由于一台设备的平台限制为 250，则聚合后的许可证最多允许 250 个情景；280 个情景超出了此限制。因此，您仅可以在控制设备上配置最多 250 个情景；每台数据设备通过配置复制也将拥有 250 个情景。在此情况下，只能将控制设备情景许可证配置为 220 个情景。
- 运营商 - 分布式站点间 VPN 所需。此许可证按设备进行授权，每台设备从服务器请求其自己的许可证。

- 强加密 (3DES) - 对于 2.3.0 前 Cisco Software Manager 本地部署；或如果您的智能账户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的账户。此许可证按设备进行授权，每台设备从服务器请求其自己的许可证。

如果选择了新的控制设备，新的控制设备继续使用聚合的许可证。它还会使用缓存的许可证配置再次请求控制设备许可证。当旧的控制设备作为数据设备重新加入集群后，它会释放控制设备许可证授权。在数据设备释放该许可证之前，如果帐户中没有可用的许可证，则控制设备的许可证可能处于一个非合规状态。保留的许可证的有效期为30天，但如果它在此宽限期过后仍处于非合规状态，您将无法对需要特殊许可证的功能进行配置更改；否则操作将不受影响。新的主用设备每12小时发送一次权利授权续约请求，直到许可证合规为止。在对许可证请求进行完整的处理之前，应避免进行配置更改。如果某台设备退出集群，缓存的控制配置将被删除，而按设备进行的授权将会保留。尤其是，您需要在非集群设备上重新请求情景许可证。

永久许可证预留

对于永久许可证预留，必须在配置集群之前为每个机箱单独购买许可证并启用。

集群准则和限制

集群的交换机

- 确保连接的交换机与集群数据接口和集群控制链路接口的 MTU 匹配。您应将集群控制链路接口 MTU 配置为比数据接口 MTU 至少高 100 字节，因此请确保适当配置集群控制链路连接的交换机。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销。此外，我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。
- 对于 Cisco IOS XR 系统，如果要设置非默认 MTU，请将 IOS XR 接口 MTU 设置为比集群设备 MTU 高 14 字节。除非使用 **mtu-ignore** 选项，否则 OSPF 邻近对等尝试可能会失败。请注意，集群设备 MTU 应与 IOS XR *IPv4* MTU 匹配。Cisco Catalyst 和 Cisco Nexus 交换机不需要进行这种调整。
- 在用于集群控制链路接口的交换机上，您可以选择在连接到集群设备的交换机端口上启用生成树 PortFast 来加快新设备加入集群的过程。
- 在交换机上，我们建议使用以下其中一种 EtherChannel 负载均衡算法：**source-dest-ip** 或 **source-dest-ip-port** （请参阅思科 Nexus OS 和思科 IOS-XE **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中的设备的流量分摊不均。请勿 更改集群设备上默认的负载均衡算法。
- 如果在交换机上更改 EtherChannel 的负载均衡算法，则交换机上的 EtherChannel 接口将暂时停止转发流量，生成树协议重新启动。在流量再次开始传输之前会存在延迟。
- 集群控制链路路径上的交换机不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。
- 端口通道绑定中断时间不得超过配置的 keepalive 间隔。

- 在 Supervisor 2T EtherChannel 上，默认的散列值分配算法是自适应算法。为了避免 VSS 设计中的非对称流量，请将连接到集群设备的端口通道上的散列算法更改为固定：

  router(config)# **port-channel** *id* **hash-distribution fixed**

  请勿全局更改算法；您可能需要对 VSS 对等链路使用自适应算法。

- 与 ASA 硬件集群不同，Firepower 4100/9300 集群支持 LACP 正常融合。因此， 对于平台， 您可以在连接的 Cisco Nexus 交换机上启用 LACP 正常融合。

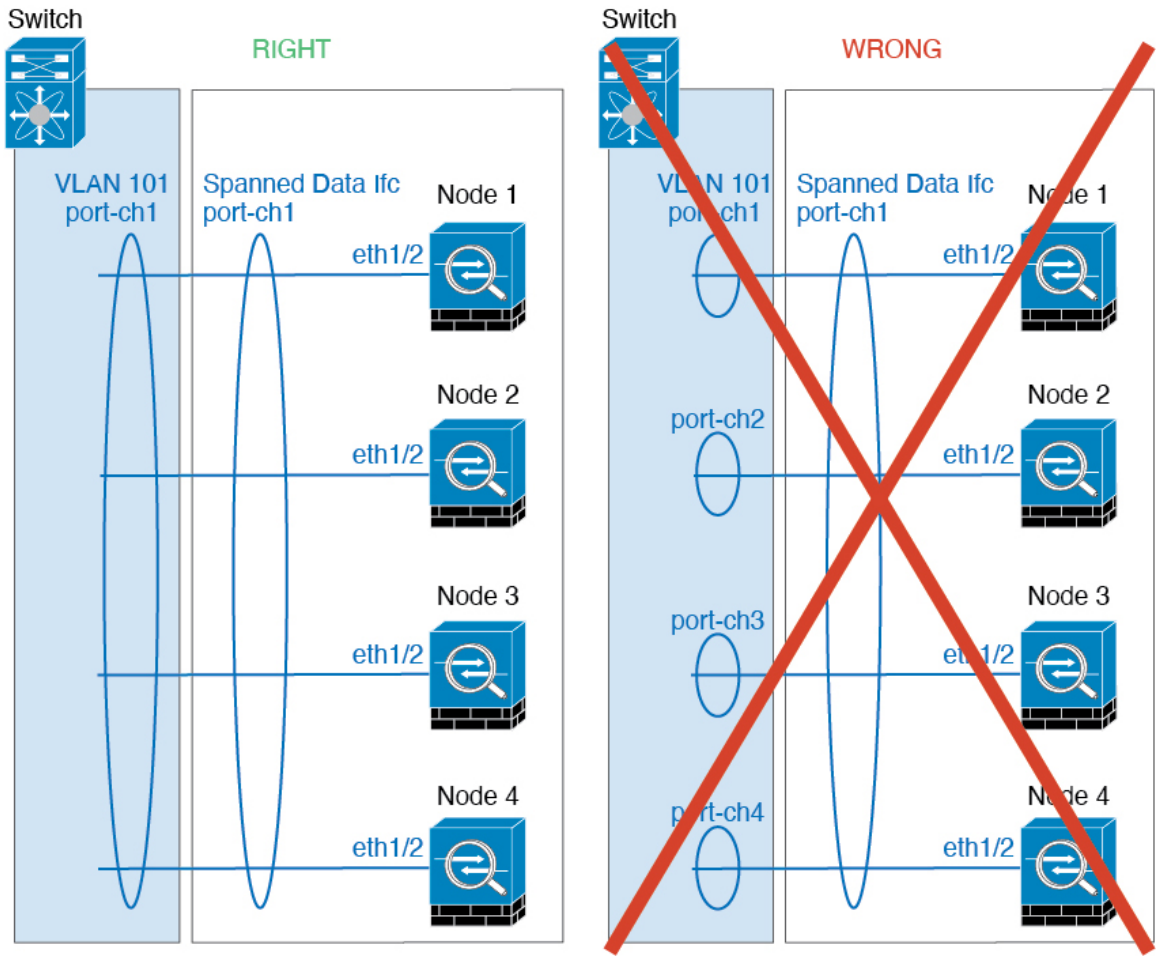
- 当发现交换机上跨区以太网通道的绑定速度缓慢时，可以对交换机上的单个接口启用快速 LACP 速率。默认情况下系统将 FXOS EtherChannel 的 LACP 速率设为快速。请注意，某些交换机（如 Nexus 系列）在执行服务中软件升级 (ISSU) 时不支持 LACP 速率“快速”，因此我们建议不要一起使用 ISSU 与集群。

集群的 EtherChannel

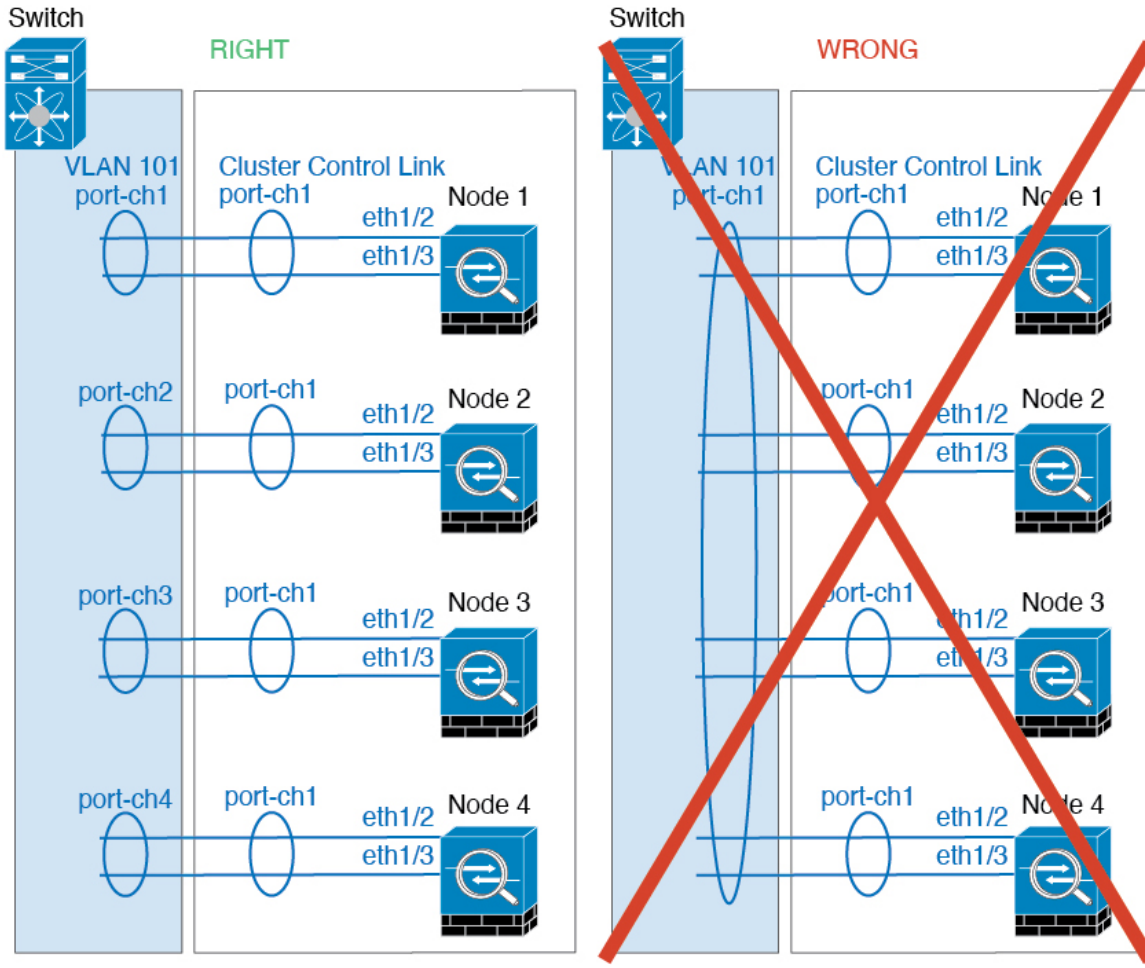
- 在低于 15.1(1)S2 的 Catalyst 3750-X 思科 IOS 软件版本中，此集群设备不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆栈连接集群设备 EtherChannel，则当控制设备交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。

- 跨网络与设备本地 EtherChannel 配置 - 请务必为跨区以太网通道和设备本地 EtherChannel 适当地配置交换机。

  - 跨区以太网通道 - 对于跨越所有集群成员的集群设备跨网络 EtherChannel，所有接口在交换机上合并为一个 EtherChannel。请确保每个接口都属于交换机上的同一个通道组。



- 设备本地 EtherChannel - 对于集群设备本地 EtherChannels，包括为集群控制链路配置的任何 EtherChannel，请务必在交换机上配置分散的 EtherChannel；请勿在交换机上将多个集群设备 EtherChannel 合并为一个 EtherChannel。



站点间集群

请参阅有关站点间集群的以下准则：

- 集群控制链路的延迟必须小于 20 微秒往返时间 (RTT)。
- 集群控制链路必须可靠，没有数据包无序或丢弃数据包的情况；例如，您应使用专用链路。
- 请勿配置连接再均衡；您不需要将连接再均衡到位于不同站点的集群成员。
- ASA 不会加密集群控制链路上转发的数据流量，因为它是专用链接，即使在数据中心互连 (DCI) 上使用也是如此。如果您使用重叠传输虚拟化 (OTV) 或将集群控制链路扩展到本地管理域外部，可以在边界路由器（例如基于 OTV 的 802.1AE MacSec）上配置加密。
- 对于传入连接而言，位于多个站点的成员之间的集群实施没有区别；因此，给定连接的连接角色可以跨越所有站点。这是预期行为。但是，如果您启用导向器本地化，系统将始终从连接所有者所在同一站点选择本地导向器角色（根据站点 ID）。此外，如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者（注意：如果不同站点间的流量非对称，且原始所

有者发生故障后远程站点继续发出流量，则远程站点节点可能成为新的所有者，但条件是该设备在重新托管期间接收到数据包。）。

- 对于导向器本地化，以下流量类型不支持本地化：NAT 或 PAT 流量；SCTP 检查的流量；分段所有者查询。
- 对于透明模式，如果集群布置于内部和外部路由器对之间（AKA 南北插入），您必须确保两个内部路由器共享一个 MAC 地址，两个外部路由器共享一个 MAC 地址。当位于站点 1 的集群成员将连接转发到位于站点 2 的成员时，目标 MAC 地址会被保留。如果该 MAC 地址与位于站点 1 的路由器相同，则数据包只会到达位于站点 2 的路由器。
- 对于透明模式，如果集群布置于每个站点上的数据网络和网关路由器之间，用作内部网络之间的防火墙（AKA 东西插入），则每个网关路由器都应使用 HSRP 等第一跳冗余协议 (FHRP) 在每个站点提供相同的虚拟 IP 和 MAC 地址目标。数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术扩展到多个站点。您需要创建过滤器，阻止发往本地网关路由器的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的网关路由器，则您需要删除所有过滤器，使流量能够成功到达另一站点的网关。
- 对于透明模式，如果集群连接到 HSRP 路由器，则必须在 ASA 上将路由器 HSRP MAC 地址添加为静态 MAC 地址表条目（请参阅 为网桥组添加静态 MAC 地址，第 909 页）。当邻接路由器使用 HSRP 时，发往 HSRP IP 地址的流量将发送到 HSRP MAC 地址，但返回流量将来自 HSRP 对中特定路由器接口的 MAC 地址。因此，ASA MAC 地址表通常仅在 HSRP IP 地址的 ASA ARP 表条目到期时更新，并且 ASA 发送 ARP 请求并接收应答。由于 ASA 的 ARP 表条目默认在 14400 秒后到期，但 MAC 地址表条目默认在 300 秒后到期，因此需要添加静态 MAC 地址条目来避免 MAC 地址表到期流量丢弃。
- 对于使用跨区以太网通道的路由模式，请配置站点特定的 MAC 地址。使用 OTV 或类似技术跨站点扩展数据 VLAN 。您需要创建过滤器，阻止发往全局 MAC 地址的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的集群，则您需要删除所有过滤器，使流量能够成功到达另一站点的集群节点。当站点间集群作为扩展网段的第一跳路由器时，不支持动态路由。

其他准则

- 当拓扑发生重大更改时（例如添加或删除 EtherChannel 接口、启用或禁用 Firepower 4100/9300 机箱 或交换机上的接口、添加额外的交换机形成 VSS、vPC、StackWise 或 StackWise Virtual），您应禁用运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有设备后，您可以重新启用运行状况检查功能。
- 将设备添加到现有集群时或重新加载设备时，会有限地暂时丢弃数据包/断开连接；这是预期行为。在某些情况下，丢弃的数据包可能会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包会使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 如果使用连接到跨区以太网通道接口的 Windows 2003 服务器，当系统日志服务器端口关闭且服务器未限制 ICMP 错误消息时，会有大量 ICMP 消息被发回集群。这些消息可能会导致集群的某些设备出现高 CPU 问题，从而可能影响性能。因此，我们建议您限制 ICMP 错误信息。
- 我们建议将 EtherChannel 连接到 VSS、vPC、StackWise 或 StackWise Virtual，以实现冗余。

- 在机箱内，您不能对某些安全模块进行集群，也不能在单机模式下运行其他安全模块；必须在集群内包含所有安全模块。

默认值

- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。
- 默认情况下，连接再均衡处于禁用状态。如果启用连接再均衡，交换负载信息的默认间隔时间为 5 秒。
- 出现故障的集群控制链路的集群自动重新加入功能设置为无限次尝试，每隔 5 分钟进行一次。
- 出现故障的数据接口的集群自动重新加入功能设置为尝试 3 次，每 5 分钟一次，递增间隔设置为 2。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

在 Firepower 4100/9300 机箱上配置集群

您可以从 Firepower 4100/9300 机箱管理引擎轻松部署集群。自动为每台设备生成所有初始配置。本节介绍可在 ASA 上执行的默认引导程序配置和可选定制。本节还将介绍如何从 ASA 中管理集群成员。您还可以通过 Firepower 4100/9300 机箱管理集群成员关系。有关详细信息，请参阅 Firepower 4100/9300 机箱文档。

过程

步骤 1 FXOS：添加 ASA 集群，第 441 页
步骤 2 ASA：配置防火墙模式和情景模式，第 452 页
步骤 3 ASA：配置数据接口，第 452 页
步骤 4 ASA：自定义集群配置，第 455 页
步骤 5 ASA：管理集群成员，第 476 页

FXOS：添加 ASA 集群

您可以将单个 Firepower 9300 机箱添加为机箱内集群，或添加多个机箱以实现机箱间集群。 对于机箱间集群，您必须单独配置每个机箱。在一个机箱上添加集群；然后，您可以在下一个机箱上输入基本相同的设置。

创建 ASA 集群

将范围设置为映像版本。

您可以从 Firepower 4100/9300 机箱管理引擎轻松部署集群。自动为每台设备生成所有初始配置。

对于多机箱集群，您必须单独配置每个机箱。在一个机箱上部署集群；然后，您可以将引导程序配置从第一个机箱复制到下一个机箱，实现轻松部署。

在 Firepower 9300 机箱中，必须对全部 3 个模块插槽）启用集群，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。

对于多情景模式，您必须先部署逻辑设备，然后在 ASA 应用中启用多情景模式。

在部署集群时，Firepower 4100/9300 机箱管理引擎将使用以下引导程序配置对每个 ASA 应用进行配置。以后如果需要，可以通过 ASA 修改引导程序配置的组成部分（以**粗体**文字显示）。

```
interface Port-channel48
   description Clustering Interface
cluster group <service_type_name>
   key <secret>
   local-unit unit-<chassis#-module#>
   site-id <number>
   cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
   priority <auto>
   health-check holdtime 3
   health-check data-interface auto-rejoin 3 5 2
   health-check cluster-interface auto-rejoin unlimited 5 1
   enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
   management-only individual
   nameif management
   security-level 0
   ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
   no shutdown

http server enable
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1
```

注释 如果禁用集群，则只能更改 **local-unit** 名称。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像上传至 Firepower 4100/9300 机箱。
- 收集以下信息：
  - 管理接口 ID、IP 地址和网络掩码
  - 网关 IP 地址

过程

步骤 1 配置接口。

a) 部署集群之前，至少添加一个“数据”类型接口或 EtherChannel（也称为端口通道）。请参阅添加 EtherChannel（端口通道），第 175 页或配置物理接口，第 173 页。

对于多机箱集群，所有数据接口必须为至少带有一个成员接口的跨区以太网通道。在每个机箱上添加同一 EtherChannel。将所有集群设备上的成员接口合并到交换机上的单个 EtherChannel 中。有关 EtherChannel 的详细信息，请参阅集群准则和限制，第 436 页。

b) 添加“管理”类型接口或 EtherChannel。请参阅添加 EtherChannel（端口通道），第 175 页或配置物理接口，第 173 页。

管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理接口不同（在 FXOS 中，您可能会看到机箱管理接口显示为 MGMT、management0 或其他类似名称）。

对于多机箱集群，在各机箱上添加相同的管理接口。

c) 对于多机箱集群，将成员接口添加到集群控制链路 EtherChannel（默认情况下为端口通道 48）。请参阅 添加 EtherChannel（端口通道），第 175 页。

请勿为与一个 Firepower 9300 机箱内的安全模块隔离的集群添加成员接口。例如，如果添加成员，则机箱假设此集群将使用多机箱，且将仅允许您使用跨区以太网通道。

在各机箱上添加相同的成员接口。　集群控制链路是每个机箱上的设备本地 EtherChannel。在交换机上对每个设备使用单独的 Etherchannel。有关 EtherChannel 的详细信息，请参阅集群准则和限制，第 436 页。

步骤 2 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 3 设置应用实例参数，包括映像版本。

a) 查看可用映像。请注意您想要使用的版本号。

show app

示例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

```
        ftd         6.3.0           cisco       Native,Container        Application Yes
```

b) 将范围设置为映像版本。

scope app asa *application_version*

示例：

```
Firepower /ssa # scope app asa 9.10.1
Firepower /ssa/app #
```

c) 将此版本设置为默认版本。

set-default

示例：

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

d) 退出到 ssa 模式。

exit

示例：

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

示例：

```
Firepower /ssa # scope app asa 9.12.1
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #
```

步骤 4 创建集群。

enter logical-device *device_name* **asa** *slots* **clustered**

- *Device_name* - 由 Firepower 4100/9300 机箱管理引擎用于配置集群设置以及分配接口；它不是在安全模块配置中使用的集群名称。必须指定全部三个安全模块，即使尚未安装硬件也是如此。
- *slots* - 将机箱模块分配给集群。对于 Firepower 4100，指定 **1**。对于 Firepower 9300，指定 **1,2,3**。您必须启用对 Firepower 9300 机箱中全部 3 个模块插槽的启用集群，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。

示例：

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

步骤 5 配置集群引导程序参数。

这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

a) 创建集群引导程序对象。

enter cluster-bootstrap

示例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

b) 设置机箱 ID。

set chassis-id *id*

集群中的每个机箱都需要唯一 ID。

c) 对于站点间集群，请将站点 ID 设置为 1 到 8 之间的值。

set site-id *number*。

要删除站点 ID，请将值设为 **0**。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

d) 为集群控制链路上的控制流量配置身份验证密钥。

set key

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

系统将提示您输入共享密钥。

共享密钥是长度介于 1 和 63 个字符之间的 ASCII 字符串。共享密钥用于生成密钥。此选项不影响数据路径流量，包括连接状态更新和转发的数据包，它们始终以明文发送。

e) 设置集群接口模式。

set mode spanned-etherchannel

跨区以太网通道模式是唯一支持的模式。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

f) 在安全模块配置中设置集群组名称。

set service-type *cluster_name*

名称必须是长度为 1 到 38 个字符的 ASCII 字符串。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

g) （可选） 设置　集群控制链路 IP 网络。

set cluster-control-link network ***a.b*.0.0**

默认情况下，　集群控制链路使用 127.2.0.0/16 网络。但是，某些网络部署不允许 127.2.0.0/16 流量通过。在这种情况下，您可以对集群指定唯一网络上的 /16 地址。

- ***a.b*.0.0** - 指定任意 /16 网络地址，环回 (127.0.0.0/8) 和组播 (224.0.0.0/4) 地址除外。如果将该值设置为 0.0.0.0，则使用默认网络：127.2.0.0。

机箱会根据机箱 ID 和插槽 ID 自动生成每台设备的集群控制链路接口 IP 地址：*a.b.chassis_id.slot_id*。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
10.10.0.0
```

h) 配置管理 IP 地址信息。

此信息用于配置安全模块配置中的管理接口。

1. 配置本地 IP 地址池，其中一个地址将被分配到接口的每个集群设备。

   set ipv4 pool *start_ip end_ip*

   set ipv6 pool *start_ip end_ip*

   至少包含与集群中的设备数量相同的地址。请注意，对于 Firepower 9300，每台机箱必须包括 3 个地址，即使未填满所有模块插槽。如果计划扩展集群，则应包含更多地址。属于当前控制设备的虚拟 IP 地址（称作“主集群 IP 地址”）不在此地址池中；请务必在同一个网络中为主集群 IP 地址保留一个 IP 地址。您可以使用 IPv4 和/或 IPv6 地址。

2. 为管理接口配置主集群 IP 地址。

   set virtual ipv4 *ip_address* **mask** *mask*

   set virtual ipv6 *ip_address* **prefix-length** *prefix*

   此 IP 地址必须与集群池地址属于同一个网络，但不在地址池中。

3. 输入网络网关地址。

   set ipv4 gateway *ip_address*

   set ipv6 gateway *ip_address*

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11 2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

i) 退出集群引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
  Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

步骤 6 配置管理引导程序参数。

这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

a) 创建管理引导程序对象。

enter mgmt-bootstrap asa

示例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 指定管理员并启用密码。

create bootstrap-key-secret PASSWORD

set value

输入值： 密码

确认值： 密码

exit

示例：

预配置的 ASA 管理员用户和启用密码在进行密码恢复时非常有用；如果您有 FXOS 访问权限，在您忘记了管理员用户密码时，可以将其重置。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 指定防火墙模式：路由或透明。

create bootstrap-key FIREWALL_MODE

set value {**routed** |**transparent**}

exit

在路由模式中，设备被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第2层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 退出管理引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

步骤 7 保存配置。

commit-buffer

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。使用 **show app-instance** 命令检查部署状态。当**管理状态**为**已启用**且**运行状态**为**在线**时，应用实例正在运行且可供使用。

示例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ --------------- ------------
ftd        cluster1   1          Enabled     Online           7.3.0.49        7.3.0.49
    Native                   In Cluster      Data Node
ftd        cluster1   2          Enabled     Online           7.3.0.49        7.3.0.49
```

```
    Native                   In Cluster      Control Node
ftd         cluster1   3         Disabled    Not Available                  7.3.0.49
    Native                   Not Applicable  None
```

步骤 8 要向集群添加其他机箱，请重复此程序，但必须配置唯一的 **chassis-id** 和正确的 **site-id**；否则，请对两个机箱使用同一配置。

请确保新机箱上的接口配置相同。您可以导出和导入 FXOS 机箱配置以简化此过程。

步骤 9 连接到控制设备 ASA 以自定义集群配置。

示例

对于机箱 1：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      enter member-port Ethernet1/1
        exit
      enter member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      enter member-port Ethernet1/3
        exit
      enter member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type data
      enable
      enter member-port Ethernet1/5
        exit
      enter member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      enter member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer
```

```
scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.27
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::27
      set key
      Key: f@arscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

对于机箱 2：

```
scope eth-uplink
  scope fabric a
    create port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    create port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    create port-channel 3
      set port-type data
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    create port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      create member-port Ethernet2/2
        exit
      exit
    create port-channel 48
      set port-type cluster
      enable
      create member-port Ethernet2/3
```

```
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.15
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::19
      set key
      Key: f@rscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

添加更多集群成员

添加或替换 ASA 集群成员。

注释 此程序仅适用于添加或替换机箱；如果将模块添加或替换到已启用集群的Firepower 9300，则该模块将自动添加。

开始之前

- 确保现有集群在此新成员的管理 IP 地址池中有足够的 IP 地址。如果没有，您需要在每个机箱上编辑现有集群引导程序配置，然后才可添加此新成员。此更改将导致重新启动逻辑设备。
- 新机箱上的接口配置必须相同。您可以导出和导入 FXOS 机箱配置以简化此过程。
- 对于多情景模式，在第一个集群成员上的ASA应用中启用多情景模式；其他集群成员将自动继承多情景模式配置。

过程

步骤 1 确定。

步骤 2 要向集群添加其他机箱，请在创建 ASA 集群，第 441 页中重复此程序，但必须配置唯一的 **chassis-id** 和正确的 **site-id**； 否则，请对两个机箱使用同一配置。

ASA：配置防火墙模式和情景模式

默认情况下，FXOS 机箱在路由防火墙模式和单情景模式下部署集群。

- 更改防火墙模式 - 要在部署后更改模式，请更改控制设备上的模式；数据设备上的模式将自动更改以实现匹配。请参阅设置防火墙模式，第 198 页。在多情景模式下，应逐个情景设置防火墙模式。
- 更改为多情景模式 - 要在部署后更改为多情景模式，请更改控制设备上的模式；数据设备上的模式将自动更改以实现匹配。请参阅启用多情景模式，第 228 页。

ASA：配置数据接口

此程序配置您在 FXOS 中部署集群时为其分配的每个数据接口的基本参数。对于多机箱集群，数据接口始终是跨区以太网通道接口。

注释 管理接口在您部署集群时预先配置。您还可以在ASA中更改管理接口参数，但此程序侧重于数据接口。管理接口是一个单独的接口，而不是跨网络接口。有关详细信息，请参阅管理接口，第431页。

开始之前

- 对于多情景模式，请在系统执行空间中开始本程序。如果尚未进入系统配置模式，请输入**changeto system** 命令。
- 对于透明模式，请配置网桥组。请参阅配置网桥虚拟接口 (BVI)，第 757 页。
- 在将跨区以太网通道用于具有多机箱的集群时，端口通道接口在集群完全启用之前不会进入工作状态。此要求可防止将流量转发到集群中并非处于活动状态的节点。

过程

步骤 1 指定接口 ID。

interface *id*

有关分配给此集群的接口，请参考 FXOS 机箱。接口 ID 可以是：

- **port-channel** *integer*
- **ethernet** *slot/port*

示例：

```
ciscoasa(config)# interface port-channel 1
```

步骤 2 启用接口：

no shutdown

步骤 3 （可选）如果准备在此接口上创建 VLAN 子接口，请立即执行此操作。

示例：

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

本程序的其余部分适用于子接口。

步骤 4 （多情景模式下）将接口分配到情景，然后使用 changeto 命令进入情景和接口模式。

示例：

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

对于多情景模式，其余的接口配置将在每个情景中完成。

步骤 5 为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。

步骤 6 根据防火墙模式，执行以下其中一项操作。

- 路由模式 - 设置 IPv4 和/或 IPv6 地址：

  (IPv4)

  ip address *ip_address* [*mask*]

  (IPv6)

  ipv6 address *ipv6-prefix*/*prefix-length*

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
  ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
  ```

不支持 DHCP、PPPoE 和 IPv6 自动配置。对于点对点连接，可以指定 31 位子网掩码 (255.255.255.254)。在此情况下，不会为网络或广播地址保留 IP 地址。也不支持手动配置链路本地地址。

- 透明模式 - 将接口分配到网桥组：

  bridge-group *number*

  示例：

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  number 为 1 到 100 之间的整数。最多可将 64 个接口分配到网桥组。您不能将同一接口分配至多个网桥组。请注意，BVI 配置包含 IP 地址。

步骤 7 设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 为 0（最低）到 100（最高）之间的整数。

步骤 8 （多机箱集群）为跨区以太网通道配置全局 MAC 地址，以避免潜在的网络连接问题。

mac-address *mac_address*

- *Mac_address* - 采用 H.H.H 格式的 MAC 地址，其中 H 是 16 位十六进制数字。例如， MAC 地址 00-0C-F1-42-4C-DE 以 000C.F142.4CDE 的形式输入。如果您还要使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。

如果是手动配置的 MAC 地址，该 MAC 地址将始终属于当前的控制设备。如果不配置 MAC 地址，则如果控制设备发生更改，新的控制设备会将新的 MAC 地址用于该接口，而这可能导致临时网络故障。

在多情景模式下，如果您在情景之间共享接口，则应改为启用自动生成 MAC 地址，这样就无需手动设置 MAC 地址。请注意，您必须使用此命令为非共享 接口手动配置 MAC 地址。

示例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

步骤 9 （站点间集群）为每个站点配置一个站点特定的 MAC 地址和 IP 地址（对于路由模式）：

mac-address *mac_address* **site-id** *number* **site-ip** *ip_address*

示例：

```
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.9.9.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.9.9.2
```

```
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.9.9.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.9.9.4
```

站点特定的 IP 地址必须与全局 IP 地址位于同一子网。供设备使用的站点特定的 MAC 地址和 IP 地址取决于您在每台设备的引导程序配置中指定的站点 ID。

ASA：自定义集群配置

如果您在部署集群或配置其他选项（例如集群运行状况监控、TCP 连接复制延迟、流移动性和其他优化）后想要更改引导程序设置，您可以在控制设备上执行此操作。

配置基本 ASA 集群参数

您可以在控制节点上自定义集群设置。

开始之前

- 对于多情景模式，请在控制单元的系统执行空间中完成本程序。要从情景更改到系统执行空间，请输入 **changeto system** 命令。
- 本地设备 name 和多个其他选项只能在 FXOS 机箱上设置，或者只能在禁用集群的情况下才能在 ASA 上进行更改，因此以下程序未包括这些选项。

过程

步骤 1 确认此设备是控制单元：

show cluster info

示例：

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state CONTROL_NODE
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state DATA_NODE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
```

```
    Last join : 20:29:57 UTC Nov 4 2015
    Last leave: 20:24:55 UTC Nov 4 2015
Unit "unit-1-1" in state DATA_NODE
    ID        : 1
    Version   : 9.5(2)
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.1.1
    CCL MAC   : 0015.c500.017f
    Last join : 20:20:53 UTC Nov 4 2015
    Last leave: 20:18:15 UTC Nov 4 2015
Unit "unit-2-1" in state DATA_NODE
    ID        : 3
    Version   : 9.5(2)
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.2.1
    CCL MAC   : 0015.c500.020f
    Last join : 20:19:57 UTC Nov 4 2015
    Last leave: 20:24:55 UTC Nov 4 2015
```

如果其他设备才是控制设备，请退出当前连接，并连接到正确的设备。

步骤 2 指定集群控制链路接口的最大传输单位至少比数据接口的最高 MTU 高 100 字节。

mtu cluster 字节

示例：

```
ciscoasa(config)# mtu cluster 9184
```

我们建议将 MTU 设置为最大；最小值为 1400 个字节。此外，我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销。例如，由于最大 MTU 为 9184，因此最高的数据接口 MTU 可以是 9084，而集群控制链路则可以设置为 9184。

步骤 3 进入集群配置模式：

cluster group *name*

步骤 4 （可选） 启用数据单元到控制单元的控制台复制：

console-replicate

默认情况下会禁用此功能。对于特定的重要事件，ASA 可将某些消息直接打印输出到控制台。如果启用了控制台复制，数据设备会将控制台消息发送到控制设备，因此您只需要监控集群的一个控制台端口。

步骤 5 设置集群事件的最低跟踪级别：

trace-level 级别

根据需要设置最低级别：

- **critical** - 重要事件（严重性=1）
- **warning** - 警告（严重性 = 2）

- **informational** - 信息事件（严重性=3）
- **debug** - 调试事件（严重性=4）

步骤 6 （可选）（仅限 Firepower 9300）确保机箱中的安全模块同时加入集群，以便在模块之间均匀分配流量。如果某个模块先于其他模块很早加入，它可能会收到超过所需的流量，因为其他模块还无法分担负载。

unit parallel-join *num_of_units* **max-bundle-delay** *max_delay_time*

- *num_of_units*- - 指定在模块可加入集群之前同一机箱中需要就绪的最小模块数（介于 1 到 3 之间）。默认值为 1，这意味着模块在加入集群之前不会等待其他模块准备就绪。例如，如果将值设置为 3，则每个模块将会等待 *max_delay_time* 或者直到全部 3 个模块都就绪后才加入集群。所有 3 个模块将大致同时请求加入集群，并几乎同时开始接收流量。
- *max_delay_time* - 指定在某个模块停止等待其他模块就绪后才加入集群之前的最大延迟时间（以秒为单位），范围介于 0 到 30 分钟之间。默认值为 0，这意味着模块在加入集群之前不会等待其他模块准备就绪。如果将 *num_of_units* 设置为 1，则该值必须为 0。如果将 *num_of_units* 设置为 2 或 3，则该值必须为 1 或更大值。此计时器按模块执行，但当第一个模块加入集群时，则所有其他模块计时器将会结束，并且其余模块也会加入集群。

例如，您将 *num_of_units* 设置为 3，并将 *max_delay_time* 设置为 5 分钟。当模块 1 启动时，会开始其 5 分钟计时器。模块 2 在 2 分钟后启动，并启动其 5 分钟计时器。模块 3 在 1 分钟后启动，因此所有模块现在将在 4 分钟时加入集群；它们不会等待计时器完成。如果模块 3 一直没有启动，则模块 1 将在 5 分钟计时器结束时加入集群，模块 2 也会加入，尽管其计时器还剩余 2 分钟；它不会等待其计时器完成。

步骤 7 配置最大集群成员数。

cluster-member-limit 编号

- *number* - 2 到 16。默认值为 16。

如果您明确知道集群中的设备数少于最大设备数（即 16 台），建议您设置实际计划的设备数。设置最大单位可让集群更好地管理资源。例如，如果您使用端口地址翻译 (PAT)，则控制设备可以将端口块分配给计划的成员数，并且不必为您不打算使用的额外设备预留端口。

步骤 8 设置从流所有者到导向器和备份所有者的流状态刷新消息（clu_keepalive 和 clu_update 消息）的保持连接间隔。

clu-keepalive-interval 秒

- 秒 - 15 到 55。默认值为 15。

您可能想将间隔设置为比默认值更长的时间，以减少集群控制链路上的流量。

配置运行状态监控并自动重新加入设置

此程序可以配置设备和接口运行状态监控。

您可能想禁用不重要的接口（例如管理接口）的运行状况检查。您可以监控任何端口通道ID或单一物理接口ID。运行状况监控不在VLAN子接口或虚拟接口（例如，VNI或BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 进入集群配置模式：

cluster group *name*

步骤 2 自定义集群设备运行状态检查功能：

health-check [**holdtime** *timeout*]

holdime 用于确定两次设备 heartbeat 状态消息之间的时间间隔，其值介于 0.3 到 45 秒；默认值为 3 秒。

为了确定设备运行状况，ASA 集群设备会在集群控制链路上将 heartbeat 消息发送到其他设备。如果设备在保持期内未接收到来自对等设备的任何heartbeat消息，则对等设备被视为无响应或无法工作。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用 ASA、Firepower 4100/9300 机箱 或交换机上的接口、或者添加额外的交换机形成 VSS、vPC、StackWise 或 StackWise Virtual），您应禁用运行状态检查功能 (**no health-check monitor-interface**)，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有设备后，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

步骤 3 在接口上禁用接口运行状态检查：

no health-check monitor-interface [*interface_id* | **service-application**]

接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定设备上发生故障，但在其他设备上的同一逻辑接口下仍有活动端口，则会从集群中删除该设备。ASA 在多长时间后从集群中删除成员取决于接口的类型以及该设备是既定成员还是正在加入集群的设备。

默认情况下，为所有接口启用运行状况检查。您可以使用此命令的**no**形式逐个接口将其禁用。您可能想禁用不重要的接口（例如管理接口）的运行状况检查。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。指定 **service-application** 以禁用对修饰器应用程序的监控。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用 ASA、Firepower 4100/9300 机箱 或交换机上的接口、或者添加额外的交换机形成 VSS、vPC、StackWise 或 StackWise Virtual），您应禁用运行状态检查功能 (**no health-check**)，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有设备后，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface port-channel1
```

步骤 4 自定义在运行状态检查发生故障后的自动重新加入集群设置：

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**- 指定内部错误的自动重新加入设置。内部故障包括：应用程序同步超时、不一致的应用程序状态等。
- **unlimited** —（**cluster-interface** 的默认值）不限制重新加入尝试的次数。
- *auto-rejoin-max* — 设置重新加入尝试次数，介于 0 和 65535 之间。**0** 禁用自动重新加入。**data-interface** 和 **system** 的默认值为 3。
- *auto_rejoin_interval* - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。设备尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- *Auto_rejoin_interval_variation* - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。对于集群接口，默认值为 **1**；对于数据接口和系统，默认值为 **2**。

示例：

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

步骤 5 设置机箱重新加入，以匹配机箱心跳故障的 **health-check system auto-rejoin** 命令。

health-check chassis-heartbeat-delay-rejoin

默认情况下，如果机箱心跳失败然后恢复，则节点会立即重新加入集群。但是，如果配置 **health-check chassis-heartbeat-delay-rejoin** 命令，则它将根据 **health-check system auto-rejoin** 命令的设置重新加入。

步骤 6 配置 ASA 将接口视为发生故障并将设备从集群中删除之前经过的防反跳时间。

health-check monitor-interface debounce-time *ms*

将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，ASA 会等待指定的毫秒数，然后才将接口标记为发生故障，并将设备从集群中删除。 对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群上的接口仅仅因为另一个集群设备在绑定端口时的速度更快便显示为故障状态。

示例：

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

步骤 7 配置机箱运行状况检查间隔：

app-agent heartbeat [**interval** *ms*] [**retry-count** *number*]

- **interval** *ms* - 设置检测信号之间的时间量，介于 100 和 6000 毫秒之间（100 的倍数）。默认值为 1000 毫秒。
- **retry-count** *Number* - 设置重试次数，介于 1 和 30 之间。默认值为 3 次重试。

ASA 将会检查其能否通过背板与主机机箱通信。

最小组合时间（间隔x重试计数）不能小于 600 毫秒。例如，如果将时间间隔设置为 100，将重试次数设置为 3，则总合并时间为 300 毫秒，这是不受支持的。例如，您可以将间隔设置为 100，将重试计数设置为 6 以满足最短时间（600 毫秒）。

示例：

```
ciscoasa(cfg-cluster)# app-agent heartbeat interval 1000 retry-count 10
```

步骤 8 （可选） 配置流量负载监控。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds* — 设置监控消息之间的时间（以秒为单位），范围介于 10 到 360 秒之间。默认值为 20 秒。
- **intervals** *intervals* — 设置 ASA 维护数据的间隔的数量，该值介于 1 到 60 之间。默认值为 30。

您可以监控集群成员的流量负载，包括总连接计数、CPU 和内存使用情况以及缓冲区丢弃。如果负载过高，且剩余的设备可以处理负载，您可以选择在设备上手动禁用集群，或调整外部交换机上的负载均衡。默认情况下启用此功能。例如，对于每个机箱中具有 3 个安全模块的 Firepower 9300 上的机箱间集群，如果机箱中的 2 个安全模块离开集群，则与该机箱的相同数量的流量将被发送到剩余的模块，并可能压垮它。您可以定期监控流量负载。如果负载过高，您可以选择手动禁用设备上的集群。

使用 **show cluster info load-monitor** 命令查看流量负载。

示例：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
Average from last 25 interval:
   0           0            0            12             28
   1           0            0            13             27
```

配置连接再均衡和集群 TCP 复制延迟

可以配置连接再均衡。 您可以为 TCP 连接启用集群复制中继，以延迟导向器/备份流的创建，从而帮助消除与短期流量相关的“不必要的工作”。请注意，如果某个设备在创建导向器/备份数据流前出现故障，则无法恢复这些数据流。同样，如果流量在创建数据流前再均衡到其他设备，则无法恢复该数据流。您不应为禁用了 TCP 随机化的流量启用 TCP 复制中继。

过程

步骤 1 进入集群配置模式：

cluster group *name*

步骤 2 （可选）为 TCP 流量启用连接再均衡：

conn-rebalance [**frequency** *seconds*]

示例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

此命令默认禁用。如果启用，ASA 会定期交换有关每秒连接数的信息，并将新连接从每秒连接数较多的设备分流到负载较低的设备。现有连接永远不会移动。此外，由于此命令仅基于每秒的连接数进行重新平衡，因此不会考虑每个节点上已建立的连接总数，并且连接总数可能并不相等。此频率的值为 1 到 360 秒，用于指定多长时间交换一次负载信息。默认值为 5 秒。

将连接分流到其他节点后，它将成为不对称连接。

请勿为站点间拓扑结构配置连接再均衡；您不需要将新的连接再均衡到位于不同站点的集群成员。

步骤 3 为 TCP 连接启用集群复制延迟：

cluster replication delay *seconds* { **http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] { **host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

示例：

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

将 *seconds* 设置为介于 1 到 15 之间的值。默认启用 **http** 延迟，时间为 5 秒。

配置站点间功能

对于站点间集群，您可以自定义配置，以提高冗余性和稳定性。

启用导向器本地化

为了提高性能并缩短数据中心的站点间集群的往返时间延迟，您可以启用导向器本地化。新的连接通常实现了负载均衡，并且由特定站点中的集群成员拥有。但是，ASA会向任意站点的成员分配导向器角色。导向器本地化支持其他导向器角色：与所有者同一站点的本地导向器和可位于任意站点的全局导向器。将所有者和导向器保留在同一站点可以提高性能。此外，如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者。当集群成员收到属于其他站点的连接的数据包时，使用全局导向器。

开始之前

- 在Firepower 4100/9300 机箱管理引擎上设置机箱的站点 ID。
- 以下流量类型不支持本地化：NAT 或 PAT 流量；SCTP 检查的流量；分段所有者查询。

过程

步骤 1 进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 启用导向器本地化：

director-localization

启用站点冗余

为保护流量免受站点故障的影响，您可以启用站点冗余。如果连接的备份所有者与所有者位于同一站点，则将从另一个站点选择一个额外的备份所有者来保护流量免受站点故障的影响。

开始之前

- 在Firepower 4100/9300 机箱管理引擎上设置机箱的站点 ID。

过程

步骤 1 进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 启用站点冗余。

site-redundancy

配置每站点免费 ARP

ASA 可以生成免费 ARP (GARP) 数据包，以确保交换基础设施始终处于最新状态：它将作为每个站点优先级最高的成员，定期生成流向全局 MAC/IP 地址的 GARP 流量。

当使用来自集群的各站点 MAC 和 IP 地址数据包使用站点特定的 MAC 地址和 IP 地址时，集群接收的数据包使用全局 MAC 地址和 IP 地址。如果流量不是定期从全局 MAC 地址生成的，您的全局 MAC 地址交换机上可能会出现 MAC 地址超时。发生超时后，以全局 MAC 地址为目标的流量将在整个交换基础设施中进行泛洪，这有可能造成性能和安全问题。

当您为每台设备设置站点 ID 和为每个跨区以太网通道设置站点 MAC 地址时，默认情况下会启用 GARP。您可以自定义 GARP 间隔，也可以禁用 GARP。

开始之前

- 在引导程序配置中为集群成员设置站点 ID。
- 在控制设备配置中为跨区以太网通道设置每站点 MAC 地址。

过程

步骤 1 进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 自定义 GARP 间隔。

site-periodic-garp interval 秒

- *seconds* — 设置 GARP 生成之间的时间（以秒为单位），介于 1 到 1000000 秒之间。默认值为 290 秒。

要禁用 GARP，请输入 **no site-periodic-garp interval**。

示例：

```
ciscoasa(cfg-cluster)# site-periodic-garp interval 500
```

配置集群流移动性

当服务器在站点之间移动时，您可以检查 LISP 流量以启用流移动性。

关于 *LISP* 检测

可以检查 LISP 流量，以便在站点间启用流移动性。

关于 LISP

利用数据中心的虚拟机移动性（例如，VMware VMotion），服务器可以在数据中心之间迁移，同时维持与客户端的连接。为了支持此类数据中心服务器移动性，路由器需要能够在服务器移动时更新通往服务器的入口路由。思科定位/ID 分离协议 (LISP) 架构将设备身份或终端标识符 (EID) 与设备位置或路由定位符 (RLOC) 分离开，并分隔到两个不同的编号空间，实现服务器迁移对客户端的透明化。例如，当服务器迁移到新的站点并且客户端向服务器发送流量时，路由器会将流量重定向到新位置。

LISP 需要充当特定角色的路由器和服务器，例如 LISP 出口隧道路由器 (ETR)、入口隧道路由器 (ITR)、第一跳路由器、映射解析器 (MR) 和映射服务器 (MS)。当服务器的第一跳路由器检测到服务器连接了其他路由器时，它会更新所有其他路由器和数据库，以便连接到客户端的 ITR 可以拦截、封装流量并将流量发送到新的服务器位置。

Cisco Secure Firewall ASA LISP 支持

ASA 本身不运行 LISP；但是，它可以通过检查 LISP 流量确定位置更改，然后使用此信息进行无缝集群操作。如果不使用 LISP 集成，当服务器移动到新站点时，流量将到达位于新站点的 ASA 集群成员，而不是原始的流所有者。新 ASA将流量转发到旧站点的 ASA，然后旧 ASA必须将流量发回新站点，才能到达服务器。此类流量流并未处于最佳状态，称为“长号”或“发夹”。

如果使用 LISP 集成，ASA 集群成员可以检查第一跳路由器与 ETR 或 ITR 之间的 LISP 流量，然后将流所有者位置更改为新站点。

LISP 准则

- ASA 集群成员必须位于第一跳路由器和该站点的 ITR 或 ETR 之间。ASA 集群本身不能作为扩展网段的第一跳路由器。
- 仅支持全分布数据流；集中数据流、半分布数据流或属于单个节点的数据流不会移动到新的所有者。半分布数据流包括应用（例如 SIP），其中作为父数据流所有者的同一 ASA 拥有所有子数据流。
- 集群仅移动第 3 和第 4 层流状态；一些应用数据可能丢失。
- 对于持续时间极短的数据流或非关键业务数据流，移动所有者可能并非最佳选择。在配置检查策略时，您可以控制该功能支持的流量类型，并应只对必要流量限制流移动性。

ASA LISP 实施

此功能包含多种相互关联的配置（本章将逐一说明）：

1. （可选）基于主机或服务器 IP 地址限制检查的 EID - 第一跳路由器可能会向与 ASA 集群无关的主机或网络发送 EID 通知消息，因此，您可以限制只向与您的集群有关的服务器或网络发送 EID。例如，如果集群仅涉及 2 个站点，但是 LISP 在 3 个站点上运行，应只包括集群涉及的 2 个站点的 EID。
2. LISP 流量检查 - ASA 检查 UDP 端口 4342 上的 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个将 EID 和站点 ID 相关联的 EID 表。例如，您应检查包含第一跳路由器源 IP 地址以及 ITR 或 ETR 目标地址的 LISP 流量。请注意，没有为 LISP 流量分配导向器，并且 LISP 流量本身不参与集群状态共享。
3. 用于启用指定流量的流移动性的服务策略 - 您应对关键业务流量启用流移动性。例如，您可以只对 HTTPS 流量和/或发送到特定服务器的流量启用流移动性。
4. 站点 ID - ASA 使用集群中每个节点的站点 ID 确定新的所有者。
5. 用于启用流移动性的集群级别配置 - 您还必须在集群级别启用流移动性。此开/关切换器允许您轻松地启用或禁用特定流量类或应用类的流移动性。

配置 *LISP* 检测

当服务器在站点之间移动时，您可以检查 LISP 流量以启用流移动性。

开始之前

- 在 Firepower 4100/9300 机箱管理引擎上设置机箱的站点 ID。
- LISP 流量未包含在 default-inspection-traffic 类中，因此，您在此过程中必须为 LISP 流量配置单独的类。

过程

步骤 1 （可选） 配置 LISP 检测映射以根据 IP 地址限制检测的 EID，并配置 LISP 预共享密钥：

a) 创建扩展 ACL；仅目标 IP 地址与 EID 嵌入式地址匹配：

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。

b) 创建 LISP 检测映射，并进入参数模式：

policy-map type inspect lisp *inspect_map_name*

parameters

c) 通过识别您创建的 ACL 定义允许的 EID：

allowed-eid access-list *eid_acl_name*

第一跳路由器或 ITR/ETR 可能会向与 ASA 集群无关的主机或网络发送 EID 通知消息，因此，您可以限制只向与您的集群有关的服务器或网络发送 EID。例如，如果集群仅涉及 2 个站点，但是 LISP 在 3 个站点上运行，应只包括集群涉及的 2 个站点的 EID。

d) 如果需要，请输入预共享密钥：

validate-key 密钥

示例：

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

步骤 2 在端口 4342 上为第一跳路由器与 ITR 或ETR 之间的 UDP 流量配置 LISP检测：

a) 配置扩展 ACL 以识别 LISP 流量：

access list *eid_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

您必须 指定 UDP 端口 4342。接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。

b) 为 ACL 创建类映射：

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) 使用可选 LISP 检测映射指定策略映射、类映射以及启用检测，然后将服务策略应用于接口（如果为新接口）：

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

如果您有现有服务策略，请指定现有策略映射名称。默认情况下，ASA 包括称为 **global_policy** 的全局策略，因此对于全局策略，请指定该名称。如果您希望全局应用该策略，还可以为每个接口创建一个服务策略。LISP 检测会双向应用于流量，因此您无需在源接口和目标接口上应用服务策略；如果流量与两个方向的类映射都匹配，则进入或退出您应用策略映射的接口的所有流量都受影响。

示例：

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
```

```
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

ASA 会检测 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个关联 EID 和站点 ID 的 EID 表。

步骤 3 为流量类启用流移动性：

a) 配置扩展 ACL 以在服务器更改站点时确定要重新分配至最佳站点的业务关键流量：

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。您应对业务关键流量启用流移动性。例如，您可以只对HTTPS流量和/或发送到特定服务器的流量启用流移动性。

b) 为 ACL 创建类映射：

class-map *flow_map_name*

match access-list *flow_acl_name*

c) 指定在其上启用了 LISP 检测的同一策略映射，再指定流类映射，然后启用流移动性：

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

示例：

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0
 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

步骤 4 进入集群组配置模式，并为集群启用流移动性：

cluster group *name*

flow-mobility lisp

此开/关使您可以轻松地启用或禁用流移动性。

示例

以下示例：

- 将 EID 限制为 10.10.10.0/24 网络上的 EID
- 检查位于 192.168.50.89 的 LISP 路由器（内部）与位于 192.168.10.8 的 ITR 或 ETR 路由器（在另一个 ASA 接口上）之间的 LISP 流量 (UDP 4342)

- 为使用 HTTPS 在 10.10.10.0/24 上进入服务器的所有内部流量启用流移动性。
- 为集群启用流移动性。

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

配置分布式站点间 VPN

默认情况下，集群使用集中式站点间VPN模式。要利用集群的可扩展性，您可以启用分布式站点间 VPN 模式。

关于分布式站点间 VPN

在分布式模式下，站点间 IPsec IKEv2 VPN 连接将跨 ASA 集群节点分发。在集群节点之间分布 VPN 连接可实现充分利用集群的容量和吞吐量，将 VPN 支持大幅扩展至集中式 VPN 功能之外。

分布式 *VPN* 连接角色

在分布式 VPN 模式下运行时，系统将为集群节点分配以下角色：

- 主用会话所有者 - 最初接收连接的节点，或将备份会话转换为主用会话的设备。所有者为完整的会话维护状态并处理数据包，包括 IKE 和 IPsec 隧道以及所有与之关联的流量。
- 备份会话所有者 - 正在处理现有主用会话的备份会话的节点。如果主用会话所有者发生故障，备份会话所有者将成为主用会话所有者，并在另一个节点上建立新的备份会话。
- 转发器 - 如果与某个 VPN 会话关联的流量被发送至一个未拥有该 VPN 会话的节点，该节点将使用集群控制链路 (CCL) 将流量转发到拥有该 VPN 会话的节点。
- 协调器 - 协调器（始终是集群的控制节点）负责计算将移动哪些会话，在哪里以及何时执行主用会话重新分发 (ASR)。它会向所有者节点 X 发送将 N 个会话移至节点 Y 的请求。成员 X 将在完成操作时向协调器发送回应，指定它已成功移动的会话数量。

分布式 *VPN* 会话的特征

分布式站点间 VPN 会话具有以下特征。否则，VPN 连接的行为与不在集群上时的行为相同。

- VPN 会话将在会话级别跨集群分布。这意味着同一集群节点将会处理 VPN 连接的 IKE 和 IPsec 隧道及其所有流量。如果 VPN 会话流量被发送至未拥有该 VPN 会话的集群节点，此流量将被转发至拥有该 VPN 会话的集群节点。
- VPN 会话拥有在整个集群内唯一存在的会话 ID。此会话 ID 将用于验证流量，做出转发决策和完成 IKE 协商。
- 在站点间VPN集线器和辐射配置中，当客户端通过集群连接（称为发夹）时，流入的会话流量和流出的会话流量可能在不同的集群节点上。
- 您可以要求将备份会话分配到另一个机箱内的安全模块上；这样可以防范机箱出现故障。或者，您可以选择在集群内的任意节点上分配备份会话；这样可以防范节点出现故障。当集群中有两个机箱时，强烈建议采用远程机箱备份。

集群事件的分布式 *VPN* 处理

事件	分布式 VPN
节点故障	此故障节点上所有主用会话的备份会话（位于另一个节点上）将变为主用状态，并根据备份策略将备份会话重新分配到另一个节点上。
机箱故障	使用远程机箱备份策略时，故障机箱上所有主用会话的备份会话（位于另一机箱中的节点上）将变为主用状态。更换节点时，这些当前处于主用状态的会话的备份会话将被重新分配到更换机箱中的节点上。 使用平面备份策略时，如果主用会话和备份会话都在故障机箱上，则连接将会断开。在另一个机箱的节点上具有备份会话的所有主用会话将会回退到备份会话。新的备份会话将被分配到存活机箱中的另一个节点。
停用集群节点	正在停用的集群节点上的所有主用会话的备份会话（位于另一个节点上）将变为主用状态，并根据备份策略将备份会话重新分配到另一个节点上。
集群节点加入	如果新节点上的VPN集群模式未设置为分布式，则控制节点将请求更改模式。 在与 VPN 模式兼容后，集群节点将被分配正常操作流中的主用和备份会话。

IPsec IKEv2 修改

在分布式站点间 VPN 模式下，IKEv2 进行了以下方面的修改：

- 使用身份取代了IP/端口元组。这将允许对数据包做出正确的转发决策，以及清理可能位于其他集群成员上的先前连接。
- 标识单个 IKEv2 会话的 (SPI) 标识符是在本地生成的 8 字节随机值，并且在整个集群中是唯一的。SPI 嵌入了时间戳和集群节点 ID。在收到 IKE 协商数据包时，如果时间戳或集群节点 ID 检查失败，则会丢弃数据包并记录一条指示原因的消息。

- IKEv2 处理已修改为通过划分集群成员来预防 NAT-T 协商失败。在接口上启用 IKEv2 后，将添加新的 ASP 分类域 *cluster_isakmp_redirect* 和规则。使用 **show asp table classify domain cluster_isakmp_redirect** 命令查看规则。

集群中分布式站点间 *VPN* 的高可用性

以下功能针对安全模块或机箱的单一故障提供恢复能力：

- 在集群中任意机箱上的另一个安全模块中备份的 VPN 会话能承受安全模块故障。
- 在另一个机箱上备份的 VPN 会话能承受机箱故障。
- 可以更改控制节点而不丢失 VPN 站点间会话。

如果在集群稳定之前发生其他故障，并且主动和备份会话都在故障节点上，那么连接可能会丢失。

当某个节点以正常方式（例如禁用VPN集群模式、重新加载集群节点和其他预期的机箱更改）离开集群时，将做出所有尝试以确保不会丢失任何会话。在这些类型的操作期间，只要为集群提供时间在操作之间重新建立会话备份，会话就不会丢失。如果在最后一个集群节点上触发正常退出，它将正常结束现有会话。

CMPv2

系统将跨所有集群节点同步 CMPv2 ID 证书和密钥对。但只有集群中的控制节点会自动续约 CMPv2 证书并重新生成密钥。控制节点会在续约时将这些新的ID证书和密钥同步至所有集群节点。通过这种方式，集群中的所有节点都能使用CMPv2证书进行身份验证，而且任何节点都能接管成为控制节点。

分布式站点间 VPN 证书

每个集群成员上都需要分布式站点间 VPN 的运营商许可证。

每个 VPN 连接都需要两个其他 *VPN* 许可的会话（其他 *VPN* 许可证是基础许可证的一部分），一个用于主用会话，一个用于备份会话。由于每个会话使用两个许可证，因此集群的最大VPN会话容量不能超过许可容量的一半。

分布式站点间 VPN 的前提条件

型号支持

- Firepower 9300
- 最多 2 个机箱上最多支持 6 个模块。您可以在每个机箱中安装不同数量的安全模块，但我们建议均匀分布。

最高 VPN 会话数

每个安全模块支持多达 6K 个 VPN 会话，跨 6 个节点最多支持约 36K 个会话。

集群节点上支持的实际会话数量取决于平台容量、分配的许可证以及每情景的资源分配。当利用率接近限制时，即使未达到每个集群节点的最大容量，也可能出现创建会话失败的情况。这是因为主

用会话分配取决于外部交换，而备份会话分配则取决于内部集群算法。建议客户相应地调整其利用率，并留出非均匀分布的空间。

分布式站点间 VPN 准则

防火墙模式

仅在路由模式下支持分布式站点间 VPN。

情景模式

分布式站点间VPN可在单情景和多情景模式下运行。但在多情景模式下，主用会话重新分发将在系统级别，而不是情景级别进行。这可以防止与情景关联的主用会话移动到包含与其他情景关联的主用会话的集群成员上，从而在不知情的情况下产生无法支持的负载。

不受支持的检查

在分布式站点间 VPN 模式下不支持或已禁用以下检测类型：

- CTIQBE
- DCERPC
- H323、H225 和 RAS
- IPSec 直通
- MGCP
- MMP
- NetBIOS
- PPTP
- RADIUS
- RSH
- RTSP
- SCCP（瘦客户端）
- SUNRPC
- TFTP
- WAAS
- WCCP
- XDMCP

其他准则

- 在分布式站点间 VPN 模式下仅支持 IKEv2 IPsec 站点间 VPN。不支持 IKEv1。在集中式 VPN 模式下支持站点间 IKEv1。
- 不支持站点间集群。
- 动态 PAT 在分布式站点间 VPN 模式下不可用。

启用分布式站点间 VPN

启用分布式站点间 VPN，以充分利用 VPN 会话集群的可扩展性优势。

注释 在集中式和分布式之间更改VPN模式需要重新加载集群中的所有节点。更改备份模式是动态的，将不会终止会话。

开始之前

根据 VPN 配置指南配置站点间 VPN。

过程

步骤 1 在集群的控制节点上进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 启用分布式站点间 VPN。

vpn-mode distributed backup flat

或

vpn-mode distributed backup remote-chassis

在**平面**备份模式下，备用会话建立在任何其他集群节点上。这将保护用户免受模块故障的影响，但不能保证提供机箱故障保护。

在**远程机箱**备份模式下，备用会话建立在集群内另一个机箱的节点上。这将同时保护用户免受模块故障和机箱故障的影响。

如果是在**单机箱**环境中配置远程机箱（特意配置或因故障所致），则在另一个机箱加入之前，将不会创建任何备份。

示例：

```
ciscoasa(cfg-cluster)# vpn-mode distributed backup remote-chassis
WARNING: Do you want to proceed with changing the vpn-mode, save the device configuration,
and initiate a reboot? [confirm]
```

重新分发分布式站点间 VPN 会话

主用会话重新分发(ASR)将在所有集群成员之间重新分发主用 VPN 会话负载。由于开始会话和结束会话的动态性质，ASR 是跨所有集群成员均衡会话的最佳做法。重复进行重新分发操作将会优化均衡。

重新分发可以在任何时间运行，应该在集群中发生任何拓扑更改后运行，并且建议在新成员加入集群后运行。重新分发的目标是创建稳定的 VPN 集群。稳定的 VPN 集群的节点之间具有几乎相等数量的主用和备份会话。

要移动某个会话，备份会话将变为主用会话，并选择另一个节点托管新的备份会话。移动会话依赖于主用会话的备份位置和该特定备份节点上已有的主用会话数量。如果备份会话节点由于某种原因不能托管主用会话，则原始节点继续作为该会话的所有者。

在多情景模式下，主用会话重新分发将在系统级别，而不是个别情景级别进行。不在情景级别执行重新分发是因为，一个情景中的主用会话可能被移动某个成员，而该成员包含另一个情景中的其他许多主用会话，从而在该集群成员上创建了更多负载。

开始之前

- 如果您想要监控重新分发活动，请启用系统日志。
- 此程序必须在集群的控制单元上执行。

过程

步骤 1 在控制节点上，查看活动会话和备份会话在集群中的分布情况。

show cluster vpn-sessiondb distribution

示例：

系统将显示如下分布信息：

```
Member 0 (unit-1-1): active: 209; backups at: 1(111), 2(98)
Member 1 (unit-1-3): active: 204; backups at: 0(108), 2(96)
Member 2 (unit-1-2): active: 0
```

每行包含成员 ID、成员名称、主用会话数以及备份会话驻留在哪些成员上。对于以上示例，用户可以读出以下信息：

- 成员 0 上具有 209 个主用会话，成员 1 上备份了 111 个会话，成员 2 上备份了 98 个会话
- 成员 1 上具有 204 个主用会话，成员 0 上备份了 108 个会话，成员 2 上备份了 96 个会话

- 成员 2 没有任何主用会话；因此，没有集群成员正在备份此节点的会话。此成员最近才加入集群。

步骤 2 重新分发会话。

cluster redistribute vpn-sessiondb

此命令会立即返回（无任何消息），同时在后台继续执行。

根据需要重新分发的会话数和集群上的负载，这可能需要一些时间。重新分发活动发生时，系统会提供包含以下短语的系统日志（此处未显示其他系统详细信息）：

系统日志短语	说明
已启动 VPN 会话重新分发	仅控制节点
已发送请求，将 *number* 个会话从 *orig-member-name* 移到 *dest-member-name*	仅控制节点
未能将会话重新分发消息发送至 *member-name*	仅控制节点
已收到请求，将 *number* 个会话从 *orig-member-name* 移到 *dest-member-name*	仅数据节点
已将 *number* 个会话移到 *member-name*	已移至指定集群的活动会话数。
未能收到 *dest-member-name* 的会话移动响应	仅控制节点
已完成 VPN 会话	仅控制节点
检测到集群拓扑更改。已终止 VPN 会话重新分发。	

步骤 3 重新输入 **show cluster vpn-sessiondb distribution** 命令以查看结果。

FXOS：删除集群设备

以下部分介绍如何临时或永久删除集群中的节点。

临时删除

例如，出现硬件或网络故障时，集群节点会自动从集群中删除。此删除是临时的，故障消除后，它们可以重新加入集群。您也可以手动禁用集群。

要检查设备当前是否在集群中，在应用程序内使用 **show cluster info** 命令查看集群状态：

```
ciscoasa# show cluster info
Clustering is not enabled
```

- 在应用程序中禁用集群 - 您可以使用应用程序 CLI 禁用集群。输入 **cluster remove unit** 名称 命令删除除您登录的设备以外的所有节点。引导程序配置保持不变，从控制节点同步的最新配置

也保持不变，因此您可于稍后重新添加该节点而不会丢失配置。如果在数据节点上输入此命令来删除控制节点，则会选择新的控制节点。

当设备处于非主用状态时，所有数据接口关闭；只有管理接口可以发送和接收流量。要恢复流量流，请重新启用集群。管理接口将保持打开，使用节点从引导程序配置接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，假设您保存了已禁用集群的配置），管理接口将被禁用。

要重新启用集群，请在 ASA 上输入 **cluster group** *name*，然后输入 **enable**。

- 禁用应用程序实例 -在 FXOS CLI 中，请参阅以下示例：

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa asa1
Firepower-chassis /ssa/slot/app-instance # disable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

要重新启用：

```
Firepower-chassis /ssa/slot/app-instance # enable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

- 关闭 安全模块/引擎 - 在 FXOS CLI 中，请参阅以下示例：

```
Firepower-chassis# scope service-profile server 1/1
Firepower-chassis /org/service-profile # power down soft-shut-down
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

要接通电源：

```
Firepower-chassis /org/service-profile # power up
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

- 关闭机箱 -在 FXOS CLI 中，请参阅以下示例：

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

永久删除

您可以使用以下方法永久删除集群节点。

- 删除逻辑设备 -在 FXOS CLI 中，请参阅以下示例：

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
```

```
Firepower-chassis /ssa* # commit-buffer
Firepower-chassis /ssa #
```

- 从服务中删除机箱或安全模块 - 如果从服务中删除设备，则可以将替换硬件添加为集群的新节点。

ASA：管理集群成员

部署集群后，您可以更改配置和管理集群成员。

成为非活动成员

要成为集群的非活动成员，请在节点上禁用集群，同时保持集群配置不变。

注释 当ASA处于非活动状态（以手动方式或因运行状况检查失败）时，所有数据接口都将关闭；只有管理专用接口可以发送和接收流量。要恢复流量传输，请重新启用集群；或者，您也可以从集群中完全删除该节点。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，您保存了已禁用集群的配置），则管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

开始之前

- 您必须使用控制台端口；不能通过远程 CLI 连接启用或禁用集群。
- 对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入**changeto system** 命令。

过程

步骤 1 进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 禁用集群：

no enable

如果此节点是控制节点，则会进行新的控制选择，并且其他成员将成为控制节点。

集群配置保持不变，因此您可于稍后再次启用集群。

停用单元

要禁用您登录的节点以外的成员，请执行以下步骤。

注释 当ASA处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。要恢复流量流，请重新启用集群。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，假设您保存了已禁用集群的配置），管理接口将被禁用。您必须使用控制台端口来进行任何进一步的配置。

开始之前

对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入 **changeto system** 命令。

过程

从集群中删除该节点：

cluster remove unit *node_name*

引导程序配置保持不变，从控制节点同步的最新配置也保持不变，因此您可于稍后重新添加该节点而不会丢失配置。如果在数据节点上输入此命令来删除控制节点，则会选择新的控制节点。

要查看成员名称，请输入 **cluster remove unit ?**，或者输入 **show cluster info** 命令。

示例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

重新加入集群

如果从集群中删除了某个节点（例如针对出现故障的接口），或者如果您手动停用了某个成员，那么您必须手动重新加入集群。

开始之前

- 您必须使用控制台端口来重新启用集群。其他接口已关闭。
- 对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入**changeto system** 命令。
- 确保故障已解决，再尝试重新加入集群。

过程

步骤 1 在控制台中，进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 启用集群。

enable

变更控制单元

⚠

注意 要更改控制节点，最好的方法是在控制节点上禁用集群，等到新的控制选举后再重新启用集群。如果必须指定要成为控制节点的具体节点，请使用本节中的程序。但是请注意，对集中功能而言，如果使用本程序强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

要更改控制节点，请执行以下步骤：

开始之前

对于多情景模式，请在系统执行空间中执行本程序。如果尚未进入系统配置模式，请输入 **changeto system** 命令。

过程

将新节点设置为控制节点：

cluster control-node unit*node_name*

示例：

```
ciscoasa(config)# cluster control-node unit asa2
```

您需要重新连接到主集群 IP 地址。

要查看成员名称，请输入 **cluster control-node unit ?**（可查阅除当前节点之外的所有名称），或输入 **show cluster info** 命令。

在整个集群范围内执行命令

要向集群中的所有成员或某个特定成员发送命令，请执行以下步骤。向所有成员发送 **show** 命令以收集所有输出并将其显示在当前设备的控制台上。（请注意，可能存在您可以在控制设备上输入的显示命令，以查看集群范围内的统计信息。）也可在整个集群范围内执行其他命令（如 **capture** 和 **copy**）。

过程

向所有成员发送命令，或者指定设备名称向某个特定成员发送命令：

cluster exec [unit *unit_name*] *command*

示例：

```
ciscoasa# cluster exec show xlate
```

要查看成员名称，请输入 **cluster exec unit ?**（查看除当前设备以外的所有名称），或输入 **show cluster info** 命令。

示例

要同时将同一捕获文件从集群中的所有设备复制到 TFTP 服务器，请在控制设备上输入以下命令：

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

多个 PCAP 文件（一个文件来自一个设备）将复制到 TFTP 服务器。目标捕获文件名会自动附加设备名称，例如 capture1_asa1.pcap、capture1_asa2.pcap 等。在本示例中，asa1 和 asa2 是集群设备名称。

以下是 **cluster exec show memory** 命令的输出示例，显示了集群内每个成员的内存信息：

```
ciscoasa# cluster exec show memory
unit-1-1(LOCAL):*******************************************************
```

```
Free memory:      108724634538 bytes (92%)
Used memory:        9410087158 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-3:***********************************************************
Free memory:      108749922170 bytes (92%)
Used memory:        9371097334 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-2:***********************************************************
Free memory:      108426753537 bytes (92%)
Used memory:        9697869087 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)
```

ASA：监控 Firepower 4100/9300 机箱上的 ASA 集群

您可以监控集群状态和连接并排除故障。

监控集群状态

请参阅以下用于监控集群状态的命令：

- **show cluster info [health], show cluster chassis info**

  如果没有关键字，**show cluster info** 命令将显示所有集群成员的状态。

  show cluster info health 命令将显示接口、设备和整个集群的当前运行状况。

  有关 **show cluster info** 命令，请参阅以下输出：

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state MASTER
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state SLAVE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
        Last join : 20:29:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
```

```
Unit "unit-1-1" in state SLAVE
    ID        : 1
    Version   : 9.5(2)
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.1.1
    CCL MAC   : 0015.c500.017f
    Last join : 20:20:53 UTC Nov 4 2015
    Last leave: 20:18:15 UTC Nov 4 2015
Unit "unit-2-1" in state SLAVE
    ID        : 3
    Version   : 9.5(2)
    Serial No.: FCH19057ML0
    CCL IP    : 127.2.2.1
    CCL MAC   : 0015.c500.020f
    Last join : 20:19:57 UTC Nov 4 2015
    Last leave: 20:24:55 UTC Nov 4 2015
```

- **show cluster info auto-join**

  显示集群设备是否将在一段延迟后自动重新加入集群，以及是否已清除故障条件（例如等待许可证、机箱运行状况检查失败，等等）。如果设备已永久禁用，或设备已在集群中，则此命令将不会显示任何输出。

  请参阅 **show cluster info auto-join** 命令的以下输出：

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Master has application down that slave has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport**{**asp** |**cp** [**detail**]}

  显示以下项目传输相关的统计信息：

  - **asp** — 数据平面传输统计信息。
  - **cp** — 控制平面传输统计信息。

如果您输入 **detail** 关键字，您可以查看集群可靠传输协议的使用情况，以便确定控制平面中的缓冲区已满时的丢包问题。请参阅 **show cluster info transport cp detail** 命令的以下输出：

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
--------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
```

```
  ROW   0          0          0
  ROB   0          0          0
  RAS   130258     218924     228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ---------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ---------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
```

```
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
============================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ------------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
============================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ------------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  显示集群历史记录，以及有关集群设备加入失败的原因或设备离开集群的原因的错误消息。

捕获整个集群范围内的数据包

有关在集群中捕获数据包的信息，请参阅以下命令：

cluster exec capture

要支持集群范围的故障排除，您可以使用 **cluster exec capture** 命令在控制节点上启用捕获集群特定流量的功能，随后集群中的所有数据节点上将自动启用此功能。

监控集群资源

请参阅以下命令以监控集群资源：

show cluster {cpu | memory | resource} [选项]，**show cluster chassis [cpu | memory | resource usage]**

显示整个集群的聚合数据。可用选项取决于数据类型：

监控集群流量

请参阅以下命令以监控集群流量：

- **show conn [detail | count], cluster exec show conn**

show conn 命令显示流量是导向器流量、备用流量还是转发器流量。在任意设备上使用 **cluster exec show conn** 命令可查看所有连接。此命令可以显示单个流的流量到达集群中不同 ASA 的方式。集群的吞吐量取决于负载均衡的效率和配置。此命令可以让您很方便地查看某个连接的流量如何流经集群，也可以帮助您了解负载均衡器对传输的性能有何影响。

以下是 **show conn detail** 命令的输出示例：

```
ciscoasa/ASA2/slave# show conn detail
15 in use, 21 most used
Cluster:
        fwd connections: 0 in use, 0 most used
        dir connections: 0 in use, 0 most used
        centralized connections: 0 in use, 44 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       M - SMTP data, m - SIP media, n - GUP
       N - inspected by Snort
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

Cluster units to ID mappings:
  ID 0: unit-2-1
  ID 1: unit-1-1
  ID 2: unit-1-2
  ID 3: unit-2-2
  ID 4: unit-2-3
  ID 255: The default cluster member ID which indicates no ownership or affiliation
          with an existing cluster member
```

- **show cluster info [conn-distribution | packet-distribution | loadbalance]**

  show cluster info conn-distribution 和 **show cluster info packet-distribution** 命令显示所有集群设备之间的流量分布。这些命令可以帮助您评估和调整外部负载均衡器。

  show cluster info loadbalance 命令显示连接再平衡统计信息。

- **show cluster info load-monitor** [**details**]

  show cluster info load-monitor 命令显示最后一个间隔的集群成员的流量负载，以及已配置的总间隔数（默认情况下为 30）。使用 **details** 关键字查看每个时间间隔的每个度量值。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
```

```
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
Average from last 30 interval:
   0           0            0            12             28
   1           0            0            13             27


ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval


Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Buffer drops captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0
```

```
         0          0          0          0          0          0
Unit ID  1
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0

Memory usage(%) captured over 30 intervals:
Unit ID  0
        25         25         30         30         30         35
        25         25         35         30         30         30
        25         25         30         25         25         35
        30         30         30         25         25         25
        25         20         30         30         30         30
Unit ID  1
        30         25         35         25         30         30
        25         25         35         25         30         35
        30         30         35         30         30         30
        25         20         30         25         25         30
        20         30         35         30         30         35

CPU usage(%) captured over 30 intervals:
Unit ID  0
        25         25         30         30         30         35
        25         25         35         30         30         30
        25         25         30         25         25         35
        30         30         30         25         25         25
        25         20         30         30         30         30
Unit ID  1
        30         25         35         25         30         30
        25         25         35         25         30         35
```

```
30          30          35          30          30          30
25          20          30          25          25          30
20          30          35          30          30          35
```

- **show cluster {access-list | conn [count] | traffic | user-identity | xlate}** [选项]，**show cluster chassis {access-list | conn | traffic | user-identity | xlate count}**

  显示整个集群的聚合数据。可用选项取决于数据类型：

  有关 **show cluster access-list** 命令，请参阅以下输出：

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

  要显示所有设备在用连接的 汇聚计数，请输入：

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
124 in use, fwd connection 0 in use, dir connection 0 in use, centralized connection
0 in use (Cluster-wide aggregated)
```

```
unit-1-1(LOCAL):*******************************************************
40 in use, 48 most used, fwd connection 0 in use, 0 most used, dir connection 0 in use,
0 most used, centralized connection 0 in use, 46 most used

unit-2-2:*******************************************************
18 in use, 40 most used, fwd connection 0 in use, 0 most used, dir connection 0 in use,
0 most used, centralized connection 0 in use, 45 most used
```

- **show asp cluster counter**

  此命令对于数据路径故障排除非常有用。

监控集群路由

有关集群路由的信息，请参阅以下命令：

- **show route cluster**
- **debug route cluster**

  显示集群的路由信息。

- **show lisp eid**

  显示 ASA EID 表，表中显示了 EID 和站点 ID。

  请参阅 **cluster exec show lisp eid** 命令的以下输出。

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):*************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:*************************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  该命令对于故障排除非常有用。

监控分布式站点间 VPN

使用以下命令监控 VPN 会话的状态和分布：

- 使用 **show cluster vpn-sessiondb distribution** 提供会话的总体分布。如果在多情景环境中运行，则必须在系统执行空间中运行此命令。

  利用此 **show** 命令可以快速查看会话，而无需在每个节点上执行 **show vpn-sessiondb summary**。

- 也可使用 **show cluster vpn-sessiondb summary** 命令提供集群上的 VPN 连接的统一视图。
- 使用 **show vpn-sessiondb** 命令的单独设备监控除了显示常见的 VPN 信息以外，还显示设备上的主用和备份会话数量。

配置集群日志记录

有关为集群配置日志记录的信息，请参阅以下命令：

logging device-id

集群中的每个节点将独立生成系统日志消息。您可以使用 **logging device-id** 命令来生成具有相同或不同设备 ID 的系统日志消息，以使消息看上去是来自集群中的相同或不同节点。

调试集群

请参阅以下用于调试集群的命令：

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | service-module | transport]**

  显示集群的调试消息。

- **debug service-module**

  显示用于刀片级别问题（包括监管程序与应用之间的运行状况检查问题）的调试消息。

- **show cluster info trace**

  show cluster info trace 命令显示调试信息，供进一步排除故障之用。

  请参阅 **show cluster info trace** 命令的以下输出：

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

  例如，如果您看到以下消息显示两个具有相同 **local-unit** 名称的节点充当控制节点，这可能意味着两个节点具有相同的 **local-unit** 名称（请检查您的配置），或者某个节点正在接收自己的广播消息（请检查您的网络）。

```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node
 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

分布式站点间 VPN 故障排除

分布式 VPN 通知

当运行分布式 VPN 的集群上发生以下错误情况时，您将收到包含确定短语的通知消息：

情况	通知
如果在尝试加入集群时，某个现有或正在加入集群的数据节点未处在分布式 VPN 模式下：	新集群成员 (*member-name*) 由于 vpn 模式不匹配而被拒绝。 和 控制节点 (*control-name*) 拒绝来自设备 (unit-name) 的注册请求，原因是：vpn 模式功能与控制节点配置不兼容
如果分布式 VPN 的集群成员上未正确地配置许可：	错误：控制节点请求集群的 vpn 模式更改为分布式。由于缺少运营商许可证，无法更改模式。
如果接收的 IKEv2 数据包的 SPI 中的时间戳或成员 ID 无效：	收到已到期的 SPI 或 检测到损坏的 SPI
如果集群无法创建备份会话：	未能创建 IKEv2 会话的备份。
IKEv2 初始联系 (IC) 处理错误：	IKEv2 协商因错误而终止：备份上找到过时的备份会话
重新分发问题：	未能将会话重新分发消息发送至 *member-name* 未能收到 *member-name* 的会话移动响应（仅限控制节点）
如果在重新分发会话期间拓扑发生更改：	检测到集群拓扑更改。已终止 VPN 会话重新分发。

您可能遇到以下情况之一：

- 当使用 **port-channel load-balance src-dst l4port**命令为 N7K 交换机配置 L4port 作为负载均衡算法时，站点间 VPN 会话仅被分发到集群中的一个机箱。集群会话分配的示例如下所示：

```
SSP-Cluster/data node(cfg-cluster)# show cluster vpn-sessiondb distribution
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
5(2501)
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

由于站点间 IKEv2 VPN 使用端口 500 作为源和目标端口，因此 IKE 数据包仅发送至 Nexus 7K 与机箱之间连接的端口通道中的其中一个链路。

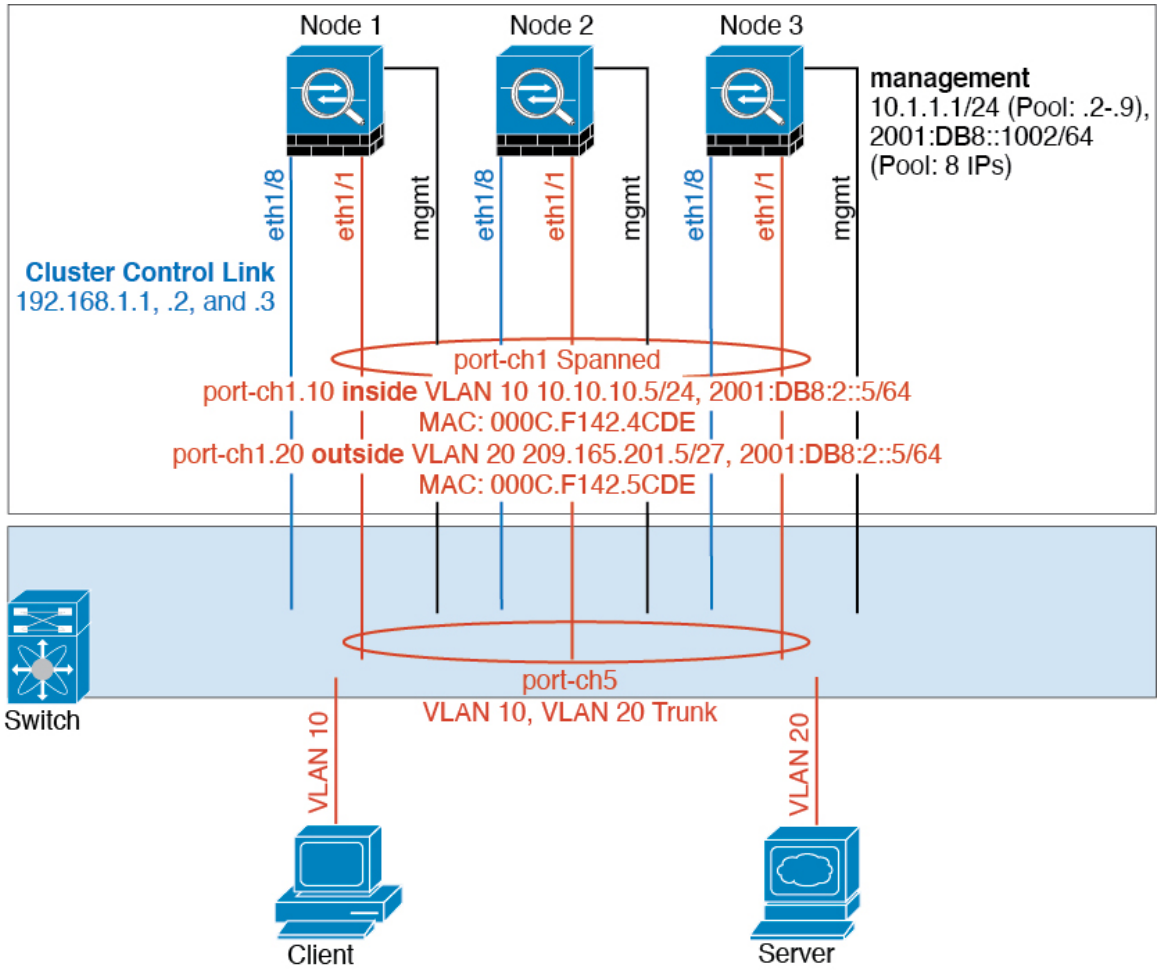
使用 **port-channel load-balance src-dst ip-l4port** 将 Nexus 7K 负载均衡算法更改为 IP 和 L4 端口。然后，IKE 数据包将被发送至所有链路，进而发送至所有节点。

要进行更即时的调整，请在集群的控制节点上执行： **cluster redistribute vpn-sessiondb** ，将主用 VPN 会话重新分发至另一机箱的集群节点。

ASA 集群示例

这些示例包含典型部署。

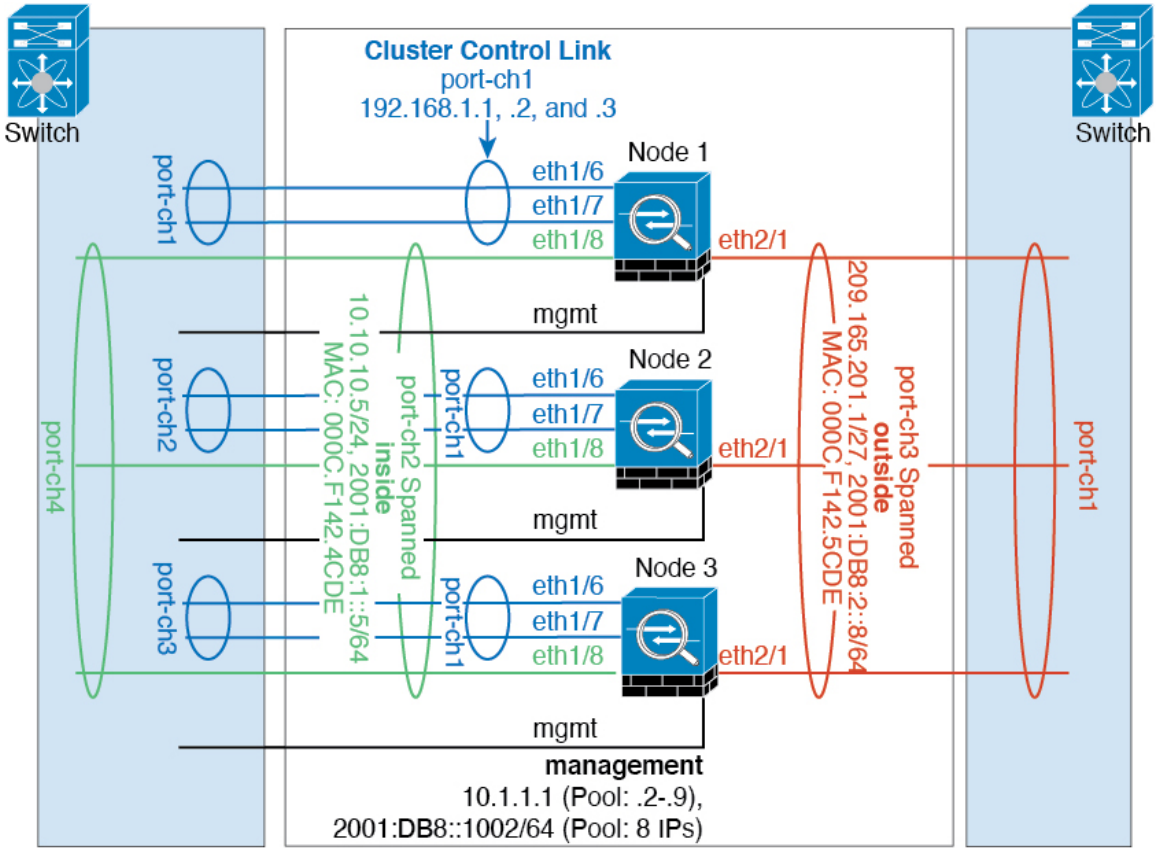
单臂防火墙



来自不同安全域的数据流量与不同的 VLAN 关联，例如，VLAN 10 用于内部网络，而 VLAN 20 用于外部网络。每台 ASA 都有一个连接到外部交换机或路由器的物理端口。启用中继使物理链路上的所有数据包都采用 802.1q 封装。ASA 是 VLAN 10 与 VLAN 20 之间的防火墙。

使用跨网络 EtherChannel 时，所有数据链路在交换机侧分组为一个 EtherChannel。如果一台 ASA 变得不可用，交换机将在其余设备之间再均衡流量。

流量分隔



您可能更愿意在内部和外部网络之间采用物理方式分离流量。

如上图所示，左侧有一个跨网络 EtherChannel 连接到内部交换机，而右侧的另一个跨网络 EtherChannel 连接到外部交换机。如果需要，您还可以在每个 EtherChannel 上创建 VLAN 子接口。

路由模式站点间集群的 OTV 配置

使用跨区以太网通道的路由模式的站点间集群能否成功，取决于OTV的配置和监控是否适当。OTV 通过在 DCI 上转发数据包来发挥重要作用。仅当在其转发表中获知 MAC 地址时，OTV 才会通过 DCI 转发单播数据包。如果在 OTV 转发表中未获知 MAC 地址，它将丢弃单播数据包。

OTV 配置示例

```
//Sample OTV config:
//3151 - Inside VLAN, 3152 - Outside VLAN, 202 - CCL VLAN
//aaaa.1111.1234 - ASA inside interface global vMAC
//0050.56A8.3D22 - Server MAC

feature ospf
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
```

```
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

因站点故障需要修改 OTV 过滤器

如果站点断开，需要删除 OTV 的过滤器，因为无需再阻止全局 MAC 地址。还需要一些其他配置。

您需要在正常工作的站点中的 OTV 交换机上添加 ASA 全局 MAC 地址的静态条目。此条目将允许另一端的 OTV 在重叠接口上添加这些条目。之所以需要此步骤，是因为如果服务器和客户端已有 ASA 的 ARP 条目（对于现有连接即是如此），它们将不再发送该 ARP。因此，OTV 将不会有机会在其转发表中获知 ASA 全局 MAC 地址。由于 OTV 的转发表中没有该全局 MAC 地址，并且根据 OTV 设计，它不会通过重叠接口泛洪发送单播数据包，则它将丢弃从服务器到全局 MAC 地址的单播数据包，现有连接将中断。

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

当另一个站点恢复时，您需要重新添加过滤器，并删除 OTV 上的此静态条目。清除两个 OTV 上的动态 MAC 地址表，从而清除全局 MAC 地址的重叠条目，这一点非常重要。

MAC 地址表清除

当站点断开并且全局 MAC 地址的静态条目已添加到 OTV 时，您需要让另一个 OTV 获知重叠接口上的全局MAC地址。在另一个站点恢复后，应清除这些条目。务必清除MAC地址表，以确保OTV的转发表中没有这些条目。

```
cluster-N7k6-OTV# show mac address-table
```

```
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

OTV ARP 缓存监控

OTV 为代理 ARP 维护通过 OTV 接口获知的 IP 地址的 ARP 缓存。

```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

站点间集群示例

以下示例显示支持的集群部署。

具有站点特定的 MAC 和 IP 地址的跨区以太网通道路由模式示例

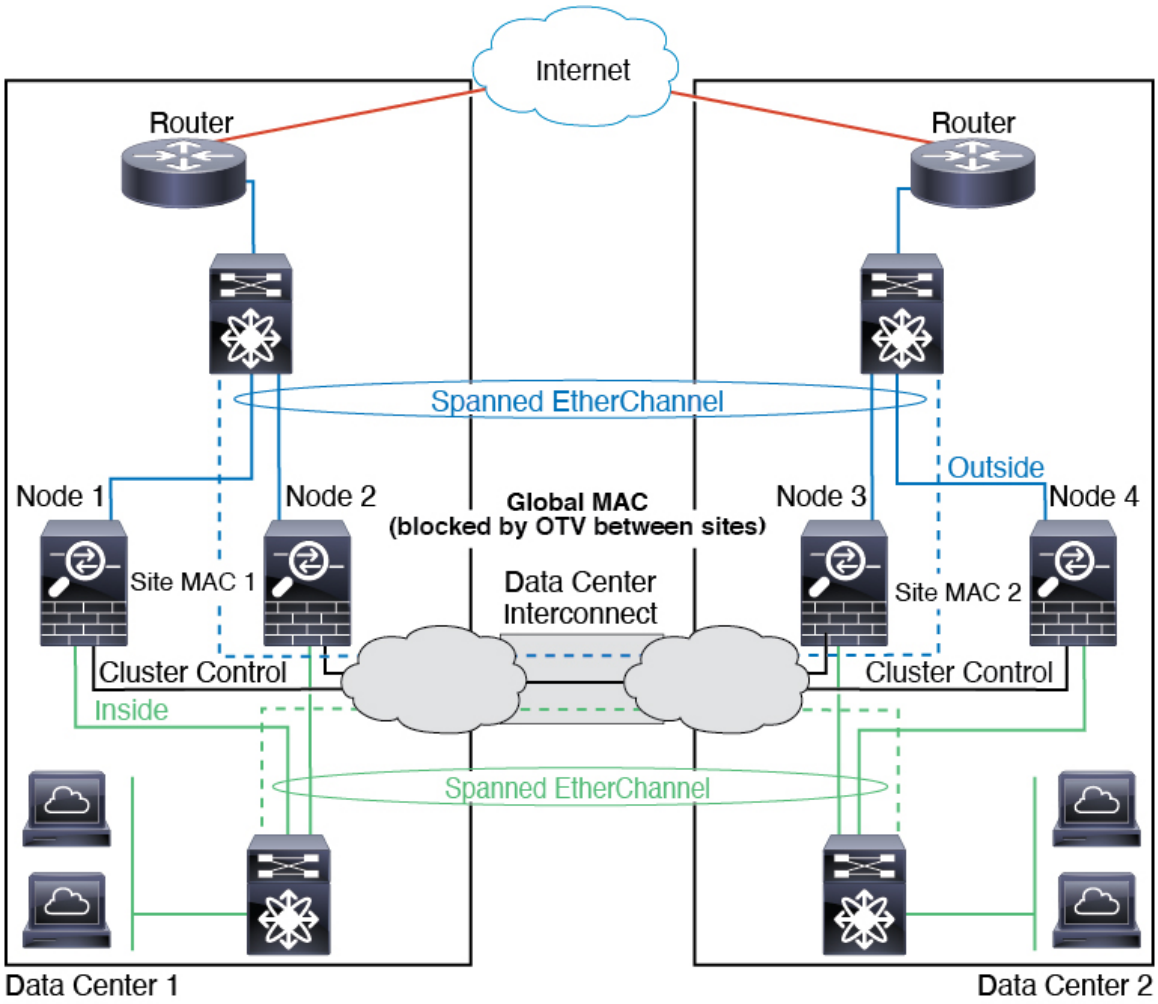
以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在每个站点上的网关路由器和内部网络之间（东西插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部网络的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术在站点之间扩展。您必须添加阻止全局 MAC 地址的过滤器，防止发往集群的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的集群节点，则您必须删除过滤器，使流量能够发送到另一站点的集群节点。您应使用 VACL 来过滤全局 MAC 地址。对于某些交换机（例如具有 F3 系列线卡的 Nexus），您还必须使用 ARP 检查屏蔽来自全局 MAC 地址的 ARP 数据包。ARP 检查要求您在 ASA 上设置站点 MAC 地址和站点 IP 地址。如果仅配置站点 MAC 地址，请禁用 ARP 检查。

集群相当于内部网络的网关。所有集群节点共享的全局虚拟 MAC 仅用于接收数据包。传出数据包使用来自每个 DC 集群的站点特定的 MAC 地址。此功能可防止交换机从两个不同端口上的两个站点获知相同全局 MAC 地址，导致 MAC 地址摆动；相反，它们仅获知站点 MAC 地址。

在此场景中：

- 从集群发送的所有出口数据包使用站点 MAC 地址，并在数据中心进行本地化。
- 发送到集群的所有入口数据包使用全局 MAC 地址发送，因此可以被两个站点的任何节点接收；OTV 的过滤器将数据中心内的流量本地化。



跨区以太网通道透明模式南北站点间集群示例

以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在内部和外部路由器之间（南北插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

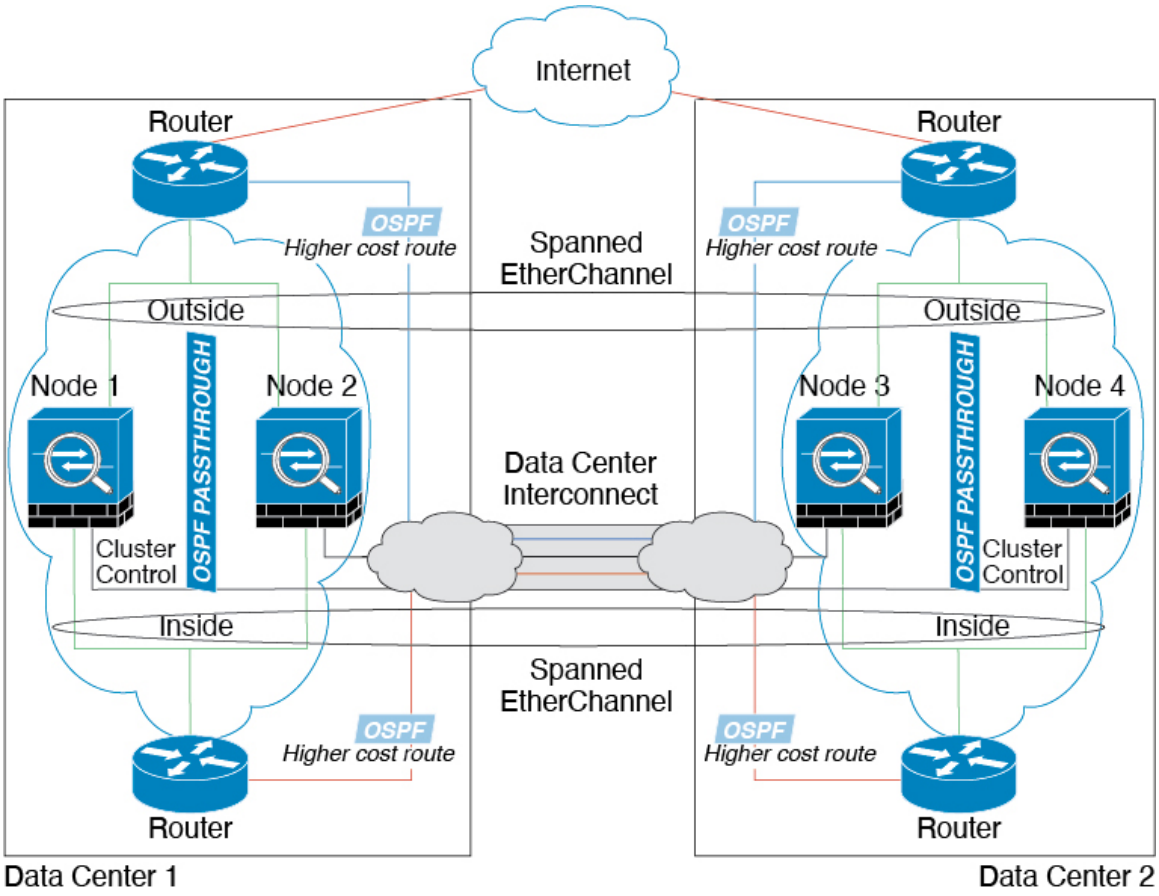
位于每个数据中心的内部和外部路由器均使用 OSPF（可通过透明的 ASA）。与 MAC 地址不同，路由器 IP 地址在所有路由器上都是唯一的。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有集群成员都中断连接。通过 ASA 的开销较低的路由必须经过位于每个站点的同一网桥组才能使集群维持非对称连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的集群成员。

位于每个站点的交换机的实施可包括：

- 站点间 VSS、vPC、StackWise 或 StackWise Virtual - 在此情景中，一台交换机安装在数据中心 1，另一台交换机安装在数据中心 2。一个方案是将位于每个数据中心的集群节点只连接到本地交换机，而冗余交换机流量通过 DCI 传输。在此情况下，连接多半会保持在每个数据中心本

地。如果 DCI 可以处理额外的流量，您也可以选择将每个节点通过 DCI 连接到两台交换机。在此情况下，流量跨数据中心分摊，因此 DCI 必须非常强健稳定。

- 位于每个站点的本地 VSS、vPC、StackWise 或 StackWise Virtual - 为了获得更高的交换机冗余能力，您可以在每个站点安装 2 对单独的冗余交换机。在此情况下，尽管集群节点仍然有一个跨区以太网通道将数据中心 1 的机箱仅连接到两台本地交换机，将数据中心 2 的机箱连接到本地交换机，但跨区以太网通道本质上是“分离的”。每个本地冗余交换机系统都会将跨区以太网通道视作站点本地的 EtherChannel。

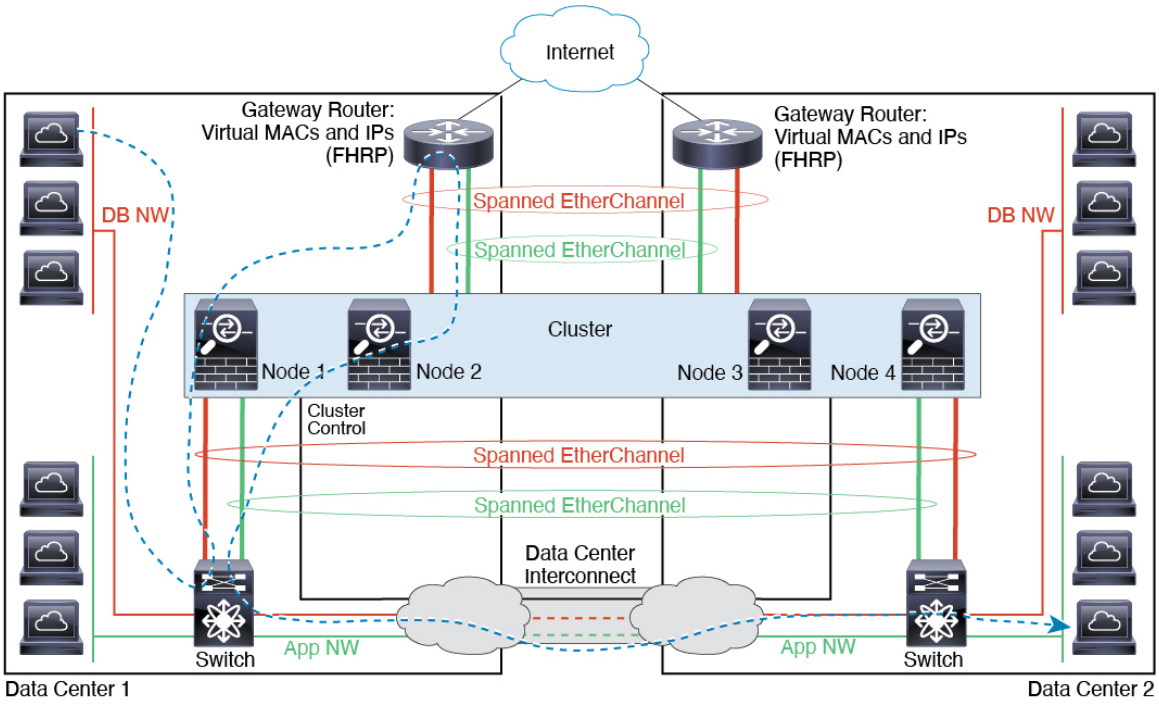


跨区以太网通道 透明模式东西站点间集群示例

以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在每个站点上的网关路由器和两个内部网络（应用网络和数据库网络）之间（东西插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。每个站点上的集群成员使用面向内部与外部应用网络和数据库网络的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

每个站点上的网关路由器使用 FHRP（例如 HSRP）在每个站点上提供相同的目标虚拟 MAC 和 IP 地址。要避免 MAC 地址意外摆动，最好使用使用 **mac-address-table static** *outside_interface mac_address* 命令将网关路由器实际 MAC 地址静态添加到 ASA MAC 地址表。如果没有这些条目，当位于站点 1 的网关与位于站点 2 的网关通信时，流量可能通过 ASA 并尝试从内部接口到达站点 2，从而导致出现问题。数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术在站点之间扩展。您必须添加过滤

器，阻止发往网关路由器的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的网关路由器，则您必须删除过滤器，使流量能够发送到另一站点的网关路由器。



集群参考

本部分包括有关集群工作原理的详细信息。

ASA 功能和集群

部分 ASA 功能不受 ASA 集群支持，还有部分功能仅在控制节点上受支持。其他功能可能对如何正确使用规定了注意事项。

集群不支持的功能

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

- 依靠 TLS 代理实现的统一通信功能
- 远程访问 VPN（SSL VPN 和 IPsec VPN）
- 虚拟隧道接口 (VTI)
- IS-IS 路由
- 以下应用检查：
  - CTIQBE

- H323、H225 和 RAS
- IPsec 穿透
- MGCP
- MMP
- RTSP
- SCCP（瘦客户端）
- WAAS
- WCCP

- 僵尸网络流量过滤器
- 自动更新服务器
- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- VPN 负载均衡
- 故障转移
- 集成路由和桥接
- 失效连接检测 (DCD)
- FIPS 型号

集群集中化功能

以下功能只有在控制节点上才受支持，且无法为集群扩展。

注释 集中功能的流量从成员节点通过集群控制链路转发到控制节点。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非控制节点的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回控制节点。

对集中功能而言，如果控制节点发生故障，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

- 以下应用检查：
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS

- PPTP
- RADIUS
- RSH
- SNMP
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- 静态路由监控
- 网络访问的身份验证和授权。记帐被分散。
- 筛选服务
- 站点间 VPN

  在集中式模式下，仅与集群的控制节点建立 VPN 连接。 这是 VPN 集群的默认模式。站点间的 VPN 也可以部署在分布式 VPN 模式，其中 S2S IKEv2 VPN 连接分布在节点之间。
- IGMP 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- PIM 组播控制平面协议的处理（数据平面转发分布于整个集群中）
- 动态路由

应用到单台设备的功能

这些功能将应用到每个 ASA 节点而非整个集群或控制节点。

- QoS - QoS 策略将于配置复制过程中在集群中同步。但是，该策略是在每个节点上独立执行。例如，如果对输出配置管制，则要对流出特定 ASA 的流量应用符合规则的速率和符合规则的突发量值。在包含 3 个节点且流量均衡分布的集群中，符合规则的速率实际上变成了集群速率的 3 倍。
- 威胁检测 - 威胁检测在各节点上独立工作；例如，排名统计信息就要视具体节点而定。以端口扫描检测为例，由于扫描的流量将在所有节点间进行负载均衡，而一个节点无法看到所有流量，因此端口扫描检测无法工作。
- 资源管理 - 多情景模式下的资源管理根据本地使用情况在每个节点上分别执行。
- LISP 流量 - UDP 端口 4342 上的 LISP 流量由每个接收节点进行检查，但是没有为其分配导向器。每个节点都会添加到集群共享的 EID 表，但是 LISP 流量本身并不参与集群状态共享。

用于网络访问的 AAA 和集群

用于网络访问的AAA由三部分组成：身份验证、授权和记账。身份验证和授权作为集中功能在集群控制节点上实施，且数据结构复制到集群数据节点。如果选举出控制节点，新的控制节点将拥有所需的所有信息，以继续不间断运行经过验证的既有用户及其相关授权。当控制节点发生变化时，用户身份验证的空闲和绝对超时将保留。

记账作为分散的功能在集群中实施。记账按每次流量完成，因此在为流量配置记账时，作为流量所有者的集群节点会将记账开始和停止消息发送到 AAA 服务器。

连接设置

连接限制在集群范围强制实施（请参阅 **set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max** 和 **set connection per-client-max** 命令）。每个节点都有根据广播消息估计的集群范围的计数器值。出于效率考虑，在集群中配置的连接限制可能不会严格按限制数量实施。每个节点在任何指定时间都可能高估或低估集群范围内的计数器值。不过，在负载均衡的集群中，该信息将随时间而更新。

FTP 和集群

- 如果 FTP 数据通道和控制通道流量由不同的集群成员所有，则数据通道所有者会将空闲超时更新定期发送到控制通道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父/子流量关系；控制流量空闲超时不会更新。
- 如果您将 AAA 用于 FTP 访问，则控制通道流集中在控制节点上。

ICMP 检查

ICMP 和 ICMP 错误数据包通过集群的流取决于是否启用 ICMP/ICMP 错误检查。不启用 ICMP 检查时，ICMP 是单向流，并且不支持导向器流。启用ICMP检查时，ICMP流变为双向流，并由导向器/备份流支持。被检查的ICMP流的一个不同之处在于导向器对转发数据包的处理：导向器会将ICMP回应应答数据包转发给流所有者，而不是将数据包返回给转发器。

组播路由和集群

在建立快速路径转发之前，控制单元会处理所有的组播路由数据包和数据数据包。在连接建立之后，每台数据设备都可以转发组播数据包。

NAT 和集群

NAT 可能会影响集群的总吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 ASA，因为负载均衡算法取决于 IP 地址和端口，NAT 会导致入站和出站数据包具有不同的 IP 地址和/或端口。当数据包到达并非 NAT 所有者的 ASA时，会通过集群控制链路转发到所有者，导致集群控制链路上存在大量流量。请注意，接收节点不会创建流向所有者的转发流量，因为NAT所有者最终可能不会根据安全和策略检查结果为数据包创建连接。

如果您仍想在集群中使用 NAT，请考虑以下准则：

- PAT 采用端口块分配 - 请参阅该功能的以下准则：

- 每主机最大流量限制并不针对整个集群，而是单独应用于每个节点。因此，在每主机最大流量限制配置为 1 的包含 3 个节点的集群中，如果在全部 3 个节点上对来自主机的流量实行负载均衡，则可以分配 3 个端口块，每个节点 1 个。
- 在执行每主机最大流量限制时，在备份池中的备份节点上创建的端口块不计算在内。
- 如果进行即时 PAT 规则修改（对 PAT 池改用全新的 IP 地址范围），会导致在新的池生效时仍在传输的转换项备份请求的转换项备份创建失败。此行为并非端口块分配功能所特有，它是一个暂时性 PAT 池问题，只发现于在集群节点之间分配池并执行流量负载均衡的集群部署。
- 在集群中操作时，不能直接更改块分配大小。只有在集群中重新加载每个设备后，新的大小才会生效。为避免重新加载每个设备，我们建议您删除所有块分配规则并清除与这些规则相关的所有转换。然后，您可以更改块大小并重新创建块分配规则。

- 对动态 PAT 使用 NAT 池地址分配 - 配置 PAT 池时，集群将池中的每个 IP 地址划分为端口块。默认情况下，每个块都是 512 个端口，但如果配置端口块分配规则，则使用块设置。这些块在集群中的各个节点之间均匀分配，因此每个节点都有一个或多个块对应 PAT 池中的每个 IP 地址。因此，在一个集群的 PAT 池中可以最少拥有一个 IP 地址，只要这足以支持您预期的 PAT 连接数即可。端口块覆盖的端口范围为 1024-65535，除非您在 PAT 池 NAT 规则中配置该选项以包含保留的端口 1-1023。
- 在多个规则中重复使用 PAT 池 - 要在多条规则中使用同一 PAT 池，必须注意规则中的接口选择。必须在所有规则中使用特定接口，或者在所有规则中使用“任意”接口。不能在规则中混合使用特定接口和“任意”接口，否则系统可能无法将返回流量与集群中的正确节点进行匹配。每条规则使用唯一的 PAT 池是最可靠的方案。
- 不使用轮询 - 集群不支持 PAT 池轮询。
- 无扩展 PAT - 集群不支持扩展 PAT。
- 控制节点管理的动态 NAT 转换 - 控制节点保留转换表并复制到数据节点。当数据节点收到需要动态 NAT 的连接并且转换不在表中时，它将请求从控制节点转换。数据节点拥有该连接。
- 过时 xlate - 连接所有者上的 xlate 空闲时间不会更新。因此，空闲时间值可能会超过空闲超时值。如果空闲计时器值高于配置的超时值（refcnt 为 0），则表示 xlate 过时。
- 每会话 PAT 功能 - 每会话 PAT 功能并非集群专用功能，但它能提高 PAT 的可扩展性，而且对集群而言，它允许每个数据节点成为 PAT 连接的所有者；相比之下，多会话 PAT 连接则必须转发到控制节点并由控制节点所有。默认情况下，所有 TCP 流量和 UDP DNS 流量均使用每会话 PAT 转换，而 ICMP 和所有其他 UDP 流量均使用多会话。您可以为 TCP 和 UDP 配置每会话 NAT 规则以更改这些默认设置，但是，您不能为 ICMP 配置每会话 PAT。对于使用多会话 PAT 的流量（例如 H.323、SIP 或 Skinny），您可以禁用关联 TCP 端口的每会话 PAT（这些 H.323 和 SIP 的 UDP 端口已默认为多会话）。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。
- 对以下检查不使用静态 PAT：
  - FTP
  - PPTP

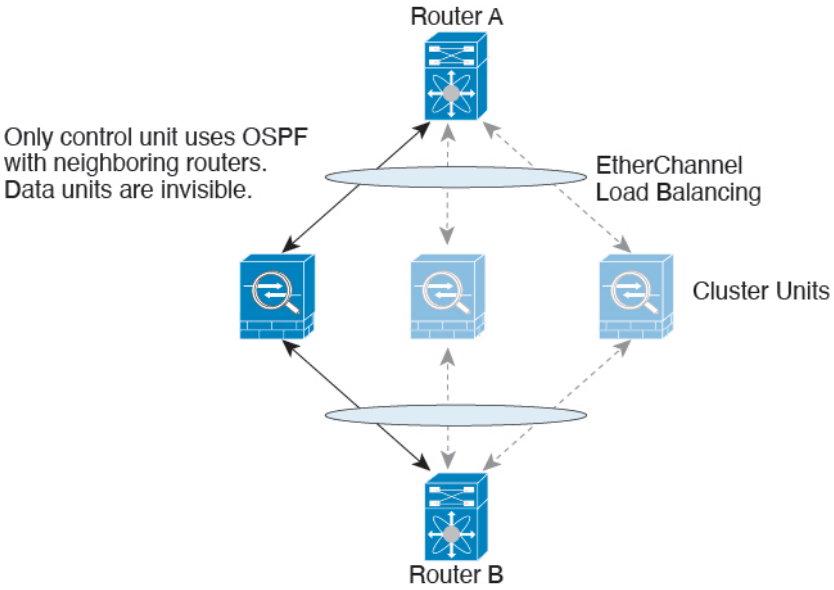
- RSH
- SQLNET
- TFTP
- XDMCP
- SIP

- 如果您有大量 NAT 规则（超过一万条），则应使用设备 CLI 中的 **asp rule-engine transactional-commit nat** 命令启用事务提交模型。否则，节点可能无法加入集群。

动态路由和集群

路由进程仅在控制单元上运行，而路由通过控制单元获知并复制到从属设备。如果路由数据包到达数据设备，它将重定向到控制设备。

图 *53:* 动态路由



在数据设备向控制设备学习路线后，每个设备将单独做出转发决策。

OSPF LSA 数据库不会从控制设备同步到数据设备。如果切换了控制设备，邻近路由器将检测到重新启动；切换是不透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。请参阅 OSPF 无间断转发功能，解决中断问题。

SCTP 和集群

SCTP 关联可以在任何节点上创建（由于负载均衡），但其多宿主连接必须位于同一节点上。

SIP 检测和集群

控制流可以在任何节点上创建（由于负载均衡），但其子数据流必须位于同一节点上。

不支持 TLS 代理配置。

SNMP 和集群

SNMP 代理按照本地 IP 地址轮询每一个ASA。您无法轮询集群的合并数据。

您应始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的控制节点时，对新控制节点的轮询将失败。

当使用 SNMPv3 进行集群时，如果您在初始集群形成后添加新的集群节点，则 SNMPv3 用户不会复制到新节点。您必须在控制节点上重新添加它们以强制用户复制到新节点，或者直接在数据节点上复制。

STUN 和集群

故障转移和集群模式支持STUN检查，因为针孔被复制。但是，节点之间不进行事务ID的复制。如果节点在收到 STUN 请求后发生故障，并且另一个节点收到 STUN 响应，则该 STUN 响应将被丢弃。

系统日志与 NetFlow 和集群

- 系统日志 - 集群中的每个节点都会生成自己的系统日志消息。您可以配置日志记录，使每个节点在系统日志消息的报头字段中使用相同或不同的设备 ID。例如，集群中的所有节点都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备 ID，则所有节点生成的系统日志消息都会看似来自一个节点。如果将日志记录配置为使用集群引导程序配置中指定的本地节点名称作为设备 ID，系统日志消息就会看似来自不同节点。
- NetFlow - 集群中的每个节点都会生成自己的 NetFlow 数据流。NetFlow 收集器只能将每台 ASA 视为单独的 NetFlow 导出器。

思科 TrustSec 和集群

只有控制节点学习安全组标记 (SGT) 信息。然后，控制节点将 SGT 填充到数据节点，数据节点可以根据安全策略对 SGT 做出匹配决策。

Cisco Secure Firewall eXtensible 操作系统 (FXOS) 机箱上的 VPN 和集群

ASA FXOS 集群支持站点间 VPN 两个相互排斥的模式之一，即集中式或分布式：

- 集中式 VPN 模式。默认模式。在集中式模式下，仅与集群的控制设备建立 VPN 连接。

  VPN 功能仅限控制设备使用，且不能利用集群的高可用性功能。如果控制设备发生故障，所有现有的 VPN 连接都将断开，通过 VPN 连接的用户将遇到服务中断。选择新的控制设备后，必须重新建立 VPN 连接。

将 VPN 隧道连接到跨接口地址时，连接会自动转移到控制设备。与 VPN 相关的密钥和证书将被复制到所有设备。

- 分布式 VPN 模式。在此模式下，站点间 IPsec IKEv2 VPN 连接将跨 ASA 集群成员分布，从而提供可扩展性。在集群成员之间分布 VPN 连接可实现充分利用集群的容量和吞吐量，将 VPN 支持大幅扩展至集中式 VPN 功能之外。

注释 集中式 VPN 集群模式支持站点间 IKEv1 和站点间 IKEv2。

分布式 VPN 集群模式仅支持站点间 IKEv2。

仅在 Firepower 9300 上支持分布式 VPN 集群模式。

集中式和分布式集群模式均不支持远程访问 VPN。

性能换算系数

将多台设备组成一个集群时，预计可以达到近似 80% 最大组合吞吐量的集群总体性能。

以 TCP 吞吐量为例，含 3 个 SM-40 模块的 Firepower 9300 在单独运行时大约可处理 135 Gbps 的实际防火墙流量。2 个机箱的最大合并吞吐量约为 270 Gbps（2 个机箱 x 135 Gbps）的 80%：216 Gbps。

控制设备选择

集群成员通过集群控制链路通信，如下选举控制设备：

1. 当您部署集群时，每台设备会每隔 3 秒广播一次选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级在您部署集群时设置且不可配置。
3. 如果某设备在 45 秒后未收到另一个具有较高优先级的设备的响应，则该设备会成为控制设备。

注释 如果多台设备并列获得最高优先级，则使用集群设备名称和序列号确定控制设备。

4. 如果节点稍后加入具有更高优先级的集群，它不会自动成为控制设备；现有控制设备始终保持为控制设备，除非它停止响应，此时会选择新的控制设备。
5. 在“裂脑”场景中，当临时存在多个控制单元时，具有最高优先级的单元将会保留角色，其他单元则恢复为数据单元角色。

注释 您可以手动强制一台设备成为控制设备。对集中功能而言，如果强制更改控制设备，则所有连接都将断开，而您必须在新的控制设备上重新建立连接。

集群中的高可用性

集群通过监控机箱、设备和接口的运行状态并在设备之间复制连接状态来提供高可用性。

机箱应用程序监控

机箱应用程序运行状况监控始终处于启用状态。Firepower 4100/9300 机箱 管理引擎会定期检查 ASA 应用程序（每秒）。如果 ASA已启动且无法与 Firepower 4100/9300 机箱管理引擎通信达到 3 秒，则 ASA会生成系统日志消息并离开集群。

如果 Firepower 4100/9300 机箱管理引擎在 45 秒后仍无法与应用程序通信，则会重新加载 ASA。如果 ASA无法与管理引擎通信，则会将自身从集群中删除。

设备运行状况监控

每台设备通过集群控制链路定期发送广播keepalive keepalive心跳数据包。如果控制节点在可配置的超时期限内未从数据节点接收任何 keepaliveheartbeat 数据包或其他数据包，则控制节点会从集群中删除该数据节点。如果数据节点未从控制节点接收数据包，则从其余节点中选择新的控制节点。

如果节点因为网络故障而不是因为节点实际故障而无法通过集群控制链路相互访问，则集群可能会进入“裂脑”场景，其中隔离的数据节点将选择自己的控制节点。例如，如果路由器在两个集群位置之间发生故障，则位于位置1的原始控制节点将从集群中删除位置2数据节点。同时，位置2的节点将选择自己的控制节点并形成自己的集群。请注意，在这种情况下，非对称流量可能会失败。恢复集群控制链路后，优先级较高的控制节点将保留控制节点的角色。有关详细信息，请参阅控制设备选择，第 506 页。

接口监控

每个节点都会监控使用中的所有硬件接口的链路状态，并向控制节点报告状态更改。对于多机箱集群，跨网络 EtherChannel 使用集群链路聚合控制协议 (cLACP)。每个机箱都会监控链路状态和 cLACP 协议消息，以确定端口在 EtherChannel 中是否仍处于活动状态，并在接口关闭时通知 ASA应用。当启用运行状况监控时，默认情况下监控有物理接口（包括 EtherChannel 接口的主 EtherChannel）。仅可监控处于开启状态的命名接口。例如，只有 EtherChannel 的所有成员端口都出现故障时，才会从集群中删除指定的 EtherChannel（取决于您的最低端口捆绑设置）。 可以选择性地禁用对每个接口的监控。

如果受监控接口在特定节点上发生故障，但在其他节点上处于活动状态，则该节点将从集群中删除。ASA在多长时间后从集群中删除节点取决于该节点是既定成员还是正在加入集群的设备。ASA 在节点加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 ASA从集群中删除。对于既定成员，节点将在 500 毫秒后删除。

对于多机箱集群，如果从集群添加或删除一个 EtherChannel，则接口运行状况监控将暂停 95 秒，以确保您有时间在每个机箱上进行更改。

修饰符应用监控

在接口上安装某种修饰符应用时，例如 Radware DefensePro 应用，ASA和该修饰符应用必须处于运行状态，以保留在集群中。只有两个应用都处于运行状态，设备才会加入集群。加入集群后，设备每 3 秒钟监控一次修饰符应用的运行状况。如果修饰符应用关闭，设备将从集群中移除。

发生故障后的状态

当集群中的节点发生故障时，该节点承载的连接将无缝转移到其他节点；流量的状态信息将通过控制节点的集群控制链路共享。

如果控制节点发生故障，则优先级最高（数字最小）的另一个集群成员将成为控制节点。

ASA将自动尝试重新加入集群，具体取决于故障事件。

注释 当ASA变成不活动状态且无法自动重新加入集群时，所有数据接口都会关闭，仅管理专用接口可以发送和接收流量。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但是，如果您重新加载而节点在集群中仍然处于非活动状态，管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

重新加入集群

当集群成员从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路在最初加入时出现故障 - 在解决集群控制链路存在的问题后，您必须通过在 ASA 端口输入 **cluster group** *name*，然后输入 **enable** 重新启用集群，以手动重新加入集群。
- 加入集群后出现故障的集群控制链路 - ASA 无限期地每 5 分钟自动尝试重新加入。此行为是可配置的。
- 出现故障的数据接口 - ASA 尝试在 5 分钟时、然后在 10 分钟时、最后在 20 分钟时重新加入。如果 20 分钟后仍加入失败，ASA 将禁用集群。解决数据接口问题之后，您必须在 ASA 控制台端口上通过输入 **cluster group** *name* 和 **enable** 来手动启用集群。此行为是可配置的。
- 设备发生故障 - 如果设备因设备运行状况检查失败而从集群中删除，则如何重新加入集群取决于失败的原因。例如，临时电源故障意味着设备会在重新启动后重新加入集群，只要集群控制链路开启即可。设备会每 5 秒尝试重新加入集群。
- 机箱应用发生通信故障 - 当 ASA 检测到机箱应用运行状况恢复后，ASA 会立即尝试重新加入集群。或者，您可以将 ASA 配置为使用与处理内部错误相同的重新加入设置（见下文）。
- 修饰器应用发生故障 - 当检测到装饰器应用备份时，ASA 会重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。 设备将尝试以下列间隔自动重新加入集群：5 分钟，10 分钟，然后是 20 分钟。此行为是可配置的。

数据路径连接状态复制

每个连接在集群中都有一个所有者和至少一个备用所有者。备用所有者在发生故障时不会接管连接；而是存储TCP/UDP状态信息，使连接在发生故障时可以无缝转移到新的所有者。备用所有者通常也是导向器。

有些流量需要 TCP 或 UDP 层以上的状态信息。请参阅下表了解支持或不支持此类流量的集群。

表 *18:* 在集群中复制的功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	-
MAC 地址表	是	-
用户标识	是	包括 AAA 规则 (uauth) 。
IPv6 邻居数据库	是	—
动态路由	是	—
SNMP 引擎 ID	否	-
适用于 Firepower 4100/9300的分布式 VPN（站点间）	是	备用会话成为主用会话，并创建一个新的备用会话。

集群管理连接的方式

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

连接角色

请参阅为每个连接定义的下列角色：

- 所有者 - 通常为最初接收连接的节点。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。如果原始所有者发生故障，则当新节点从连接接收到数据包时，导向器会从这些节点中选择新的所有者。
- 备用所有者 - 存储从所有者接收的 TCP/UDP 状态信息的节点，以便在出现故障时可以无缝地将连接转移到新的所有者。在发生故障时，备用所有者不会接管连接。如果所有者处于不可用状态，从该连接接收数据包的第一个节点（根据负载均衡而定）联系备用所有者获取相关的状态信息，以便成为新的所有者。

  只要导向器（见下文）与所有者不是同一节点，导向器也可以是备用所有者。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  对于 Firepower 9300 上的在一个机箱中包括多达 3 个集群节点的集群，如果备用所有者与所有者在同一机箱上，则将从另一个机箱中选择一个额外的备用所有者来保护流量免受机箱故障的影响。

  如果您对站点间集群启用导向器本地化，则有两个备用所有者角色：本地备用和全局备用。所有者始终选择与自身位于同一站点（基于站点 ID）的本地备用。全局备用可以位于任何站点，甚至可以与本地备用是同一个节点。所有者向两个备用所有者发送连接状态信息。

如果启用站点冗余，并且备用所有者与所有者位于同一站点，则将从另一个站点选择一个额外的备用所有者来保护流量免受站点故障的影响。机箱备份和站点备份是独立的，因此流量在某些情况将同时具有机箱备份和站点备份。

- 导向器 - 处理来自转发器的所有者查找请求的节点。当所有者收到新连接时，会根据源/目的 IP 地址和端口的散列值（有关 ICMP 散列详细信息，请参见下文）选择导向器，然后向导向器发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他节点，该节点会向导向器查询哪一个节点是所有者，以便转发数据包。一个连接只有一个导向器。如果导向器发生故障，所有者会选择一个新的导向器。

  只要导向器与所有者不是同一节点，导向器也可以是备用所有者（见上文）。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  如果您对站点间集群启用导向器本地化，则有两个导向器角色：本地导向器和全局导向器。所有者始终选择与它自身位于同一站点（基于站点 ID）的本地导向器。全局导向器可以位于任何站点，甚至可以与本地导向器是同一节点。如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者。

  ICMP/ICMPv6 散列详细信息：

  - 对于 Echo 数据包，源端口为 ICMP 标识符，目的端口为 0。
  - 对于 Reply 数据包，源端口为 0，目的端口为 ICMP 标识符。
  - 对于其他数据包，源端口和目的端口均为 0。

- 转发器 - 向所有者转发数据包的节点。如果转发者收到并非其所有的连接的数据包，则会向导向器查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向器也可以是转发者。如果启用导向器本地化，转发器将始终向本地导向器查询。如果本地导向器未获知所有者，例如，当集群成员收到所有者位于其他站点上的连接的数据包时，转发者将仅查询全局导向器。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN Cookie 直接获知所有者，因此无需向导向器查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向器查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。一个连接了可以有多个转发器；采用良好的负载均衡方法可以做到没有转发器，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。

注释 不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

当连接使用端口地址转换 (PAT) 时，PAT 类型（每会话或多会话）会对哪个集群成员将成为新连接的所有者产生影响：

- 每会话 PAT - 所有者是接收连接中的初始数据包的节点。

  默认情况下，TCP 和 DNS UDP 流量均使用每会话 PAT。

- 多会话 PAT - 所有者始终是控制节点。如果多会话 PAT 连接最初由数据节点接收，则数据节点会将连接转发给控制节点。

  默认情况下，UDP（DNS UDP 除外）和 ICMP 流量使用多会话 PAT，因此这些连接始终归控制节点所有。

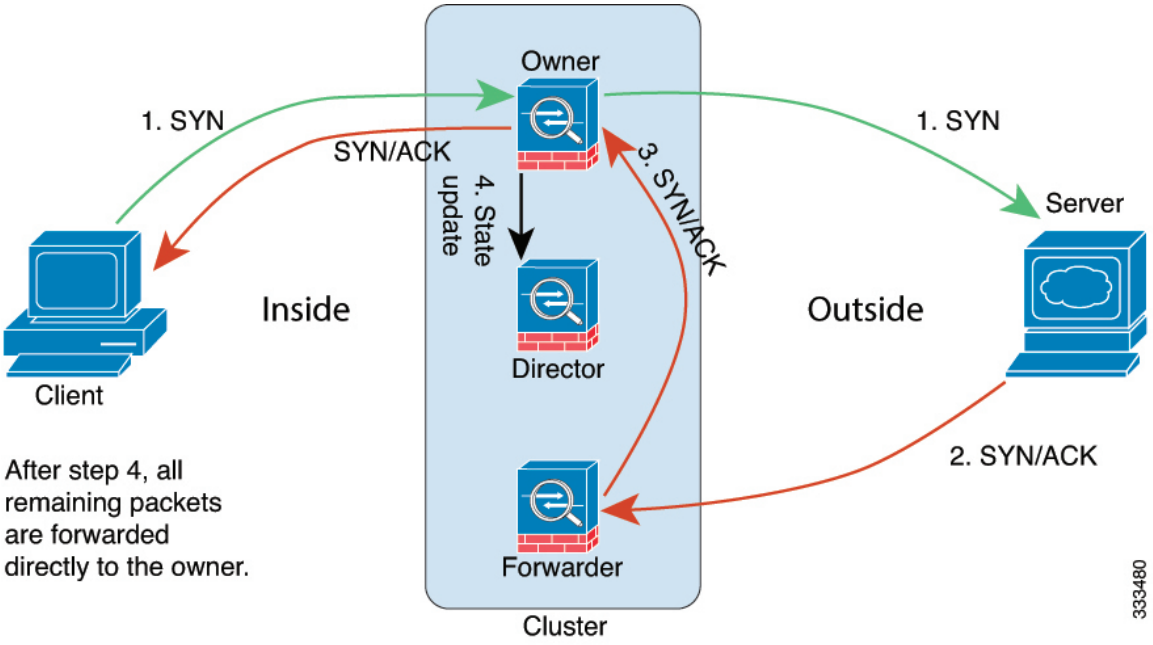
您可以更改 TCP 和 UDP 的每会话 PAT 默认设置，以便根据配置按每会话或多会话处理这些协议的连接。对于 ICMP，您不能更改默认的多会话 PAT。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。

新连接所有权

通过负载均衡将新连接定向到集群节点时，该连接的两个方向都由此节点所有。如果该连接有任何数据包到达其他节点，这些数据包都会通过集群控制链路被转发到所有者节点。如果反向流量到达其他节点，会被重定向回原始节点。

TCP 的数据流示例

以下图例显示了新连接的建立。



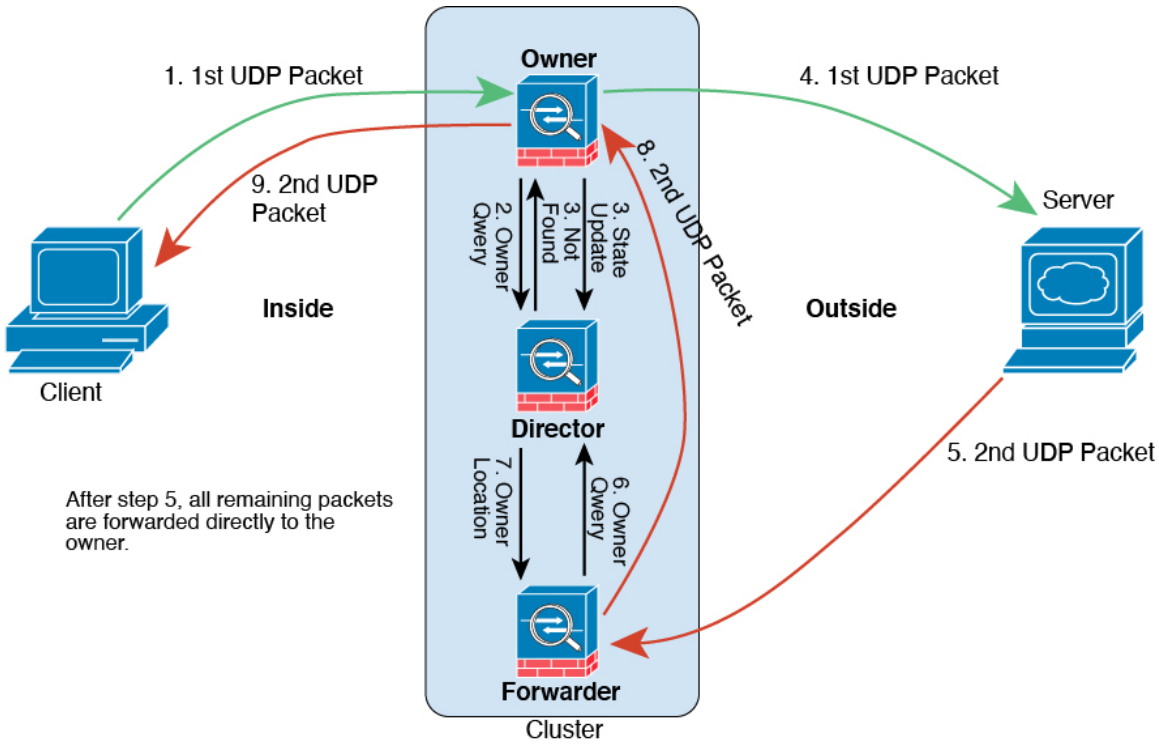
1. SYN 数据包从客户端发出，被传送到一台 ASA（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。

2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 ASA（基于负载均衡方法）。此 ASA是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，并记录TCP状态信息以及所有者。导向器将充当该连接的备用所有者。
6. 传送到转发器的任何后续数据包都会被转发到所有者。
7. 如果数据包被传送到任何其他节点，它将向导向器查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向器发送状态更新。

ICMP 和 UDP 的数据流示例

以下图例显示了新连接的建立。

1. 图 *54: ICMP* 和 *UDP* 数据流



第一个 UDP 数据包从客户端发出，被传送到一个ASA（基于负载均衡方法）。

2. 收到第一个数据包的节点查询基于源/目的 IP 地址和端口的散列值选择的导向器节点。

3. 导向器找不到现有流，创建导向器流并将数据包转发回前一个节点。换句话说，导向器已为此流选择了所有者。
4. 所有者创建流，向导向器发送状态更新，然后将数据包转发到服务器。
5. 第二个 UDP 数据包从服务器发出，并被传送到转发器。
6. 转发器向导向器查询所有权信息。对于 DNS 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。
7. 导向器向转发器回复所有权信息。
8. 转发器创建转发流以记录所有者信息，并将数据包转发给所有者。
9. 所有者将数据包转发到客户端。

跨集群实现新 TCP 连接再均衡

如果上游或下游路由器的负载平衡功能导致流量分布不平衡，则可以配置新的连接再平衡，这样每秒新连接数较高的节点就会将新 TCP 流量重定向到其他节点。现有流量将不会移至其他节点。

由于此命令仅基于每秒的连接数进行重新平衡，因此不会考虑每个节点上已建立的连接总数，并且连接总数可能并不相等。

将连接分流到其他节点后，它将成为不对称连接。

请勿为站点间拓扑结构配置连接再均衡；您不需要将新的连接再均衡到位于不同站点的集群成员。

Firepower 4100/9300上 ASA 集群的历史记录

功能名称	版本	功能信息
机箱心跳故障后重新加入集群的可配置延迟 (Firepower 4100/9300)	9.20(2)	默认情况下，如果机箱心跳失败然后恢复，则节点会立即重新加入集群。但是，如果配置 **health-check chassis-heartbeat-delay-rejoin** 命令，则它将根据 **health-check system auto-rejoin** 命令的设置重新加入。 新增/修改的命令：**health-check chassis-heartbeat-delay-rejoin**
流状态的可配置集群保持连接间隔	9.20(1)	流所有者向导向器和备份所有者发送保持连接（clu_keepalive 消息）和更新（clu_update 消息），以刷新流状态。您现在可以设置保持连接的间隔。默认值为 15 秒，您也可以将间隔设为 15 到 55 秒。您可能想将间隔设置得更长，以减少集群控制链路上的流量。 新增/修改的命令：**clu-keepalive-interval**
删除偏差语言	9.19(1)	包含术语“主”和“从”的命令、命令输出和系统日志消息已被更改为“控制”和“数据”。 新增/修改的命令：**cluster control-node**、**enable as-data-node**、**prompt**、**show cluster history**、**show cluster info**

功能名称	版本	功能信息
改进了 Firepower 4100/9300 上集群的 PAT 端口块分配	9.16（1）	改进的PAT端口块分配可确保控制设备保留端口以供加入节点，并主动回收未使用的端口。为了最好地优化分配，您可以使用 **cluster-member-limit** 命令来设置您计划在集群中拥有的最大节点数。然后，控制单元可以分配端口块到计划的节点数量，并且不必为您不打算使用的额外节点预留端口。默认值为16节点。您还可以监控系统日志747046，以确保有足够的端口可用于新节点。 新增/修改的命令：**cluster-member-limit**、**show nat pool cluster** [**summary**]、**show nat pool ip detail**
show cluster history 命令改进	9.16（1）	我们为 **show cluster history** 命令添加了其他输出。 新增/修改的命令：**show cluster history brief**、**show cluster history latest**、**show cluster history reverse**、**show cluster history time**
并行配置同步到数据设备	9.14(1)	控制设备现在默认将配置更改并行同步到数据设备。以前，同步是按顺序发生的。 新增/修改的命令：**config-replicate-parallel**
集群加入失败或逐出的消息已添加到 **show cluster history**	9.14(1)	关于集群设备无法加入集群或离开集群的新消息添加到了 **show cluster history** 命令。 新增/修改的命令：**show cluster history**
集群中的“死连接检测”(DCD) 支持的发起方和响应方信息。	9.13(1)	如果启用死连接检测(DCD)，则可以使用该**show conn detail** 命令获取有关发起人和响应方的信息。通过死连接检测，您可以保持非活动连接，并且 **show conn** 输出会告诉您终端的探测频率。此外，在集群中现在还支持 DCD。 新增/修改的命令：**show conn**（仅输出）
监控集群的流量负载	9.13(1)	现在，您可以监控集群成员的流量负载，包括总连接计数、CPU和内存使用情况以及缓冲区丢弃。如果负载过高，且剩余的设备可以处理负载，您可以选择在设备上手动禁用集群，或调整外部交换机上的负载均衡。默认情况下启用此功能。 新增/修改的命令：**debug cluster load-monitor**、**load-monitor**、**show cluster info load-monitor**
加快加入集群的速度	9.13(1)	当数据设备与控制设备具有相同的配置时，它将跳过同步配置步骤并更快加入。默认情况下启用此功能。此功能在每个设备上分别配置，不会从控制设备复制到数据设备。 注释 某些配置命令与加速集群加入不兼容;如果设备上存在这些命令，即使已启用加速集群加入，也将始终出现配置同步。您必须删除不兼容的配置，以加速集群加入工作。使用 **show cluster info unit-join-acceleration incompatible-config** 查看不兼容的配置。 新增/修改的命令： **unit join-acceleration**、**show cluster info unit-join-acceleration incompatible-config**

功能名称	版本	功能信息
适用于集群的每站点免费 ARP	9.12(1)	现在，ASA 可以生成免费 ARP (GARP) 数据包，以确保交换基础设施始终处于最新状态：它将作为每个站点优先级最高的成员，定期生成流向全局 MAC/IP 地址的 GARP 流量。当使用来自集群的各站点 MAC 和 IP 地址数据包使用站点特定的 MAC 地址和 IP 地址时，集群接收的数据包使用全局MAC地址和IP地址。如果流量不是定期从全局MAC地址生成的，您的全局 MAC 地址交换机上可能会出现 MAC 地址超时。发生超时后，以全局 MAC 地址为目标的流量将在整个交换基础设施中进行泛洪，这有可能造成性能和安全问题。当您为每台设备设置站点ID和为每个跨区以太网通道设置站点MAC地址时，默认情况下会启用 GARP。 新增/修改的命令：**site-periodic-garp interval**
设备按机箱并行加入集群	9.10(1)	对于 Firepower 9300，此功能可确保机箱中的安全模块同时加入集群，以便在模块之间均匀分配流量。如果某个模块先于其他模块很早加入，它可能会收到超过所需的流量，因为其他模块还无法分担负载。 新增/修改的命令：**unit parallel-join**
Firepower 4100/9300 的集群控制链路可自定义 IP 地址	9.10(1)	默认情况下， 集群控制链路使用 127.2.0.0/16 网络。现在，可以在 FXOS 中部署集群时设置网络。机箱根据机箱 ID 和插槽 ID 自动生成每个设备的集群控制链路接口 IP 地址：127.2.*chassis_id*.*slot_id*。但是，某些网络部署不允许 127.2.0.0/16 流量通过。因此，您现在可以为 FXOS 中的集群控制链路设置一个自定义的 /16 子网（环回 (127.0.0.0/8) 和组播 (224.0.0.0/4) 地址除外）。 新增/修改的 FXOS 命令：**set cluster-control-link network**
集群接口防反跳时间现在应用于从故障状态更改为正常运行状况的接口	9.10(1)	在发生接口状态更新时，ASA 会等待 **health-check monitor-interface debounce-time** 命令或 ASDM **配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群**菜单项中指定的毫秒数，然后才将接口标记为发生故障，并将设备从集群中删除。此功能现在应用于从故障状态更改为正常运行状态的接口。例如，对于从故障状态转换为正常运行状态的EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群上的接口仅仅因为另一个集群设备在绑定端口时的速度更快便显示为故障状态。 未修改任何命令。
内部故障后自动重新加入集群	9.9(2)	过去，许多错误条件导致集群设备从集群中移除，并且在解决问题后需要手动重新加入集群。现在，设备默认将尝试以下列时间间隔自动重新加入集群：5 分钟、10 分钟以及 20 分钟。这些值是可配置的。内部故障包括：应用程序同步超时、不一致的应用程序状态等。 新增或修改的命令：**health-check system auto-rejoin**、**show cluster info auto-join**
显示集群可靠传输协议消息的传输相关统计信息	9.9(2)	现在，您可以查看每台设备的集群可靠传输缓冲区使用情况，因此您可以确定在控制平面的缓冲区已满时发生的丢包问题。 新增或修改的命令：**show cluster info transport cp detail**

功能名称	版本	功能信息
cluster remove unit命令行为与 **no enable** 行为匹配	9.9(1)	现在，**cluster remove unit** 命令将从集群中删除一个设备，直到您手动重新启用集群或重新加载，类似于 **no enable** 命令。以前，如果从 FXOS 重新部署了引导程序配置，则集群会重新启用。现在，即使重新部署了引导程序配置，仍然保持禁用状态。但是，重新加载 ASA 将重新启用集群。 新增或修改的命令：**cluster remove unit**
改进了机箱运行状况检查故障检测	9.9(1)	现在，您可以为机箱运行状况检查配置较低的保持时间：100 毫秒。以前的最小值为 300 毫秒。请注意，最小组合时间（间隔x重试计数）不能小于 600 毫秒。 新增或修改的命令：**app-agent heartbeat interval**
站点间集群冗余	9.9(1)	站点间冗余可确保流量的备份所有者将始终位于不同于该所有者的另一站点。此功能可防范站点发生故障。 新增或修改的命令：**site-redundancy**、**show asp cluster counter change**、**show asp table cluster chash-table**、**show conn flag**
通过 Firepower 9300 上的集群支持分布式站点间 VPN	9.9(1)	Firepower 9300 上的 ASA 集群在分布式模式下支持站点间 VPN。使用分布式模式能够在 ASA 集群的成员之间分布多个站点间 IPsec IKEv2 VPN 连接，而不仅分布在控制设备上（如集中模式一样）。这将在集中式 VPN 功能的基础上大幅扩展 VPN 支持，并提供高可用性。分布式站点间 VPN 在最多由两个机箱组成的集群上运行，每个机箱最多包含三个模块（集群成员总共包含六个），每个模块最多支持 6K 个活动会话（总共 12K 个），最多支持大约 36K 个活动会话（总共 72K 个）。 新增或修改的命令：**cluster redistribute vpn-sessiondb**、**show cluster vpn-sessiondb**、**vpn mode**、**show cluster resource usage**、**show vpn-sessiondb**、**show connection detail**、**show crypto ikev2**
改进的集群设备运行状况检查故障检测	9.8(1)	现在可为设备运行状态检查配置更短的保持时间：最小值为 0.3 秒。过去的最小值为 0.8 秒。此功能可将设备运行状态检查消息传递方案从控制平面中的 *keepalives* 更改为数据平面中的 *heartbeats*。使用心跳设置可改进集群的可靠性和响应能力，使其不易受控制平面 CPU 占用和调度延迟所影响。请注意，配置较低的保持时间值会增加集群控制链路消息活动。我们建议您在配置低保持时间值之前先分析网络状况；例如，确保在保持时间/3 范围内通过集群控制链路返回从一台设备到另一台设备的 ping，因为在一个保持时间间隔内有三次心跳消息。如果在将保持时间设置为 0.3 - 0.7 后对 ASA 软件降级，则此设置将恢复为默认的 3 秒，因为新设置不受支持。 修改了以下命令：**health-check holdtime**、**show asp drop cluster counter**、**show cluster info health details**
Firepower 4100/9300 机箱可配置防反跳时间，以将接口标记为发生故障	9.8(1)	您现在可以配置 ASA 将接口视为发生故障并将设备从集群中删除之前经过的防反跳时间。此功能可以加快接口故障检测的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，ASA 会等待指定的毫秒数，然后才将接口标记为发生故障，并将设备从集群中删除。默认的防反跳时间是 500 毫秒，该时间的范围是 300 毫秒至 9 秒。 新增或修改的命令：**health-check monitor-interface debounce-time**

功能名称	版本	功能信息
Firepower 4100/9300 机箱上的 ASA 的站点间集群改进	9.7(1)	现在，您可以在部署 ASA 集群时为每个 Firepower 4100/9300 机箱配置站点 ID。以前，您必须在 ASA 应用中配置站点 ID；此新功能简化了最初的部署。请注意，您不能再在 ASA 配置中设置站点 ID。此外，为了实现与站点间集群的最佳兼容性，我们建议您升级到 ASA 9.7(1) 和 FXOS 2.1.1，升级版包含对稳定性和性能的多项改进。 修改了以下命令：**site-id**
导向器本地化：数据中心的站点间集群改进	9.7(1)	为了提高性能和将流量保存在数据中心站点间集群的某个站点内，您可以启用导向器本地化。新的连接通常实现了负载均衡，并且由特定站点中的集群成员拥有。但是，ASA 会向任意站点的成员分配导向器角色。导向器本地化支持其他导向器角色：与所有者同一站点的本地导向器和可位于任意站点的全局导向器。将所有者和导向器保留在同一站点可以提高性能。此外，如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者。当集群成员收到属于其他站点的连接的数据包时，使用全局导向器。 引入或修改了以下命令：**director-localization**、**show asp table cluster chash**、**show conn**、**show conn detail**
支持 16 个机箱 Firepower 4100 系列	9.6(2)	现在，您可以向 Firepower 4100 系列的集群中添加最多 16 个机箱。 未修改任何命令。
支持 Firepower 4100 系列	9.6(1)	使用 FXOS 1.1.4，ASA 在 Firepower 4100 系列上支持机箱间集群。 未修改任何命令。
在路由、跨区以太网通道模式下支持站点特定的 IP 地址	9.6(1)	对于使用跨区以太网通道的路由模式下的站点间集群，除了站点特定的MAC地址以外，现在还可配置站点特定的IP地址。添加站点IP地址后，允许您对重叠传输虚拟化 (OTV) 设备使用 ARP 检测来防止通过数据中心互联 (DCI) 传输的全局 MAC 地址的 ARP 响应（可能导致路由问题）。对于无法使用 VACL 来过滤 MAC 地址的某些交换机，需要使用 ARP 检测。 修改了以下命令：**mac-address**、**show interface**
16 个模块的机箱间集群，以及 Firepower 9300 ASA 应用的站点间集群	9.5(2.1)	现在您可利用 FXOS 1.1.3 启用机箱内集群，并扩展至站点间集群。最多可以包含 16 个模块。例如，您可以在 16 个机箱中使用 1 个模块，或者在 8 个机箱中使用 2 个模块，也可以使用最多提供 16 个模块的任意组合。 未修改任何命令。
在路由防火墙模式下，跨区以太网通道支持站点间集群的站点特定的 MAC 地址	9.5(2)	现在您可以在路由防火墙模式下对跨区以太网通道使用站点间集群。要避免 MAC 地址摆动，请为每个集群成员配置一个站点ID，这样就可在站点的设备间共享每个接口的站点特定 MAC 地址。 我们引入或修改了以下命令：**site-id**、**mac-address site-id**、**show cluster info**、**show interface**
自定义接口或集群控制链路发生故障时的ASA集群自动重新加入行为	9.5(2)	现在您可以自定义接口或集群控制链路发生故障时的自动重新加入行为。 我们引入了以下命令：**health-check auto-rejoin**

功能名称	版本	功能信息
ASA 集群支持 GTPv1 和 GTPv2	9.5(2)	ASA 集群现在支持 GTPv1 和 GTPv2 检测。 未修改任何命令。
TCP 连接的集群复制延迟	9.5(2)	该功能可以延迟导向器/备份流的创建，从而避免与短期流量相关的“不必要的工作”。 引入了以下命令：**cluster replication delay**
针对站点间流移动性的 LISP 检测	9.5(2)	思科定位编号分离协议 (LISP) 架构将设备身份与设备位置分离开，并分隔到两个不同的编号空间，使服务器迁移对客户端透明化。ASA 可以通过检测 LISP 流量确定位置更改，并使用此信息进行无缝集群操作；ASA 集群成员检查第一跳路由器与出口隧道路由器 (ETR) 或入口隧道路由器 (ITR) 之间的 LISP 流量，然后将流所有者位置更改为新站点。 引入或修改了以下命令：**allowed-eid**、**clear cluster info flow-mobility counters**、**clear lisp eid**、**cluster flow-mobility lisp**、**debug cluster flow-mobility**、**debug lisp eid-notify-intercept**、**flow-mobility lisp**、**inspect lisp**、**policy-map type inspect lisp**、**site-id**、**show asp table classify domain inspect-lisp**、**show cluster info flow-mobility counters**、**show conn**、**show lisp eid**、**show service-policy**、**validate-key**
现在支持在故障转移和 ASA 集群中增强运营商级 NAT	9.5(2)	对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。现在支持在故障转移和 ASA 集群部署中使用此功能。 修改了以下命令：**show local-host**
可配置级别集群跟踪条目	9.5(2)	默认情况下，所有级别的集群事件都储存在跟踪缓冲区中，包括大量低级事件。要将跟踪事件级别限制为更高级别，您可以设置集群跟踪事件的最低级别。 引入了以下命令：**trace-level**
Firepower 9300 的机箱内 ASA 集群	9.4(1.150)	最多可对 Firepower 9300 机箱内的 3 个安全模块建立集群。机箱中的所有模块都必须属于该集群。 引入了以下命令：**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis**

第 12 章

ASA 集群部署集群

通过集群，您可以将多台 ASA virtual 组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。您可以使用以下命令部署 ASA virtual 集群：

- 的 KVM
- 的 VMware

注释 仅支持路由防火墙模式。

注释 使用集群时，有些功能不受支持。请参阅集群不支持的功能，第 569 页。

- 关于 ASA Virtual 集群，第 519 页
- ASA Virtual集群的许可证，第 525 页
- ASA Virtual集群要求和前提条件，第 525 页
- ASA Virtual集群的准则，第 526 页
- 使用 Day0 配置来配置 ASA Virtual集群，第 527 页
- 部署后配置 ASA Virtual 集群，第 530 页
- 自定义集群操作，第 542 页
- 管理集群节点，第 552 页
- 监控 ASA Virtual集群，第 557 页
- ASA Virtual集群示例，第 568 页
- 集群参考，第 569 页
- ASA Virtual集群的历史记录，第 583 页

关于 ASA Virtual 集群

本节介绍集群架构及其工作原理。

集群如何融入网络中

集群包含多台防火墙，作为单一设备工作。要用作集群，该防火墙需要以下基础设施：

- 独立的网络（称为集群控制链路），通过 VXLAN 接口用于集群内的通信。VXLAN 充当第 3 层物理网络上的第 2 层虚拟网络，让 ASA virtual 能够通过集群控制链路发送广播/组播消息。
- 对每台防火墙的管理访问权限，用于进行配置和监控。ASA virtual 部署包括用于管理集群节点的 Management 0/0 接口。

将集群接入网络中时，上游和下游路由器需要能够使用第 3 层单独接口和以下方法之一使出入集群的数据实现负载均衡：

- 策略型路由 - 上游和下游路由器使用路由映射和 ACL 在节点之间执行负载均衡。
- 等价多路径路由 - 上游和下游路由器使用等价静态或动态路由在节点之间执行负载均衡。

注释 不支持第 2 层跨区以太网通道。

集群节点

集群节点协调工作来实现安全策略和流量的共享。本节介绍每种节点角色的性质。

引导程序配置

您要在每台设备上配置最低的引导程序配置，包括集群名称、集群控制链路接口和其他集群设置。启用集群的第一个节点通常成为控制节点。在后续节点上启用集群时，这些设备将作为数据节点加入集群。

控制和数据节点角色

一个集群成员是控制节点。如果多个集群节点同时上线，则控制节点由引导程序配置中的优先级设置决定；优先级可设置为 1 到 100，其中 1 为最高优先级。所有其他成员都是数据节点。 通常，当您首次创建集群时，您添加的第一个节点会成为控制节点，因为它是到目前为止集群中的唯一节点。

必须只能在控制节点上执行所有配置（引导程序配置除外）；然后配置将被复制到数据节点中。如果是接口等物理资产，控制节点的配置将被镜像到所有数据节点。例如，如果将以太网接口 1/2 配置为内部接口，将以太网接口 1/1 配置为外部接口，则这些接口也将在数据节点上用作内部和外部接口。

有些功能在集群中无法扩展，控制节点将处理这些功能的所有流量。

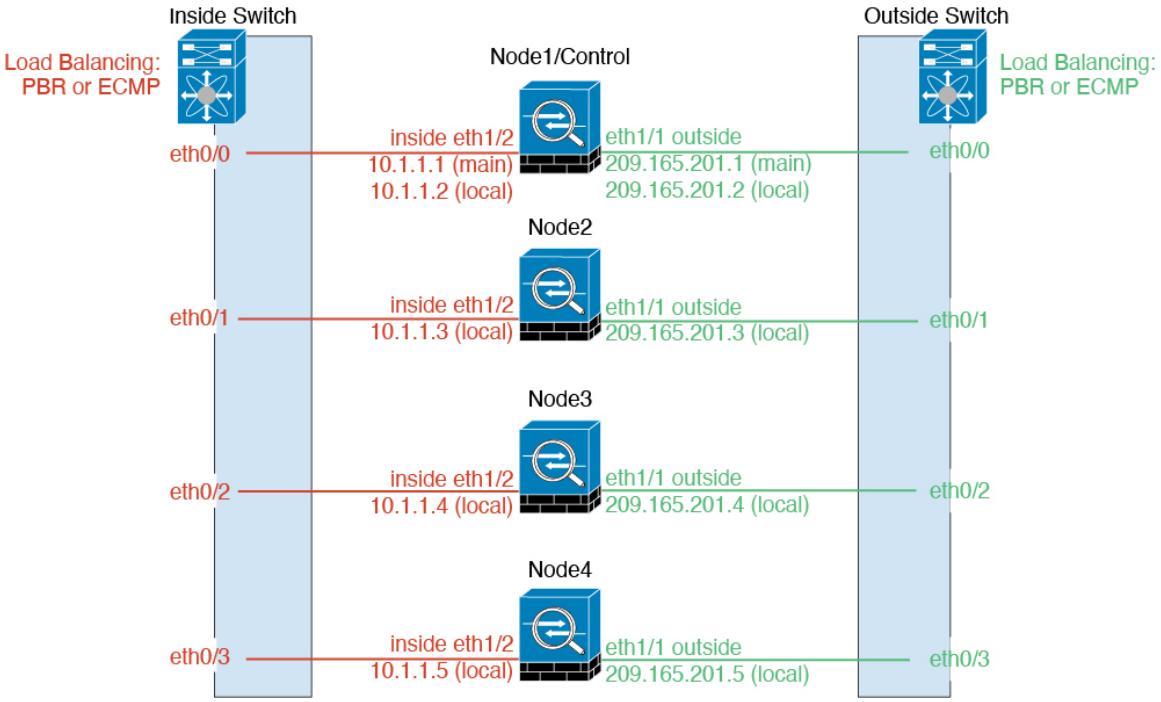
独立接口

您可以将集群接口配置为独立接口。

独立接口是正常的路由接口，每个接口都有自己的 本地 *IP* 地址 用于路由。每个接口的 主集群 *IP* 地址 是固定地址，始终属于控制节点。当控制节点更改时，主集群IP地址将转移到新的控制节点，使集群的管理得以无缝继续。

由于接口配置只能在控制节点上配置，因此您可以通过接口配置设置一个IP地址池，供集群节点上的给定接口（包括控制节点上的一个接口）使用。

必须在上游交换机上分别配置负载均衡。



注释 不支持第 2 层跨区以太网通道。

基于策略的路由

使用独立接口时，每个 ASA 接口都会保留自己的 IP 地址和 MAC 地址。基于策略的路由 (PBR) 是一种负载均衡方法。

如果已经在使用 PBR 并希望充分利用现有的基础设施，我们建议使用此方法。

PBR 根据路由映射和 ACL 作出路由决定。您必须在集群中的所有 ASA 之间手动划分流量。由于 PBR 是静态路由，因此可能有时候无法实现最佳的负载均衡效果。为了获得最佳性能，建议您配置 PBR 策略，以便连接的转发数据包和返回数据包定向到同一个 ASA。例如，如果您有一台思科路由器，使用带对象跟踪的思科 IOS PBR 即可实现冗余。思科 IOS 对象跟踪使用 ICMP ping 监控每台 ASA。然后，PBR可根据特定ASA的可访问性来启用或禁用路由映射。有关详细信息，请参阅以下 URL：

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

同等成本的多路径路由

使用独立接口时，每个 ASA 接口都会保留自己的 IP 地址和 MAC 地址。等价多路径 (ECMP) 路由是一种负载均衡方法。

如果已经在使用 ECMP 并希望充分利用现有的基础设施，我们建议使用此方法。

ECMP 路由可以通过路由指标并列最优的多条“最佳路径”转发数据包。它与 EtherChannel 一样，也可以使用源和目标 IP 地址及/或源和目标端口的散列值将数据包发送到下一跃点。如果将静态路由用于 ECMP 路由，则 ASA 故障会导致问题；如果继续使用该路由，发往故障 ASA 的流量将丢失。因此，如果使用静态路由，请务必要使用静态路由监控功能，例如对象跟踪。我们还建议使用动态路由协议来添加和删除路由，在这种情况下，您必须配置每台 ASA 使之加入动态路由。

集群控制链路

每个节点必须将一个接口作为集群控制链路的 VXLAN (VTEP) 接口。 有关 VXLAN 的详细信息，请参阅VXLAN 接口 ， 第 719 页。

VXLAN 隧道端点

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

VTEP 源接口

VTEP 源接口是一个计划要将其与 VNI 接口相关联的常规ASA virtual 接口。您可以将一个 VTEP 源接口配置为集群控制链路。源接口会被保留，以便仅供集群控制链路使用。每个 VTEP 源接口在同一子网上都有一个 IP 地址。此子网应与所有其他流量隔离，并且只包括集群控制链路接口。

VNI 接口

VNI 接口类似于 VLAN 接口：它是一个虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。您只能配置一个 VNI 接口。每个 VNI 接口在同一子网上都有一个 IP 地址。

对等体 VTEP

与数据接口的常规 VXLAN 只允许单个 VTEP 对等体不同，ASA virtual 集群允许您配置多个对等体。

集群控制链路流量概述

集群控制链路流量包括控制流量和数据流量。

控制流量包括：

- 控制节点选举。
- 配置复制。

- 运行状况监控。

数据流量包括：

- 状态复制。
- 连接所有权查询和数据包转发。

集群控制链路故障

如果某台设备的集群控制链路线路协议关闭，则集群将被禁用；数据接口关闭。当您修复集群控制链路之后，必须通过重新启用集群来手动重新加入集群。

注释 当 ASA virtual 处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。管理接口将保持打开，使用设备从 DHCP 或集群 IP 池接收的 IP 地址。如果使用集群 IP池，在重新加载而设备在集群中仍然处于非活动状态时，则管理接口将无法访问（因为它届时将使用与控制节点相同的主 IP 地址）。您必须使用控制台端口（如果可用）来进行任何进一步配置。

配置复制

集群中的所有节点共享一个配置。您只能在控制节点上进行配置更改（引导程序配置除外），这些更改会自动同步到集群中的所有其他节点。

ASA Virtual集群管理

使用 ASA virtual集群的一个好处可以简化管理。本节介绍如何管理集群。

管理网络

我们建议将所有节点都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理接口

使用 Management 0/0 接口进行管理。

注释 您不能为管理接口启用动态路由。您必须使用静态路由。

您可以使用静态寻址或 DHCP 作为管理 IP 地址。

如果您使用静态寻址，则可以使用集群的主集群 IP 地址是集群的固定地址，而该集群始终属于当前的控制节点。您还要为每个接口配置一个地址范围，以便包括当前控制节点在内的每个节点都可以使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问；当控制节点更改时，主集群 IP 地址将转移到新的控制节点，使集群的管理得以无缝继续。本地 IP 地址用于路由，在排除故障时

也非常有用。例如，您可以连接到主集群 IP 地址来管理集群，该地址始终属于当前的控制节点。要管理单个成员，您可以连接到本地 IP 地址。对于 TFTP 或系统日志等出站管理流量，包括控制节点在内的每个节点都使用本地 IP 地址连接到服务器。

如果使用 DHCP，则不使用本地地址池或主集群 IP 地址。

注释 传入设备的流量必须指向节点的管理 IP 地址；传入设备的流量不会通过群集控制链路转发到任何其他节点。

控制节点管理与数据节点管理

所有管理和监控均可在控制节点上进行。从控制节点中，您可以检查所有节点的运行时统计信息、资源使用情况或其他监控信息。您也可以向集群中的所有节点发出命令，并将控制台消息从数据节点复制到控制节点。

如果需要，您可以直接监控数据节点。虽然在控制节点上可以执行文件管理，但在数据节点上也可以如此（包括备份配置和更新映像）。以下功能在控制节点上不可用：

- 监控每个节点的集群特定统计信息。
- 监控每个节点的系统日志（控制台复制启用时发送至控制台的系统日志除外）。
- SNMP
- NetFlow

加密密钥复制

当您在控制节点上创建加密密钥时，该密钥将复制到所有数据节点。如果您有连接到主集群 IP 地址的 SSH 会话，则控制节点发生故障时连接将断开。新控制节点对 SSH 连接使用相同的密钥，这样当您重新连接到新的控制节点时，无需更新缓存的 SSH 主机密钥。

ASDM 连接证书 IP 地址不匹配

默认情况下，ASDM 连接将根据本地 IP 地址使用自签名证书。如果使用 ASDM 连接到主集群 IP 地址，则可能会因证书使用的是本地 IP 地址而不是主集群 IP 地址，系统会显示一则警告消息，指出 IP 地址不匹配。您可以忽略该消息并建立 ASDM 连接。但是，为了避免此类警告，您也可以注册一个包含主集群 IP 地址和 IP 地址池中所有本地 IP 地址的证书。然后，您可将此证书用于每个集群成员。有关详细信息，请参阅 https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html。

站点间集群

对于站点间安装，您只要遵循建议的准则即可充分发挥 ASA virtual 集群的作用。

您可以将每个集群机箱配置为属于单独的站点 ID。站点 ID 用于使用 LISP 检查、导向器本地化来实现流量移动，以提高性能、减少数据中心的站点间集群的往返时间延迟以及连接的站点冗余，其中流量流的备用所有者始终位于与所有者不同的站点上。

有关站点间集群的详细信息，请参阅以下各节：

- 调整数据中心互联的规模 - ASA Virtual集群要求和前提条件，第 525 页
- 站点间准则 - ASA Virtual集群的准则，第 526 页
- 配置集群流移动性 -配置集群流移动性，第 548 页
- 启用导向器本地化 - 启用导向器本地化，第 547 页
- 启用站点冗余 - 启用导向器本地化，第 547 页
- 站点间示例：独立接口路由模式南北站点间集群示例，第 568 页

ASA Virtual集群的许可证

每个集群节点都需要相同的模型许可证。我们建议为所有节点使用相同数量的CPU和内存，否则将限制所有节点上的性能，以匹配功能最低的成员。吞吐量级别将从控制节点复制到每个数据节点，以便它们匹配。

注释 如果取消注册 ASA virtual 从而使得其未经许可，则在重新加载 ASA virtual 后，它将恢复到严格的速率限制状态。未经许可的低性能集群节点将对整个集群的性能产生负面影响。请务必保留所有集群节点的许可，或删除任何未经许可的节点。

ASA Virtual集群要求和前提条件

型号要求

- ASAv30, ASAv50, ASAv100
- 下列私有云服务：
  - 的 KVM
  - 的 VMware
- 在 2x8 部署配置中，两个主机上的集群最多有 16 个节点。我们建议您在两台主机 (2x8) 上各部署最多八个 ASAv，从而形成一个包含 16 个节点的集群。

ASA Virtual 支持的平台及软件要求

集群中的所有节点：

- 必须是相同型号。我们建议对所有节点都使用相同数量的CPU和内存，否则所有节点上的性能将受到限制，以匹配性能最低的节点。
- 除在映像升级时以外，必须运行完全相同的软件。支持无中断升级。不匹配的软件版本可能会导致性能不佳，因此请务必在同一维护窗口中升级所有节点。
- 在配置复制之前，新的集群成员对初始集群控制链路通信必须使用与控制节点相同的 SSL 加密设置（**ssl encryption** 命令）。

ASA Virtual集群的准则

故障转移

集群不支持故障转移。

IPv6

集群控制链路只有在使用 IPv4 时才受支持。

其他准则

- 当拓扑发生重大更改时（例如启用或禁用ASA或交换机上的接口、添加额外的交换机形成VSS或 vPC），您应禁用运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用接口运行状况检查功能。
- 将节点添加到现有集群时或重新加载节点时，会有限地暂时丢弃数据包/断开连接；这是预期的行为。有些时候，丢弃的数据包会挂起连接；例如，丢弃FTP连接的FIN/ACK数据包将使FTP客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 我们不支持数据接口的 VXLAN；只有集群控制链路支持 VXLAN。
- 将更改复制到集群中的所有节点需要时间。如果进行较大的更改，例如，添加使用对象组的访问控制规则（在部署时会拆分为多个规则），完成更改所需的时间可能会超过集群节点响应的超时时间与成功消息。如果发生这种情况，您可能会看到“无法复制命令”消息。您可以忽略此消息。

ASA Virtual 集群默认设置

- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。
- 用于发生故障的集群控制链路的集群自动重新加入功能为每 5 分钟尝试无限次。
- 用于发生故障的数据接口的集群自动重新加入功能为每 5 分钟尝试 3 次，增量间隔设置为 2。

- 默认情况下，连接再均衡处于禁用状态。如果启用连接再均衡，交换负载信息的默认间隔时间为 5 秒。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

使用 Day0 配置来配置 ASA Virtual集群

控制节点 Day0 配置

控制节点的以下Day0配置包括了引导程序配置，后面是将被复制到数据节点的接口配置。粗体文本显示了您需要为数据节点 Day0 配置更改的值。

注释 此配置仅包括以集群为中心的配置。Day0配置还应包括许可、SSH访问、ASDM访问等其他设置。有关 Day0 配置的详细信息，请参阅入门指南。

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
network-object host 10.6.6.53
network-object host 10.6.6.54
!
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
security-level 0
ip address 10.6.6.51 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
```

```
peer-group cluster-peers
!
! Management Interface Using DHCP
interface management 0/0
nameif management
ip address dhcp setroute
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
local-unit A
cluster-interface vni1 ip 10.2.2.1 255.255.255.0
priority 1
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
!
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

数据节点 Day 0 配置

数据节点的以下 Day0 配置仅包括引导程序配置。粗体文本显示您需要在控制节点 Day0 配置中更改的值。

注释 此配置仅包括以集群为中心的配置。Day0 配置还应包括许可、SSH 访问、ASDM 访问等其他设置。有关 Day0 配置的详细信息，请参阅入门指南。

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
network-object host 10.6.6.53
network-object host 10.6.6.54
```

```
!
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
security-level 0
ip address 10.6.6.52 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
peer-group cluster-peers
!
! Management Interface Using DHCP
interface management 0/0
nameif management
ip address dhcp setroute
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
local-unit B
cluster-interface vni1 ip 10.2.2.2 255.255.255.0
priority 2
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
```

```
!
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

部署后配置 ASA Virtual 集群

要在部署 ASA virtual 后配置集群，请执行以下任务。

配置接口设置

在每个节点上配置集群接口模式，以及在控制节点上配置接口。当数据节点加入集群时，接口配置将被复制到数据节点。请注意，集群控制链路在引导程序配置过程中进行配置。

在每个节点上配置集群接口模式

在启用集群之前，您需要将防火墙转换为使用独立接口。由于集群会限制您可以使用的接口类型，因此此过程允许您检查现有配置中是否存在不兼容的接口，然后阻止配置任何不受支持的接口。

开始之前

- 您必须在要添加到集群中的每台 ASA virtual 上分别设置模式。
- 使用控制台端口（如果可用）或 SSH（如果已配置）连接到 ASA virtual CLI。如果这些选项都不可用，则可以使用 ASDM 配置集群。

过程

步骤 1 显示任何不兼容的配置，以便稍后强制设置接口模式并修复配置；该模式不会随以下命令而更改：

cluster interface-mode individual check-details

示例：

```
ciscoasa(config)# cluster interface-mode individual check-details
```

注意
设置接口模式之后，您可以使用 SSH 继续连接到接口；但是，如果您在配置管理接口使其符合集群要求（例如添加集群 IP 池或从 DHCP 获取 IP 地址）之前重新加载 ASA，则将无法重新连接，因为与集群不兼容的接口配置已删除。在此情况下，您必须连接到控制台端口（如果可用）来修复接口配置。

步骤 2 为集群设置接口模式：

cluster interface-mode individual force

示例：

```
ciscoasa(config)# cluster interface-mode individual force
```

不存在默认设置；您必须明确选择模式。如果尚未设置模式，则无法启用集群。

force 选项可直接更改模式而无需检查配置中是否存在不兼容的设置。更改模式后，您需要手动修复任何配置问题。由于任何接口配置都只能在设置完模式后修复，因此我们建议使用 **force** 选项，这样您至少可以从现有配置着手。设置模式后，您可以重新运行 **check-details** 选项来获得更多参考信息。

如果不使用 **force** 选项，当存在任何不兼容的配置时，系统将提示您清除配置并重新加载，从而需要您连接到控制台端口（如果可用）来重新配置管理访问。如果您的配置兼容（极为罕见），则会更改模式并保留配置。如果您不想清除配置，则可以键入 **n** 退出命令。

要删除接口模式，请输入 **no cluster interface-mode** 命令。

配置独立接口

启用集群之前，您必须修改所有当前配置了 IP 地址的接口，使其准备好加入集群。在使用静态 IP 地址进行管理时，您可能至少需要修改 SSH 当前连接到的管理接口。至于其他接口，您可以在启用集群之前或之后配置；我们建议预配置所有接口，以便将完整的配置同步到新的集群节点。

本节介绍如何将接口配置为与集群兼容的独立接口。独立接口是正常的路由接口，每个接口都从 IP 地址池获取自己的 IP 地址。集群的主集群 IP 地址是集群的固定地址，始终属于当前的控制节点。所有数据接口都必须是独立接口。

对于管理接口，您可以配置 IP 地址池，也可以使用 DHCP；只有管理接口支持从 DHCP 获取地址。要使用 DHCP，请勿使用此程序；而是照常配置（请参阅配置常规路由模式接口参数，第 753 页）。

开始之前

- （可选）配置子接口。
- 对于管理接口，您可以使用静态地址，也可以使用 DHCP。如果使用静态 IP 地址并使用 SSH 远程连接到管理接口，则未来数据节点的当前 IP 地址仅供临时使用。
  - 每个成员都将从控制节点上定义的集群 IP 池中分配到一个 IP 地址。
  - 集群 IP 池不能包含网络中已在使用的地址，包括未来辅助设备的 IP 地址。

    例如：

    1. 将控制节点配置为使用 10.1.1.1。
    2. 其他节点使用 10.1.1.2、10.1.1.3 和 10.1.1.4。
    3. 在控制节点上配置集群 IP 池时，不能在地址池中包含地址 .2、.3 或 .4，因其已在使用中。
    4. 反之，您需要使用该网络中的其他 IP 地址，如 .5、.6、.7 和 .8。

注释 地址池需要的地址数量与包括控制节点在内的集群成员数相等；原始.1地址是属于当前控制节点的主集群 IP 地址。

5. 加入集群之后，临时使用的旧地址将被弃用并可用于它处。

过程

步骤 1 配置本地 IP 地址池（IPv4 和/或 IPv6），其中一个地址将被分配到每个集群节点作为接口地址：

(IPv4)

ip local pool *poolname first-address* — *last-address* [**mask** *mask*]

(IPv6)

ipv6 local pool *poolname ipv6-address*/*prefix-length number_of_addresses*

示例：

```
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8:45:1003/64 8
```

至少包含与集群中的节点数量相同的地址。如果计划扩展集群，则应包含更多地址。属于当前控制节点的主集群 IP 地址不在此地址池中；请务必在同一个网络中为主集群 IP 地址保留一个 IP 地址。

您无法预先确定分配到每个节点的确切本地地址；要查看每个节点上使用的地址，请输入**show ip**[**v6**] **local pool** *poolname* 命令。每个集群成员在加入集群时都会分配到一个成员 ID。此 ID 决定了所用的来自地址池中的本地 IP。

步骤 2 进入接口配置模式：

interface *interface_id*

示例：

```
ciscoasa(config)# interface gigabitethernet 0/1
```

步骤 3 为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。

步骤 4 设置主集群 IP 地址并确定集群池：

(IPv4)

ip address *ip_address* [*mask*] **cluster-pool** *poolname*

(IPv6)

ipv6 address *ipv6-address*/*prefix-length* **cluster-pool** *poolname*

示例：

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8:45:1003::99/64 cluster-pool insipv6
```

此 IP 地址必须与集群池地址属于同一个网络，但不在地址池中。您可以配置 IPv4 和/或 IPv6 地址。

不支持 DHCP、PPPoE 和 IPv6 自动配置；您必须手动配置 IP 地址。也不支持手动配置链路本地地址。

步骤 5 设置安全级别，其中 *number* 为 0（最低）到 100（最高）之间的整数：

security-level 编号

示例：

```
ciscoasa(config-if)# security-level 100
```

步骤 6 启用接口：

no shutdown

示例

以下是将管理接口 0/0、千兆以太网接口 0/0 和千兆以太网接口 0/1 配置为独立接口的示例：

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface management 0/0
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8:45:1001::99/64 cluster-pool mgmtipv6
security-level 100
no shutdown

ip local pool out 209.165.200.225-209.165.200.232
ipv6 local pool outipv6 2001:DB8:45:1002/64 8

interface gigabitethernet 0/0
nameif outside
ip address 209.165.200.233 255.255.255.224 cluster-pool out
ipv6 address 2001:DB8:45:1002::99/64 cluster-pool outipv6
security-level 0
no shutdown
```

```
ip local pool ins 192.168.1.2-192.168.1.9
ipv6 local pool insipv6 2001:DB8:45:1003/64 8

interface gigabitethernet 0/1
nameif inside
ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ipv6 address 2001:DB8:45:1003::99/64 cluster-pool insipv6
security-level 100
no shutdown
```

创建引导程序配置

集群中的每个节点都需要有引导程序配置才能加入集群。

配置控制节点引导程序设置

集群中的每个节点都需要有引导程序配置才能加入集群。通常，您配置为加入集群的第一个节点将是控制节点。启用集群后，集群会在选举时间结束后选举出一个控制节点。最初只有一个节点在集群中，该节点将成为控制节点。添加到集群的后续节点将是数据节点。

开始之前

- 请备份配置，以防稍后要退出集群而需要恢复配置。
- 除集群控制链路和管理接口（它可以选择使用 DHCP）外，配置中的任何接口都必须使用集群 IP 池进行配置，然后才能启用集群。如果有以前就存在的接口配置，您可以清除该接口配置 (**clear configure interface**)，也可以将接口转换为集群接口后再启用集群。
- 将节点添加到正在运行的集群时，可能会有限地暂时丢弃数据包/断开连接；这是预期行为。
- 启用巨集帧预留以用于集群控制链路，以便您可以将集群控制链路MTU设置为建议值。请参阅 **jumbo-frame reservation** 命令。启用巨帧会导致 ASA 重新加载，因此您必须在继续此程序之前执行此步骤。

过程

步骤 1 加入集群之前，为集群控制链路接口配置一个 VXLAN 接口。

稍后，您要在启用集群时将此接口确定为集群控制链路。

集群控制链路接口配置不会从控制节点复制到数据节点；但是，必须在每个节点上使用相同的配置。由于此配置不会复制，您必须在每个节点上分别配置集群控制链路接口。

a) 通过创建网络对象组来识别 VTEP 对等体 IP 地址。

有关网络对象组的详细信息，请参阅 ASA 防火墙配置指南中的“访问控制对象”一章。

VTEP 之间的基础 IP 网络独立于 VNI 接口使用的集群控制链路网络。每个 VTEP 源接口在同一子网上都有一个 IP 地址。此子网应与所有其他流量隔离，并且只包括集群控制链路接口。

示例：

以下是使用内联定义的主机来创建网络对象组的示例：

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object host 10.6.6.51
ciscoasa(network-object-group)# network-object host 10.6.6.52
ciscoasa(network-object-group)# network-object host 10.6.6.53
ciscoasa(network-object-group)# network-object host 10.6.6.54
```

以下是创建引用独立网络对象的网络对象组的示例：

```
ciscoasa(config)# object network xyz
ciscoasa(config-network-object)# range 10.6.6.51 10.6.6.54

ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object object xyz
```

b) 配置 VTEP 源接口。

interface *interface_id*

nve-only cluster

nameif *name*

ip address *ip_address subnet_mask*

no shutdown

IP 地址应作为对等体之一包含在网络对象组中。

示例：

```
ciscoasa(config)# interface gigabitethernet 0/7
ciscoasa(config-if)# nve-only cluster
ciscoasa(config-if)# nameif ccl
ciscoasa(config-if)# ip address 10.6.6.51 255.255.255.0
ciscoasa(config-if)# no shutdown
```

c) 将 VTEP 源接口与 NVE 实例相关联。

nve 1

source-interface *interface-name*

peer-group *network_object_name*

只能指定一个 NVE 实例，其中 ID 为 1。

默认情况下，系统会为 NVE 实例添加 **encapsulation vxlan** 命令；无需显式添加该命令。

示例：

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface ccl
ciscoasa(cfg-nve)# peer-group cluster-peers
```

d) 指定 VTEP 接口的最大传输单位至少比数据接口的最高 MTU 高 154 字节。

mtu *interface_name bytes*

由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销（100 字节）和 VXLAN 开销（54 字节）。将 MTU 设置为介于 1554 和 9198 字节之间的，但不在 2561 和 8362 字节之间。由于块池处理，此 MTU 大小不是系统运行的最佳值。默认 MTU 为 1554 字节。当数据接口设置为 1500 时，我们建议将集群控制链路 MTU 设置为 1654；此值需要巨帧预留（请参阅 **jumbo-frame reservation** 命令）。

例如，在使用巨帧时，由于最大 MTU 为 9198 字节，因此最高的数据接口 MTU 可以是 9044，而集群控制链路则可以设置为 9198。

此命令会被复制到数据节点，但我们建议您将此设置与引导程序设置一起配置。

示例：

```
ciscoasa(config)# mtu ccl 1654
```

e) （可选） 设置 VXLAN UDP 端口。

vxlan 端口号

默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。如果网络使用非标准端口，可以对其进行更改。

示例：

```
ciscoasa(config)# vxlan port 5678
```

f) 创建 VNI 接口。

interface vni *vni_num*

segment-id *id*

vtep-nve 1

示例：

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
```

- 将 VNI 数字设置为 1 和 10000 之间的值。此 ID 仅为内部接口标识符。
- 将网段 ID 设置为 1 和 16777215 之间的值。网段 ID 用于 VXLAN 标记。

不要为接口配置名称或任何其他参数。

步骤 2 为集群命名并进入集群配置模式：

cluster group 名称

示例：

```
ciscoasa(config)# cluster group pod1
```

名称必须是长度为 1 到 38 个字符的 ASCII 字符串。每个节点只能配置一个集群组。集群的所有成员必须使用同一名称。

步骤 3 为此集群成员命名：

local-unit *node_name*

使用唯一的 ASCII 字符串，长度必须为 1 到 38 个字符。每个节点必须具有唯一的名称。集群中不允许存在名称重复的节点。

示例：

```
ciscoasa(cfg-cluster)# local-unit node1
```

步骤 4 指定集群控制链路 VNI 接口：

cluster-interface *vni_interface_id* **ip** *ip_address mask*

示例：

```
ciscoasa(cfg-cluster)# cluster-interface vni1 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on VNI1
```

指定 IP 地址的 IPv4 地址；此接口不支持 IPv6。对于每个节点，在同一网络上指定不同的 IP 地址。VNI 网络是在物理 VTEP 网络上运行的加密虚拟网络。

步骤 5 设置控制节点选择的此节点的优先级：

priority *priority_number*

示例：

```
ciscoasa(cfg-cluster)# priority 1
```

优先级的值为 1 到 100，其中 1 为最高优先级。

步骤 6 （可选）设置身份验证密钥以便控制集群控制链路上的流量：

key *shared_secret*

示例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

共享密钥是长度介于 1 和 63 个字符之间的 ASCII 字符串。共享密钥用于生成密钥。此命令不会影响数据路径流量，包括始终以明文发送的连接状态更新和转发数据包。

步骤 7 启用集群：

enable [**noconfirm**]

示例：

```
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands? [Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

输入 **enable** 命令时，ASA 将扫描正在运行的配置，查找集群不支持的功能的不兼容命令，包括默认配置中可能存在的命令。系统会提示您删除不兼容命令。如果您选择 **No**，则不会启用集群。使用 **noconfirm** 关键字可绕过确认步骤并自动删除不兼容命令。

对于启用的第一个节点，会进行控制节点选择。由于到目前为止第一个节点应该是集群的唯一成员，因此它将成为控制节点。请勿在此期间执行任何配置更改。

要禁用集群，请输入 **no enable** 命令。

注释
如果禁用集群，所有数据接口将关闭，只有管理接口会处于活动状态。

示例

以下是首先配置管理接口，内部和外部接口以及 VXLAN 集群控制链路，然后再为名为“node1”的 ASA 启用集群，由于该设备是第一台添加到集群的设备，因此将成为控制节点。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8:45:1001::99/64 cluster-pool mgmtipv6
    security-level 100
    no shutdown

ip local pool out 209.165.200.225-209.165.200.232
ipv6 local pool outipv6 2001:DB8:45:1002/64 8

interface gigabitethernet 0/0
    nameif outside
    ip address 209.165.200.233 255.255.255.224 cluster-pool out
    ipv6 address 2001:DB8:45:1002::99/64 cluster-pool outipv6
    security-level 0
    no shutdown
```

```
ip local pool ins 192.168.1.2-192.168.1.9
ipv6 local pool insipv6 2001:DB8:45:1003/64 8

interface gigabitethernet 0/1
    nameif inside
    ip address 192.168.1.1 255.255.255.0 cluster-pool ins
    ipv6 address 2001:DB8:45:1003::99/64 cluster-pool insipv6
    security-level 100
    no shutdown

object-group network cluster-peers
    network-object host 10.6.6.51
    network-object host 10.6.6.52
    network-object host 10.6.6.53
    network-object host 10.6.6.54

interface gigabitethernet 0/7
    nve-only cluster
    nameif ccl
    ip address 10.6.6.51 255.255.255.0
    no shutdown

nve 1
    source-interface ccl
    peer-group cluster-peers

mtu ccl 1654

interface vni 1
    segment-id 1000
    vtep-nve 1

cluster group pod1
    local-unit node1
    cluster-interface vni1 ip 192.168.1.1 255.255.255.0
    priority 1
    key 67impala
    enable noconfirm
```

配置数据节点引导程序设置

执行以下程序配置数据节点。

开始之前

- 请备份配置，以防稍后要退出集群而需要恢复配置。
- 除集群控制链路和管理接口（它可以选择使用 DHCP）外，配置中的任何接口都必须使用集群 IP 池进行配置，然后才能启用集群。如果有以前就存在的接口配置，您可以清除该接口配置 (**clear configure interface**)，也可以将接口转换为集群接口后再启用集群。
- 将节点添加到正在运行的集群时，可能会有限地暂时丢弃数据包/断开连接；这是预期行为。
- 启用巨集帧预留以用于集群控制链路，以便您可以将集群控制链路MTU设置为建议值。请参阅 **jumbo-frame reservation** 命令。启用巨帧会导致 ASA 重新加载，因此您必须在继续此程序之前执行此步骤。

过程

步骤 1 配置集群控制链路接口，其必须与您为控制节点配置的接口相同。请务必为 VTEP 源接口提供其他 IP 地址（以**粗体**显示）。

示例：

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object host 10.6.6.51
ciscoasa(network-object-group)# network-object host 10.6.6.52
ciscoasa(network-object-group)# network-object host 10.6.6.53
ciscoasa(network-object-group)# network-object host 10.6.6.54
ciscoasa(config)# interface gigabitethernet 0/7
ciscoasa(config-if)# nve-only cluster
ciscoasa(config-if)# nameif ccl
ciscoasa(config-if)# ip address 10.6.6.52 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface ccl
ciscoasa(cfg-nve)# peer-group cluster-peers
ciscoasa(config)# mtu ccl 1654
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
```

步骤 2 确定集群名称，其必须与您为控制节点配置的集群名称相同：

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 3 用唯一的字符串为此集群成员命名：

local-unit *node_name*

示例：

```
ciscoasa(cfg-cluster)# local-unit node2
```

指定长度为 1 到 38 个字符的 ASCII 字符串。

每个节点必须具有唯一的名称。集群中不允许存在名称重复的节点。

步骤 4 指定您为控制节点配置的同一集群控制链路接口，但在每个节点的相同网络上指定不同的 IP 地址：

cluster-interface *vni_interface_id* **ip** *ip_address mask*

示例：

```
ciscoasa(cfg-cluster)# cluster-interface vni1 ip 192.168.1.2 255.255.255.0
INFO: Non-cluster interface config is cleared on VNI1
```

指定 IP 地址的 IPv4 地址；此接口不支持 IPv6。此接口不能配置 **nameif**。

步骤 5 如果您使用站点间集群，则请为此节点设置站点 ID，以使其能使用站点特定的 MAC 地址：

site-id 编号

示例：

```
ciscoasa(cfg-cluster)# site-id 2
```

number介于 1 到 8 之间。

步骤 6 设置此节点在控制节点选择的优先级，通常设置为高于控制节点的值：

priority *priority_number*

示例：

```
ciscoasa(cfg-cluster)# priority 2
```

设置值为 1 到 100 的优先级，其中 1 为最高优先级。

步骤 7 设置一个身份验证密钥，使其与您为控制节点设置的密钥相同：

示例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

步骤 8 启用集群：

enable as-data-node

使用 **enable as-data-node** 命令可避免任何配置不兼容（主要是任何尚未进行集群配置的接口的存在）。此命令可确保加入集群的数据节点不可能在任何当前选举中成为控制节点。从属设备的配置将被同步自控制节点的配置覆盖。

要禁用集群，请输入 **no enable** 命令。

注释
如果禁用集群，所有数据接口将关闭，只有管理接口会处于活动状态。

示例

以下示例包括数据节点 node2 的配置：

```
object-group network cluster-peers
    network-object host 10.6.6.51
    network-object host 10.6.6.52
    network-object host 10.6.6.53
    network-object host 10.6.6.54

interface gigabitethernet 0/7
    nve-only cluster
    nameif ccl
```

```
    ip address 10.6.6.52 255.255.255.0
    no shutdown

nve 1
    source-interface ccl
    peer-group cluster-peers

mtu ccl 1654

interface vni 1
    segment-id 1000
    vtep-nve 1

cluster group pod1
    local-unit node2
    cluster-interface vni1 ip 192.168.1.2 255.255.255.0
    priority 2
    key 67impala
    enable noconfirm
```

自定义集群操作

作为第 0 天配置的一部分，或者在部署集群之后，您可以自定义集群运行状况监控、TCP 连接复制延迟、流移动性和其他优化。

在控制节点上执行这些程序。

配置基本 ASA 集群参数

您可以在控制节点上自定义集群设置。

过程

步骤 1 进入集群配置模式：

cluster group *name*

步骤 2 （可选） 启用数据节点到控制节点的控制台复制：

console-replicate

默认情况下会禁用此功能。对于特定的重要事件，ASA 可将某些消息直接打印输出到控制台。如果启用了控制台复制，数据节点会将控制台消息发送到控制节点，因此您只需要监控集群的一个控制台端口。

步骤 3 设置集群事件的最低跟踪级别：

trace-level 级别

根据需要设置最低级别：

- **critical** - 重要事件（严重性=1）
- **warning** - 警告（严重性 = 2）
- **informational** - 信息事件（严重性=3）
- **debug** - 调试事件（严重性=4）

步骤 4 设置从流所有者到导向器和备份所有者的流状态刷新消息（clu_keepalive 和 clu_update 消息）的保持连接间隔。

clu-keepalive-interval 秒

- 秒 - 15 到 55。默认值为 15。

您可能想将间隔设置为比默认值更长的时间，以减少集群控制链路上的流量。

配置运行状态监控并自动重新加入设置

此程序可以配置节点和接口运行状态监控。

您可能想禁用不重要的接口（例如管理接口）的运行状况检查。运行状况监控不在 VLAN 子接口上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

步骤 2 自定义集群节点运行状况检查功能。

health-check [**holdtime** 超时]

为了确定节点运行状况，ASA 集群节点会在集群控制链路上将 heartbeat 消息发送到其他节点。如果节点在保持期内未接收到来自对等节点的任何 heartbeat 消息，则对等节点被视为无响应或无法工作。

- **holdtime** 超时 - 用于确定两次设备 heartbeat状态消息之间的时间间隔，其值介于 0.3到 45 秒；默认值为 3 秒。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用 ASA、或交换机上的接口），您应禁用运行状态检查功能，还要禁用对已禁用接口的接口监控 (**no health-check monitor-interface**)。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

步骤 3 在接口上禁用接口运行状况检查。

no health-check monitor-interface *interface_id*

接口运行状态检查将监控链路故障。ASA 在多长时间后从集群中删除成员取决于该节点是既定成员还是正在加入集群的设备。默认情况下，为所有接口启用运行状况检查。您可以使用此命令的**no** 形式逐个接口将其禁用。您可能想禁用不重要的接口（例如管理接口）的运行状况检查。

- *interface_id* - 禁用接口监控。运行状况监控不在 VLAN 子接口上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用 ASA、或交换机上的接口），您应禁用运行状态检查功能 (**no health-check**)，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management1/1
```

步骤 4 自定义在运行状况检查发生故障后的自动重新加入集群设置。

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**- 指定内部错误的自动重新加入设置。内部故障包括：应用程序同步超时、不一致的应用程序状态等。
- **unlimited** —（**cluster-interface** 的默认值）不限制重新加入尝试的次数。
- *auto-rejoin-max* — 设置重新加入尝试次数，介于 0 和 65535 之间。**0** 禁用自动重新加入。**data-interface** 和 **system** 的默认值为 3。
- *auto_rejoin_interval* - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。节点尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- *Auto_rejoin_interval_variation* - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。对于集群接口，默认值为 **1**，而对于数据接口和系统，默认值为 **2**。

示例：

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

步骤 5 配置 ASA 将接口视为发生故障并将节点从集群中删除之前经过的防反跳时间。

health-check monitor-interface debounce-time *ms*

示例：

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，ASA 会等待指定的毫秒数，然后才将接口标记为发生故障，并将节点从集群中删除。

步骤 6 （可选） 配置流量负载监控。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds* — 设置监控消息之间的时间（以秒为单位），范围介于 10 到 360 秒之间。默认值为 20 秒。
- **intervals** *intervals* — 设置 ASA 维护数据的间隔的数量，该值介于 1 到 60 之间。默认值为 30。

您可以监控集群成员的流量负载，包括总连接计数、CPU 和内存使用情况以及缓冲区丢弃。如果负载过高，且剩余的节点可以处理负载，您可以选择在节点上手动禁用集群，或调整外部交换机上的负载均衡。默认情况下启用此功能。您可以定期监控流量负载。如果负载过高，您可以选择手动禁用节点上的集群。

使用 **show cluster info load-monitor** 命令查看流量负载。

示例：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
   1           0            0            13              27
```

示例

以下示例将 health-check holdtime 配置为 0.3 秒；禁用GUANLI 0/0 接口上的监控；将数据接口的 auto-rejoin 设置为从 2 分钟开始的 4 次尝试，将 duration 增至上一次间隔的 3 倍；以及将集群控制链路的 auto-rejoin 设为 6 次尝试，每隔 2 分钟一次。

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3
ciscoasa(cfg-cluster)# no health-check monitor-interface management0/0
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
```

```
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1
```

配置连接再均衡和集群 TCP 复制延迟

可以配置连接再均衡。如果上游或下游路由器的负载均衡功能导致流量分摊不均衡，您可以将过载的节点配置为将新的 TCP 流量重定向到其他节点。现有流量将不会移至其他节点。

为 TCP 连接启用集群复制延迟有助于延迟创建导向器/备份数据流，从而消除与短期数据流相关的“非必要工作”。请注意，如果某个节点在创建导向器/备份数据流前出现故障，则无法恢复这些数据流。同样，如果流量在创建数据流前再均衡到其他节点，则无法恢复该数据流。不应为已对其禁用 TCP 随机化的流量启用 TCP 复制延迟。

过程

步骤 1 为 TCP 连接启用集群复制延迟：

cluster replication delay *seconds* { **http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] { **host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

示例：

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

将 *seconds* 设置为介于 1 到 15 之间的值。默认启用 **http** 延迟，时间为 5 秒。

步骤 2 进入集群配置模式：

cluster group *name*

步骤 3 （可选）为 TCP 流量启用连接再均衡：

conn-rebalance [**frequency** *seconds*]

示例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

此命令默认禁用。如果启用，ASA 会定期交换有关每秒连接数的信息，并将新连接从每秒连接数较多的设备分流到负载较低的设备。现有连接永远不会移动。此外，由于此命令仅基于每秒的连接数进行重新平衡，因此不会考虑每个节点上已建立的连接总数，并且连接总数可能并不相等。此频率的值为 1 到 360 秒，用于指定多长时间交换一次负载信息。默认值为 5 秒。

将连接分流到其他节点后，它将成为不对称连接。

请勿为站点间拓扑结构配置连接再均衡；您不需要将连接再均衡到位于不同站点的集群成员。

配置站点间功能

对于站点间集群，您可以自定义配置，以提高冗余性和稳定性。

启用导向器本地化

为了提高性能并缩短数据中心的站点间集群的往返时间延迟，您可以启用导向器本地化。新的连接通常实现了负载均衡，并且由特定站点中的集群成员拥有。但是，ASA 会向任意站点的成员分配导向器角色。导向器本地化支持其他导向器角色：与所有者同一站点的本地导向器和可位于任意站点的全局导向器。将所有者和导向器保留在同一站点可以提高性能。此外，如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者。当集群成员收到属于其他站点的连接的数据包时，使用全局导向器。

开始之前

- 在引导程序配置中为集群成员设置站点 ID。
- 以下流量类型不支持本地化：NAT 或 PAT 流量；SCTP 检查的流量；分段所有者查询。

过程

步骤 1 进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 启用导向器本地化。

director-localization

启用站点冗余

为保护流量免受站点故障的影响，您可以启用站点冗余。如果连接的备份所有者与所有者位于同一站点，则将从另一个站点选择一个额外的备份所有者来保护流量免受站点故障的影响。

开始之前

- 在引导程序配置中为集群成员设置站点 ID。

过程

步骤 1 进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

步骤 2 启用站点冗余。

site-redundancy

配置集群流移动性

当服务器在站点之间移动时，您可以检查 LISP 流量以启用流移动性。

关于 LISP 检测

可以检查 LISP 流量，以便在站点间启用流移动性。

关于 *LISP*

利用数据中心的虚拟机移动性（例如，VMware VMotion），服务器可以在数据中心之间迁移，同时维持与客户端的连接。为了支持此类数据中心服务器移动性，路由器需要能够在服务器移动时更新通往服务器的入口路由。思科定位/ID 分离协议 (LISP) 架构将设备身份或终端标识符 (EID) 与设备位置或路由定位符 (RLOC) 分离开，并分隔到两个不同的编号空间，实现服务器迁移对客户端的透明化。例如，当服务器迁移到新的站点并且客户端向服务器发送流量时，路由器会将流量重定向到新位置。

LISP 需要充当特定角色的路由器和服务器，例如 LISP 出口隧道路由器 (ETR)、入口隧道路由器 (ITR)、第一跳路由器、映射解析器 (MR) 和映射服务器 (MS)。当服务器的第一跳路由器检测到服务器连接了其他路由器时，它会更新所有其他路由器和数据库，以便连接到客户端的 ITR 可以拦截、封装流量并将流量发送到新的服务器位置。

ASA LISP 支持

ASA 本身不运行 LISP；但是，它可以通过检查 LISP 流量确定位置更改，然后使用此信息进行无缝集群操作。如果不使用 LISP 集成，当服务器移动到新站点时，流量将到达位于新站点的 ASA 集群成员，而不是原始的流所有者。新 ASA将流量转发到旧站点的 ASA，然后旧 ASA必须将流量发回新站点，才能到达服务器。此类流量流并未处于最佳状态，称为“长号”或“发夹”。

如果使用 LISP 集成，ASA 集群成员可以检查第一跳路由器与 ETR 或 ITR 之间的 LISP 流量，然后将流所有者位置更改为新站点。

LISP 准则

- ASA 集群成员必须位于第一跳路由器和该站点的 ITR 或 ETR 之间。ASA 集群本身不能作为扩展网段的第一跳路由器。
- 仅支持全分布数据流；集中数据流、半分布数据流或属于单个节点的数据流不会移动到新的所有者。半分布数据流包括应用（例如 SIP），其中作为父数据流所有者的同一 ASA 拥有所有子数据流。
- 集群仅移动第 3 和第 4 层流状态；一些应用数据可能丢失。
- 对于持续时间极短的数据流或非关键业务数据流，移动所有者可能并非最佳选择。在配置检查策略时，您可以控制该功能支持的流量类型，并应只对必要流量限制流移动性。

ASA LISP 实施

此功能包含多种相互关联的配置（本章将逐一说明）：

1. （可选）基于主机或服务器 IP 地址限制检查的 EID - 第一跳路由器可能会向与 ASA 集群无关的主机或网络发送 EID 通知消息，因此，您可以限制只向与您的集群有关的服务器或网络发送 EID。例如，如果集群仅涉及 2 个站点，但是 LISP 在 3 个站点上运行，应只包括集群涉及的 2 个站点的 EID。
2. LISP 流量检查 - ASA 检查 UDP 端口 4342 上的 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个将 EID 和站点 ID 相关联的 EID 表。例如，您应检查包含第一跳路由器源 IP 地址以及 ITR 或 ETR 目标地址的 LISP 流量。请注意，没有为 LISP 流量分配导向器，并且 LISP 流量本身不参与集群状态共享。
3. 用于启用指定流量的流移动性的服务策略 - 您应对关键业务流量启用流移动性。例如，您可以只对 HTTPS 流量和/或发送到特定服务器的流量启用流移动性。
4. 站点 ID - ASA 使用集群中每个节点的站点 ID 确定新的所有者。
5. 用于启用流移动性的集群级别配置 - 您还必须在集群级别启用流移动性。此开/关切换器允许您轻松地启用或禁用特定流量类或应用类的流移动性。

配置 LISP 检测

当服务器在站点之间移动时，您可以检查 LISP 流量以启用流移动性。

开始之前

- 根据配置控制节点引导程序设置，第 534 页和配置数据节点引导程序设置，第 539 页，为每个集群设备分配一个站点 ID。
- LISP 流量未包含在 default-inspection-traffic 类中，因此，您在此过程中必须为 LISP 流量配置单独的类。

过程

步骤 1 （可选） 配置 LISP 检测映射以根据 IP 地址限制检测的 EID，并配置 LISP 预共享密钥：

a) 创建扩展 ACL；仅目标 IP 地址与 EID 嵌入式地址匹配：

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。

b) 创建 LISP 检测映射，并进入参数模式：

policy-map type inspect lisp *inspect_map_name*

parameters

c) 通过识别您创建的 ACL 定义允许的 EID：

allowed-eid access-list *eid_acl_name*

第一跳路由器或 ITR/ETR 可能会向与 ASA 集群无关的主机或网络发送 EID 通知消息，因此，您可以限制只向与您的集群有关的服务器或网络发送 EID。例如，如果集群仅涉及 2 个站点，但是 LISP 在 3 个站点上运行，应只包括集群涉及的 2 个站点的 EID。

d) 如果需要，请输入预共享密钥：

validate-key 密钥

示例：

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

步骤 2 在端口 4342 上为第一跳路由器与 ITR 或ETR 之间的 UDP 流量配置 LISP检测：

a) 配置扩展 ACL 以识别 LISP 流量：

access list *eid_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

您必须 指定 UDP 端口 4342。接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。

b) 为 ACL 创建类映射：

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) 使用可选 LISP 检测映射指定策略映射、类映射以及启用检测，然后将服务策略应用于接口（如果为新接口）：

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

如果您有现有服务策略，请指定现有策略映射名称。默认情况下，ASA 包括称为 **global_policy** 的全局策略，因此对于全局策略，请指定该名称。如果您希望全局应用该策略，还可以为每个接口创建一个服务策略。LISP 检测会双向应用于流量，因此您无需在源接口和目标接口上应用服务策略；如果流量与两个方向的类映射都匹配，则进入或退出您应用策略映射的接口的所有流量都受影响。

示例：

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

ASA 会检测 LISP 流量是否包含第一跳路由器与 ITR 或 ETR 之间发送的 EID 通知消息。ASA 维护着一个关联 EID 和站点 ID 的 EID 表。

步骤 3 为流量类启用流移动性：

a) 配置扩展 ACL 以在服务器更改站点时确定要重新分配至最佳站点的业务关键流量：

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

接受 IPv4 和 IPv6 ACL。有关确切的 **access-list extended** 语法，请参阅命令参考。您应对业务关键流量启用流移动性。例如，您可以只对HTTPS流量和/或发送到特定服务器的流量启用流移动性。

b) 为 ACL 创建类映射：

class-map *flow_map_name*

match access-list *flow_acl_name*

c) 指定在其上启用了 LISP 检测的同一策略映射，再指定流类映射，然后启用流移动性：

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

示例：

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0
 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

步骤 4 进入集群组配置模式，并为集群启用流移动性：

cluster group *name*

flow-mobility lisp

此开/关使您可以轻松地启用或禁用流移动性。

示例

以下示例：

- 将 EID 限制为 10.10.10.0/24 网络上的 EID
- 检查位于 192.168.50.89 的 LISP 路由器（内部）与位于 192.168.10.8 的 ITR 或 ETR 路由器（在另一个 ASA 接口上）之间的 LISP 流量 (UDP 4342)
- 为使用 HTTPS 在 10.10.10.0/24 上进入服务器的所有内部流量启用流移动性。
- 为集群启用流移动性。

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

管理集群节点

部署集群后，您可以更改配置和管理集群节点。

成为非活动节点

要成为集群的非活动成员，请在节点上禁用集群，同时保持集群配置不变。

注释 当ASA处于非活动状态（以手动方式或因运行状况检查失败）时，所有数据接口都将关闭；只有管理专用接口可以发送和接收流量。要恢复流量传输，请重新启用集群；或者，您也可以从集群中完全删除该节点。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，您保存了已禁用集群的配置），则管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

过程

步骤 1 进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 禁用集群：

no enable

如果此节点是控制节点，则会进行新的控制选择，并且其他成员将成为控制节点。

集群配置保持不变，因此您可于稍后再次启用集群。

从控制节点停用数据节点

要禁用您登录的节点以外的成员，请执行以下步骤。

注释 当ASA处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。要恢复流量流，请重新启用集群。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，假设您保存了已禁用集群的配置），管理接口将被禁用。您必须使用控制台端口来进行任何进一步的配置。

过程

从集群中删除该节点：

cluster remove unit *node_name*

引导程序配置保持不变，从控制节点同步的最新配置也保持不变，因此您可于稍后重新添加该节点而不会丢失配置。如果在数据节点上输入此命令来删除控制节点，则会选择新的控制节点。

要查看成员名称，请输入 **cluster remove unit ?**，或者输入 **show cluster info** 命令。

示例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

重新加入集群

如果从集群中删除了某个节点（例如针对出现故障的接口），或者如果您手动停用了某个成员，那么您必须手动重新加入集群。

过程

步骤 1 在控制台中，进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 启用集群。

enable

离开集群

要完全退出集群，需要删除整个集群引导程序配置。由于每个节点上的当前配置相同（从主用设备同步），因此退出集群就意味着要么从备份恢复集群前的配置，要么清除现有配置并重新开始配置以免 IP 地址冲突。

过程

步骤 1 对于数据节点，禁用集群：

cluster group *cluster_name* **no enable**

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

在数据节点上启用集群时，您无法进行配置更改。

步骤 2 清除集群配置：

clear configure cluster

ASA 将关闭所有接口，包括管理接口和集群控制链路。

步骤 3 禁用集群接口模式：

no cluster interface-mode

模式并非存储于配置中，因此必须手动重置。

步骤 4 如果有备份配置，可将备份配置复制到正在运行的配置中：

copy *backup_cfg* **running-config**

示例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

步骤 5 将配置保存到启动配置：

write memory

步骤 6 如果没有备份配置，请重新配置管理访问。例如，确保更改接口 IP 地址，并恢复正确的主机名。

更改控制节点

⚠

注意 要更改控制节点，最好的方法是在控制节点上禁用集群，等到新的控制选举后再重新启用集群。如果必须指定要成为控制节点的具体节点，请使用本节中的程序。但是请注意，对集中功能而言，如果使用本程序强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

要更改控制节点，请执行以下步骤：

过程

将新节点设置为控制节点：

cluster control-node unit*node_name*

示例：

```
ciscoasa(config)# cluster control-node unit asa2
```

您需要重新连接到主集群 IP 地址。

要查看成员名称，请输入 **cluster control-node unit ?**（可查阅除当前节点之外的所有名称），或输入 **show cluster info** 命令。

在整个集群范围内执行命令

要向集群中的所有节点或某个特定节点发送命令，请执行以下步骤。向所有节点发送 **show** 命令以收集所有输出并将其显示在当前节点的控制台上。也可在整个集群范围内执行其他命令（如 **capture** 和 **copy**）。

过程

发送命令到所有节点，或者如果指定了节点名称，则发送到特定节点：

cluster exec [**unit** *node_name*] *command*

示例：

```
ciscoasa# cluster exec show xlate
```

要查看节点名称，请输入 **cluster exec unit ?**（可查阅除当前节点之外的所有名称），或输入 **show cluster info** 命令。

示例

要同时将同一捕获文件从集群中的所有节点复制到TFTP服务器，请在控制节点上输入以下命令：

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

多个 PCAP 文件（一个文件来自一个节点）将复制到 TFTP 服务器。目标捕获文件名会自动附加节点名称，例如 capture1_asa1.pcap、capture1_asa2.pcap 等。在本例中，asa1和asa2是集群节点名称。

监控 ASA Virtual集群

您可以监控集群状态和连接并排除故障。

监控集群状态

请参阅以下命令来监控集群状态：

- **show cluster info** [**health** [**details**]]

  如果没有关键字，**show cluster info** 命令将显示所有集群成员的状态。

  show cluster info health 命令将显示接口、节点和整个集群的当前运行状况。**details** 关键字显示心跳消息失败的次数。

  请参阅 **show cluster info** 命令的以下输出：

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
```

```
    CCL MAC   : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2011
    Last leave: N/A
Unit "A" in state CONTROL_NODE
    ID        : 2
    Site ID   : 2
          Version   : 9.4(1)
    Serial No.: JAB0815R0JY
    CCL IP    : 10.0.0.1
    CCL MAC   : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2011
    Last leave: N/A
Unit "B" in state DATA_NODE
    ID        : 3
    Site ID   : 2
          Version   : 9.4(1)
    Serial No.: P3000000191
    CCL IP    : 10.0.0.2
    CCL MAC   : 000b.fcf8.c61e
    Last join : 19:13:50 UTC Sep 23 2011
    Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info auto-join**

  显示集群节点是否将在一段延迟后自动重新加入集群，以及是否已清除故障条件（例如等待许可证、机箱运行状况检查失败，等等）。如果节点已永久禁用，或节点已在集群中，则此命令将不会显示任何输出。

  请参阅 **show cluster info auto-join** 命令的以下输出：

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Control node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport**{**asp** |**cp** [**detail**]}

  显示以下项目传输相关的统计信息：

- **asp** — 数据平面传输统计信息。
- **cp** — 控制平面传输统计信息。

如果您输入 **detail** 关键字，您可以查看集群可靠传输协议的使用情况，以便确定控制平面中的缓冲区已满时的丢包问题。请参阅 **show cluster info transport cp detail** 命令的以下输出：

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
--------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-------------------------------------------
        0         2         3
  U     1         3308122   4370233
```

```
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  -------------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  -------------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
```

```
      R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                       578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                       572         99%
  Cluster VPN Unique ID Client                     1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  显示集群历史记录，以及有关集群节点加入失败的原因或节点离开集群的原因的错误消息。

捕获整个集群范围内的数据包

有关在集群中捕获数据包的信息，请参阅以下命令：

cluster exec capture

要支持集群范围的故障排除，您可以使用 **cluster exec capture** 命令在控制节点上启用捕获集群特定流量的功能，随后集群中的所有数据节点上将自动启用此功能。

监控集群资源

请参阅以下命令以监控集群资源：

show cluster {**cpu** | **memory** | **resource**} [*options*]

显示整个集群的聚合数据。可用 *options* 取决于数据类型。

监控集群流量

请参阅以下命令以监控集群流量：

- **show conn [detail], cluster exec show conn**

  show conn 命令显示一个传输是导向者、备用还是转发者传输。在任意节点上使用 **cluster exec show conn** 命令可查看所有连接。此命令可以显示单个流的流量到达集群中不同 ASA 的方式。集群的吞吐量取决于负载均衡的效率和配置。此命令可以让您很方便地查看某个连接的流量如何流经集群，也可以帮助您了解负载均衡器对传输的性能有何影响。

  show conn detail 命令还显示哪些流应 遵守流移动性。

  以下是 **show conn detail** 命令的输出示例：

```
ciscoasa/ASA2/data node# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic received
 at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface NP
Identity
Ifc Locally received: 716 (8 byte/s)
```

  要对连接流进行故障排除，请先在任意节点上输入 **cluster exec show conn** 命令查看所有节点上的连接。寻找具有以下标志的流：导向者 (Y)、备用 (y) 和转发者 (z)。下例显示了三台 ASA 上的一条从 172.18.124.187:22 到 192.168.103.131:44727 的 SSH 连接；ASA 1 带有 z 标志，表示其是该连接的转发者；ASA3 带有 Y 标志，表示其是该连接的导向者；而 ASA2 则没有特殊的标志，表示其是所有者。在出站方向，此连接的数据包进入 ASA2 上的内部接口并从外部接口流出。在入站方向，此连接的数据包进入 ASA 1 和 ASA3 上的外部接口，通过集群控制链路被转发到 ASA2，然后流出 ASA2 上的内部接口。

```
ciscoasa/ASA1/control node# cluster exec show conn
```

```
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:****************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:****************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0,
flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance** | **flow-mobility counters**]

  show cluster info conn-distribution 和 **show cluster info packet-distribution** 命令显示流量在所有集群节点上的分布。这些命令可以帮助您评估和调整外部负载均衡器。

  show cluster info loadbalance 命令显示连接再均衡统计信息。

  The **show cluster info flow-mobility counters** 命令显示 EID 移动和流所有者移动信息。请参阅 **show cluster info flow-mobility counters** 的以下输出：

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 4
EID movement notification processed : 4
Flow owner moving requested         : 2
```

- **show cluster info load-monitor** [**details**]

  show cluster info load-monitor 命令显示最后一个间隔的集群成员的流量负载，以及已配置的总间隔数（默认情况下为 30）。使用 **details** 关键字查看每个时间间隔的每个度量值。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 30 interval:
   0           0            0            12              28
   1           0            0            13              27


ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B
```

```
 1  A_1

Information from all units with 20 second interval


Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Buffer drops captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Memory usage(%) captured over 30 intervals:
```

```
Unit ID  0
        25          25          30          30          30          35
        25          25          35          30          30          30
        25          25          30          25          25          35
        30          30          30          25          25          25
        25          20          30          30          30          30
Unit ID  1
        30          25          35          25          30          30
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35

CPU usage(%) captured over 30 intervals:
Unit ID  0
        25          25          30          30          30          35
        25          25          35          30          30          30
        25          25          30          25          25          35
        30          30          30          25          25          25
        25          20          30          30          30          30
Unit ID  1
        30          25          35          25          30          30
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35
```

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  显示整个集群的聚合数据。可用 *options* 取决于数据类型。

  请参阅 **show cluster access-list** 命令的以下输出：

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
```

```
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

要显示所有节点在用连接的汇聚计数，请输入：

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):************************************************************
  100 in use, 100 most used

  cl1:*************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  此命令对于数据路径故障排除非常有用。

监控集群路由

有关集群路由的信息，请参阅以下命令：

- **show route cluster**
- **debug route cluster**

显示集群的路由信息。

- **show lisp eid**

  显示 ASA EID 表，表中显示了 EID 和站点 ID。

  请参阅 **cluster exec show lisp eid** 命令的以下输出。

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):**********************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:**********************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  该命令对于故障排除非常有用。

配置集群日志记录

有关为集群配置日志记录的信息，请参阅以下命令：

logging device-id

集群中的每个节点将独立生成系统日志消息。您可以使用 **logging device-id** 命令来生成具有相同或不同设备 ID 的系统日志消息，以使消息看上去是来自集群中的相同或不同节点。

监控集群接口

请参阅以下用于监控集群接口的命令：

- **show cluster interface-mode**

  显示集群接口模式。

调试集群

请参阅以下用于调试集群的命令：

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  显示集群的调试消息。

- **debug cluster flow-mobility**

显示与集群流移动性相关的事件。

- **debug lisp eid-notify-intercept**

  当 eid-notify 被拦截时显示事件。

- **show cluster info trace**

  show cluster info trace 命令显示调试信息，供进一步排除故障之用。

  请参阅 **show cluster info trace** 命令的以下输出：

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

  例如，如果您看到以下消息显示两个具有相同**local-unit**名称的节点充当控制节点，这可能意味着两个节点具有相同的**local-unit**名称（请检查您的配置），或者某个节点正在接收自己的广播消息（请检查您的网络）。

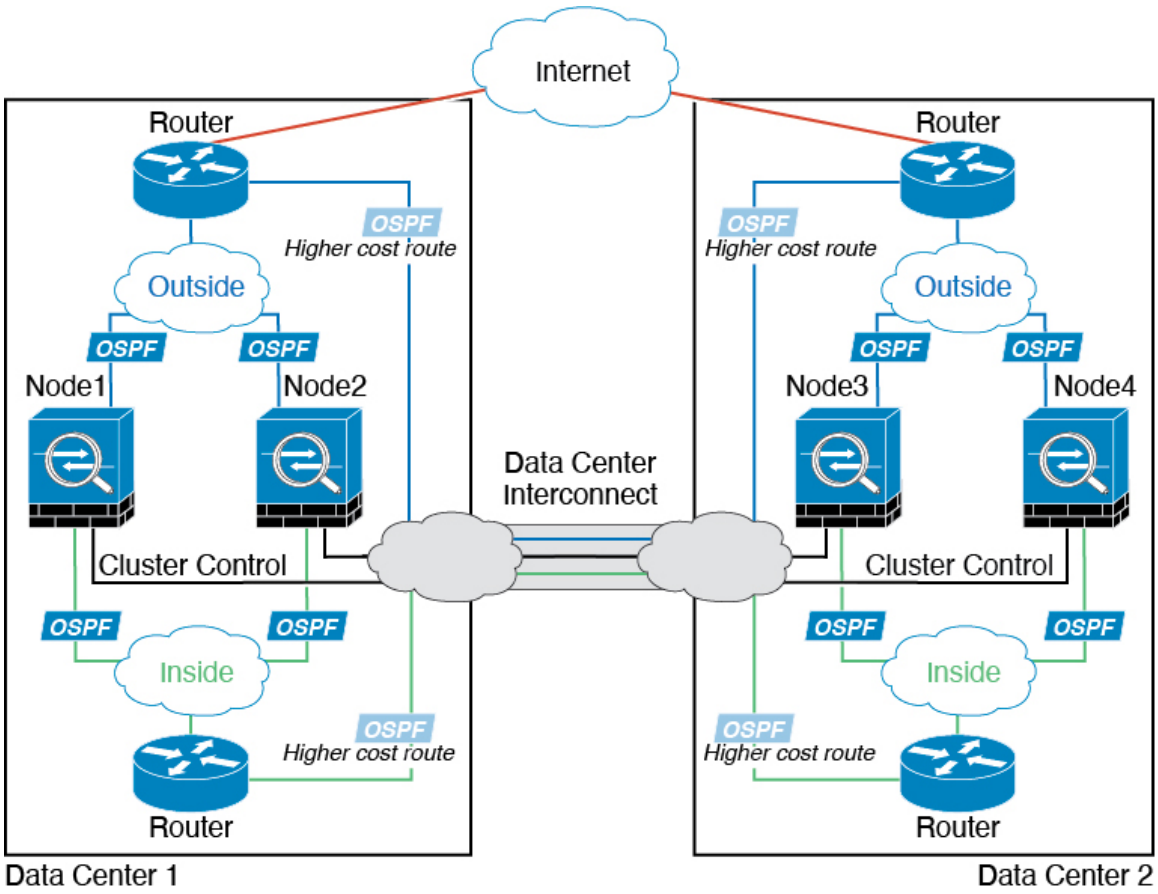
```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node
 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

ASA Virtual集群示例

这些示例包括典型部署中所有与集群相关的 ASA 配置。

独立接口路由模式南北站点间集群示例

以下示例显示的 2 个 ASA 集群节点分别位于 2 个部署在内部和外部路由器之间（南北插入）的数据中心。集群节点由集群控制链路通过 DCI 连接。位于每个数据中心的内部和外部路由器使用 OSPF 和 PBR 或 ECMP 在集群成员之间对流量执行负载均衡。通过指定 DCI 中开销较高的路由可将流量保持在每个数据中心内（除非给定站点上的所有ASA集群节点都中断连接）。如果一个站点上的所有集群节点都发生故障，流量将从每台路由器通过 DCI 发往另一个站点上的 ASA 集群节点。



集群参考

本部分包括有关集群工作原理的详细信息。

ASA 功能和集群

部分 ASA 功能不受 ASA 集群支持，还有部分功能仅在控制节点上受支持。其他功能可能对如何正确使用规定了注意事项。

集群不支持的功能

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

- 依靠 TLS 代理实现的统一通信功能
- 远程访问 VPN（SSL VPN 和 IPsec VPN）
- 虚拟隧道接口 (VTI)
- 以下应用检查：

- CTIQBE
- H323、H225 和 RAS
- IPsec 穿透
- MGCP
- MMP
- RTSP
- SCCP（瘦客户端）
- WAAS
- WCCP

- 僵尸网络流量过滤器
- 自动更新服务器
- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- VPN 负载均衡
- Azure 上的故障转移
- 集成路由和桥接
- FIPS 型号

集群集中化功能

以下功能只有在控制节点上才受支持，且无法为集群扩展。

注释 集中功能的流量从成员节点通过集群控制链路转发到控制节点。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非控制节点的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回控制节点。

对集中功能而言，如果控制节点发生故障，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

- 以下应用检查：
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS

- PPTP
- RADIUS
- RSH
- SNMP
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- 静态路由监控
- 网络访问的身份验证和授权。记帐被分散。
- 筛选服务
- 站点间 VPN
- 组播路由

应用到单个节点的功能

这些功能将应用到每个 ASA 节点而非整个集群或控制节点。

- QoS - QoS 策略将于配置复制过程中在集群中同步。但是，该策略是在每个节点上独立执行。例如，如果对输出配置管制，则要对流出特定 ASA 的流量应用符合规则的速率和符合规则的突发量值。在包含 3 个节点且流量均衡分布的集群中，符合规则的速率实际上变成了集群速率的 3 倍。
- 威胁检测 - 威胁检测在各节点上独立工作；例如，排名统计信息就要视具体节点而定。以端口扫描检测为例，由于扫描的流量将在所有节点间进行负载均衡，而一个节点无法看到所有流量，因此端口扫描检测无法工作。
- 资源管理 - 多情景模式下的资源管理根据本地使用情况在每个节点上分别执行。
- LISP 流量 - UDP 端口 4342 上的 LISP 流量由每个接收节点进行检查，但是没有为其分配导向器。每个节点都会添加到集群共享的 EID 表，但是 LISP 流量本身并不参与集群状态共享。

用于网络访问的 AAA 和集群

用于网络访问的 AAA 由三部分组成：身份验证、授权和记账。身份验证和授权作为集中功能在集群控制节点上实施，且数据结构复制到集群数据节点。如果选举出控制节点，新的控制节点将拥有所需的所有信息，以继续不间断运行经过验证的既有用户及其相关授权。当控制节点发生变化时，用户身份验证的空闲和绝对超时将保留。

记账作为分散的功能在集群中实施。记账按每次流量完成，因此在为流量配置记账时，作为流量所有者的集群节点会将记账开始和停止消息发送到 AAA 服务器。

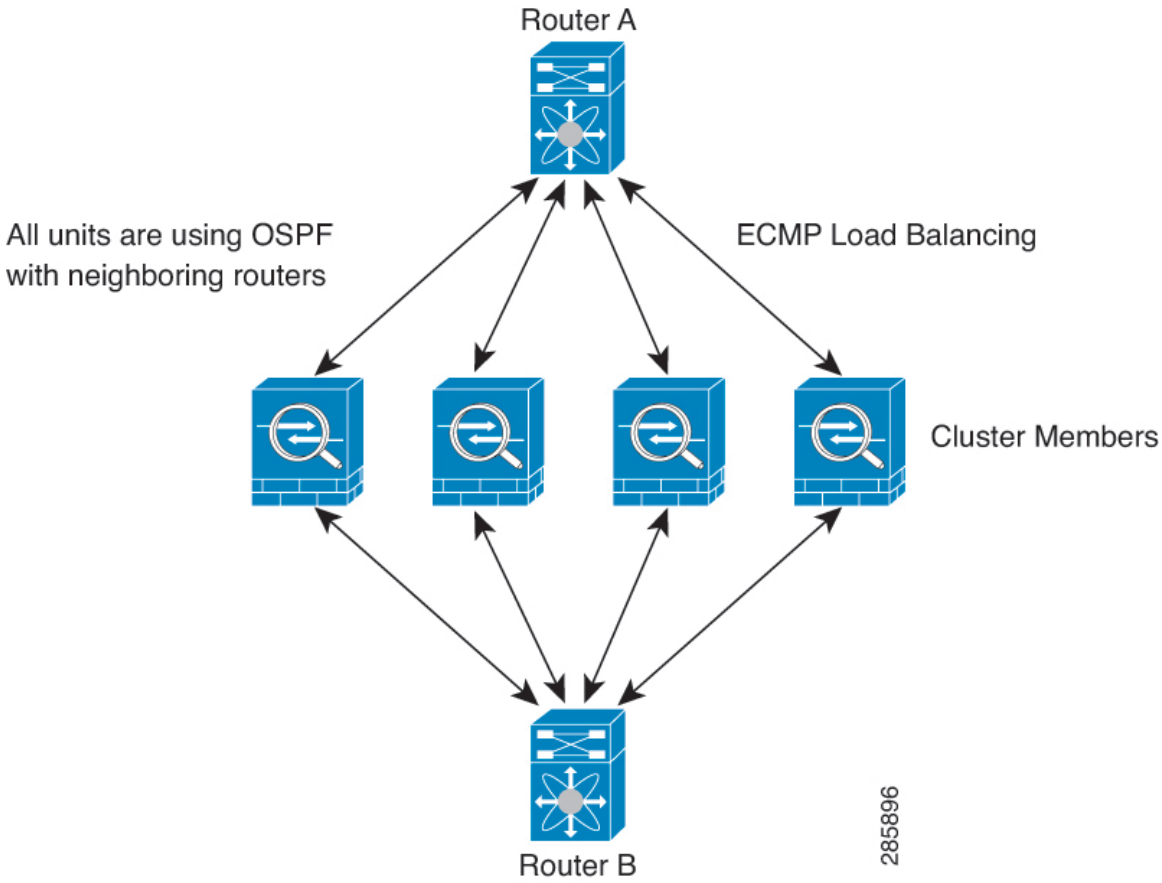
连接设置和集群

连接限制在集群范围强制实施（请参阅 **set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max** 和 **set connection per-client-max** 命令）。每个节点都有根据广播消息估计的集群范围的计数器值。出于效率考虑，在集群中配置的连接限制可能不会严格按限制数量实施。每个节点在任何指定时间都可能高估或低估集群范围内的计数器值。不过，在负载均衡的集群中，该信息将随时间而更新。

动态路由和集群

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *55:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一个节点。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每个节点在与外部路由器通信时，都会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

EIGRP 与单个接口模式下的集群对等体不构成邻居关系。

注释 如果该集群为实现冗余有多个设备与同一个路由器相邻，则非对称路由可能会造成不可接受的流量损失。要避免非对称路由，请将所有这些节点接口分组到同一流量区域中。请参阅配置流量区域，第 806 页。

FTP 和集群

- 如果 FTP 数据通道和控制通道流量由不同的集群成员所有，则数据通道所有者会将空闲超时更新定期发送到控制通道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父/子流量关系；控制流量空闲超时不会更新。
- 如果您将 AAA 用于 FTP 访问，则控制通道流集中在控制节点上。

ICMP检测和集群

ICMP 和 ICMP 错误数据包通过集群的流取决于是否启用 ICMP/ICMP 错误检查。不启用 ICMP 检查时，ICMP 是单向流，并且不支持导向器流。启用 ICMP 检查时，ICMP 流变为双向流，并由导向器/备份流支持。被检查的 ICMP 流的一个不同之处在于导向器对转发数据包的处理：导向器会将 ICMP 回应应答数据包转发给流所有者，而不是将数据包返回给转发器。

组播路由和集群

在独立接口模式下，设备并不单独处理组播。所有数据和路由数据包都由控制设备进行处理和转发，从而避免数据包复制。

NAT 和集群

NAT 可能会影响集群的总吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 ASA，因为负载均衡算法取决于 IP 地址和端口，NAT 会导致入站和出站数据包具有不同的 IP 地址和/或端口。当数据包到达并非 NAT 所有者的 ASA时，会通过集群控制链路转发到所有者，导致集群控制链路上存在大量流量。请注意，接收节点不会创建流向所有者的转发流量，因为 NAT 所有者最终可能不会根据安全和策略检查结果为数据包创建连接。

如果您仍想在集群中使用 NAT，请考虑以下准则：

- 不使用代理 ARP - 对于独立接口，切勿为映射的地址发送代理 ARP 回复。这可以防止邻接路由器与可能已经不在集群中的 ASA 保持对等关系。对于指向主集群 IP 地址的映射地址，上游路由器需要静态路由或带对象跟踪的 PBR。这对跨网络 EtherChannel 来说不是问题，因为只有一个 IP 地址与集群接口关联。
- 不对独立接口使用接口 PAT - 独立接口不支持接口 PAT。
- PAT 采用端口块分配 - 请参阅该功能的以下准则：

- 每主机最大流量限制并不针对整个集群，而是单独应用于每个节点。因此，在每主机最大流量限制配置为 1 的包含 3 个节点的集群中，如果在全部 3 个节点上对来自主机的流量实行负载均衡，则可以分配 3 个端口块，每个节点 1 个。
- 在执行每主机最大流量限制时，在备份池中的备份节点上创建的端口块不计算在内。
- 如果进行即时 PAT 规则修改（对 PAT 池改用全新的 IP 地址范围），会导致在新的池生效时仍在传输的转换项备份请求的转换项备份创建失败。此行为并非端口块分配功能所特有，它是一个暂时性 PAT 池问题，只发现于在集群节点之间分配池并执行流量负载均衡的集群部署。
- 在集群中操作时，不能直接更改块分配大小。只有在集群中重新加载每个设备后，新的大小才会生效。为避免重新加载每个设备，我们建议您删除所有块分配规则并清除与这些规则相关的所有转换。然后，您可以更改块大小并重新创建块分配规则。

- 对动态 PAT 使用 NAT 池地址分配 - 配置 PAT 池时，集群将池中的每个 IP 地址划分为端口块。默认情况下，每个块都是 512 个端口，但如果配置端口块分配规则，则使用块设置。这些块在集群中的各个节点之间均匀分配，因此每个节点都有一个或多个块对应 PAT 池中的每个 IP 地址。因此，在一个集群的 PAT 池中可以最少拥有一个 IP 地址，只要这足以支持您预期的 PAT 连接数即可。端口块覆盖的端口范围为 1024-65535，除非您在 PAT 池 NAT 规则中配置该选项以包含保留的端口 1-1023。
- 在多个规则中重复使用 PAT 池 - 要在多条规则中使用同一 PAT 池，必须注意规则中的接口选择。必须在所有规则中使用特定接口，或者在所有规则中使用“任意”接口。不能在规则中混合使用特定接口和“任意”接口，否则系统可能无法将返回流量与集群中的正确节点进行匹配。每条规则使用唯一的 PAT 池是最可靠的方案。
- 不使用轮询 - 集群不支持 PAT 池轮询。
- 无扩展 PAT - 集群不支持扩展 PAT。
- 控制节点管理的动态 NAT 转换 - 控制节点保留转换表并复制到数据节点。当数据节点收到需要动态 NAT 的连接并且转换不在表中时，它将请求从控制节点转换。数据节点拥有该连接。
- 过时 xlate - 连接所有者上的 xlate 空闲时间不会更新。因此，空闲时间值可能会超过空闲超时值。如果空闲计时器值高于配置的超时值（refcnt 为 0），则表示 xlate 过时。
- 每会话 PAT 功能 - 每会话 PAT 功能并非集群专用功能，但它能提高 PAT 的可扩展性，而且对集群而言，它允许每个数据节点成为 PAT 连接的所有者；相比之下，多会话 PAT 连接则必须转发到控制节点并由控制节点所有。默认情况下，所有 TCP 流量和 UDP DNS 流量均使用每会话 PAT 转换，而 ICMP 和所有其他 UDP 流量均使用多会话。您可以为 TCP 和 UDP 配置每会话 NAT 规则以更改这些默认设置，但是，您不能为 ICMP 配置每会话 PAT。对于使用多会话 PAT 的流量（例如 H.323、SIP 或 Skinny），您可以禁用关联 TCP 端口的每会话 PAT（这些 H.323 和 SIP 的 UDP 端口已默认为多会话）。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。
- 对以下检查不使用静态 PAT：
  - FTP
  - PPTP

- RSH
- SQLNET
- TFTP
- XDMCP
- SIP

- 如果您有大量 NAT 规则（超过一万条），则应使用设备 CLI 中的 **asp rule-engine transactional-commit nat** 命令启用事务提交模型。否则，节点可能无法加入集群。

SCTP 和集群

SCTP 关联可以在任何节点上创建（由于负载均衡），但其多宿主连接必须位于同一节点上。

SIP 检测和集群

控制流可以在任何节点上创建（由于负载均衡），但其子数据流必须位于同一节点上。

不支持 TLS 代理配置。

SNMP 和集群

SNMP 代理按照本地 IP 地址轮询每一个ASA。您无法轮询集群的合并数据。

您应始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的控制节点时，对新控制节点的轮询将失败。

当使用 SNMPv3 进行集群时，如果您在初始集群形成后添加新的集群节点，则 SNMPv3 用户不会复制到新节点。您必须在控制节点上重新添加它们以强制用户复制到新节点，或者直接在数据节点上复制。

STUN 和集群

故障转移和集群模式支持STUN检查，因为针孔被复制。但是，节点之间不进行事务ID的复制。如果节点在收到 STUN 请求后发生故障，并且另一个节点收到 STUN 响应，则该 STUN 响应将被丢弃。

系统日志与 NetFlow 和集群

- 系统日志 - 集群中的每个节点都会生成自己的系统日志消息。您可以配置日志记录，使每个节点在系统日志消息的报头字段中使用相同或不同的设备 ID。例如，集群中的所有节点都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备 ID，则所有节点生成的系统日志消息都会看似来自一个节点。如果将日志记录配置为使用集群引导程序配置中指定的本地节点名称作为设备 ID，系统日志消息就会看似来自不同节点。
- NetFlow - 集群中的每个节点都会生成自己的 NetFlow 数据流。NetFlow 收集器只能将每台 ASA 视为单独的 NetFlow 导出器。

思科 TrustSec 和集群

只有控制节点学习安全组标记 (SGT) 信息。然后，控制节点将 SGT 填充到数据节点，数据节点可以根据安全策略对 SGT 做出匹配决策。

VPN 和集群

站点间 VPN 是集中功能；只有控制节点支持 VPN 连接。

注释 集群不支持远程访问 VPN。

VPN 功能仅限控制节点使用，且不能利用集群的高可用性功能。如果控制节点发生故障，所有现有的 VPN 连接都将断开，VPN 用户将遇到服务中断。选择新的控制节点后，必须重新建立 VPN 连接。

对于使用 PBR 或 ECMP 时与独立接口的连接，您必须始终连接到主集群 IP 地址而非本地地址。

与 VPN 相关的密钥和证书将被复制到所有节点。

性能换算系数

将多台设备组成一个集群时，预计可以达到近似 80% 最大组合吞吐量的集群总体性能。

例如，如果您的型号在单独运行时可以处理大约 10 Gbps 的流量，则对于 8 台设备的集群，最大组合吞吐量约为 80 Gbps（8 台设备 x 10 Gbps）的 80%：64 Gbps。

控制节点选择

集群节点通过集群控制链路通信，如下选举控制节点：

1. 当为节点启用集群（或当节点首次启动时已启用集群）时，设备会每 3 秒广播一个选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级设置在 1 和 100 之间，其中 1 为最高优先级。
3. 如果某节点在 45 秒后未收到另一个具有较高优先级的节点的响应，则该设备会成为控制节点。

注释 如果多个节点并列获得最高优先级，则使用集群节点名称和序列号确定控制节点。

4. 如果节点稍后加入具有更高优先级的集群，它不会自动成为控制节点；现有控制节点始终保持为控制节点，除非它停止响应，此时会选择新的控制节点。
5. 在“裂脑”场景中，当临时存在多个控制节点时，具有最高优先级的节点将会保留角色，而其他节点则恢复为数据节点角色。

注释 您可以手动强制节点成为控制节点。对集中功能而言，如果强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

ASA Virtual 集群中的高可用性

ASA virtual 集群通过监控节点和接口的运行状况并在节点之间复制连接状态来提供高可用性。

节点运行状况监控

每个节点通过集群控制链路定期发送广播保持连接心跳数据包。如果控制节点在可配置的超时期限内未从数据节点接收任何keepalive心跳数据包或其他数据包，则控制节点会从集群中删除该数据节点。如果数据节点未从控制节点接收数据包，则从其余节点中选择新的控制节点。

如果节点因为网络故障而不是因为节点实际故障而无法通过集群控制链路相互访问，则集群可能会进入“裂脑”场景，其中隔离的数据节点将选择自己的控制节点。例如，如果路由器在两个集群位置之间发生故障，则位于位置1的原始控制节点将从集群中删除位置2数据节点。同时，位置2的节点将选择自己的控制节点并形成自己的集群。请注意，在这种情况下，非对称流量可能会失败。恢复集群控制链路后，优先级较高的控制节点将保留控制节点的角色。

有关详细信息，请参阅控制节点选择，第 576 页。

接口监控

每个节点都会监控使用中的所有已命名的硬件接口的链路状态，并向控制节点报告状态更改。

当您启用运行状况监控时，默认情况下会监控所有物理接口；您可以选择按接口禁用监控。只能监控已命名接口。

如果某个节点被监控的接口发生故障，则将从集群中删除该设备。ASA 在多长时间后从集群中删除成员取决于该节点是既定成员还是正在加入集群的设备。ASA 在节点加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 ASA 从集群中删除。无论状态如何，节点都会在 500 毫秒后被删除。

发生故障后的状态

当集群中的节点发生故障时，该节点承载的连接将无缝转移到其他节点；流量的状态信息将通过控制节点的集群控制链路共享。

如果控制节点发生故障，则优先级最高（数字最小）的另一个集群成员将成为控制节点。

ASA将自动尝试重新加入集群，具体取决于故障事件。

注释 当ASA变成不活动状态且无法自动重新加入集群时，所有数据接口都会关闭，仅管理专用接口可以发送和接收流量。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但是，如果您重新加载而节点在集群中仍然处于非活动状态，管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

重新加入集群

当集群节点从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路在最初加入时出现故障 - 在解决集群控制链路存在的问题后，您必须通过在 CLI 输入 **cluster group***name*，然后输入 **enable** 来重新启用集群 ，以手动重新加入集群。
- 加入集群后出现故障的集群控制链路 - ASA 无限期地每 5 分钟自动尝试重新加入。此行为是可配置的。
- 出现故障的数据接口 - ASA 尝试在 5 分钟时、然后在 10 分钟时、最后在 20 分钟时重新加入。如果 20 分钟后仍加入失败，ASA 将禁用集群。解决数据接口问题之后，您必须在 CLI 上通过输入**cluster group** *name*，然后输入**enable** 来手动启用集群。此行为是可配置的。
- 节点存在故障 - 如果节点因节点运行状况检查失败而从集群中删除，则如何重新加入集群取决于失败的原因。例如，临时电源故障意味节点将在重新启动时重新加入集群，只要集群控制链路打开并且仍然使用 **enable** 命令启用集群。ASA 每 5 秒钟尝试重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。节点将尝试以下列间隔自动重新加入集群：5 分钟，10 分钟，然后是 20 分钟。此行为是可配置的。

数据路径连接状态复制

每个连接在集群中都有一个所有者和至少一个备用所有者。备用所有者在发生故障时不会接管连接；而是存储TCP/UDP状态信息，使连接在发生故障时可以无缝转移到新的所有者。备用所有者通常也是导向器。

有些流量需要 TCP 或 UDP 层以上的状态信息。请参阅下表了解支持或不支持此类流量的集群。

表 *19:* 在集群中复制的功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	-
MAC 地址表	是	-
用户标识	是	包括 AAA 规则 (uauth) 。
IPv6 邻居数据库	是	—

流量	状态支持	备注
动态路由	是	—
SNMP 引擎 ID	否	-
适用于 Firepower 4100/9300的分布式 VPN（站点间）	是	备用会话成为主用会话，并创建一个新的备用会话。

ASA Virtual集群管理连接的方式

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

连接角色

请参阅为每个连接定义的下列角色：

- 所有者 - 通常为最初接收连接的节点。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。如果原始所有者发生故障，则当新节点从连接接收到数据包时，导向器会从这些节点中选择新的所有者。
- 备用所有者 - 存储从所有者接收的 TCP/UDP 状态信息的节点，以便在出现故障时可以无缝地将连接转移到新的所有者。在发生故障时，备用所有者不会接管连接。如果所有者处于不可用状态，从该连接接收数据包的第一个节点（根据负载均衡而定）联系备用所有者获取相关的状态信息，以便成为新的所有者。

  只要导向器（见下文）与所有者不是同一节点，导向器也可以是备用所有者。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  对于 Firepower 9300 上的在一个机箱中包括多达 3 个集群节点的集群，如果备用所有者与所有者在同一机箱上，则将从另一个机箱中选择一个额外的备用所有者来保护流量免受机箱故障的影响。

  如果您对站点间集群启用导向器本地化，则有两个备用所有者角色：本地备用和全局备用。所有者始终选择与自身位于同一站点（基于站点 ID）的本地备用。全局备用可以位于任何站点，甚至可以与本地备用是同一个节点。所有者向两个备用所有者发送连接状态信息。

  如果启用站点冗余，并且备用所有者与所有者位于同一站点，则将从另一个站点选择一个额外的备用所有者来保护流量免受站点故障的影响。机箱备份和站点备份是独立的，因此流量在某些情况将同时具有机箱备份和站点备份。

- 导向器 - 处理来自转发器的所有者查找请求的节点。当所有者收到新连接时，会根据源/目的 IP 地址和端口的散列值（有关 ICMP 散列详细信息，请参见下文）选择导向器，然后向导向器发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他节点，该节点会向导向器查询哪一个节点是所有者，以便转发数据包。一个连接只有一个导向器。如果导向器发生故障，所有者会选择一个新的导向器。

  只要导向器与所有者不是同一节点，导向器也可以是备用所有者（见上文）。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

如果您对站点间集群启用导向器本地化，则有两个导向器角色：本地导向器和全局导向器。所有者始终选择与它自身位于同一站点（基于站点 ID）的本地导向器。全局导向器可以位于任何站点，甚至可以与本地导向器是同一节点。如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者。

ICMP/ICMPv6 散列详细信息：

- 对于 Echo 数据包，源端口为 ICMP 标识符，目的端口为 0。
- 对于 Reply 数据包，源端口为 0，目的端口为 ICMP 标识符。
- 对于其他数据包，源端口和目的端口均为 0。

- 转发器 - 向所有者转发数据包的节点。如果转发者收到并非其所有的连接的数据包，则会向导向器查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向器也可以是转发者。如果启用导向器本地化，转发器将始终向本地导向器查询。如果本地导向器未获知所有者，例如，当集群成员收到所有者位于其他站点上的连接的数据包时，转发者将仅查询全局导向器。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN Cookie 直接获知所有者，因此无需向导向器查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向器查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。一个连接了可以有多个转发器；采用良好的负载均衡方法可以做到没有转发器，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。

注释 不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

当连接使用端口地址转换 (PAT) 时，PAT 类型（每会话或多会话）会对哪个集群成员将成为新连接的所有者产生影响：

- 每会话 PAT - 所有者是接收连接中的初始数据包的节点。

  默认情况下，TCP 和 DNS UDP 流量均使用每会话 PAT。

- 多会话 PAT - 所有者始终是控制节点。如果多会话 PAT 连接最初由数据节点接收，则数据节点会将连接转发给控制节点。

  默认情况下，UDP（DNS UDP 除外）和 ICMP 流量使用多会话 PAT，因此这些连接始终归控制节点所有。

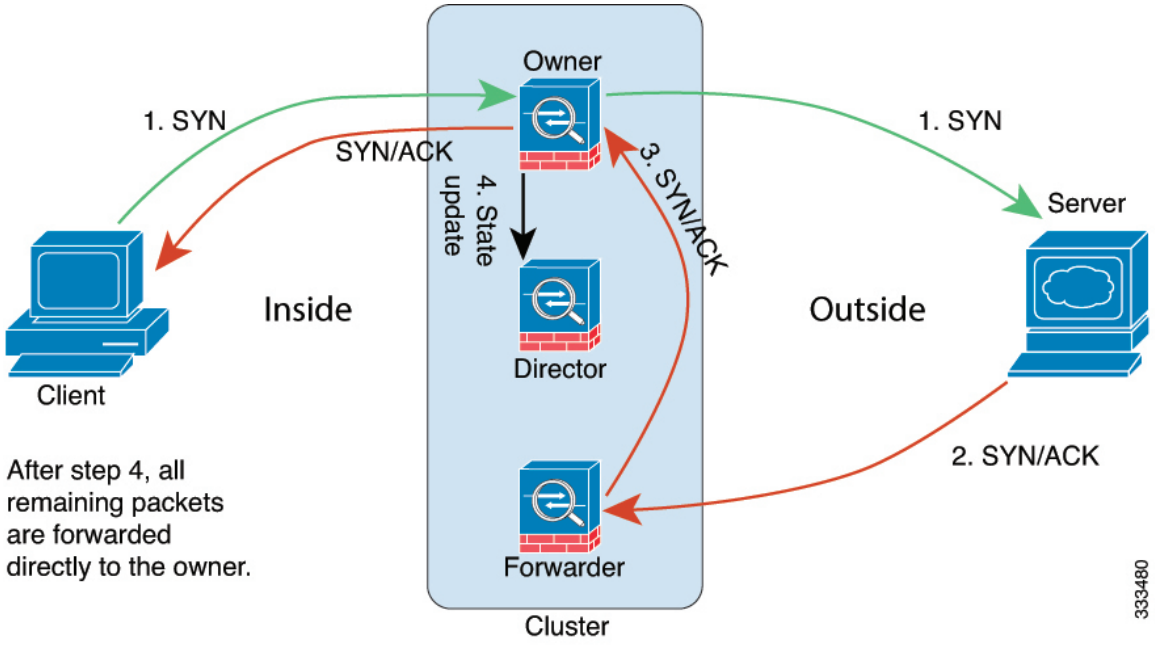
您可以更改 TCP 和 UDP 的每会话 PAT 默认设置，以便根据配置按每会话或多会话处理这些协议的连接。对于 ICMP，您不能更改默认的多会话 PAT。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。

新连接所有权

通过负载均衡将新连接定向到集群节点时，该连接的两个方向都由此节点所有。如果该连接有任何数据包到达其他节点，这些数据包都会通过集群控制链路被转发到所有者节点。为了获得最佳性能，对于要到达同一个节点的流量的两个方向以及要在节点之间均摊的流量，都需要执行适当的外部负载均衡。如果反向流量到达其他节点，会被重定向回原始节点。

TCP 的数据流示例

以下图例显示了新连接的建立。



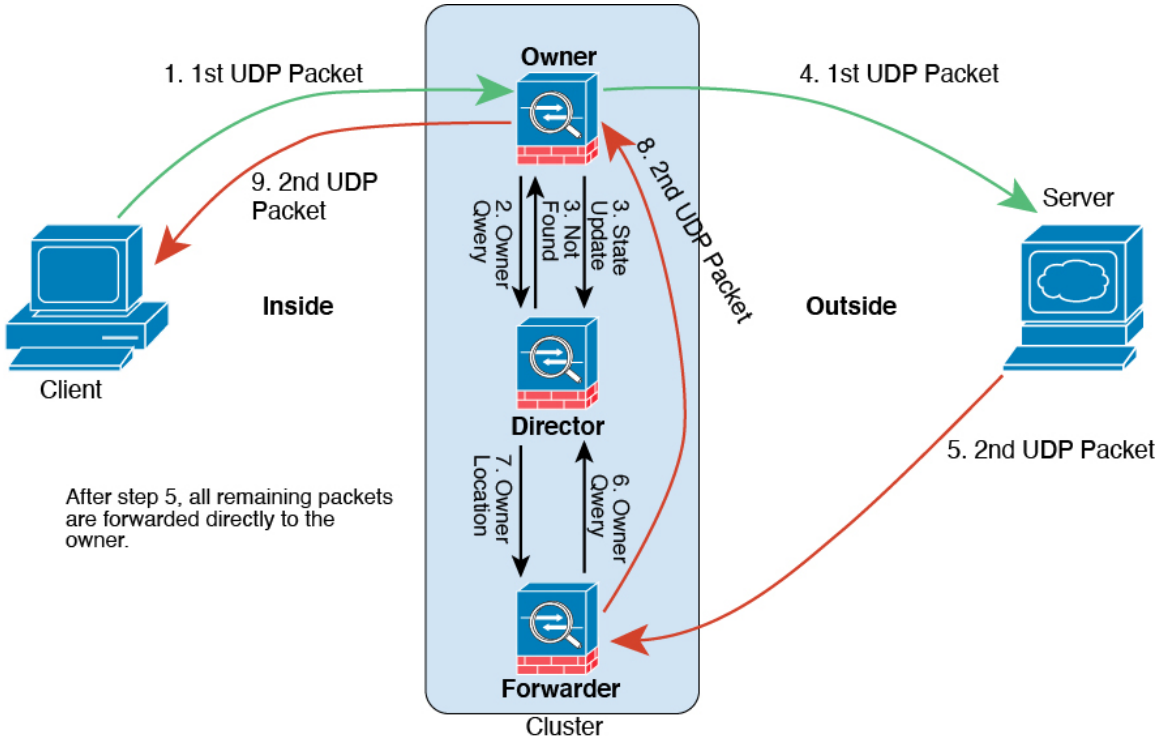
1. SYN 数据包从客户端发出，被传送到一台 ASA（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 ASA（基于负载均衡方法）。此 ASA是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，并记录TCP状态信息以及所有者。导向器将充当该连接的备用所有者。
6. 传送到转发器的任何后续数据包都会被转发到所有者。

7. 如果数据包被传送到任何其他节点，它将向导向器查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向器发送状态更新。

ICMP 和 UDP 的数据流示例

以下图例显示了新连接的建立。

1. 图 *56: ICMP* 和 *UDP* 数据流



第一个 UDP 数据包从客户端发出，被传送到一个ASA（基于负载均衡方法）。

2. 收到第一个数据包的节点查询基于源/目的 IP 地址和端口的散列值选择的导向器节点。
3. 导向器找不到现有流，创建导向器流并将数据包转发回前一个节点。换句话说，导向器已为此流选择了所有者。
4. 所有者创建流，向导向器发送状态更新，然后将数据包转发到服务器。
5. 第二个 UDP 数据包从服务器发出，并被传送到转发器。
6. 转发器向导向器查询所有权信息。对于 DNS 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。
7. 导向器向转发器回复所有权信息。
8. 转发器创建转发流以记录所有者信息，并将数据包转发给所有者。
9. 所有者将数据包转发到客户端。

跨集群实现新 TCP 连接再均衡

如果上游或下游路由器的负载平衡功能导致流量分布不平衡，则可以配置新的连接再平衡，这样每秒新连接数较高的节点就会将新 TCP 流量重定向到其他节点。现有流量将不会移至其他节点。

由于此命令仅基于每秒的连接数进行重新平衡，因此不会考虑每个节点上已建立的连接总数，并且连接总数可能并不相等。

将连接分流到其他节点后，它将成为不对称连接。

请勿为站点间拓扑结构配置连接再均衡；您不需要将新的连接再均衡到位于不同站点的集群成员。

ASA Virtual集群的历史记录

功能名称	版本	功能信息
流状态的可配置集群保持连接间隔	9.20(1)	流所有者向导向器和备份所有者发送保持连接（clu_keepalive 消息）和更新（clu_update 消息），以刷新流状态。您现在可以设置保持连接的间隔。默认值为 15 秒，您也可以将间隔设为 15 到 55 秒。您可能想将间隔设置得更长，以减少集群控制链路上的流量。 新增/修改的命令：**clu-keepalive-interval**
删除偏差语言	9.19(1)	包含术语“主”和“从”的命令、命令输出和系统日志消息已被更改为“控制”和“数据”。 新增/修改的命令：**cluster control-node**、**enable as-data-node**、**prompt**、**show cluster history**、**show cluster info**
适用于 VMware 和 KVM 的 ASAv30、ASAv50 和 ASAv100 集群	9.17(1)	通过 ASA virtual 集群，您可以将最多 16 个 ASA virtual 组合成单个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。ASA virtual 集群支持在路由防火墙模式下使用“单个接口”模式；不支持跨区以太网通道。ASA virtual 将 VXLAN 虚拟接口 (VNI) 用于集群控制链路。 新增/修改的命令：**cluster-interface vni**、**nve-only cluster**、**peer-group**、**show cluster info**、**show cluster info instance-type**、**show nve 1**

第 13 章

在公共云中为 ASA Virtual 部署 ASA 集群

通过集群，您可以将多台 ASA virtual 组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。您可以使用以下方法在公共云中部署 ASA virtual 集群：

- 的 Amazon Web Services (AWS)
- 的 Microsoft Azure

目前仅支持路由防火墙模式。

注释 使用集群时，有些功能不受支持。请参阅集群不支持的功能，第 641 页。

- 关于公共云中的 ASA Virtual 集群，第 585 页
- ASA Virtual 集群许可证，第 589 页
- ASA Virtual 集群要求和前提条件，第 590 页
- ASA Virtual 集群准则，第 591 页
- 在 AWS 中部署集群，第 592 页
- 在 Azure 中部署集群，第 610 页
- 自定义集群操作，第 621 页
- 管理集群节点，第 625 页
- 监控集群，第 629 页
- 集群参考，第 641 页
- 关于公共云中的 ASA Virtual 集群的历史记录，第 655 页

关于公共云中的 ASA Virtual 集群

本节介绍集群架构及其工作原理。

集群如何融入网络中

集群包含多台防火墙，作为单一设备工作。要用作集群，该防火墙需要以下基础设施：

- 独立的网络（称为集群控制链路），通过 VXLAN 接口用于集群内的通信。VXLAN 充当第 3 层物理网络上的第 2 层虚拟网络，让 ASA virtual 能够通过集群控制链路发送广播/组播消息。
- 负载均衡器 - 对于外部负载均衡，您有以下选择：
  - AWS 网关负载均衡器

    AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。ASA virtual 支持使用 Geneve 接口单臂代理且具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。
  - 使用内部和外部路由器（例如思科云服务路由器）的等价多路径路由 (ECMP)

    ECMP 路由可以通过路由指标并列最优的多条“最佳路径”转发数据包。它与 EtherChannel 一样，也可以使用源和目标 IP 地址及/或源和目标端口的散列值将数据包发送到下一跃点。如果将静态路由用于 ECMP 路由，则 ASA virtual 故障会导致问题；如果继续使用该路由，发往故障 ASA virtual 的流量将丢失。因此，如果使用静态路由，请务必要使用静态路由监控功能，例如对象跟踪。我们还建议使用动态路由协议来添加和删除路由，在这种情况下，您必须配置每台 ASA virtual 使之加入动态路由。

注释 负载均衡不支持第 2 层跨区以太网通道。

集群节点

集群节点协调工作来实现安全策略和流量的共享。本节介绍每种节点角色的性质。

引导程序配置

您要在每台设备上配置最低的引导程序配置，包括集群名称、集群控制链路接口和其他集群设置。启用集群的第一个节点通常成为控制节点。在后续节点上启用集群时，这些设备将作为数据节点加入集群。

控制和数据节点角色

一个集群成员是控制节点。如果多个集群节点同时上线，则控制节点由引导程序配置中的优先级设置决定；优先级可设置为 1 到 100，其中 1 为最高优先级。所有其他成员都是数据节点。 通常，当您首次创建集群时，您添加的第一个节点会成为控制节点，因为它是到目前为止集群中的唯一节点。

必须只能在控制节点上执行所有配置（引导程序配置除外）；然后配置将被复制到数据节点中。如果是接口等物理资产，控制节点的配置将被镜像到所有数据节点。例如，如果将以太网接口 1/2 配置为内部接口，将以太网接口 1/1 配置为外部接口，则这些接口也将在数据节点上用作内部和外部接口。

有些功能在集群中无法扩展，控制节点将处理这些功能的所有流量。

独立接口

您可以将集群接口配置为独立接口。

独立接口是正常的路由接口，每个接口都有自己的本地 IP 地址。必须仅在控制节点上配置接口配置，并且每个接口都要使用 DHCP。

注释 不支持第 2 层跨区以太网通道。

集群控制链路

每个节点必须将一个接口作为集群控制链路的 VXLAN (VTEP) 接口。 有关 VXLAN 的详细信息，请参阅VXLAN 接口，第 719 页。

VXLAN 隧道端点

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

VTEP 源接口

VTEP 源接口是一个计划要将其与 VNI 接口相关联的常规ASA virtual 接口。您可以将一个 VTEP 源接口配置为集群控制链路。源接口会被保留，以便仅供集群控制链路使用。每个 VTEP 源接口在同一子网上都有一个 IP 地址。此子网应与所有其他流量隔离，并且只包括集群控制链路接口。

VNI 接口

VNI 接口类似于 VLAN 接口：它是一个虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。您只能配置一个 VNI 接口。每个 VNI 接口在同一子网上都有一个 IP 地址。

对等体 VTEP

与数据接口的常规 VXLAN 只允许单个 VTEP 对等体不同，ASA virtual 集群允许您配置多个对等体。

集群控制链路流量概述

集群控制链路流量包括控制流量和数据流量。

控制流量包括：

- 控制节点选举。
- 配置复制。

- 运行状况监控。

数据流量包括：

- 状态复制。
- 连接所有权查询和数据包转发。

集群控制链路故障

如果某台设备的集群控制链路线路协议关闭，则集群将被禁用；数据接口关闭。当您修复集群控制链路之后，必须通过重新启用集群来手动重新加入集群。

注释 当 ASA virtual 处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。管理接口将保持打开，使用设备从 DHCP 或集群 IP 池接收的 IP 地址。如果使用集群 IP池，在重新加载而设备在集群中仍然处于非活动状态时，则管理接口将无法访问（因为它届时将使用与控制节点相同的主 IP 地址）。您必须使用控制台端口（如果可用）来进行任何进一步配置。

配置复制

集群中的所有节点共享一个配置。您只能在控制节点上进行配置更改（引导程序配置除外），这些更改会自动同步到集群中的所有其他节点。

ASA Virtual集群管理

使用 ASA virtual集群的一个好处可以简化管理。本节介绍如何管理集群。

管理网络

我们建议将所有节点都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理接口

使用 Management 0/0 接口进行管理。

注释 您不能为管理接口启用动态路由。您必须使用静态路由。

您可以使用静态寻址或 DHCP 作为管理 IP 地址。

如果您使用静态寻址，则可以使用集群的主集群 IP 地址是集群的固定地址，而该集群始终属于当前的控制节点。您还要为每个接口配置一个地址范围，以便包括当前控制节点在内的每个节点都可以使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问；当控制节点更改时，主集群 IP 地址将转移到新的控制节点，使集群的管理得以无缝继续。本地 IP 地址用于路由，在排除故障时

也非常有用。例如，您可以连接到主集群 IP 地址来管理集群，该地址始终属于当前的控制节点。要管理单个成员，您可以连接到本地 IP 地址。对于 TFTP 或系统日志等出站管理流量，包括控制节点在内的每个节点都使用本地 IP 地址连接到服务器。

如果使用 DHCP，则不使用本地地址池或主集群 IP 地址。

注释 传入设备的流量必须指向节点的管理 IP 地址；传入设备的流量不会通过群集控制链路转发到任何其他节点。

控制节点管理与数据节点管理

所有管理和监控均可在控制节点上进行。从控制节点中，您可以检查所有节点的运行时统计信息、资源使用情况或其他监控信息。您也可以向集群中的所有节点发出命令，并将控制台消息从数据节点复制到控制节点。

如果需要，您可以直接监控数据节点。虽然在控制节点上可以执行文件管理，但在数据节点上也可以如此（包括备份配置和更新映像）。以下功能在控制节点上不可用：

- 监控每个节点的集群特定统计信息。
- 监控每个节点的系统日志（控制台复制启用时发送至控制台的系统日志除外）。
- SNMP
- NetFlow

加密密钥复制

当您在控制节点上创建加密密钥时，该密钥将复制到所有数据节点。如果您有连接到主集群 IP 地址的 SSH 会话，则控制节点发生故障时连接将断开。新控制节点对 SSH 连接使用相同的密钥，这样当您重新连接到新的控制节点时，无需更新缓存的 SSH 主机密钥。

ASDM 连接证书 IP 地址不匹配

默认情况下，ASDM 连接将根据本地 IP 地址使用自签名证书。如果使用 ASDM 连接到主集群 IP 地址，则可能会因证书使用的是本地 IP 地址而不是主集群 IP 地址，系统会显示一则警告消息，指出 IP 地址不匹配。您可以忽略该消息并建立 ASDM 连接。但是，为了避免此类警告，您也可以注册一个包含主集群 IP 地址和 IP 地址池中所有本地 IP 地址的证书。然后，您可将此证书用于每个集群成员。有关详细信息，请参阅 https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html。

ASA Virtual 集群许可证

每个集群节点都需要相同的模型许可证。我们建议为所有节点使用相同数量的 CPU 和内存，否则将限制所有节点上的性能，以匹配功能最低的成员。吞吐量级别将从控制节点复制到每个数据节点，以便它们匹配。

注释 如果取消注册 ASA virtual 从而使得其未经许可，则在重新加载 ASA virtual 后，它将恢复到严格的速率限制状态。未经许可的低性能集群节点将对整个集群的性能产生负面影响。请务必保留所有集群节点的许可，或删除任何未经许可的节点。

ASA Virtual 集群要求和前提条件

型号要求

- ASAv30, ASAv50, ASAv100
- 以下公共云服务：
  - 的 Amazon Web Services (AWS)
  - 的 Microsoft Azure
- 最多 16 个节点

另请参阅《ASA Virtual 入门指南》中有关 ASA Virtual 的一般要求。

硬件和软件要求

集群中的所有节点：

- 必须在同一个性能层。我们建议对所有节点都使用相同数量的CPU和内存，否则所有节点上的性能将受到限制，以匹配性能最低的节点。
- 除在映像升级时以外，必须运行完全相同的软件。支持无中断升级。不匹配的软件版本可能会导致性能不佳，因此请务必在同一维护窗口中升级所有节点。
- 支持单个可用性区域部署。
- 集群控制链路接口必须位于同一子网中，因此集群应部署在同一子网中。

MTU

确保连接到集群控制链路的端口配置了正确（更高）的 MTU。如果存在不匹配的 MTU，则集群形成将失败。默认情况下，集群控制链路 MTU 会被设置为比数据接口高 154 字节。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销（100 字节）加上 VXLAN 开销（54 字节）。

对于具有 GWLB 的 AWS，数据接口使用 Geneve 封装。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。您应将源接口 MTU 设置为网络 MTU + 306 字节。因此，对于标准的 1500 MTU 网络路径，源接口 MTU 应为 1806，而集群控制链路 MTU 应为 +154, 1960。

对于具有 GWLB 的 Azure，数据接口使用 VXLAN 封装。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。您应将源接口 MTU 设置为网络 MTU + 54 字节。

下表显示了建议的集群控制链路 MTU 和数据接口 MTU。

注释 我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。

表 *20:* 建议的 *MTU*

公共云	集群控制链路 MTU	数据接口 MTU
具有 GWLB 的 AWS	1960	1806
AWS	1654	1500
具有 GWLB 的 Azure	1554	1454
Azure	1554	1400

ASA Virtual 集群准则

高可用性

集群不支持高可用性。

IPv6

集群控制链路只有在使用 IPv4 时才受支持。

其他准则

- 当拓扑发生重大更改时（例如添加或删除 EtherChannel 接口、启用或禁用 ASA Virtual 或交换机上的接口、添加额外的交换机形成冗余交换机系统），您应禁用运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑更改完成且配置更改已同步到所有设备后，您可以重新启用接口运行状态检查功能。
- 将节点添加到现有集群时或重新加载节点时，会有限地暂时丢弃数据包/断开连接；这是预期的行为。有些时候，丢弃的数据包会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包将使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 对于解密的 TLS/SSL 连接，解密状态不同步，如果连接所有者失败，则解密的连接将重置。需要与新节点建立新的连接。未解密的连接（它们匹配“不解密”规则）不受影响，并且可以正确复制。
- 不支持动态扩展。

- 在每个维护窗口完成后执行全局部署。
- 确保不要一次从自动扩展组 (AWS) 或规模集 (Azure) 中删除多个设备。我们还建议您先在设备上运行 **cluster disable** 命令，然后再从组东扩展组 (AWS) 或规模集(Azure) 中删除设备。
- 如果要禁用集群中的数据节点和控制节点，我们建议您在禁用控制节点之前先禁用数据节点。如果在集群中有其他数据节点时禁用了某个控制节点，则必须将其中一个数据节点升级为控制节点。请注意，角色更改可能会对集群造成干扰。
- 在本指南中提供的 Day 0 配置脚本中，您可以根据需要更改 IP 地址，提供自定义接口名称，并更改 CCL-Link 接口的顺序。

集群默认设置

- 将自动生成 cLACP 系统 ID 且系统优先级默认为 1。
- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。
- 用于发生故障的集群控制链路的集群自动重新加入功能为每 5 分钟尝试无限次。
- 用于发生故障的数据接口的集群自动重新加入功能为每 5 分钟尝试 3 次，增量间隔设置为 2。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

在 AWS 中部署集群

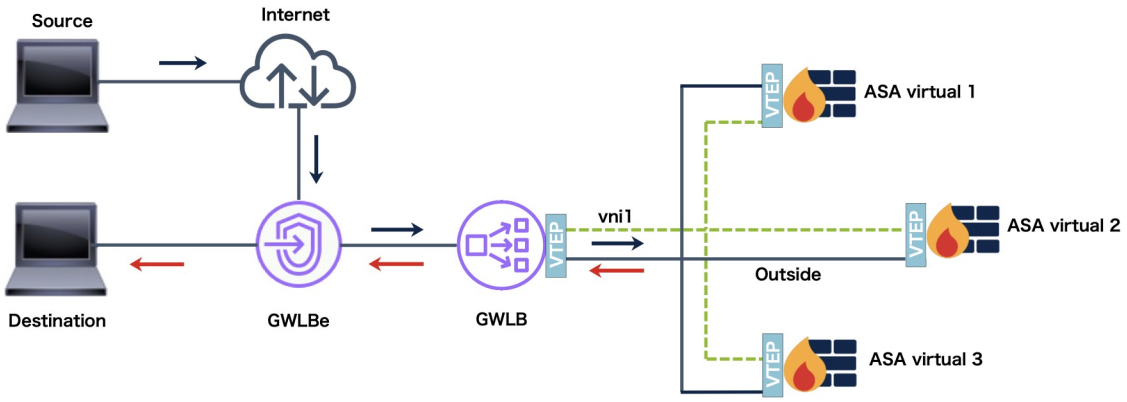
要在 AWS 中部署集群，您可以手动部署或使用 CloudFormation 模板来部署堆栈。您可以将集群与 AWS 网关负载均衡器或非本地负载均衡器（例如思科云服务路由器）配合使用。

AWS 网关负载均衡器和 Geneve 单臂代理

注释 这是 Geneve 接口当前唯一支持的使用案例。

AWS网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。ASA Virtual支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示了从网关负载均衡器终端转发到网关负载均衡器的流量。网关负载均衡器会在多个ASA Virtual之间进行均衡，这些流量在丢弃流量或将其发送回网关负载均衡器之前对其进行检查（掉头流量）。然后，网关负载均衡器会将流量发送回网关负载均衡器终端和目的地。

图 *57: Geneve* 单臂代理



拓扑示例

ASA Virtual 在 AWS 区域的单个和多个可用性区域中使用自动缩放进行集群

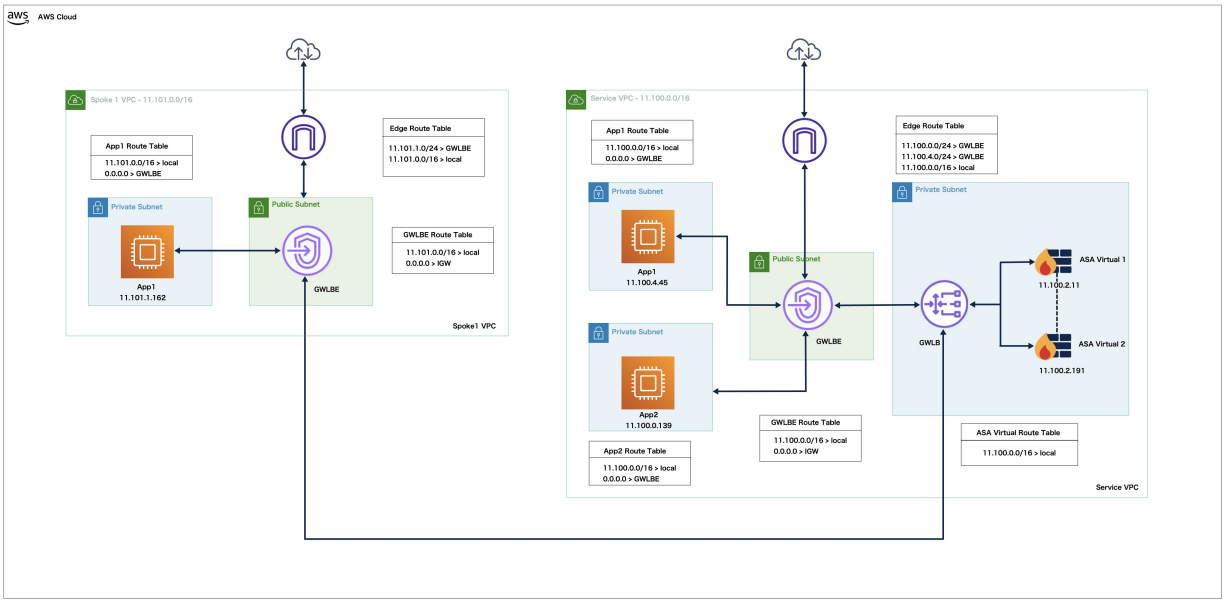
可用性区域是指一个 AWS 区域内独立运行的独立数据中心或一组独立数据中心。每个区域都有自己的网络基础设施、连接和电源，从而确保一个区域的故障不会影响到其他区域。为了提高冗余和可靠性，公司在灾难恢复计划中使用多个可用性区域。

跨多个可用性区域部署 ASA Virtual 并配置支持动态扩展的集群可以显着增强基础设施的可用性和可扩展性。此外，在同一区域利用多个可用性区域可以提供额外的冗余，并在发生故障时保证高可用性。

您可以修改集群控制链路 (CCL) 的 IP 分配机制，以支持 AWS 上 ASA Virtual 群集的单可用性区域和多可用性区域部署。下面给出的拓扑结构描述了具有自动扩展能力的单个和多个可用性区域中的入站和出站流量。

ASA Virtual 在单个可用性区域中使用自动缩放进行集群

集群中有两个连接到 GWLB 的 ASA Virtual 实例。

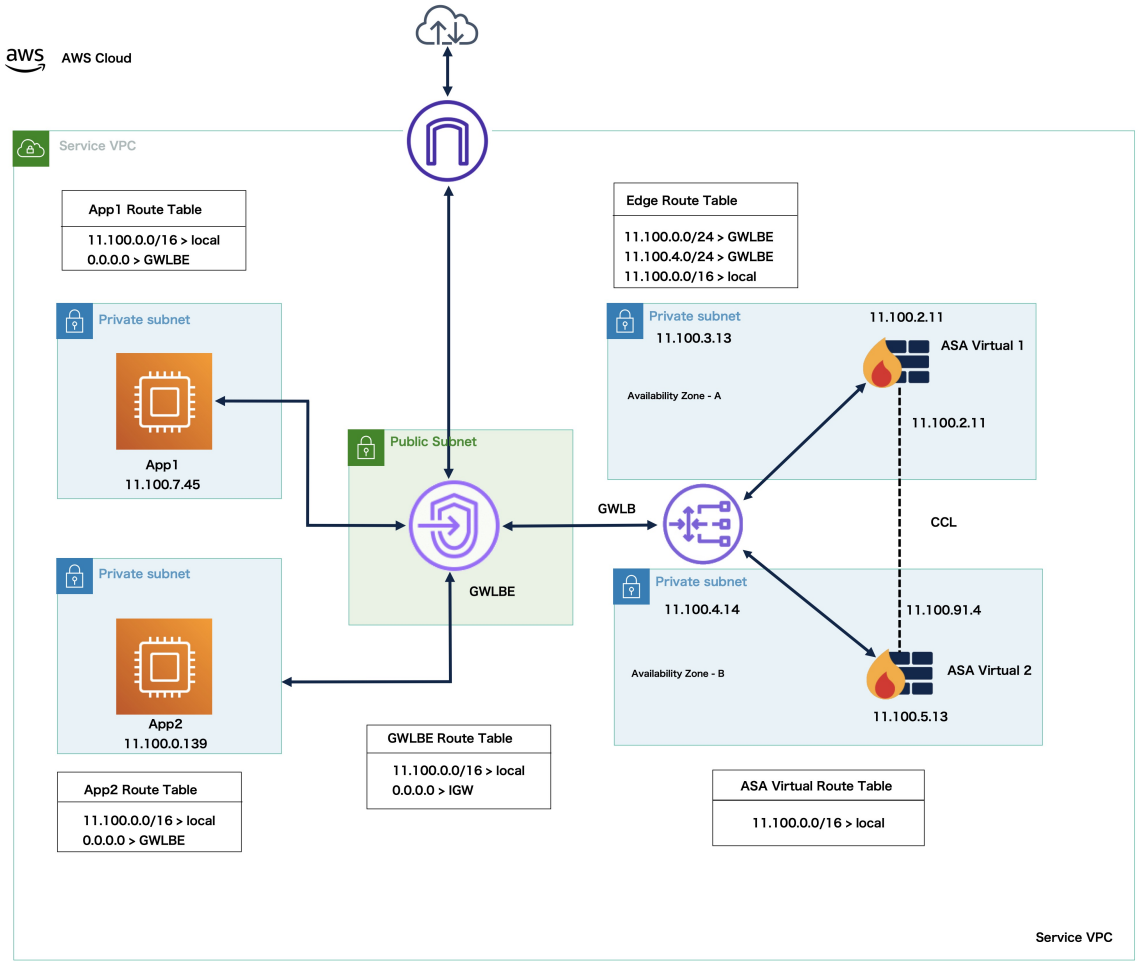


来自互联网的入站流量会进入GWLB端点，然后由端点将流量传输到GWLB。然后，流量被转发到ASA Virtual 集群。集群中的 ASA Virtual 实例检测到流量后，将其转发到应用虚拟机 App1。

来自 App1 的出站流量将传输到 GWLB 终端 > GWLB > ASAv > GWLB > GWLB 终端，然后由 GWLB 终端发送到互联网。

ASA Virtual 使用自动缩放解决方案在多个可用性区域中使用自动缩放进行集群

集群中有两个 ASA Virtual 实例连接到 GWLB，它们位于不同的可用性区域。

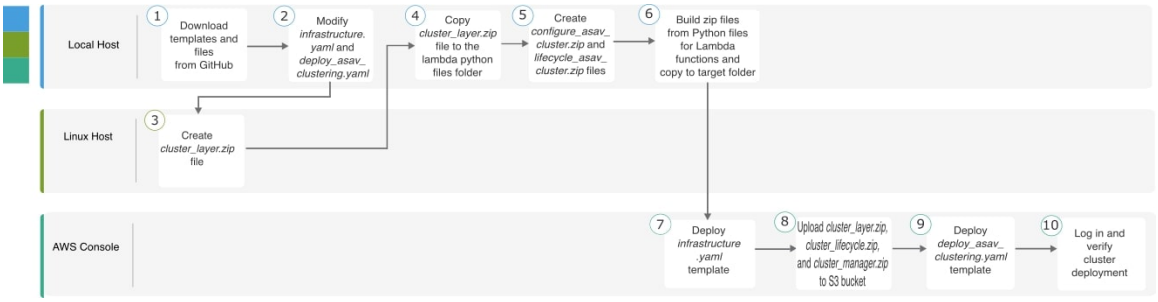


来自互联网的入站流量会进入GWLB端点，然后由端点将流量传输到GWLB。然后，根据可用性区域将流量路由到 ASA Virtual 集群。集群中的 ASA Virtual 实例检测到流量后，将其转发到应用虚拟机 App1。

在 AWS 上部署 ASA Virtual 集群的端到端流程

基于模板的部署

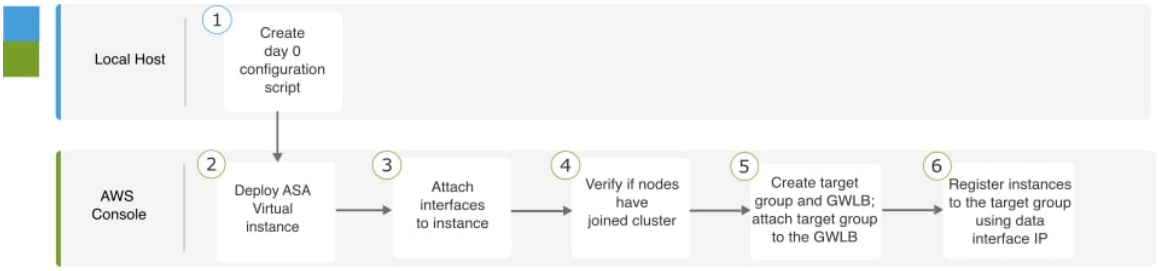
以下流程图说明了在 AWS 上基于模板部署 ASA Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从 GitHub 下载模板和文件。
2	本地主机	修改 *infrastructure.yaml* 和 *deploying_asav_clustering.yaml* 模板。
3	Linux 主机	创建 *cluster_layer.zip* 文件。
4	本地主机	将 *cluster_layer.zip* 文件复制到 Lambda python files 文件夹。
5	本地主机	创建 *configure_asav_cluster.zip* 和 *lifecycle_asav_cluster.zip* 文件。
6	本地主机	从 Python 文件为 Lambda 函数构建 zip 文件，并复制到目标文件夹。
7	AWS 控制台	部署 *Infrastructure.yaml* 模板。
8	AWS 控制台	将 cluster_layer.zip、cluster_lifecycle.zip 和 cluster_manager.zip 上传 S3 存储桶。
9	AWS 控制台	部署 *deploy_asav_clustering.yaml* 模板。
10	AWS 控制台	登录并验证集群部署。

手动部署

以下流程图说明了在 AWS 上手动部署 ASA Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	创建 AWS 的 Day-0 配置
2	AWS 控制台	部署 ASA Virtual 实例。
3	AWS 控制台	将接口连接到实例。
4	AWS 控制台	验证节点是否已加入集群。
5	AWS 控制台	创建目标组和 GWLB；将目标组附加到 GWLB。
6	AWS 控制台	使用数据接口 IP 向目标组注册实例。

模板

以下提供的模板可在GitHub中获取。参数值一目了然，包括模板中给出的参数名称、默认值、允许值和说明。

- Infrastructure.yaml - 基础设施部署模板。
- deploy_asav_clustering.yaml - 用于集群部署的模板。

注释 在部署集群节点之前，请确保检查支持的AWS实例类型列表。此列表可在*deploy_asav_clustering.yaml*模板中的参数 InstanceType 的允许值下找到。

在 AWS 中使用 GWLB 配置 ASA Virtual 集群的目标故障转移

AWS中的ASA Virtual集群利用网关负载均衡器(GWLB)来均衡网络数据包并将其转发到指定的ASA Virtual 节点。GWLB 用于在目标节点发生故障转移或取消注册的情况下，继续向该节点发送网络数据包。

AWS 中的目标故障转移功能使 GWLB 能够在计划维护期间取消注册或目标节点发生故障的情况下将网络数据包重定向到正常运行的目标节点。它利用集群的状态故障转移。

注释 如果目标节点在 GWLB 使用 SSH、SCP、CURL 或其他协议路由流量时发生故障，则将流量重定向到正常运行的目标可能会出现延迟。此延迟是由于流量的重新平衡和重新路由导致的。

在 AWS 中，您可以通过 AWS ELB API 或 AWS 控制台来配置目标故障转移。

- AWS API - 在 AWS Elastic Load Balancing (ELB) API - *modify-target-group-attributes* 中，您可以通过修改以下两个新参数来定义流量处理行为。
  - target_failover.on_unhealthy - 定义当目标变得运行不正常时 GWLB 如何处理网络流量。
  - target_failover.on_deregistration - 定义当目标取消注册时 GWLB 如何处理网络流量。

  以下命令显示了定义这两个参数的 API 参数配置示例。

```
aws elbv2 modify-target-group-attributes \
--target-group-arn arn:aws:elasticloadbalancing:…/my-targets/73e2d6bc24d8a067 \
--attributes \
Key=target_failover.on_unhealthy, Value=rebalance[no_rebalance] \
Key=target_failover.on_deregistration, Value=rebalance[no_rebalance]
```

  有关详细信息，请参阅 AWS 文档中的 TargetGroupAttribute。

- AWS 控制台 – 在 EC2 控制台中，您可以通过配置以下选项来启用目标组页面上的目标故障转移选项。
  - 编辑目标组属性
  - 启用目标故障转移
  - 验证再平衡流量

  有关如何启用目标故障转移的详细信息，请参阅在 AWS 中为 ASA Virtual 启用目标故障转移。

使用 CloudFormation 模板在 AWS 中部署堆栈

使用自定义 CloudFormation 模板在 AWS 中部署堆栈。

开始之前

- 您需要一台安装了 Python 3 的 Linux 计算机。

过程

步骤 1 准备模板。

a) 将 github 存储库克隆到本地文件夹。请参阅https://github.com/CiscoDevNet/cisco-asav/tree/master/cluster/aws。

b) 使用所需的参数修改 **infrastructure.yaml** 和 **deploy_asav_clustering.yaml**。

c) 创建名为 **cluster_layer.zip** 的文件，为 Lambda 函数提供必要的 Python 库。

我们建议使用安装了 Python 3.9 的 Amazon Linux 创建 **cluster_layer.zip** 文件。

注释
如果您需要 Amazon Linux 环境，可以使用 Amazon Linux 2023 AMI 或运行最新版本的 Amazon Linux 的 AWS Cloudshell 创建 EC2 实例。

要创建 cluster-layer.zip 文件，您需要先创建包含 python 库软件包详细信息的 **requirements.txt** 文件，然后运行 shell 脚本。

1. 通过指定 python 软件包详细信息来创建 **requirements.txt** 文件。

   以下是您在 **requirements.txt** 文件中提供的示例软件包详细信息：

```
$ cat requirements.txt
pycryptodome
paramiko
requests
scp
jsonschema
cffi
zipp
importlib-metadata
```

2. 运行以下 shell 脚本以创建 **cluster_layer.zip**文件。

```
$ pip3 install --platform manylinux2014_x86_64
--target=./python/lib/python3.9/site-packages
--implementation cp --python-version 3.9 --only-binary=:all:
--upgrade -r requirements.txt
$ zip -r cluster_layer.zip ./python
```

注释
如果在安装期间遇到依赖项冲突错误（例如 urllib3 或加密），建议您在 **requirements.txt** 文件中包含冲突软件包及其建议版本。之后，您可以再次运行安装来解决冲突。

d) 将生成的 **cluster_layer.zip** 文件复制到 lambda python files 文件夹。

e) 创建 **configure_asav_cluster.zip** 和 **lifecycle_asav_cluster.zip** 文件

可以在克隆存储库顶级目录中找到 make.py 文件。这样会将 python 文件压缩为 Zip 文件并复制到目标文件夹。

python3 make.py build

注释
在部署集群之前，请确保已根据基础设施要求（例如 ASAv 集群自动扩展部署所需的 VPC、子网、S3 存储桶）自定义 AWS CFT 模板文件 - **Infrastructure.yaml** 和 **deploy_asav_clustering.yaml**。

步骤 2 部署 **Infrastructure.yaml** 并记下集群部署的输出值。在部署基础设施堆栈之前，必须确定将使用的 AWS 区域和可用性区域。每个 AWS 区域都有一组不同的可用性区域和 VPC 基础设施，因此必须为部署选择正确的区域和可用性区域。

a) 在 AWS 控制台上，转到 **CloudFormation** 并点击**创建堆栈 (Create stack)**；选择**使用新资源（标准）(With new resources [standard])**。

b) 选择**上传模板文件 (Upload a template file)**，点击**选择文件 (Choose file)**，然后从目标文件夹中选择 **infrastructure.yaml**。

c) 点击**下一步 (Next)** 并提供所需的信息。

d) 为集群输入唯一的**集群名称**和**集群编号**。

e) 从**可用性区域 (Availability Zone)** 列表中选择可用性区域。此字段仅列出基于 AWS 区域的可用性区域，您选择该区域是为了使用 ClusterFormation 模板部署基础设施堆栈。

f) 在**内部子网 CIDR (Inside subnet CIDR)** 字段中输入用逗号分隔的预定义子网 CIDR 值。

g) 从 从 **Lambda AZ 列表 (List of Lambda AZs)** 中选择 Lambda 跨可用性区域通信所需的可用性区域。

h) 点击**下一步 (Next)**，然后点击**创建堆栈 (Create stack)**。

系统将显示 CREATE_COMPLETE 信息，说明基础设施堆栈的部署状态。

i) 在部署完成后，转到**输出 (Outputs)** 并记下 S3 **BucketName**。

图 ***58: infrastructure.yaml*** 的输出

Outputs (13)

Search outputs

Key	Value	Description	Export name
AZ	sa-east-1a	Availability zone	-
BucketName	ran-cls-infra-s3bucketcluster-kckr7518u00l	Name of the Amazon S3 bucket	-
BucketUrl	http://ran-cls-infra-s3bucketcluster-kckr7518u00l.s3-website-sa-east-1.amazonaws.com	URL of S3 Bucket Static Website	-
CCLSubnetId	subnet-050feb347e57eba99	CCL subnet ID	-
EIPforNATgw	52.67.246.95	EIP reserved for NAT GW	-
InInterfaceSGId	sg-0333e92f36b2aa0bf	Security Group ID for Instances Inside Interface	-
InsideSubnetIds	subnet-047c0a2beffb5a70f	Inside subnet ID	-
InstanceSGId	sg-0c0c6bfb5ba5f1c10	Security Group ID for Instances Management Interface	-
LambdaSecurityGroupId	sg-01771b0d3012a40c5	Security Group ID for Lambda Functions	-
LambdaSubnetIds	subnet-0fb24785c687d50e4,subnet-0f1996a02ffaa2e62	List of lambda subnet IDs (comma seperated)	-
MgmtSubnetIds	subnet-02d4a757b95a9a5b9	Mangement subnet ID	-
UseGWLB	Yes	Use Gateway Load Balancer	-
VpcName	vpc-003b592ad2518d03d	Name of the VPC created	-

步骤 3 将 **cluster_layer.zip**、**configure_asav_cluster.zip** 和 **lifecycle_asav_cluster.zip** 上传到通过 **infrastructure.yaml** 创建的 S3 存储桶。

步骤 4 部署 **deploy_asav_clustering.yaml**：

a) 转到 **CloudFormation**，点击**创建堆栈 (Create stack)**，然后选择**使用新资源（标准）(With new resources [standard])**。

b) 依次点击**上传模板文件 (Upload a template file)**、**选择文件 (Choose file)**，然后从目标文件夹中选择 **deploy_asav_clustering.yaml**。

c) 点击**下一步 (Next)** 并提供所需的信息。

d) 提供以下集群和基础设施配置信息。

参数	允许的值/类型	说明
集群配置		

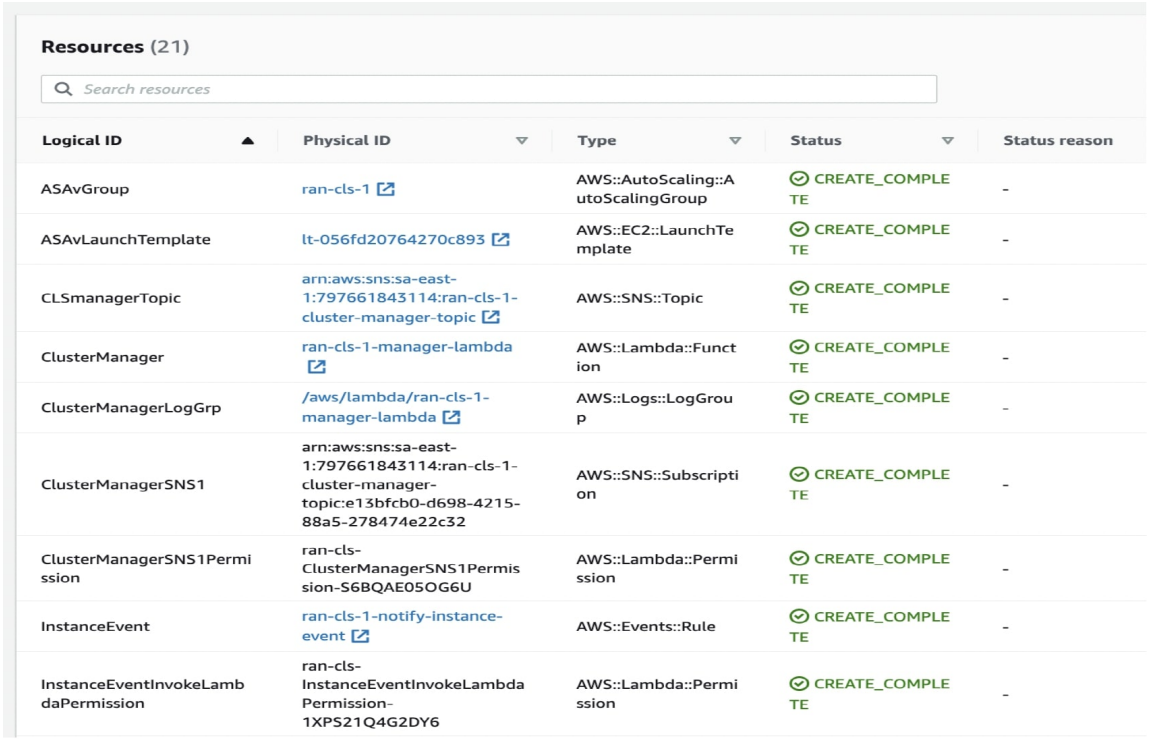
参数	允许的值/类型	说明
集群名称	字符串	这是集群名称前缀。集群编号将作为后缀添加。
集群编号	字符串	这是集群编号。这将作为集群名称的后缀 (msa-asa-infra)。例如，如果此值为 **1**，则组名称将为 *msa-asa-infra-1*。 它应至少为 1 个数字，但不超过 3 个数字。默认值：1。
集群规模	数字	这是集群中 ASA Virtual 节点的总数。 最小值：1 最大值：16
基础设施详细信息		
可用性区域数量	字符串	这是部署 ASA Virtual 的可用性区域总数。（根据地区的不同，可用性区域的数量从最少 1 个到最多 3 个不等）。 子网将在这些可用性区域内创建。 此列表中可用的可用性区域基于为部署集群而选择的区域。 **注释** Lambda 跨两个可用性区域创建。管理子网和内部子网根据此参数在三个可用性区域内创建。
输入有效的可用性区域列表	字符串	可用性区域列表基于您计划部署的区域。 在可用性区域列表中，选择有效的可用性区域（1 个或 2 个可用性区域或 3 个可用性区域）。 计数应与可用性区域数量参数的值匹配。
集群电子邮件通知	字符串	集群事件电子邮件将被发送到的邮件地址。您必须接受订用电子邮件请求，才能收到此电子邮件通知。 示例：admin@company.com
GWLB 配置		
部署 GWLB 终端	字符串	点击**是 (Yes)** 部署 GWLB 端点。 默认情况下，该值设置为**否 (No)**。
GWLBE 的 VPC ID	字符串	输入 VPC 以部署网关负载均衡器终端。 **注释** 如果不部署 GWLB 终端，请不要在此字段中输入任何值。

参数	允许的值/类型	说明
GWLBE 的子网 ID	字符串	仅输入一个子网 ID。 注释 如果不部署 GWLB 终端，请不要在此字段中输入任何值。 确保子网属于正确的 VPC 以及您指定的可用性区域。
目标故障转移	字符串	当目标发生故障或取消注册时，启用目标故障转移支持。（默认情况下，此参数的值设置为 **rebalance**）。 • **no_rebalance**：将现有流量导向故障目标，将新流量导向健康目标，从而确保向后兼容性。 • **rebalance**：重新分配现有流量，同时确保新流量流向正常运行的目标。
输入 GWLB 的运行状况检查端口	字符串	输入 GWLB 的运行状况检查端口。 注释 默认情况下，此端口不得用于流量。 确保您提供的值是有效的 TCP 端口。默认值：80
思科 ASAv 实例配置		
ASAv 实例类型	字符串	思科 ASAv EC2 实例类型。 确保 AWS 区域支持您选择的实例类型。 默认情况下，**c5.xlarge** 处于选中状态。
ASAv 实例许可证类型	字符串	选择思科 ASAv EC2 实例许可证类型。确保您在 **AMI-ID** 参数中输入的 AMI ID 的许可类型相同。 默认情况下，选择 **BYOL**。
ASAv 智能软件许可证令牌	字符串	（可选）提供用于注册 ASAv 设备的思科智能软件许可证令牌。
ASAv AMI-ID	字符串	根据地区、版本和许可证类型（BYOL 或 PAYG）选择正确的 AMI ID。 ASAv 9.19 及更高版本支持集群，ASAv 9.22 及更高版本支持自动扩展和多可用性区域增强功能。 类型：AWS::EC2::Image::Id 默认情况下：ami-024f546cb9cbae1bb
ASAv 密码	字符串	ASAv 实例密码。

参数	允许的值/类型	说明
		密码将在 ASAv 可访问后激活。 最小长度必须为 8 个字符。密码可以是纯文本密码，也可以是 KMS 加密密码。
Cpu 阈值	CommaDelimitedList	（可选）指定非零的下阈值和上阈值将创建比例策略。如果选择 (0,0)，则不会创建 CPU 扩展警报或策略。评估点和数据点采用默认值或建议值。 默认情况下，此模板中启用**自动缩放**。部署后可以禁用自动缩放。

e) 点击**下一步 (Next)**。
f) 点击以确认所有 AWS CloudFormation 选项。
g) 点击**提交 (Submit)** 以部署集群。
h) 点击**下一步 (Next)**，然后点击**创建堆栈 (Create Stack)**。

图 ***59:*** 已部署的资源



状态从 CREATE_IN_PROGRESS 变为 CREATE COMPLETE，表示部署成功。

步骤 5 通过登录到任何一个节点并输入 **show cluster info** 命令来验证集群部署。

```
show cluster info
```

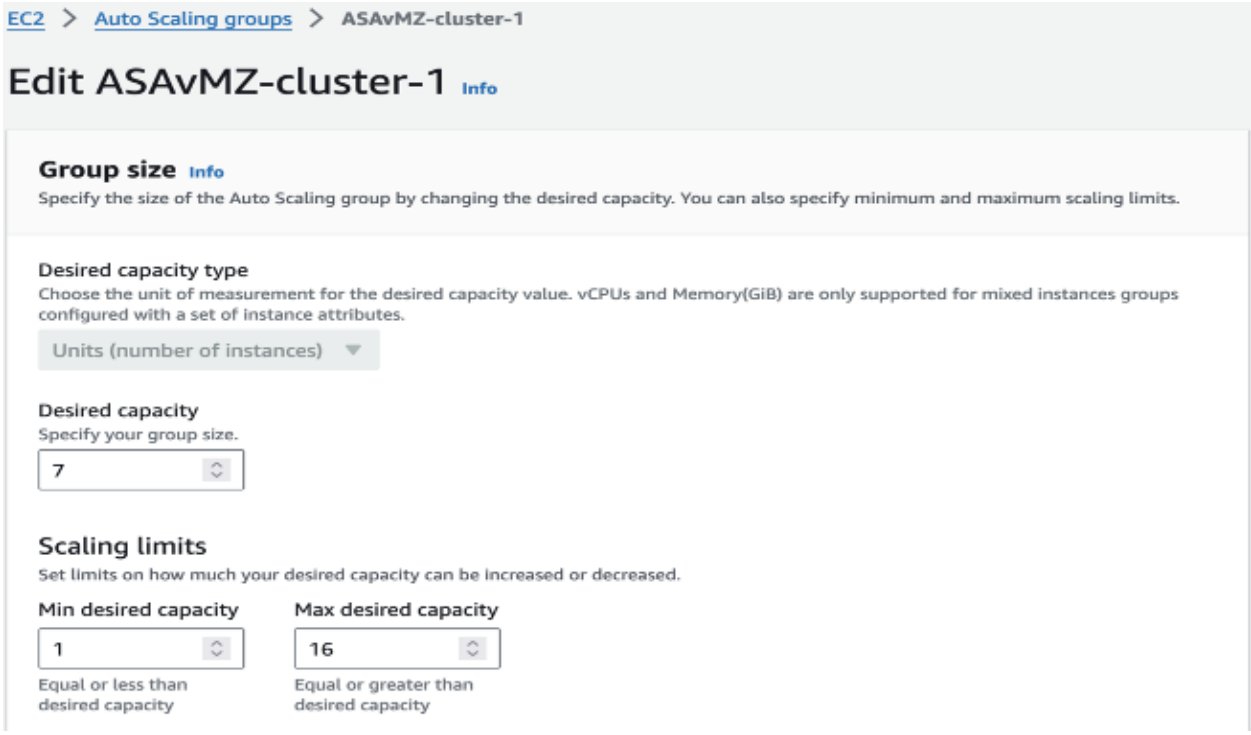
```
Cluster oneclicktest-cluster: On
Interface mode: individual
Cluster Member Limit : 16
This is "200" in state CONTROL_NODE
ID : 0
Version : 9.19.1
Serial No.: 9AU42EN5D1E
CCL IP : 1.1.1.200
CCL MAC : 4201.0a0a.0fc7
Module : ASAv
Resource : 4 cores / 8192 MB RAM
Last join : 15:26:22 UTC Jul 17 2022
Last leave: N/A
Other members in the cluster:
Unit "204" in state DATA_NODE
ID : 1
Version : 9.19.1
Serial No.: 9AJ9N46947R
CCL IP : 1.1.1.204
CCL MAC : 4201.0a0a.0fcb
Module : ASAv
Resource : 4 cores / 8192 MB RAM
Last join : 16:57:42 UTC Jul 17 2022
Last leave: 16:03:25 UTC Jul 17 2022
```

自动缩放参数配置

部署完成后，必须指定 ASAv Autoscale 组的**最小 (Minimum)**、**最大 (Maximum)** 和**期望 (Desired)** 容量。您必须验证自动缩放功能。

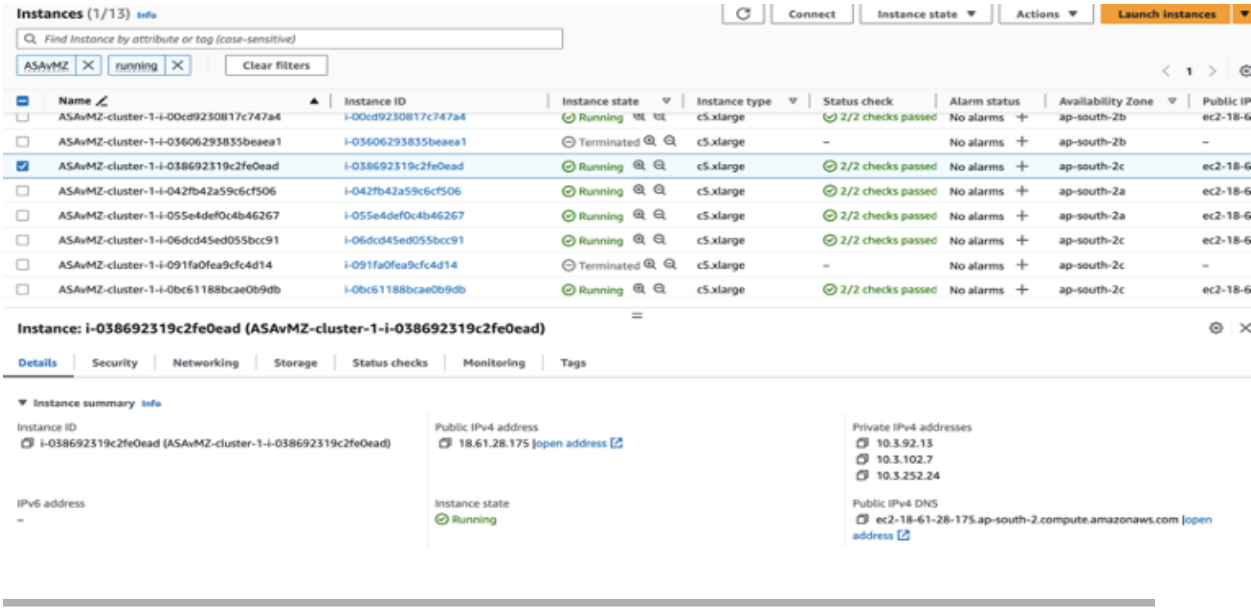
过程

步骤 1 在 AWS 控制台中，依次选择 **服务 (Services)** > **EC2** > **自动扩展组 (Auto Scaling groups)** > **已创建 ClusterAutoscale 组 (Created ClusterAutoscale group)**。



步骤 2 配置所需容量 **(Desired capacity)**，然后设置扩展限制 **(Scaling limits)** 容量。

步骤 3 在 AWS Cloudwatch 警报中检查 CPU 指标数据是否可用，缩放是否按预期进行。



通过更新堆叠在 ASA Virtual 集群中配置所需的 IMDSv2 模式

您可以为 AWS 上已部署的 ASA Virtual 自动缩放组实例配置 IMDSv2 必需模式。

Before you begin

仅 ASA Virtual 9.20.3 及更高版本支持 IMDSv2 必需模式。在为您的部署配置 IMDSv2 Required 模式之前，请确保您现有实例的版本与 IMDSv2 API 兼容（升级到 9.20.3 版或更高版本）。

Procedure

步骤 1 在 AWS 控制台中，转到 **CloudFormation** ，然后点击**堆栈 (Stacks)**。

步骤 2 选择初始部署的集群实例的堆栈。

步骤 3 点击**更新**。

步骤 4 在**更新堆栈 (Update stack)** 页面上，点击**替换现有模板 (Replace existing template)**。

步骤 5 在 **指定模板** 部分下，点击 **上传模板文件**。

步骤 6 选择并上传支持 IMDSv2 的模板。

步骤 7 为模板中的输入参数提供值。

步骤 8 更新堆栈。

在 AWS 中手动部署集群

要手动部署集群，请准备 Day-0 配置并部署每个节点。

创建 AWS 的 Day-0 配置

使用以下命令为每个集群节点提供引导程序配置：

网关负载均衡器示例

以下运行配置示例会为网关负载均衡器创建一个配置，其中一个用于掉头流量的Geneve接口和一个用于集群控制链路的 VXLAN 接口。

```
cluster interface-mode individual force
policy-map global_policy
class inspection_default
no inspect h323 h225
no inspect h323 ras
no inspect rtsp
no inspect skinny

int m0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
no shut

interface TenGigabitEthernet0/0
nameif geneve-vtep-ifc
security-level 0
ip address dhcp
```

```
no shutdown

interface TenGigabitEthernet0/1
nve-only cluster
nameif ccl_link
security-level 0
ip address dhcp
no shutdown

interface vni1
description Clustering Interface
segment-id 1
vtep-nve 1

interface vni2
proxy single-arm
nameif ge
security-level 0
vtep-nve 2

object network ccl_link
range 10.1.90.4 10.1.90.254 //Mandatory user input, use same range on all nodes
object-group network cluster_group
network-object object ccl_link
nve 2
encapsulation geneve
source-interface geneve-vtep-ifc
nve 1
encapsulation vxlan
source-interface ccl_link
peer-group cluster_group

cluster group asav-cluster // Mandatory user input, use same cluster name on all nodes
local-unit 1 //Value in bold here must be unique to each node
cluster-interface vni1 ip 1.1.1.1 255.255.255.0 //Value in bold here must be unique to each
 node
priority 1
enable noconfirm

mtu geneve-vtep-ifc 1806
mtu ccl_link 1960
aaa authentication listener http geneve-vtep-ifc port 7575 //Use same port number on all
nodes
jumbo-frame reservation
wr mem
```

注释 对于 AWS 运行状况检查设置，请务必指定您在此处设置的 **aaa authentication listener http** 端口。

非本地负载均衡器示例

以下示例会创建一个配置，用于具有管理接口、内部接口和外部接口的非本地负载均衡器，以及用于集群控制链路的 VXLAN 接口。

```
cluster interface-mode individual force
interface Management0/0
management-only
nameif management
ip address dhcp
```

```
interface GigabitEthernet0/0
no shutdown
nameif outside
ip address dhcp

interface GigabitEthernet0/1
no shutdown
nameif inside
ip address dhcp

interface GigabitEthernet0/2
nve-only cluster
nameif ccl_link
ip address dhcp
no shutdown

interface vni1
description Clustering Interface
segment-id 1
vtep-nve 1

jumbo-frame reservation
mtu ccl_link 1654
object network ccl_link
range 10.1.90.4 10.1.90.254          //mandatory user input
object-group network cluster_group
network-object object ccl_link

nve 1
encapsulation vxlan
source-interface ccl_link
peer-group cluster_group

cluster group asav-cluster          //mandatory user input
local-unit 1                        //mandatory user input
cluster-interface vni1 ip 10.1.1.1 255.255.255.0  //mandatory user input
priority 1
enable
```

注释 如果要复制并粘贴上面给出的配置，请确保从配置中删除 **//mandatory user input**。

部署集群节点

部署集群节点以便形成集群。

过程

步骤 1 使用具有所需数量的接口的集群 Day 0 配置部署 ASA Virtual 实例 - 如果使用网关负载均衡器 (GWLB)，则为三个接口；如果使用非本地负载均衡器，则为四个接口。在 **配置实例详细信息 > 高级详细信息** 部分中，粘贴您的 day0 配置。

注释
确保按以下顺序将接口连接到实例。

- AWS 网关负载均衡器 - 三个接口 - 管理、诊断、内部和集群控制链路。

- 非本地负载均衡器 - 四个接口 - 管理、内部、外部和集群控制链路。

有关在 AWS 上部署 ASA Virtual 的更多信息，请参阅 在 AWS 上部署 ASA Virtual。

步骤 2 重复步骤 1 以部署所需数量的其他节点。

步骤 3 使用 ASA Virtual 控制台上的 **show cluster info** 命令验证是否所有节点都已成功加入集群。

步骤 4 配置 AWS 网关负载均衡器。

a) 创建目标组和 GWLB。

b) 将目标组连接到 GWLB。

注释
确保将 GWLB 配置为使用正确的安全组、侦听程序配置和运行状况检查设置。

c) 使用IP地址向目标组注册数据接口（内部接口）。有关详细信息，请参阅创建网关负载均衡器。

在 AWS 中为 ASA Virtual 启用目标故障转移

ASA Virtual 的数据接口已注册到 AWS 中的 GWLB 目标组。在 ASA Virtual 集群中，每个实例都与一个目标组关联。GWLB 进行负载平衡，并将流量发送到该运行状况正常的实例，而该实例已被识别或注册为目标组中目标节点。

开始之前

您必须已通过手动方法或使用 CloudFormation 模板在 AWS 中部署 ASA Virtual 堆栈。

如果您使用 CloudFormation 模板部署集群，您还可以通过分配集群部署文件 `deploy_asav_clustering.yaml` 的 **GWLB 配置**部分下提供的 **rebalance** 属性来启用 **Target Failover** 参数。在模板中，默认情况下，此参数的值设置为 **rebalance**。但在 AWS 控制台上，此参数的默认值设置为 **no_rebalance**。

其中，

- **no_rebalance** - GWLB 继续将网络流量发送到发生故障或已取消注册的目标。
- **重新平衡**- 当现有目标发生故障或取消注册时，GWLB 将网络流量发送到另一个正常运行的目标。

有关在 AWS 中部署堆栈的信息，请参阅：

- 在 AWS 中手动部署集群
- 使用 CloudFormation 模板在 AWS 中部署堆栈

过程

步骤 1 在 AWS 控制台上，转到**服务 (Services) > EC2**

步骤 2 点击**目标组 (Target Groups)** 以查看目标组页面。

步骤 3 选择并打开 ASA Virtual 实例 IP 地址注册到的目标组。系统将显示目标组详细信息页面。

步骤 4 转到**属性 (Attributes)** 菜单。

步骤 5 点击**编辑 (Edit)** 以编辑属性。

步骤 6 将**再平衡流 (Rebalance flows)** 滑块按钮切换到右侧。这使目标故障转移能够配置 GWLB，以便在目标故障转移或注销注册时，将现有网络数据包重新平衡并转发到正常运行的目标节点。

在 Azure 中部署集群

在 Azure 服务链中，ASA Virtual 充当可以拦截互联网和客户服务之间的数据包的透明网关。Azure 上的 ASA Virtual 实例集群可通过将多节点 ASAv 抽象化为单个设备，从而帮助它们扩展吞吐量。

ASAv 包含两个逻辑接口 - 面向互联网的**外部接口**和面向客户服务的**内部接口**。这些接口可通过使用成对代理中的 VXLAN 网段在 ASAv 的单个网络接口卡 (NIC) 上定义。

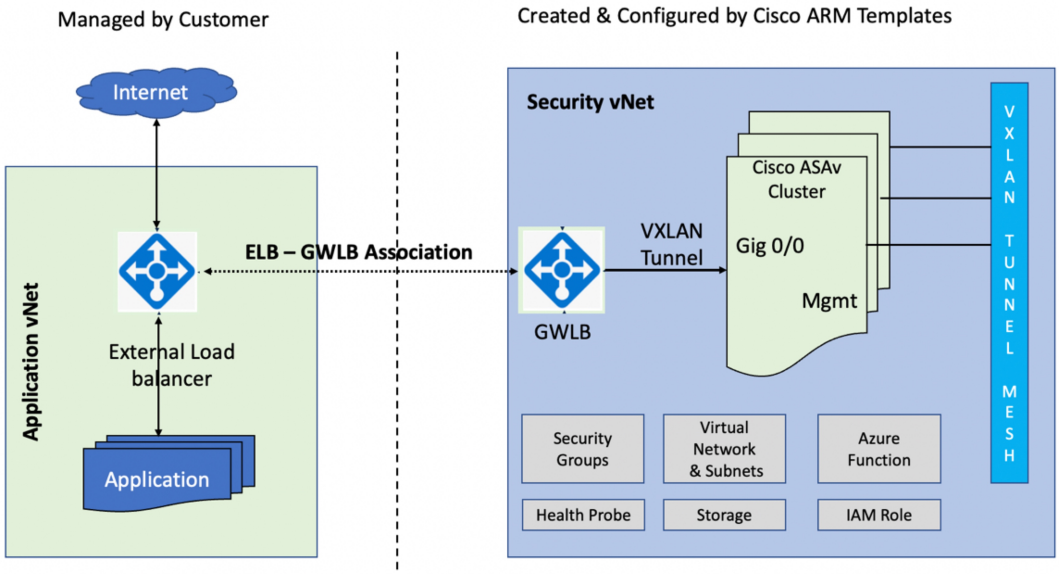
关于 Azure 网关负载均衡器

通过将 VXLAN 网段路由到 ASAv 进行流量检查，Azure 网关负载均衡器 (GWLB) 可帮助您均衡和管理入站和出站流量。在 ASAv 集群环境中，Azure GWLB 会根据流量负载自动扩展 ASAv 节点的吞吐量级别。GWLB 可以确保流量对称或路由到网络虚拟设备，而无需手动更新路由。使用此功能，数据包可以在两个方向上遍历同一网络路径。

下图显示了从外部 VXLAN 网段上的公共网关负载均衡器转发到 Azure GWLB 的流量。**网关负载均衡器**主要在多个 ASAv 之间平衡流量，这些 ASAv 会在丢弃流量或将其送回内部 VXLAN 网段的 GWLB 之前对流量进行检查。然后，Azure GWLB 会将流量发送回公共网关负载均衡器和目的地。

下图说明了 Azure 中 GWLB 和 ASAv 之间的网络流量。

图 *60:* 具有 *GWLB* 的 *Azure* 上的 *ASAv* 集群



关于 Azure 中的集群部署

您可以使用自定义的 Azure 资源管理器 (ARM) 模板为 Azure GWLB 部署虚拟机规模集。

在集群部署后，您可以使用 day0 配置或通过 Azure 门户上的函数应用来手动配置集群上的每个节点。

使用 Azure 资源管理器模板来部署集群

部署集群节点（虚拟机规模集），使它们使用 Azure 资源管理器 (ARM) 模板来形成集群。

开始之前

- 要手动创建 Azure 集群，您必须准备具有 day0 配置的配置文本文件。请参阅准备用于在 Azure 上创建集群的配置文件。

过程

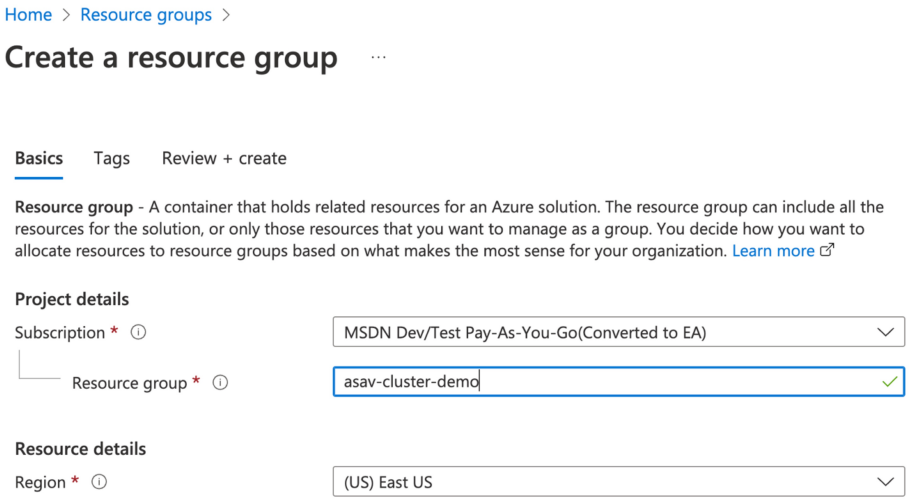
步骤 1 准备模板。

a) 将 GitHub 存储库克隆到本地文件夹。请参阅https://github.com/CiscoDevNet/cisco-asav/tree/master/cluster/azure。

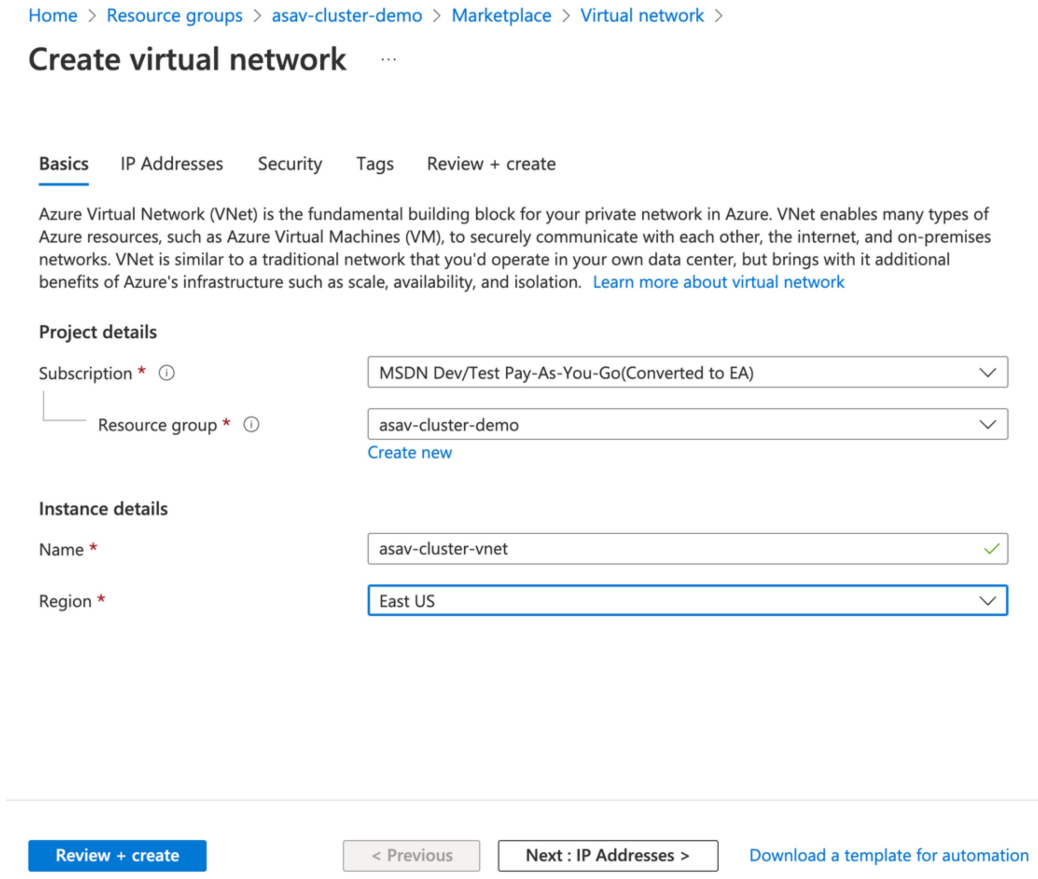
b) 对于 GWLB，请使用所需参数来修改 `azure_asav_gwlb_cluster.json` 和 `asav-gwlb-cluster-config.txt`。

步骤 2 登录 Azure 门户：https://portal.azure.com。

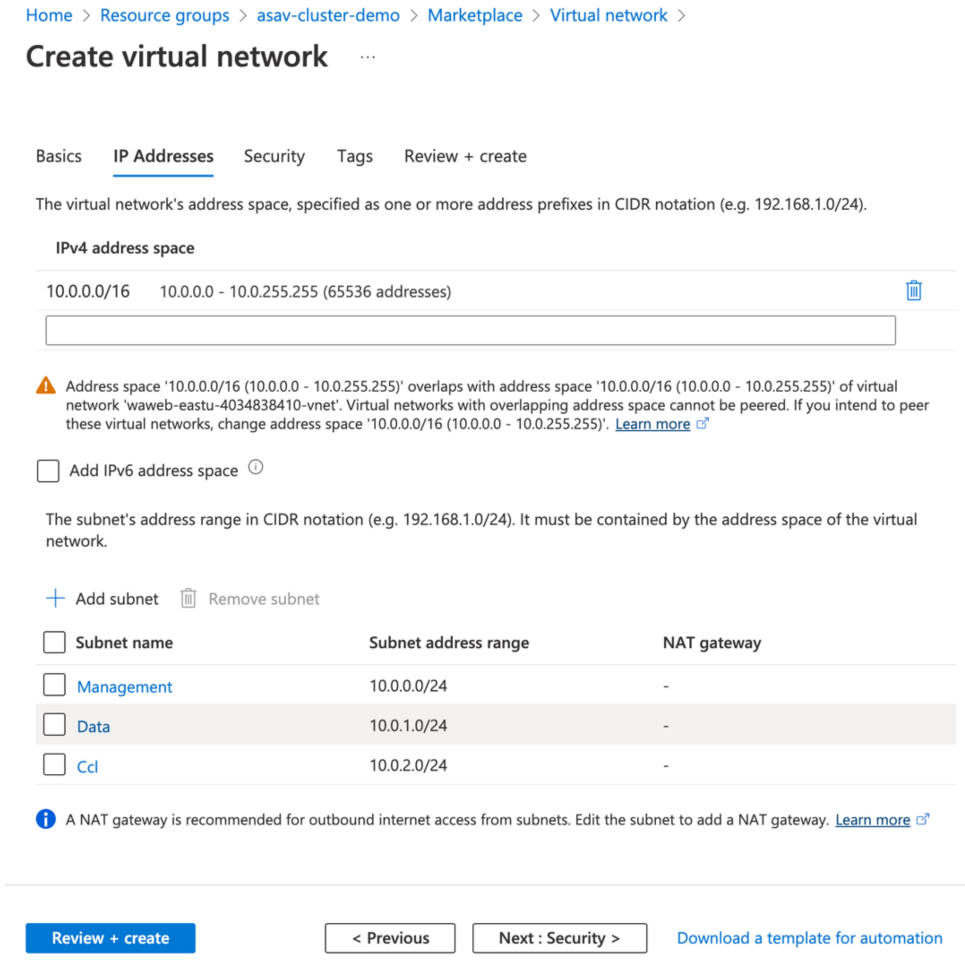
步骤 3 创建一个资源组。



步骤 4 为 ASAv 集群创建具有三个子网的虚拟网络：管理、外部和集群控制链路 (CCL)。



步骤 5 添加子网。



步骤 6 部署自定义模板。

a) 点击**创建 (Create) > > 模板部署 (Template deployment)**（使用自定义模板部署）。

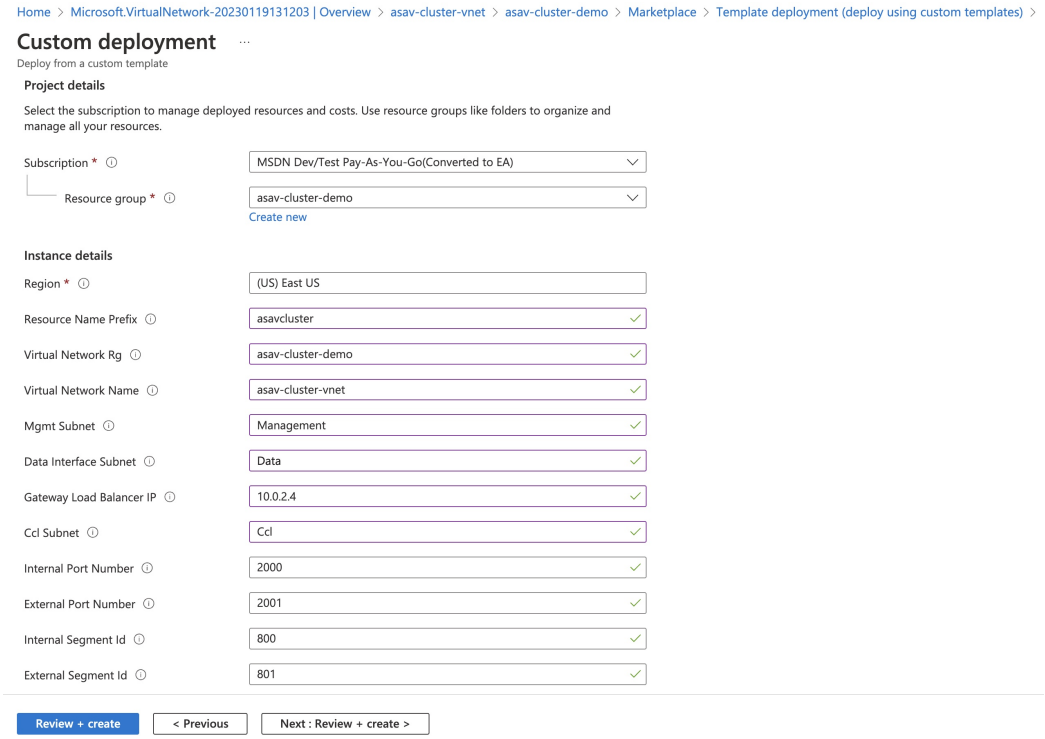
b) 点击“在编辑器中生成自己的模板 (Build your own template in the editor)”。

c) 点击**加载文件 (Load File)**，然后根据 Azure 中使用的负载均衡器类型上传 `azure_asav_gwlb_cluster.json`。

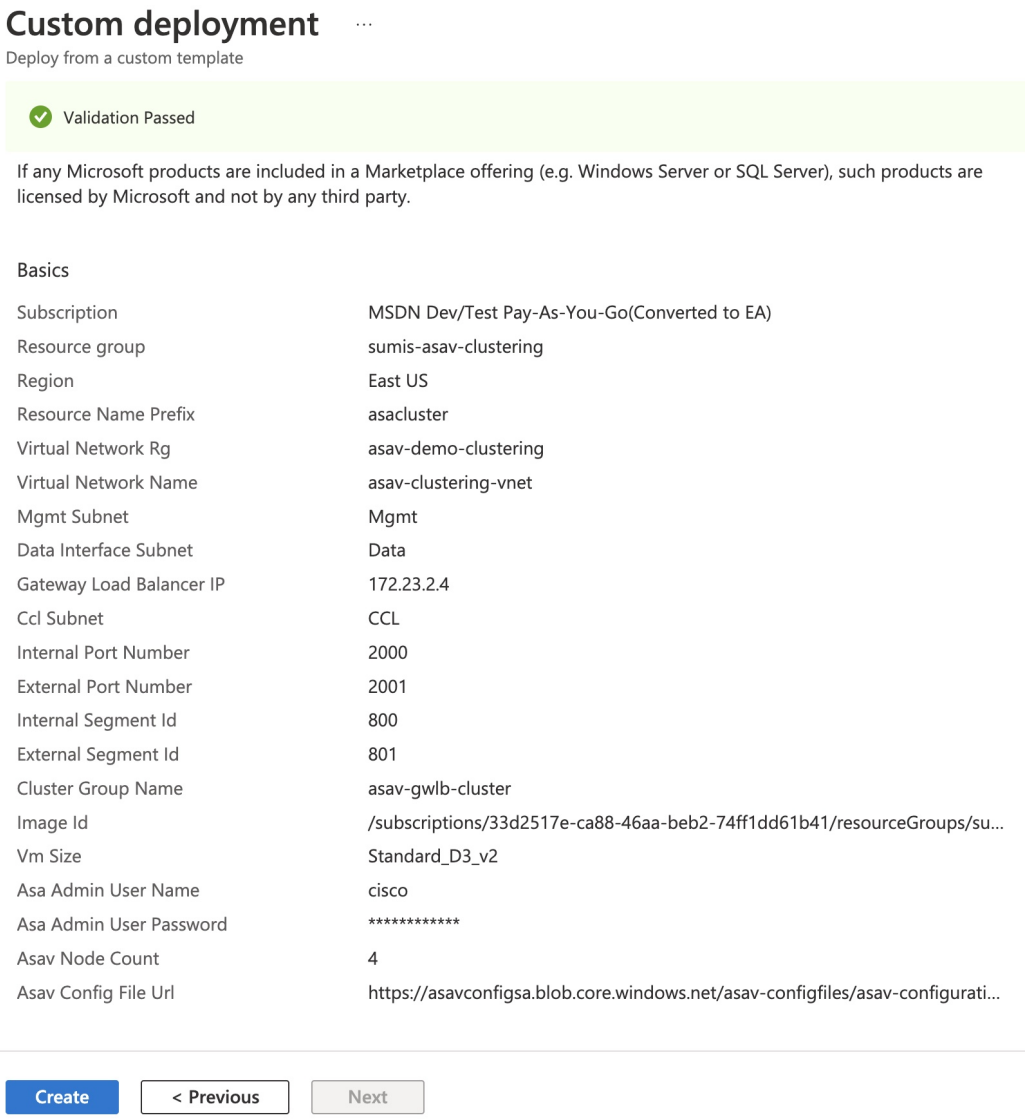
d) 点击**保存 (Save)**。

步骤 7 配置实例详细信息。

步骤 8 输入所需的值，然后点击**查看 + 创建 (Review + create)**。



步骤 9 在验证通过后，点击**创建 (Create)**。



Custom deployment

Deploy from a custom template

Validation Passed

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Basics

Subscription	MSDN Dev/Test Pay-As-You-Go(Converted to EA)
Resource group	sumis-asav-clustering
Region	East US
Resource Name Prefix	asacluster
Virtual Network Rg	asav-demo-clustering
Virtual Network Name	asav-clustering-vnet
Mgmt Subnet	Mgmt
Data Interface Subnet	Data
Gateway Load Balancer IP	172.23.2.4
Ccl Subnet	CCL
Internal Port Number	2000
External Port Number	2001
Internal Segment Id	800
External Segment Id	801
Cluster Group Name	asav-gwlb-cluster
Image Id	/subscriptions/33d2517e-ca88-46aa-beb2-74ff1dd61b41/resourceGroups/su...
Vm Size	Standard_D3_v2
Asa Admin User Name	cisco
Asa Admin User Password	**********
Asav Node Count	4
Asav Config File Url	https://asavconfigsa.blob.core.windows.net/asav-configfiles/asav-configurati...

Create | < Previous | Next

步骤 10 在实例运行后，通过登录到任何一个节点并输入 **show cluster info** 命令来验证集群部署。

```
> show cluster info
Cluster gwlb-cluster-template-with-AN: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "12" in state CONTROL_NODE
        ID        : 0
        Version   : 99.19(1)180
        Serial No.: 9AKGFV8VH4G
        CCL IP    : 10.1.1.12
        CCL MAC   : 000d.3a55.5470
        Module    : NGFWv
        Resource  : 8 cores / 28160 MB RAM
        Last join : 11:13:24 UTC Sep 5 2022
        Last leave: N/A
```

下一步做什么

在 Azure 中配置集群，第 616 页。

在 Azure 中配置集群

要在 Azure 中的 ASAv 节点上配置集群，您可以使用配置文件或使用 Azure 函数应用来进行手动配置。您可以将集群与本地 GWLB 配合使用。

准备用于在 Azure 上创建集群的配置文件

您可以使用配置文件或 Azure 门户上的函数应用在 ASA virtual 节点上手动配置集群。

要在 ASA virtual 节点上手动配置集群，您必须已配置 `asav-gwlb-cluster-config.txt`。在此文件中，您必须定义在集群 ASA virtual 节点中配置的参数，例如范围对象、day0、集群组名称、许可类型等。

本节介绍了如何创建集群配置文件，以使用 GWLB 配置 Azure 中的 ASA virtual 节点。

过程

步骤 1 从思科 GitHub 存储库目录 `asav-cluster/sample-config-file` 下载 **asav-gwlb-cluster-config.txt**。

步骤 2 您可以为创建集群准备 day0 配置。

以下的 day0 配置示例可帮助您了解使用 GWLB 在 Azure 中创建集群所需的参数。

- **用于 GWLB 集群创建的 Day0 配置示例**

  以下是用于 GWLB 集群创建的 `asav-gwlb-cluster-config.txt` 文件中所需的 day0 配置示例。

```
cluster interface-mode individual force
            policy-map global_policy
            class inspection_default
            no inspect h323 h225
            no inspect h323 ras
            no inspect rtsp
            no inspect skinny

        interface GigabitEthernet0/0
            nameif vxlan_tunnel
            security-level 0
            ip address dhcp
            no shutdown

        interface GigabitEthernet0/1
            nve-only cluster
            nameif ccl_link
            security-level 0
            ip address dhcp
            no shutdown

        interface vni1
```

```
    description ClusterInterface
    segment-id 1
    vtep-nve 1

interface vni2
    proxy paired
    nameif GWLB-backend-pool
    internal-segment-id 800
    external-segment-id 801
    internal-port 2000
    external-port 2001
    security-level 0
    vtep-nve 2

object network ccl#link
    range <CCLSubnetStartAddress> <CClSubnetEndAddress>
    object-group network cluster#group
    network-object object ccl#link

nve 1
    encapsulation vxlan
    source-interface ccl_link
    peer-group cluster#group

nve 2
    encapsulation vxlan
    source-interface vxlan_tunnel
    peer ip <GatewayLoadbalancerIp>

mtu vxlan_tunnel 1454
mtu ccl_link 1374
cluster group <ClusterGroupName>
local-unit <Last Octet of CCL Interface IP>
cluster-interface vni1 ip 1.1.1.<Last Octet of CCL Interface IP> 255.255.255.0

priority 1
enable
```

在上述 day0 配置示例中，当提及封装类型为 **vxlan** 时，则 GWLB 相关配置已启用。**InternalPort** 和 **ExternalPort** 用于 vxlan 隧道接口配置，而 **InternalSegId** 和 **ExternalSegId** 用作内部和外部接口的标识符。

注释

在 day0 配置中，必须指定集群控制链路的起始地址 (`<CCLSubnetStartAddress>`) 和结束地址。因此，`StartAddress` 必须始终以 `x.x.x.4` 开头，并且 `EndAddress` 必须在最佳范围内。建议仅指定所需数量的地址（最多 16 个），因为添加大量地址可能会影响性能。

例如：如果 CCL 子网是 `192.168.3.0/24`，则 `StartAddress` 将为 `192.168.3.4` 而 `EndAddress` 会是 `192.168.3.30`。

以下是 vni 接口所需的配置示例。

```
interface vni2
        proxy paired
        nameif GWLB-backend-pool
        internal-segment-id 800
        external-segment-id 801
        internal-port 2000
        external-port 2001
        security-level 0
```

```
vtep-nve 2
```

步骤 3 将配置文件上传到 Azure 存储，并记下该位置的路径 (URL)。在 ASA virtual 节点上手动配置集群时需要此 URL 路径。

使用配置文件手动配置集群

使用配置文件在 Azure 中手动配置 ASAv 节点上的集群。

开始之前

您必须已准备好配置文件，并记录下上传文件的 Azure 存储位置。请参阅“为 Azure 准备集群配置文件”。

过程

步骤 1 登录到 Azure 门户。

步骤 2 打开 Azure 上部署的 ASAv 实例。

步骤 3 运行以下命令，通过提供已上传到 Azure 存储容器的文件的 URL 将集群配置文件复制到 ASAv 节点。

copy <Config File URL> running-config

步骤 4 运行以下命令以便在 ASAv 实例上配置集群

```
cluster group <ClusterGroupName>
         local-unit <Last Octet of the Management Interface IP>
         cluster-interface vni1 ip 1.1.1.<Last Octet of the Management Interface IP>
255.255.255.0
         priority 1
         enable
```

步骤 5 重复步骤 2 至 4，在所有 ASAv 节点上配置集群。

使用 Azure 函数应用来配置集群

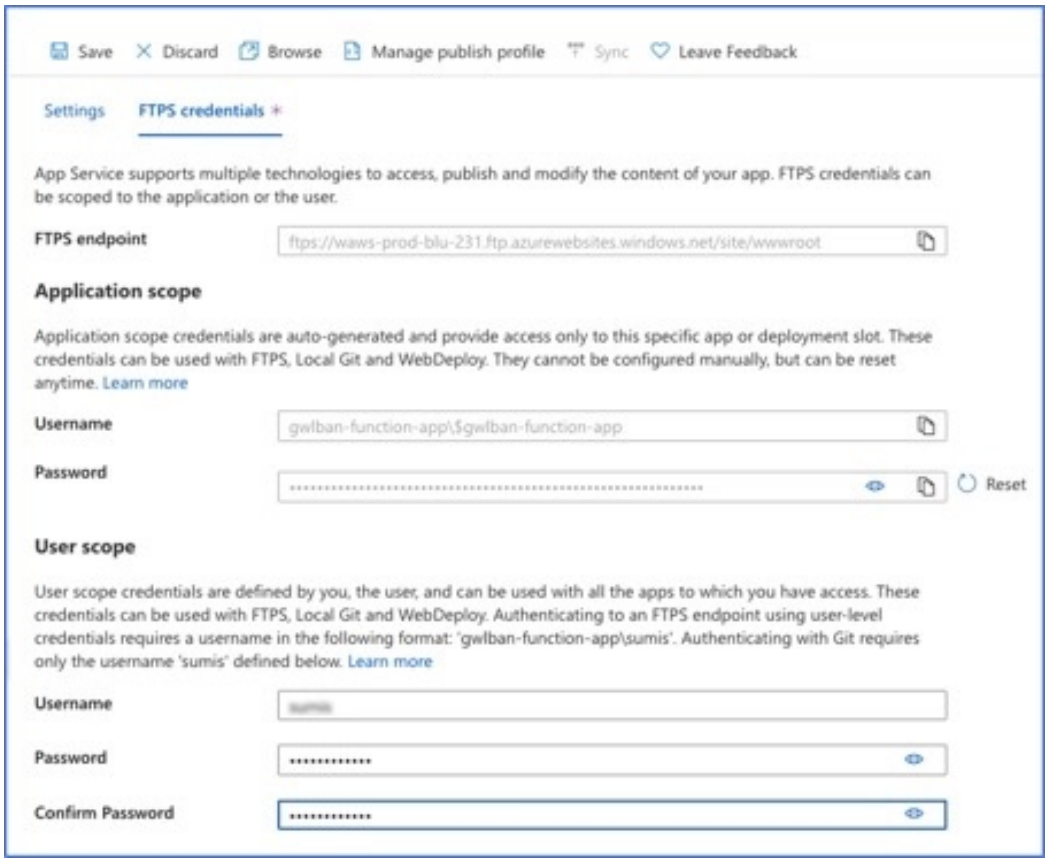
使用 Azure 函数应用服务在 Azure 中的 ASAv 节点上配置集群。

过程

步骤 1 登录到 Azure 门户。

步骤 2 点击**函数应用 (Function App)**。

步骤 3 通过点击**部署中心 (Deployment Center)** > **FTPS 凭证 (FTPS credentials)** > **用户范围 (User scope)** > **配置用户名和密码 (Configure Username and Password)** > 来创建 FTPS 凭证，然后点击**保存 (Save)**。



步骤 4 通过在本地终端中执行以下命令，将 `Cluster_Function.zip` 文件上传到函数应用。

curl -X POST -u <Userscope_Username> --data-binary @"Cluster_Function.zip" https://<Function_App_Name>.scm.azurewebsites.net/api/zipdeploy

图 ***61:*** 功能

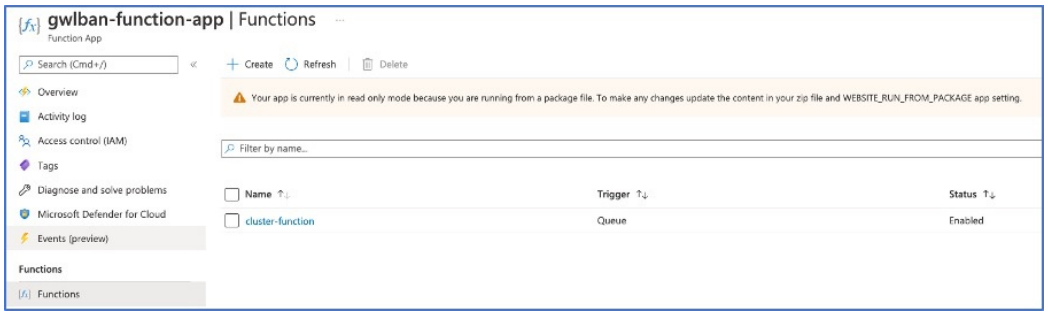


图 *62:* 队列

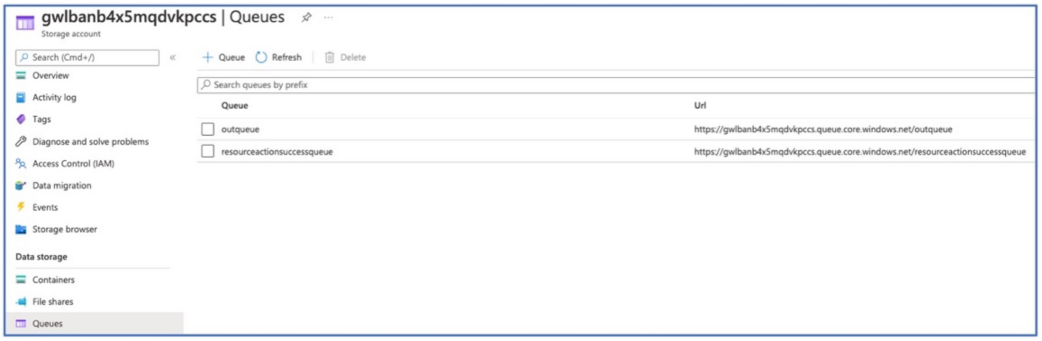
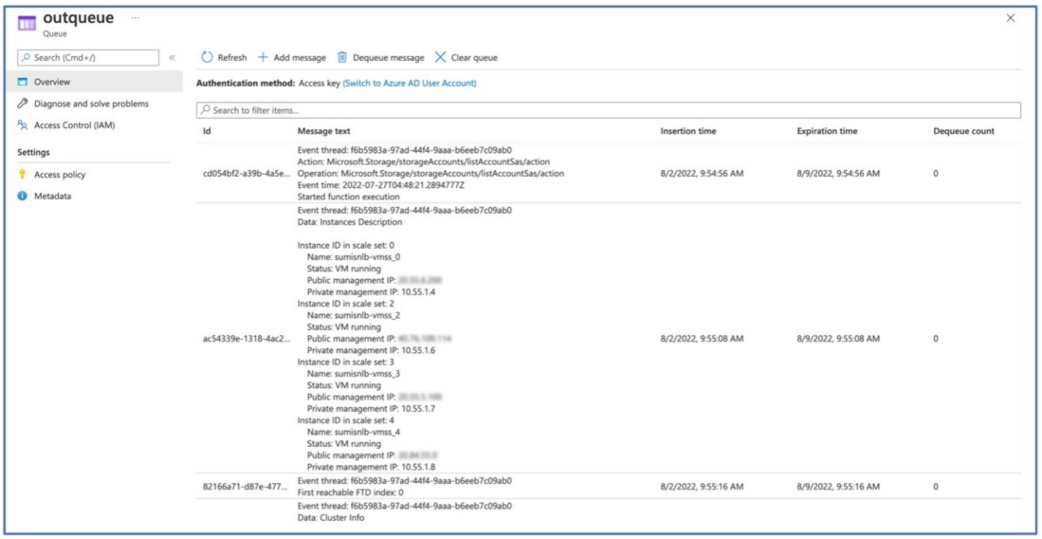


图 *63:* 出站队列



函数将被上传到函数应用。功能将启动，而您可以在存储帐户的出站队列中看到日志。

在执行此功能后，将在所有 ASAv 节点上启用集群。

Azure 中的 ASA Virtual 集群故障排除

流量问题

如果流量不起作用，请验证以下内容：

1. 使用负载均衡器验证 ASA Virtual 实例的运行状况探测状态是否正常。

   如果 ASA Virtual 实例的运行状况探测状态为不正常，请执行以下操作：

   1. 验证 ASA Virtual 中配置的静态路由。
   2. 验证默认网关是否为数据子网的网关 IP。

3. 确保 ASA Virtual 实例接收运行状况探测流量。
4. 验证 ASA Virtual 中配置的访问策略是否允许运行状况探测流量。

集群问题

如果未形成集群，请验证以下内容：

- 网络虚拟化终端（仅 NVE）集群接口的 IP 地址。确保您可以 ping 其他节点的仅 NVE 集群接口。
- 仅 NVE 集群接口的 IP 地址是对象组的一部分。确保通过对象组来配置 NVE。
- 集群组中的集群接口具有正确的 VNI 接口。此 VNI 接口具有相应对象组的 NVE。
- 每个节点都有自己的IP接口，请验证节点是否应该能够相互执行ping操作，以确保集群中节点之间的连接。
- 验证模板部署期间提及的CCL子网的开始地址和结束地址是否正确。起始地址必须以子网中的第一个可用的 IP 地址开头。例如，如果子网是 192.168.1.0/24。那么起始地址应为 192.168.1.4（前三个 IP 地址由 Azure 保留）

角色相关问题

如果在同一资源组中再次部署资源时出现任何与角色相关的错误，请执行以下操作：

如果存在与特定角色相关的任何问题，则会显示错误消息。

以下是错误消息的示例。

"error": {

"code": "RoleAssignmentUpdateNotPermitted",

"message": "Tenant ID, application ID, principal ID, and scope are not allowed to be updated." }

通过从终端执行以下命令来删除下列角色。

- 用于删除存储队列数据参与者角色的命令：

  az role assignment delete --resource-group <Resource Group Name> --role "Storage Queue Data Contributor"

- 用于删除参与者角色的命令：

  az role assignment delete --resource-group <Resource Group Name> --role "Contributor"

自定义集群操作

作为第 0 天配置的一部分，或者在部署集群之后，您可以自定义集群运行状况监控、TCP 连接复制延迟、流移动性和其他优化。

在控制节点上执行这些程序。

配置基本 ASA 集群参数

您可以在控制节点上自定义集群设置。

过程

步骤 1 进入集群配置模式：

cluster group *name*

步骤 2 （可选） 启用数据节点到控制节点的控制台复制：

console-replicate

默认情况下会禁用此功能。对于特定的重要事件，ASA 可将某些消息直接打印输出到控制台。如果启用了控制台复制，数据节点会将控制台消息发送到控制节点，因此您只需要监控集群的一个控制台端口。

步骤 3 设置集群事件的最低跟踪级别：

trace-level 级别

根据需要设置最低级别：

- **critical** - 重要事件（严重性=1）
- **warning** - 警告（严重性 = 2）
- **informational** - 信息事件（严重性=3）
- **debug** - 调试事件（严重性=4）

步骤 4 设置从流所有者到导向器和备份所有者的流状态刷新消息（clu_keepalive 和 clu_update 消息）的保持连接间隔。

clu-keepalive-interval 秒

- 秒 - 15 到 55。默认值为 15。

您可能想将间隔设置为比默认值更长的时间，以减少集群控制链路上的流量。

配置运行状态监控并自动重新加入设置

此程序可以配置节点和接口运行状态监控。

您可能想禁用不重要的接口（例如管理接口）的运行状况检查。运行状况监控不在 VLAN 子接口上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

步骤 2 自定义集群节点运行状况检查功能。

health-check [**holdtime** 超时]

为了确定节点运行状况，ASA 集群节点会在集群控制链路上将 heartbeat 消息发送到其他节点。如果节点在保持期内未接收到来自对等节点的任何 heartbeat 消息，则对等节点被视为无响应或无法工作。

- **holdtime** 超时 - 用于确定两次设备 heartbeat状态消息之间的时间间隔，其值介于 0.3到 45 秒；默认值为 3 秒。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用 ASA、或交换机上的接口），您应禁用运行状态检查功能，还要禁用对已禁用接口的接口监控 (**no health-check monitor-interface**)。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

步骤 3 在接口上禁用接口运行状况检查。

no health-check monitor-interface *interface_id*

接口运行状态检查将监控链路故障。ASA 在多长时间后从集群中删除成员取决于该节点是既定成员还是正在加入集群的设备。默认情况下，为所有接口启用运行状况检查。您可以使用此命令的 **no** 形式逐个接口将其禁用。您可能想禁用不重要的接口（例如管理接口）的运行状况检查。

- *interface_id* - 禁用接口监控。运行状况监控不在 VLAN 子接口上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用 ASA、或交换机上的接口），您应禁用运行状态检查功能 (**no health-check**)，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management1/1
```

步骤 4 自定义在运行状况检查发生故障后的自动重新加入集群设置。

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**- 指定内部错误的自动重新加入设置。内部故障包括：应用程序同步超时、不一致的应用程序状态等。
- **unlimited** —（**cluster-interface** 的默认值）不限制重新加入尝试的次数。
- *auto-rejoin-max* — 设置重新加入尝试次数，介于 0 和 65535 之间。**0** 禁用自动重新加入。**data-interface** 和 **system** 的默认值为 3。
- *auto_rejoin_interval* - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。节点尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- *Auto_rejoin_interval_variation* - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。对于集群接口，默认值为 **1**，而对于数据接口和系统，默认值为 **2**。

示例：

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

步骤 5 配置 ASA 将接口视为发生故障并将节点从集群中删除之前经过的防反跳时间。

health-check monitor-interface debounce-time *ms*

示例：

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，ASA 会等待指定的毫秒数，然后才将接口标记为发生故障，并将节点从集群中删除。

步骤 6 （可选） 配置流量负载监控。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds* — 设置监控消息之间的时间（以秒为单位），范围介于 10 到 360 秒之间。默认值为 20 秒。
- **intervals** *intervals* — 设置 ASA 维护数据的间隔的数量，该值介于 1 到 60 之间。默认值为 30。

您可以监控集群成员的流量负载，包括总连接计数、CPU 和内存使用情况以及缓冲区丢弃。如果负载过高，且剩余的节点可以处理负载，您可以选择在节点上手动禁用集群，或调整外部交换机上的负载均衡。默认情况下启用此功能。您可以定期监控流量负载。如果负载过高，您可以选择手动禁用节点上的集群。

使用 **show cluster info load-monitor** 命令查看流量负载。

示例：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
   1           0            0            13              27
```

示例

以下示例将 health-check holdtime 配置为 0.3 秒；禁用GUANLI 0/0 接口上的监控；将数据接口的 auto-rejoin 设置为从 2 分钟开始的 4 次尝试，将 duration 增至上一次间隔的 3 倍；以及将集群控制链路的 auto-rejoin 设为 6 次尝试，每隔 2 分钟一次。

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3
ciscoasa(cfg-cluster)# no health-check monitor-interface management0/0
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1
```

管理集群节点

部署集群后，您可以更改配置和管理集群节点。

成为非活动节点

要成为集群的非活动成员，请在节点上禁用集群，同时保持集群配置不变。

注释 当ASA处于非活动状态（以手动方式或因运行状况检查失败）时，所有数据接口都将关闭；只有管理专用接口可以发送和接收流量。要恢复流量传输，请重新启用集群；或者，您也可以从集群中完全删除该节点。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，您保存了已禁用集群的配置），则管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

过程

步骤 1 进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 禁用集群：

no enable

如果此节点是控制节点，则会进行新的控制选择，并且其他成员将成为控制节点。

集群配置保持不变，因此您可于稍后再次启用集群。

从控制节点停用数据节点

要禁用您登录的节点以外的成员，请执行以下步骤。

注释 当ASA处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。要恢复流量流，请重新启用集群。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，假设您保存了已禁用集群的配置），管理接口将被禁用。您必须使用控制台端口来进行任何进一步的配置。

过程

从集群中删除该节点：

cluster remove unit *node_name*

引导程序配置保持不变，从控制节点同步的最新配置也保持不变，因此您可于稍后重新添加该节点而不会丢失配置。如果在数据节点上输入此命令来删除控制节点，则会选择新的控制节点。

要查看成员名称，请输入 **cluster remove unit ?**，或者输入 **show cluster info** 命令。

示例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2
```

```
ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

重新加入集群

如果从集群中删除了某个节点（例如针对出现故障的接口），或者如果您手动停用了某个成员，那么您必须手动重新加入集群。

过程

步骤 1 在控制台中，进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 启用集群。

enable

离开集群

要完全退出集群，需要删除整个集群引导程序配置。由于每个节点上的当前配置相同（从主用设备同步），因此退出集群就意味着要么从备份恢复集群前的配置，要么清除现有配置并重新开始配置以免 IP 地址冲突。

过程

步骤 1 对于数据节点，禁用集群：

cluster group *cluster_name* **no enable**

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

在数据节点上启用集群时，您无法进行配置更改。

步骤 2 清除集群配置：

clear configure cluster

ASA 将关闭所有接口，包括管理接口和集群控制链路。

步骤 3 禁用集群接口模式：

no cluster interface-mode

模式并非存储于配置中，因此必须手动重置。

步骤 4 如果有备份配置，可将备份配置复制到正在运行的配置中：

copy *backup_cfg* **running-config**

示例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

步骤 5 将配置保存到启动配置：

write memory

步骤 6 如果没有备份配置，请重新配置管理访问。例如，确保更改接口 IP 地址，并恢复正确的主机名。

更改控制节点

注意 要更改控制节点，最好的方法是在控制节点上禁用集群，等到新的控制选举后再重新启用集群。如果必须指定要成为控制节点的具体节点，请使用本节中的程序。但是请注意，对集中功能而言，如果使用本程序强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

要更改控制节点，请执行以下步骤：

过程

将新节点设置为控制节点：

cluster control-node unit*node_name*

示例：

```
ciscoasa(config)# cluster control-node unit asa2
```

您需要重新连接到主集群 IP 地址。

要查看成员名称，请输入 **cluster control-node unit ?**（可查阅除当前节点之外的所有名称），或输入 **show cluster info** 命令。

在整个集群范围内执行命令

要向集群中的所有节点或某个特定节点发送命令，请执行以下步骤。向所有节点发送 **show** 命令以收集所有输出并将其显示在当前节点的控制台上。也可在整个集群范围内执行其他命令（如 **capture** 和 **copy**）。

过程

发送命令到所有节点，或者如果指定了节点名称，则发送到特定节点：

cluster exec [**unit** *node_name*] *command*

示例：

```
ciscoasa# cluster exec show xlate
```

要查看节点名称，请输入 **cluster exec unit ?**（可查阅除当前节点之外的所有名称），或输入 **show cluster info** 命令。

示例

要同时将同一捕获文件从集群中的所有节点复制到 TFTP 服务器，请在控制节点上输入以下命令：

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

多个 PCAP 文件（一个文件来自一个节点）将复制到 TFTP 服务器。目标捕获文件名会自动附加节点名称，例如 capture1_asa1.pcap、capture1_asa2.pcap 等。在本例中，asa1和asa2是集群节点名称。

监控集群

您可以监控集群状态和连接并排除故障。

监控集群状态

请参阅以下命令来监控集群状态：

- **show cluster info** [**health** [**details**]]

  如果没有关键字，**show cluster info** 命令将显示所有集群成员的状态。

  show cluster info health 命令将显示接口、节点和整个集群的当前运行状况。**details** 关键字显示心跳消息失败的次数。

  请参阅 **show cluster info** 命令的以下输出：

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state CONTROL_NODE
      ID        : 2
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state DATA_NODE
      ID        : 3
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info auto-join**

  显示集群节点是否将在一段延迟后自动重新加入集群，以及是否已清除故障条件（例如等待许可证、机箱运行状况检查失败，等等）。如果节点已永久禁用，或节点已在集群中，则此命令将不会显示任何输出。

  请参阅 **show cluster info auto-join** 命令的以下输出：

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Control node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport**{**asp** |**cp** [**detail**]}

  显示以下项目传输相关的统计信息：

  - **asp** — 数据平面传输统计信息。
  - **cp** — 控制平面传输统计信息。

    如果您输入 **detail** 关键字，您可以查看集群可靠传输协议的使用情况，以便确定控制平面中的缓冲区已满时的丢包问题。请参阅 **show cluster info transport cp detail** 命令的以下输出：

    ```
    ciscoasa# show cluster info transport cp detail
    Member ID to name mapping:
      0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

    Legend:
      U    - unreliable messages
      UE   - unreliable messages error
      SN   - sequence number
      ESN  - expecting sequence number
      R    - reliable messages
      RE   - reliable messages error
      RDC  - reliable message deliveries confirmed
      RA   - reliable ack packets received
      RFR  - reliable fast retransmits
      RTR  - reliable timer-based retransmits
      RDP  - reliable message dropped
      RDPR - reliable message drops reported
      RI   - reliable message with old sequence number
      RO   - reliable message with out of order sequence number
      ROW  - reliable message with out of window sequence number
      ROB  - out of order reliable messages buffered
    ```

```
  RAS  - reliable ack packets sent

This unit as a sender
-------------------------
       all       0         2         3
  U    123301    3867966   3230662   3850381
  UE   0         0         0         0
  SN   1656a4ce  acb26fe   5f839f76  7b680831
  R    733840    1042168   852285    867311
  RE   0         0         0         0
  RDC  699789    934969    740874    756490
  RA   385525    281198    204021    205384
  RFR  27626     56397     0         0
  RTR  34051     107199    111411    110821
  RDP  0         0         0         0
  RDPR 0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
       0         2         3
  U    111847    121862    120029
  R    7503      665700    749288
  ESN  5d75b4b3  6d81d23   365ddd50
  RI   630       34278     40291
  RO   0         582       850
  ROW  0         566       850
  ROB  0         16        0
  RAS  1571      123289    142256

This unit as a receiver of unicast messages
-------------------------------------------
       0         2         3
  U    1         3308122   4370233
  R    513846    879979    1009492
  ESN  4458903a  6d841a84  7b4e7fa7
  RI   66024     108924    102114
  RO   0         0         0
  ROW  0         0         0
  ROB  0         0         0
  RAS  130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
```

```
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
==========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
==========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
==========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  显示集群历史记录，以及有关集群节点加入失败的原因或节点离开集群的原因的错误消息。

捕获整个集群范围内的数据包

有关在集群中捕获数据包的信息，请参阅以下命令：

cluster exec capture

要支持集群范围的故障排除，您可以使用 **cluster exec capture** 命令在控制节点上启用捕获集群特定流量的功能，随后集群中的所有数据节点上将自动启用此功能。

监控集群资源

请参阅以下命令以监控集群资源：

show cluster {**cpu** | **memory** | **resource**} [*options*]

显示整个集群的聚合数据。可用 *options* 取决于数据类型。

监控集群流量

请参阅以下命令以监控集群流量：

- **show conn [detail], cluster exec show conn**

  show conn 命令显示一个传输是导向者、备用还是转发者传输。在任意节点上使用 **cluster exec show conn** 命令可查看所有连接。此命令可以显示单个流的流量到达集群中不同 ASA 的方式。集群的吞吐量取决于负载均衡的效率和配置。此命令可以让您很方便地查看某个连接的流量如何流经集群，也可以帮助您了解负载均衡器对传输的性能有何影响。

  show conn detail 命令还显示哪些流应 遵守流移动性。

  以下是 **show conn detail** 命令的输出示例：

```
ciscoasa/ASA2/data node# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
```

```
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic received
 at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface NP
Identity
Ifc Locally received: 716 (8 byte/s)
```

要对连接流进行故障排除，请先在任意节点上输入 **cluster exec show conn** 命令查看所有节点上的连接。寻找具有以下标志的流：导向者 (Y)、备用 (y) 和转发者 (z)。下例显示了三台 ASA 上的一条从 172.18.124.187:22 到 192.168.103.131:44727 的 SSH 连接；ASA 1 带有 z 标志，表示其是该连接的转发者；ASA3 带有 Y 标志，表示其是该连接的导向者；而 ASA2 则没有特殊的标志，表示其是所有者。在出站方向，此连接的数据包进入 ASA2 上的内部接口并从外部接口流出。在入站方向，此连接的数据包进入 ASA 1 和 ASA3 上的外部接口，通过集群控制链路被转发到 ASA2，然后流出 ASA2 上的内部接口。

```
ciscoasa/ASA1/control node# cluster exec show conn
ASA1(LOCAL):**************************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**************************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:**************************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0,
flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance** | **flow-mobility counters**]

  show cluster info conn-distribution 和 **show cluster info packet-distribution** 命令显示流量在所有集群节点上的分布。这些命令可以帮助您评估和调整外部负载均衡器。

  show cluster info loadbalance 命令显示连接再均衡统计信息。

  The **show cluster info flow-mobility counters** 命令显示 EID 移动和流所有者移动信息。请参阅 **show cluster info flow-mobility counters** 的以下输出：

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 4
EID movement notification processed : 4
Flow owner moving requested         : 2
```

- **show cluster info load-monitor** [**details**]

  show cluster info load-monitor 命令显示最后一个间隔的集群成员的流量负载，以及已配置的总间隔数（默认情况下为 30）。使用 **details** 关键字查看每个时间间隔的每个度量值。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 30 interval:
   0           0            0            12              28
   1           0            0            13              27
```

```
ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval


Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0
```

```
         0          0          0          0          0          0

Buffer drops captured over 30 intervals:
Unit ID  0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
Unit ID  1
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0
         0          0          0          0          0          0

Memory usage(%) captured over 30 intervals:
Unit ID  0
        25         25         30         30         30         35
        25         25         35         30         30         30
        25         25         30         25         25         35
        30         30         30         25         25         25
        25         20         30         30         30         30
Unit ID  1
        30         25         35         25         30         30
        25         25         35         25         30         35
        30         30         35         30         30         30
        25         20         30         25         25         30
        20         30         35         30         30         35

CPU usage(%) captured over 30 intervals:
Unit ID  0
```

```
        25          25          30          30          30          35
        25          25          35          30          30          30
        25          25          30          25          25          35
        30          30          30          25          25          25
        25          20          30          30          30          30
Unit ID  1
        30          25          35          25          30          30
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35
```

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  显示整个集群的聚合数据。可用 *options* 取决于数据类型。

  请参阅 **show cluster access-list** 命令的以下输出：

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
```

```
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

要显示所有节点在用连接的汇聚计数，请输入：

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):**************************************************************
  100 in use, 100 most used

  cl1:*********************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  此命令对于数据路径故障排除非常有用。

监控集群路由

有关集群路由的信息，请参阅以下命令：

- **show route cluster**
- **debug route cluster**

  显示集群的路由信息。

- **show lisp eid**

  显示 ASA EID 表，表中显示了 EID 和站点 ID。

  请参阅 **cluster exec show lisp eid** 命令的以下输出。

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):***************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:**********************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  该命令对于故障排除非常有用。

配置集群日志记录

有关为集群配置日志记录的信息，请参阅以下命令：

logging device-id

集群中的每个节点将独立生成系统日志消息。您可以使用**logging device-id**命令来生成具有相同或不同设备 ID 的系统日志消息，以使消息看上去是来自集群中的相同或不同节点。

监控集群接口

请参阅以下用于监控集群接口的命令：

- **show cluster interface-mode**

  显示集群接口模式。

调试集群

请参阅以下用于调试集群的命令：

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  显示集群的调试消息。

- **debug cluster flow-mobility**

  显示与集群流移动性相关的事件。

- **debug lisp eid-notify-intercept**

  当 eid-notify 被拦截时显示事件。

- **show cluster info trace**

  show cluster info trace命令显示调试信息，供进一步排除故障之用。

  请参阅 **show cluster info trace** 命令的以下输出：

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

  例如，如果您看到以下消息显示两个具有相同**local-unit**名称的节点充当控制节点，这可能意味着两个节点具有相同的**local-unit**名称（请检查您的配置），或者某个节点正在接收自己的广播消息（请检查您的网络）。

```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
```

```
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node
 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

集群参考

本部分包括有关集群工作原理的详细信息。

ASA 功能和集群

部分 ASA 功能不受 ASA 集群支持，还有部分功能仅在控制节点上受支持。其他功能可能对如何正确使用规定了注意事项。

集群不支持的功能

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

- 依靠 TLS 代理实现的统一通信功能
- 远程访问 VPN（SSL VPN 和 IPsec VPN）
- 虚拟隧道接口 (VTI)
- 以下应用检查：
  - CTIQBE
  - H323、H225 和 RAS
  - IPsec 穿透
  - MGCP
  - MMP
  - RTSP
  - SCCP（瘦客户端）
  - WAAS
  - WCCP
- 僵尸网络流量过滤器
- 自动更新服务器
- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- VPN 负载均衡

- Azure 上的故障转移
- 集成路由和桥接
- FIPS 型号

集群集中化功能

以下功能只有在控制节点上才受支持，且无法为集群扩展。

注释 集中功能的流量从成员节点通过集群控制链路转发到控制节点。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非控制节点的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回控制节点。

对集中功能而言，如果控制节点发生故障，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

- 以下应用检查：
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- 静态路由监控
- 网络访问的身份验证和授权。记帐被分散。
- 筛选服务
- 站点间 VPN
- 组播路由

应用到单个节点的功能

这些功能将应用到每个 ASA 节点而非整个集群或控制节点。

- QoS - QoS 策略将于配置复制过程中在集群中同步。但是，该策略是在每个节点上独立执行。例如，如果对输出配置管制，则要对流出特定 ASA 的流量应用符合规则的速率和符合规则的突发量值。在包含 3 个节点且流量均衡分布的集群中，符合规则的速率实际上变成了集群速率的 3 倍。
- 威胁检测 - 威胁检测在各节点上独立工作；例如，排名统计信息就要视具体节点而定。以端口扫描检测为例，由于扫描的流量将在所有节点间进行负载均衡，而一个节点无法看到所有流量，因此端口扫描检测无法工作。

用于网络访问的 AAA 和集群

用于网络访问的 AAA 由三部分组成：身份验证、授权和记账。身份验证和授权作为集中功能在集群控制节点上实施，且数据结构复制到集群数据节点。如果选举出控制节点，新的控制节点将拥有所需的所有信息，以继续不间断运行经过验证的既有用户及其相关授权。当控制节点发生变化时，用户身份验证的空闲和绝对超时将保留。

记账作为分散的功能在集群中实施。记账按每次流量完成，因此在为流量配置记账时，作为流量所有者的集群节点会将记账开始和停止消息发送到 AAA 服务器。

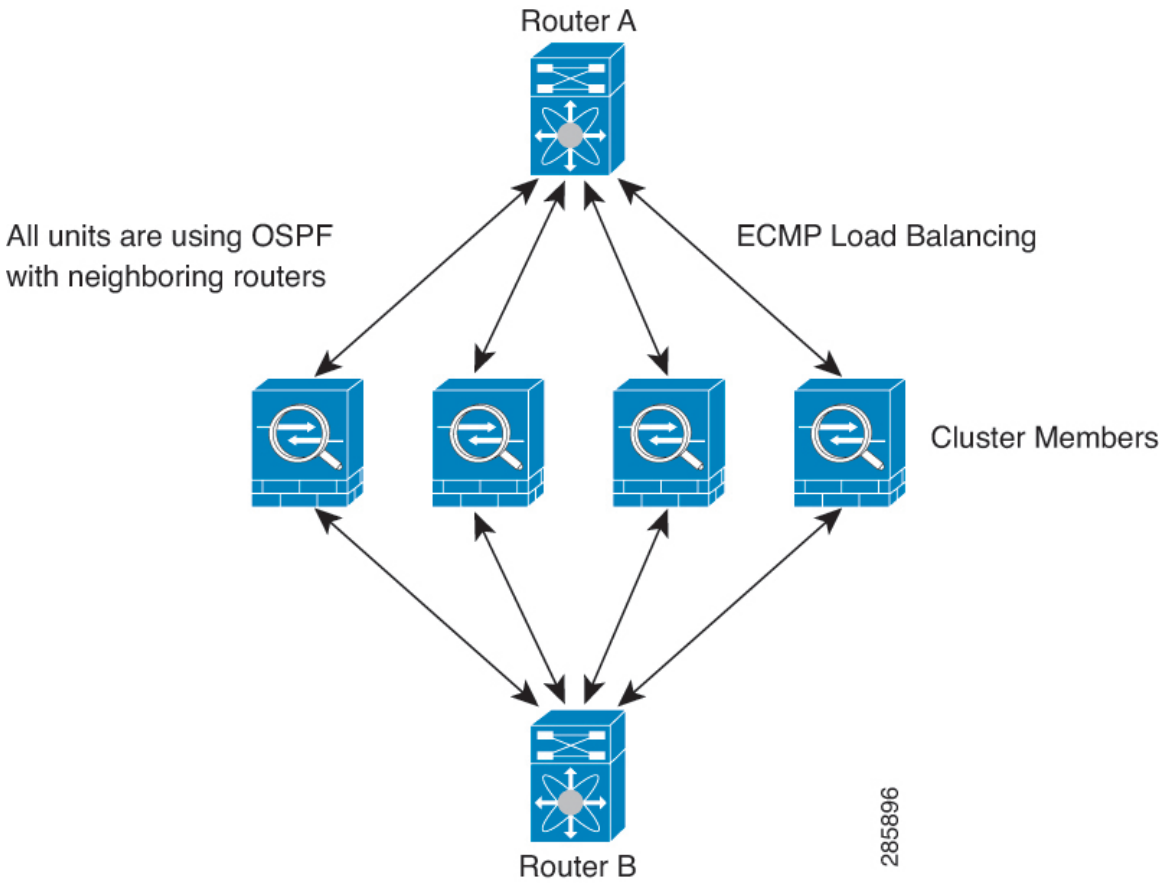
连接设置和集群

连接限制在集群范围强制实施（请参阅 **set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max** 和 **set connection per-client-max** 命令）。每个节点都有根据广播消息估计的集群范围的计数器值。出于效率考虑，在集群中配置的连接限制可能不会严格按限制数量实施。每个节点在任何指定时间都可能高估或低估集群范围内的计数器值。不过，在负载均衡的集群中，该信息将随时间而更新。

动态路由和集群

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *64:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一个节点。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每个节点在与外部路由器通信时，都会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

EIGRP 与单个接口模式下的集群对等体不构成邻居关系。

注释 如果该集群为实现冗余有多个设备与同一个路由器相邻，则非对称路由可能会造成不可接受的流量损失。要避免非对称路由，请将所有这些节点接口分组到同一流量区域中。请参阅配置流量区域，第 806 页。

FTP 和集群

- 如果 FTP 数据通道和控制通道流量由不同的集群成员所有，则数据通道所有者会将空闲超时更新定期发送到控制通道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父/子流量关系；控制流量空闲超时不会更新。

- 如果您将 AAA 用于 FTP 访问，则控制通道流集中在控制节点上。

ICMP检测和集群

ICMP 和 ICMP 错误数据包通过集群的流取决于是否启用 ICMP/ICMP 错误检查。不启用 ICMP 检查时，ICMP 是单向流，并且不支持导向器流。启用 ICMP 检查时，ICMP 流变为双向流，并由导向器/备份流支持。被检查的ICMP流的一个不同之处在于导向器对转发数据包的处理：导向器会将ICMP回应应答数据包转发给流所有者，而不是将数据包返回给转发器。

组播路由和集群

在独立接口模式下，设备并不单独处理组播。所有数据和路由数据包都由控制设备进行处理和转发，从而避免数据包复制。

NAT 和集群

NAT 可能会影响集群的总吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 ASA，因为负载均衡算法取决于 IP 地址和端口，NAT 会导致入站和出站数据包具有不同的 IP 地址和/或端口。当数据包到达并非 NAT 所有者的 ASA时，会通过集群控制链路转发到所有者，导致集群控制链路上存在大量流量。请注意，接收节点不会创建流向所有者的转发流量，因为NAT所有者最终可能不会根据安全和策略检查结果为数据包创建连接。

如果您仍想在集群中使用 NAT，请考虑以下准则：

- 不使用代理 ARP - 对于独立接口，切勿为映射的地址发送代理 ARP 回复。这可以防止邻接路由器与可能已经不在集群中的 ASA 保持对等关系。对于指向主集群 IP 地址的映射地址，上游路由器需要静态路由或带对象跟踪的 PBR。这对跨网络 EtherChannel 来说不是问题，因为只有一个 IP 地址与集群接口关联。

- PAT 采用端口块分配 - 请参阅该功能的以下准则：

  - 每主机最大流量限制并不针对整个集群，而是单独应用于每个节点。因此，在每主机最大流量限制配置为 1 的包含 3 个节点的集群中，如果在全部 3 个节点上对来自主机的流量实行负载均衡，则可以分配 3 个端口块，每个节点 1 个。

  - 在执行每主机最大流量限制时，在备份池中的备份节点上创建的端口块不计算在内。

  - 如果进行即时 PAT 规则修改（对 PAT 池改用全新的 IP 地址范围），会导致在新的池生效时仍在传输的转换项备份请求的转换项备份创建失败。此行为并非端口块分配功能所特有，它是一个暂时性 PAT 池问题，只发现于在集群节点之间分配池并执行流量负载均衡的集群部署。

  - 在集群中操作时，不能直接更改块分配大小。只有在集群中重新加载每个设备后，新的大小才会生效。为避免重新加载每个设备，我们建议您删除所有块分配规则并清除与这些规则相关的所有转换。然后，您可以更改块大小并重新创建块分配规则。

- 对动态 PAT 使用 NAT 池地址分配 - 配置 PAT 池时，集群将池中的每个 IP 地址划分为端口块。默认情况下，每个块都是 512 个端口，但如果配置端口块分配规则，则使用块设置。这些块在集群中的各个节点之间均匀分配，因此每个节点都有一个或多个块对应 PAT 池中的每个 IP 地

址。因此，在一个集群的 PAT 池中可以最少拥有一个 IP 地址，只要这足以支持您预期的 PAT 连接数即可。端口块覆盖的端口范围为 1024-65535，除非您在 PAT 池 NAT 规则中配置该选项以包含保留的端口 1-1023。

- 在多个规则中重复使用 PAT 池 - 要在多条规则中使用同一 PAT 池，必须注意规则中的接口选择。必须在所有规则中使用特定接口，或者在所有规则中使用“任意”接口。不能在规则中混合使用特定接口和“任意”接口，否则系统可能无法将返回流量与集群中的正确节点进行匹配。每条规则使用唯一的 PAT 池是最可靠的方案。
- 不使用轮询 - 集群不支持 PAT 池轮询。
- 无扩展 PAT - 集群不支持扩展 PAT。
- 控制节点管理的动态 NAT 转换 - 控制节点保留转换表并复制到数据节点。当数据节点收到需要动态 NAT 的连接并且转换不在表中时，它将请求从控制节点转换。数据节点拥有该连接。
- 过时 xlate - 连接所有者上的 xlate 空闲时间不会更新。因此，空闲时间值可能会超过空闲超时值。如果空闲计时器值高于配置的超时值（refcnt 为 0），则表示 xlate 过时。
- 每会话 PAT 功能 - 每会话 PAT 功能并非集群专用功能，但它能提高 PAT 的可扩展性，而且对集群而言，它允许每个数据节点成为 PAT 连接的所有者；相比之下，多会话 PAT 连接则必须转发到控制节点并由控制节点所有。默认情况下，所有 TCP 流量和 UDP DNS 流量均使用每会话 PAT 转换，而 ICMP 和所有其他 UDP 流量均使用多会话。您可以为 TCP 和 UDP 配置每会话 NAT 规则以更改这些默认设置，但是，您不能为 ICMP 配置每会话 PAT。对于使用多会话 PAT 的流量（例如 H.323、SIP 或 Skinny），您可以禁用关联 TCP 端口的每会话 PAT（这些 H.323 和 SIP 的 UDP 端口已默认为多会话）。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。
- 对以下检查不使用静态 PAT：
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 如果您有大量 NAT 规则（超过一万条），则应使用设备 CLI 中的 **asp rule-engine transactional-commit nat** 命令启用事务提交模型。否则，节点可能无法加入集群。

SCTP 和集群

SCTP 关联可以在任何节点上创建（由于负载均衡），但其多宿主连接必须位于同一节点上。

SIP 检测和集群

控制流可以在任何节点上创建（由于负载均衡），但其子数据流必须位于同一节点上。

不支持 TLS 代理配置。

SNMP 和集群

SNMP 代理按照本地 IP 地址轮询每一个ASA。您无法轮询集群的合并数据。

您应始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的控制节点时，对新控制节点的轮询将失败。

当使用 SNMPv3 进行集群时，如果您在初始集群形成后添加新的集群节点，则 SNMPv3 用户不会复制到新节点。您必须在控制节点上重新添加它们以强制用户复制到新节点，或者直接在数据节点上复制。

STUN 和集群

故障转移和集群模式支持STUN检查，因为针孔被复制。但是，节点之间不进行事务ID的复制。如果节点在收到 STUN 请求后发生故障，并且另一个节点收到 STUN 响应，则该 STUN 响应将被丢弃。

系统日志和集群

- 系统日志 - 集群中的每个节点都会生成自己的系统日志消息。您可以配置日志记录，使每个节点在系统日志消息的报头字段中使用相同或不同的设备 ID。例如，集群中的所有节点都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备 ID，则所有节点生成的系统日志消息都会看似来自一个节点。如果将日志记录配置为使用集群引导程序配置中指定的本地节点名称作为设备 ID，系统日志消息就会看似来自不同节点。
- NetFlow - 集群中的每个节点都会生成自己的 NetFlow 数据流。NetFlow 收集器只能将每台 ASA 视为单独的 NetFlow 导出器。

思科 TrustSec 和集群

只有控制节点学习安全组标记 (SGT) 信息。然后，控制节点将 SGT 填充到数据节点，数据节点可以根据安全策略对 SGT 做出匹配决策。

VPN 和集群

站点间 VPN 是集中功能；只有控制节点支持 VPN 连接。

注释 集群不支持远程访问 VPN。

VPN 功能仅限控制节点使用，且不能利用集群的高可用性功能。如果控制节点发生故障，所有现有的 VPN 连接都将断开，VPN 用户将遇到服务中断。选择新的控制节点后，必须重新建立 VPN 连接。

对于使用 PBR 或 ECMP 时与独立接口的连接，您必须始终连接到主集群 IP 地址而非本地地址。

与 VPN 相关的密钥和证书将被复制到所有节点。

性能换算系数

将多台设备组成一个集群时，预计可以达到近似 80% 最大组合吞吐量的集群总体性能。

例如，如果您的型号在单独运行时可以处理大约 10 Gbps 的流量，则对于 8 台设备的集群，最大组合吞吐量约为 80 Gbps（8 台设备 x 10 Gbps）的 80%：64 Gbps。

控制节点选择

集群节点通过集群控制链路通信，如下选举控制节点：

1. 当为节点启用集群（或当节点首次启动时已启用集群）时，设备会每 3 秒广播一个选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级设置在 1 和 100 之间，其中 1 为最高优先级。
3. 如果某节点在 45 秒后未收到另一个具有较高优先级的节点的响应，则该设备会成为控制节点。

注释 如果多个节点并列获得最高优先级，则使用集群节点名称和序列号确定控制节点。

4. 如果节点稍后加入具有更高优先级的集群，它不会自动成为控制节点；现有控制节点始终保持为控制节点，除非它停止响应，此时会选择新的控制节点。
5. 在“裂脑”场景中，当临时存在多个控制节点时，具有最高优先级的节点将会保留角色，而其他节点则恢复为数据节点角色。

注释 您可以手动强制节点成为控制节点。对集中功能而言，如果强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

集群中的高可用性

集群通过监控节点和接口的运行状况并在节点之间复制连接状态来提供高可用性。

节点运行状况监控

每个节点通过集群控制链路定期发送广播保持连接心跳数据包。如果控制节点在可配置的超时期限内未从数据节点接收任何keepalive心跳数据包或其他数据包，则控制节点会从集群中删除该数据节点。如果数据节点未从控制节点接收数据包，则从其余节点中选择新的控制节点。

如果节点因为网络故障而不是因为节点实际故障而无法通过集群控制链路相互访问，则集群可能会进入“裂脑”场景，其中隔离的数据节点将选择自己的控制节点。例如，如果路由器在两个集群位置之间发生故障，则位于位置1的原始控制节点将从集群中删除位置2数据节点。同时，位置2的节点将选择自己的控制节点并形成自己的集群。请注意，在这种情况下，非对称流量可能会失败。恢复集群控制链路后，优先级较高的控制节点将保留控制节点的角色。

接口监控

每个节点都会监控使用中的所有已命名的硬件接口的链路状态，并向控制节点报告状态更改。

当您启用运行状况监控时，默认情况下会监控所有物理接口；您可以选择按接口禁用监控。只能监控已命名接口。

如果某个节点被监控的接口发生故障，则将从集群中删除该设备。ASA 在多长时间后从集群中删除成员取决于该节点是既定成员还是正在加入集群的设备。ASA 在节点加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 ASA 从集群中删除。无论状态如何，节点都会在 500 毫秒后被删除。

发生故障后的状态

如果控制节点发生故障，则优先级最高（数字最小）的另一个集群成员将成为控制节点。

ASA将自动尝试重新加入集群，具体取决于故障事件。

注释 当ASA变成不活动状态且无法自动重新加入集群时，所有数据接口都会关闭，仅管理专用接口可以发送和接收流量。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但是，如果您重新加载而节点在集群中仍然处于非活动状态，管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

重新加入集群

当集群节点从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路在最初加入时出现故障 - 在解决集群控制链路存在的问题后，您必须通过在 CLI 输入 **cluster group***name*，然后输入 **enable** 来重新启用集群 ，以手动重新加入集群。
- 加入集群后出现故障的集群控制链路 - ASA 无限期地每 5 分钟自动尝试重新加入。此行为是可配置的。
- 出现故障的数据接口 - ASA 尝试在 5 分钟时、然后在 10 分钟时、最后在 20 分钟时重新加入。如果 20 分钟后仍加入失败，ASA 将禁用集群。解决数据接口问题之后，您必须在 CLI 上通过输入**cluster group** *name*，然后输入**enable** 来手动启用集群。此行为是可配置的。

- 节点存在故障 - 如果节点因节点运行状况检查失败而从集群中删除，则如何重新加入集群取决于失败的原因。例如，临时电源故障意味节点将在重新启动时重新加入集群，只要集群控制链路打开并且仍然使用 **enable** 命令启用集群。ASA 每 5 秒钟尝试重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。节点将尝试以下列间隔自动重新加入集群：5 分钟，10 分钟，然后是 20 分钟。此行为是可配置的。

数据路径连接状态复制

每个连接在集群中都有一个所有者和至少一个备用所有者。备用所有者在发生故障时不会接管连接；而是存储 TCP/UDP 状态信息，使连接在发生故障时可以无缝转移到新的所有者。备用所有者通常也是导向器。

有些流量需要 TCP 或 UDP 层以上的状态信息。请参阅下表了解支持或不支持此类流量的集群。

表 *21:* 在集群中复制的功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	-
MAC 地址表	是	-
用户标识	是	包括 AAA 规则 (uauth) 。
IPv6 邻居数据库	是	—
动态路由	是	—
SNMP 引擎 ID	否	-
适用于 Firepower 4100/9300的分布式 VPN（站点间）	是	备用会话成为主用会话，并创建一个新的备用会话。

集群管理连接的方式

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

连接角色

请参阅为每个连接定义的下列角色：

- 所有者 - 通常为最初接收连接的节点。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。如果原始所有者发生故障，则当新节点从连接接收到数据包时，导向器会从这些节点中选择新的所有者。

- 备用所有者 - 存储从所有者接收的 TCP/UDP 状态信息的节点，以便在出现故障时可以无缝地将连接转移到新的所有者。在发生故障时，备用所有者不会接管连接。如果所有者处于不可用状态，从该连接接收数据包的第一个节点（根据负载均衡而定）联系备用所有者获取相关的状态信息，以便成为新的所有者。

  只要导向器（见下文）与所有者不是同一节点，导向器也可以是备用所有者。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  对于 Firepower 9300 上的在一个机箱中包括多达 3 个集群节点的集群，如果备用所有者与所有者在同一机箱上，则将从另一个机箱中选择一个额外的备用所有者来保护流量免受机箱故障的影响。

  如果您对站点间集群启用导向器本地化，则有两个备用所有者角色：本地备用和全局备用。所有者始终选择与自身位于同一站点（基于站点 ID）的本地备用。全局备用可以位于任何站点，甚至可以与本地备用是同一个节点。所有者向两个备用所有者发送连接状态信息。

  如果启用站点冗余，并且备用所有者与所有者位于同一站点，则将从另一个站点选择一个额外的备用所有者来保护流量免受站点故障的影响。机箱备份和站点备份是独立的，因此流量在某些情况将同时具有机箱备份和站点备份。

- 导向器 - 处理来自转发器的所有者查找请求的节点。当所有者收到新连接时，会根据源/目的 IP 地址和端口的散列值（有关 ICMP 散列详细信息，请参见下文）选择导向器，然后向导向器发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他节点，该节点会向导向器查询哪一个节点是所有者，以便转发数据包。一个连接只有一个导向器。如果导向器发生故障，所有者会选择一个新的导向器。

  只要导向器与所有者不是同一节点，导向器也可以是备用所有者（见上文）。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  如果您对站点间集群启用导向器本地化，则有两个导向器角色：本地导向器和全局导向器。所有者始终选择与它自身位于同一站点（基于站点 ID）的本地导向器。全局导向器可以位于任何站点，甚至可以与本地导向器是同一节点。如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者。

  ICMP/ICMPv6 散列详细信息：

  - 对于 Echo 数据包，源端口为 ICMP 标识符，目的端口为 0。
  - 对于 Reply 数据包，源端口为 0，目的端口为 ICMP 标识符。
  - 对于其他数据包，源端口和目的端口均为 0。

- 转发器 - 向所有者转发数据包的节点。如果转发者收到并非其所有的连接的数据包，则会向导向器查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向器也可以是转发者。如果启用导向器本地化，转发器将始终向本地导向器查询。如果本地导向器未获知所有者，例如，当集群成员收到所有者位于其他站点上的连接的数据包时，转发者将仅查询全局导向器。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN Cookie 直接获知所有者，因此无需向导向器查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向器查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。一个连接了可以有多个转发器；采用良好的

负载均衡方法可以做到没有转发器，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。

注释 不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

当连接使用端口地址转换 (PAT) 时，PAT 类型（每会话或多会话）会对哪个集群成员将成为新连接的所有者产生影响：

- 每会话 PAT - 所有者是接收连接中的初始数据包的节点。

  默认情况下，TCP 和 DNS UDP 流量均使用每会话 PAT。

- 多会话 PAT - 所有者始终是控制节点。如果多会话 PAT 连接最初由数据节点接收，则数据节点会将连接转发给控制节点。

  默认情况下，UDP（DNS UDP 除外）和 ICMP 流量使用多会话 PAT，因此这些连接始终归控制节点所有。

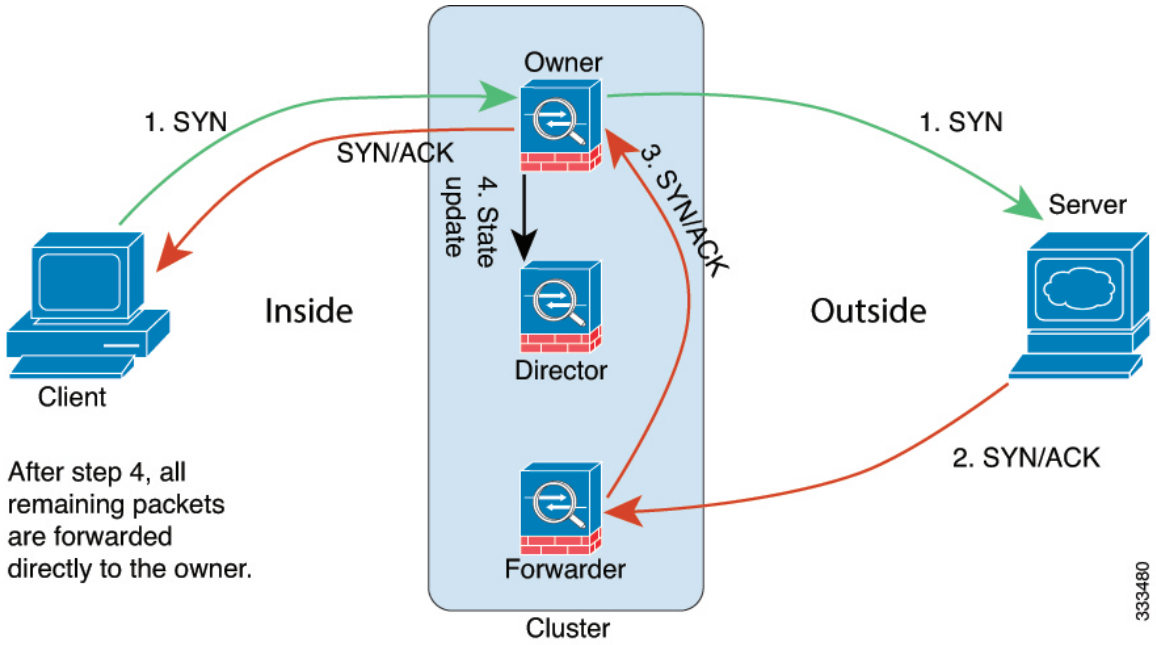
您可以更改 TCP 和 UDP 的每会话 PAT 默认设置，以便根据配置按每会话或多会话处理这些协议的连接。对于 ICMP，您不能更改默认的多会话 PAT。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。

新连接所有权

通过负载均衡将新连接定向到集群节点时，该连接的两个方向都由此节点所有。如果该连接有任何数据包到达其他节点，这些数据包都会通过集群控制链路被转发到所有者节点。为了获得最佳性能，对于要到达同一个节点的流量的两个方向以及要在节点之间均摊的流量，都需要执行适当的外部负载均衡。如果反向流量到达其他节点，会被重定向回原始节点。

TCP 的数据流示例

以下图例显示了新连接的建立。

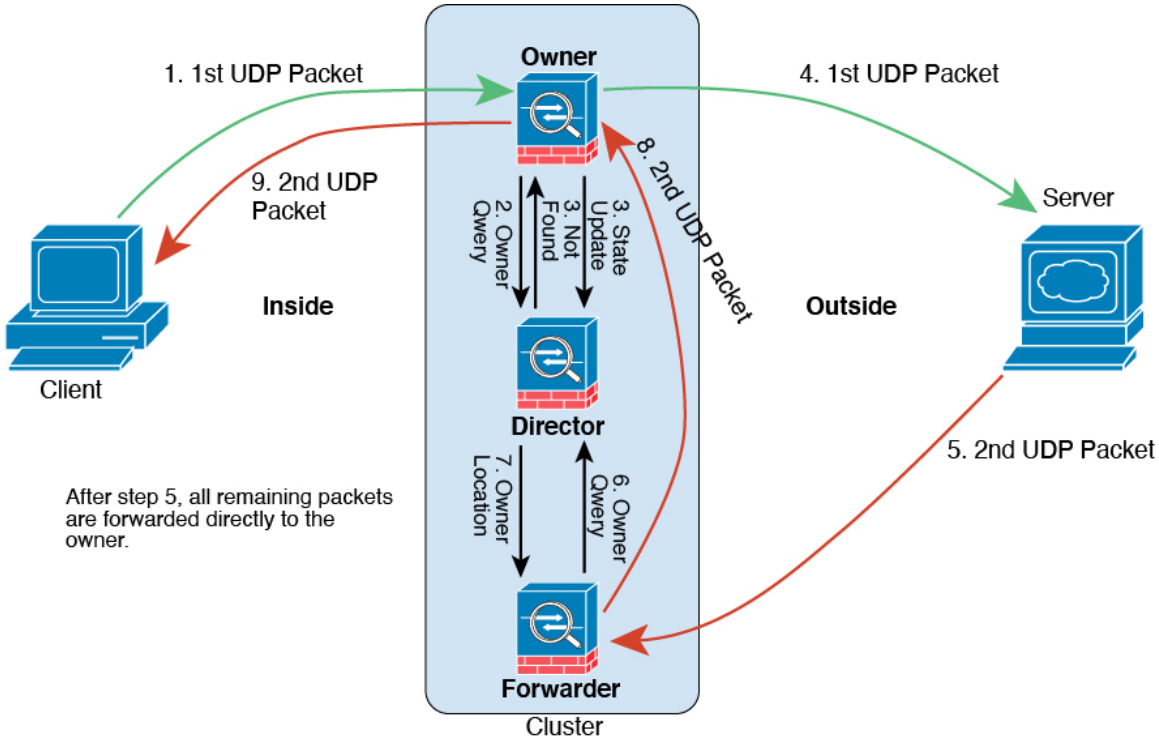


1. SYN 数据包从客户端发出，被传送到一台 ASA（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 ASA（基于负载均衡方法）。此 ASA是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，并记录TCP状态信息以及所有者。导向器将充当该连接的备用所有者。
6. 传送到转发器的任何后续数据包都会被转发到所有者。
7. 如果数据包被传送到任何其他节点，它将向导向器查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向器发送状态更新。

ICMP 和 UDP 的数据流示例

以下图例显示了新连接的建立。

1. 图 *65: ICMP* 和 *UDP* 数据流



第一个 UDP 数据包从客户端发出，被传送到一个ASA（基于负载均衡方法）。

2. 收到第一个数据包的节点查询基于源/目的 IP 地址和端口的散列值选择的导向器节点。
3. 导向器找不到现有流，创建导向器流并将数据包转发回前一个节点。换句话说，导向器已为此流选择了所有者。
4. 所有者创建流，向导向器发送状态更新，然后将数据包转发到服务器。
5. 第二个 UDP 数据包从服务器发出，并被传送到转发器。
6. 转发器向导向器查询所有权信息。对于 DNS 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。
7. 导向器向转发器回复所有权信息。
8. 转发器创建转发流以记录所有者信息，并将数据包转发给所有者。
9. 所有者将数据包转发到客户端。

关于公共云中的 ASA Virtual 集群的历史记录

特性	Version	详细信息
Azure 上的 ASA Virtual：使用网关负载均衡的集群	9.20(2)	我们现在支持使用 Azure 资源管理器 (ARM) 模板在 Azure 上部署 ASA Virtual 集群，然后将 ASA Virtual 配置为使用网关负载均衡器 (GWLB) 来实现网络流量负载均衡。
在 AWS 中使用 GWLB 配置 ASA Virtual 集群的目标故障转移	9.20(2)	AWS 中的目标故障转移功能使 GWLB 能够在计划维护期间取消注册或目标节点发生故障的情况下将网络数据包重定向到正常运行的目标节点。它利用集群的状态故障转移。
流状态的可配置集群保持连接间隔	9.20(2)	流所有者向导向器和备份所有者发送保持连接（clu_keepalive 消息）和更新（clu_update 消息），以刷新流状态。您现在可以设置保持连接的间隔。默认值为 15 秒，您也可以将间隔设为 15 到 55 秒。您可能想将间隔设置得更长，以减少集群控制链路上的流量。 新增/修改的命令：**clu-keepalive-interval**
ASA Virtual Amazon Web Services (AWS) 集群	9.19(1)	ASA Virtual 支持 AWS 上最多 16 个节点的单个接口集群。无论是否有 AWS 网关负载均衡器，您都可以使用集群。
Amazon Web 服务 (AWS) 集群中的 ASA Virtual IMDSv2 支持	9.22	ASA Virtual 支持 AWS 上的 IMDSv2。您可以通过更新堆栈来启用“IMDSv2 必需”模式。

第 III 部分

接口

- 基本接口配置， 第 659 页
- Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口的基本接口配置， 第 675 页
- EtherChannel 接口， 第 693 页
- 环回接口， 第 705 页
- VLAN 子接口， 第 711 页
- VXLAN 接口， 第 719 页
- 路由模式接口和透明模式接口， 第 749 页
- 高级接口配置， 第 787 页
- 流量区域， 第 797 页

第 14 章

基本接口配置

本章介绍基本接口配置，包括以太网设置和巨帧配置。

注释 在多情景模式下，请在系统执行空间中完成本节所述的所有任务。 要从情景更改到系统执行空间，请输入 **changeto system** 命令。

注释 对于平台模式中的 和 Firepower 4100/9300 机箱Firepower 2100 ，您可以在 FXOS 操作系统中配置基本接口设置。有关详细信息，请参阅机箱的配置或快速入门指南。

- 关于基本接口配置， 第 659 页
- 基本接口配置的相关准则， 第 661 页
- 基本接口配置的默认设置， 第 662 页
- 启用物理接口和配置以太网参数， 第 662 页
- 启用巨帧支持（ASA Virtual、ISA 3000） ， 第 665 页
- 管理 Cisco Secure Firewall 3100/4200的网络模块， 第 666 页
- 监控接口， 第 670 页
- 基本接口示例， 第 671 页
- 基本接口配置的历史记录， 第 672 页

关于基本接口配置

本节介绍接口功能与特殊接口。

Auto-MDI/MDIX 功能

对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的

自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

管理接口

管理接口是一个仅用于管理流量的独立接口，具体情况视型号而定。

管理接口概述

可以通过连接至以下接口来管理 ASA：

- 任何直通流量接口
- 专用的管理插槽/端口接口（如果适用于所用的型号）

您可以需要根据管理访问，第 1237 页来配置对接口的管理访问权限。

管理插槽/端口接口

下表列出了每个型号的管理接口。

表 *22:* 每个型号的管理接口

型号	**Management 0/0**	**Management 1/1**	**管理 1/2**	可针对直通流量进行配置	允许子接口
Firepower 1000	—	是	—	是	是
Cisco Secure Firewall 1200	—	是	—	是	是
Cisco Secure Firewall 3100	—	是	—	是	是
Cisco Secure Firewall 4200	—	是	是	是	是
Firepower 4100/9300	不适用 接口 ID 取决于分配给 ASA 逻辑设备的管理类型物理接口	-	—	—	是
ISA 3000	—	是	-	—	—
ASAv	是	-	—	是	—

将任何接口用于管理专用流量

若想将任何接口（包括 EtherChannel 接口）用作管理专用接口，您只需将该接口配置为用于管理流量（请参阅 **management-only** 命令）。

透明模式下的管理接口

在透明防火墙模式下，除了允许的最大数量的直通流量接口，您还可以将管理接口（物理接口、子接口[如果所用的型号支持]用作单独的仅管理接口。您不能将任何其他接口类型用作管理接口。对于 Firepower 4100/9300 机箱，管理接口 ID 取决于分配给 ASA 逻辑设备的管理类型接口。

在多情景模式下，您无法跨情景共享任何接口，包括管理接口。要在Firepower设备型号上为每个情景提供管理，您可以创建管理接口的子接口，然后向每个情景分配管理子接口。然而，不允许管理接口上有子接口，因此这些型号需要为了针对每个情景进行管理，您必须连接到数据接口。对于 Firepower 4100/9300 机箱，管理接口及其子接口不会被识别为情景中允许的特殊管理接口；您必须在这种情况下将管理子接口视为数据接口，并将其添加到 BVI。

管理接口不属于普通网桥组的一部分。请注意，出于操作目的，管理接口属于不可配置网桥组的一部分。

注释 在透明防火墙模式下，管理接口以与数据接口相同的方式更新 MAC 地址表；因此不应将管理和数据接口连接到同一个交换机，除非将其中一个交换机端口配置为路由端口（默认情况下，Catalyst交换机在所有的 VLAN 交换机端口上共享一个 MAC 地址）。否则，如果流量从物理连接的交换机到达管理接口，那么 ASA 会更新 MAC 地址表，以使用管理接口而非数据接口访问交换机。此操作会导致流量临时中断；出于安全考虑，ASA 在至少 30 秒的时间内不会为了从交换机传输至数据接口的数据包而再次更新 MAC 地址表。

基本接口配置的相关准则

透明防火墙模式

对于多情景透明模式，每个情景必须使用不同的接口；您不能在情景之间共享一个接口。

故障转移

您不能与数据接口共享一个故障转移接口或状态接口。

其他准则

有些管理相关服务在启用非管理接口和ASA实现“系统就绪”状态之前不可用。在“系统就绪”状态下，ASA 会生成以下系统日志消息：

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

基本接口配置的默认设置

本节列出了接口的默认设置（如果没有出厂默认配置）。

接口的默认状态

接口的默认状态取决于类型和情景模式。

在多情景模式下，默认启用所有已分配的接口，而不考虑接口在系统执行空间中的状态。但是，要使流量通过该接口，还必须在系统执行空间中启用该接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

在单模式下或在系统执行空间中，接口具有以下默认状态：

- 物理接口 - 已禁用。
- VLAN 子接口 - 已启用。但是，要使流量通过子接口，还必须启用物理接口。
- VXLAN VNI 接口 - 已启用。
- EtherChannel port-channel 接口（ISA 3000）- 已启用。但是，要使流量通过 EtherChannel 接口，还必须启用通道组物理接口。
- EtherChannel port-channel 接口（其他型号）- 已禁用。

注释 对于 Firepower 4100/9300，您可以出于管理需要同时启用和禁用机箱和 ASA 上的接口。必须在两个操作系统中都启用能够正常运行的接口。由于接口状态可独立控制，因此机箱与 ASA 之间可能出现不匹配的情况。

默认速度和双工

- 默认情况下，铜缆 (RJ-45) 接口的速度和双工设置为自动协商。

默认连接器类型

有些型号包含两个连接器类型：铜缆 RJ-45 和光纤 SFP。RJ-45 是默认接口。您可以将 ASA 配置为使用光纤 SFP 连接器。

默认 MAC 地址

默认情况下，物理接口使用烧录 MAC 地址，物理接口的所有子接口均使用相同的烧录 MAC 地址。

启用物理接口和配置以太网参数

本节介绍如何执行以下操作：

- 启用物理接口
- 设置特定的速度和双工（如有）
- (Cisco Secure Firewall 1200/3100/4200) 为流量控制暂停帧
- (Cisco Secure Firewall 3100/4200) 设置前向纠错

开始之前

对于多情景模式，请在系统执行空间中完成本程序。要从情景更改到系统执行空间，请输入**changeto system** 命令。

过程

步骤 1 指定要配置的接口：

interface *physical_interface*

示例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID 包含类型、插槽和端口号，格式为 type[slot/]port。

物理接口类型包括：

- 以太网

  gigabitethernet
- **tengigabitethernet**
- **management**

依次输入类型和插槽/端口，例如 **gigabitethernet0/1**。类型与插槽/端口之间的空格是可选的。

步骤 2 （可选） 设置速度（因型号而异）。

speed {**auto** | *speed* | **nonegotiate** | **sfp-detect**}

示例：

```
ciscoasa(config-if)# speed 100
```

对于 Firepower 1100 光纤接口，**speed nonegotiate** 会将速度设置为1000 Mbps，并禁用流量控制参数和远程故障信息的链路协商。 对于 Cisco Secure Firewall 1200/3100/4200，请参阅 **negotiate-auto** 命令。

（仅 Cisco Secure Firewall 1200/3100/4200 ）选择 **sfp-detect** 来检测 SFP 以检测已安装的 SFP 模块的速度并使用适当的速度。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。

步骤 3 (Cisco Secure Firewall 1200/3100/4200) 设置自动协商。

negotiate-auto

自动协商与速度分开设置。

示例：

```
ciscoasa(config-if)# negotiate-auto
```

步骤 4 （可选） 设置 RJ-45 接口的双工：

duplex {**auto** | **full** | **half**}

SFP 接口仅支持全复用。

示例：

```
ciscoasa(config-if)# duplex full
```

步骤 5 （可选） (Cisco Secure Firewall 3100/4200) 对于 25 Gbps 及更高的接口，请设置前向纠错 (FEC)。

fec {**auto** | **cl108-rs** | **cl74-fc** | **cl91-rs** | **disable**}

对于 EtherChannel 成员接口，必须先配置 FEC，然后才能将其添加到 EtherChannel。使用 **自动** 时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

注释
如果从 EtherChannel 中删除接口，则在重新启动 ASA 后，FEC 和自动协商配置将更改。您需要再次手动配置 FEC 和自动协商，因为这是预期行为。

表 *23:* 用于自动设置的默认 *FEC*

收发器类型	固定端口默认 **FEC**（以太网 **1/9** 至 **1/16**）	网络模块默认 **FEC**
25G-SR	cl108-rs	cl108-rs
25G-LR	cl108-rs	cl108-rs
10/25G-CSR	cl108-rs	cl74-fc
25G-AOC*x*M	cl74-fc	cl74-fc
25G-CU2.5/3M	自动协商	自动协商
25G-CU4/5M	自动协商	自动协商
25/50/100G	cl91-rs	cl91-rs

步骤 6 （可选） (Cisco Secure Firewall 1200/3100/4200) 在千兆位和更高版本的接口上启用暂停 (XOFF) 帧以进行流量控制：

flowcontrol send on

示例：

```
ciscoasa(config-if)# flowcontrol send on
```

流量控制通过允许拥塞节点在另一端暂停链路操作，从而让连接的以太网端口能够在拥塞期间控制流量速率。如果ASA端口遇到拥塞（内部交换机上的排队资源耗尽）并且无法接收更多流量，则它会通过发送暂停帧来通知另一个端口停止发送，直到状况恢复正常为止。在收到暂停帧后，发送设备会停止发送任何数据包，从而防止在拥塞期间丢失任何数据包。

注释
ASA 支持传输暂停帧，以便远程对等体可以对流量进行速率控制。

但是，不支持接收暂停帧。

内部交换机有一个包含 8000 个缓冲区的全局池，而每个缓冲区都有 250 个字节，并且交换机会为每个端口动态分配缓冲区。当缓冲区使用量超过全局高水位标记（2 MB [8000 个缓冲区]）时，会在每个启用了流量控制的接口上发送暂停帧；当特定接口的缓冲区超过端口高水位标记（0.3125 MB [1250 个缓冲区]）时，会从该接口发送暂停帧。在发送暂停后，如果缓冲区使用率降低至低水位标记之下（全局 1.25 MB [5000 个缓冲区]；每个端口 0.25 MB [1000 buffers]），则可发送 XON 帧。链接伙伴可在收到 XON 帧之后恢复流量。

系统仅支持 802.3x 中定义的流量控制帧。系统不支持基于优先级的流量控制。

步骤 7 启用接口：

no shutdown

示例：

```
ciscoasa(config-if)# no shutdown
```

要显示接口，请输入 **shutdown** 命令。如果输入 **shutdown** 命令，则还可关闭所有子接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

启用巨帧支持（ASA Virtual、ISA 3000）

巨型帧是指大于标准最大值 1518 字节（包括第 2 层报头和 VLAN 报头）的以太网数据包，最大为 9216 字节。您可以通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配较多内存可能会有碍于最大限度地利用其他功能（例如 ACL）。请注意，ASA MTU 设置的负载大小不包括第 2 层（14 字节）和 VLAN 报头（4 字节），因此最大 MTU 是 9198，具体取决于您的型号。

此程序仅适用于 ISA 3000 和 ASA virtual。其他型号默认支持巨型帧。

RAM 小于 8GB 的 ASAv5 和 ASAv10 不支持巨型帧。

开始之前

- 在多情景模式下，请在系统执行空间中设置此选项。
- 此设置的更改要求您重新加载 ASA。
- 确保要将需要传送巨型帧的每个接口的 MTU 设置为大于默认值 1500 的值；例如使用 **mtu** 命令将该值设置为 9198。在多情景模式下，请在每个情景中设置 MTU。
- 请务必调整 TCP MSS，以对非 IPsec 流量禁用此功能（使用 **sysopt connection tcpmss 0** 命令），或者根据 MTU 增加 TCP MSS 的值。

过程

启用巨型帧支持：

jumbo-frame reservation

示例

以下示例将启用巨型帧预留、保存配置并重新加载 ASA：

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

管理 Cisco Secure Firewall 3100/4200的网络模块

如果在首次打开防火墙之前安装网络模块，则无需执行任何操作；网络模块已启用并可供使用。

如果您需要在初始启动后更改网络模块安装，请参阅以下程序。

配置分支端口

您可以为每个 40GB 或更高的接口配置 10GB 分支端口。此程序介绍如何断开和重新加入端口。分支端口可以像任何其他物理以太网端口一样使用，包括添加到 EtherChannel。

如果一个接口已经在您的配置中使用，那么您必须手动删除与不再存在的接口相关的任何配置。

开始之前

- 您必须使用受支持的分支电缆。有关详细信息，请参阅硬件安装指南。
- 对于集群或故障转移，请确保集群/故障转移链路未使用父接口（用于分支）或子接口（用于重新加入）；如果该接口正用于集群/故障转移链路，则无法对其进行更改。

过程

步骤 1 从 40GB 或更高的接口分支出 10GB 端口。

breakout *slot port*

例如，要断开 Ethernet2/1 40GB 接口，应为 插槽 指定 **2** ，为 端口指定 **1** 。子接口将被标识为 Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3 和 Ethernet2/1/4。

对于集群或故障转移，请在控制节点/主用设备上执行此步骤；接口更改将复制到其他节点。

示例：

```
ciscoasa(config)# breakout 2 1
ciscoasa(config)# breakout 2 2
ciscoasa(config)# breakout 2 3
ciscoasa(config)# breakout 2 4
```

步骤 2 重新加入分支端口以恢复接口。

no breakout *slot port*

对于集群或故障转移，请在控制节点/主用设备上执行此步骤；模块状态被复制到其他节点。

您必须重新加入该接口的所有子端口。

示例：

```
ciscoasa(config)# no breakout 2 1
```

增加网络模块

要在初始启动后将网络模块添加到防火墙，请执行以下步骤。添加新模块需要重新加载。对于集群或故障转移，不支持零停机时间，因此请确保在维护窗口期间执行此程序。

过程

步骤 1 根据硬件安装指南安装网络模块。您可以在防火墙打开时安装网络模块。

对于集群或故障转移，请在所有节点上安装网络模块。

步骤 2 重新加载防火墙；请参阅 重新加载 ASA，第 39 页。

对于集群或故障转移，请重新加载所有节点。由于具有不同网络模块的节点无法加入集群/故障转移对，因此您需要使用新模块重新加载所有节点，然后它们才能重组集群/故障转移对。

步骤 3 启用网络模块。

no netmod 2 disable

对于集群或故障转移，请在控制节点/主用设备上执行此步骤；模块状态被复制到其他节点。

示例：

```
ciscoasa(config)# no netmod 2 disable
```

热插拔网络模块

您可以将网络模块热插拔为相同类型的新模块，而无需重新加载。但是，您必须关闭当前模块才能安全地将其删除。此程序介绍如何关闭旧模块、安装新模块以及如何启用它。

对于集群或故障转移，如果集群控制链路/故障转移链路在模块上，则不能禁用该模块。

过程

步骤 1 对于集群或故障转移，请执行以下步骤。

- **集群**- 确保要执行热插拔的设备是数据节点（请参阅 更改控制节点，第 382 页）；然后中断节点，使其不再位于集群中。请参阅成为非活动节点，第 378 页或停用节点，第 379 页。

  如果集群控制链路在网络模块上，则必须离开集群。请参阅离开集群，第 381 页。不允许禁用具有主动集群控制链路的网络模块。

- **故障转移**-请确保要执行热插拔的设备是备用节点。请参阅强制故障转移，第 301 页。

  如果故障转移链路位于网络模块上，则必须禁用故障转移。请参阅禁用故障转移，第 302 页。不允许禁用具有主动故障转移链路的网络模块。

步骤 2 禁用网络模块。

netmod 2 disable

示例：

```
ciscoasa(config)# netmod 2 disable
```

步骤 3 根据硬件安装指南更换网络模块。您可以在防火墙通电时更换网络模块。

步骤 4 启用网络模块。

no netmod 2 disable

示例：

```
ciscoasa(config)# no netmod 2 disable
```

步骤 5 对于集群或故障转移，请执行以下步骤。

- **集群 (Clustering)** - 将节点添加回集群。请参阅重新加入集群，第 380 页。
- **故障转移**- 如果禁用故障转移，则重新进行故障转移。

将网络模块更换为其他类型

如果您更换了其他类型的网络模块，则需要重新加载。如果新模块的接口少于旧模块，则必须手动删除与不再存在的接口相关的任何配置。对于集群或故障转移，不支持零停机时间，因此请确保在维护窗口期间执行此程序。

过程

步骤 1 禁用网络模块。

netmod 2 disable

对于集群或故障转移，请在控制节点/主用设备上执行此步骤；模块状态被复制到其他节点。不保存配置；重新加载时，系统将使用保存的配置启用该模块。

示例：

```
ciscoasa(config)# netmod 2 disable
```

步骤 2 根据硬件安装指南更换网络模块。您可以在防火墙通电时更换网络模块。

对于集群或故障转移，请在所有节点上安装网络模块。

步骤 3 重新加载防火墙；请参阅重新加载 ASA，第 39 页。

对于集群或故障转移，请重新加载所有节点。由于具有不同网络模块的节点无法加入集群/故障转移对，因此您需要使用新模块重新加载所有节点，然后它们才能重组集群/故障转移对。

步骤 4 如果在重新加载之前保存了配置，则必须重新启用该模块。

拆卸网络模块

如果要永久删除网络模块，请执行以下步骤。拆卸网络模块需要重新加载。对于集群或故障转移，不支持零停机时间，因此请确保在维护窗口期间执行此程序。

开始之前

对于集群或故障转移，请确保集群/故障转移链路不在网络模块上；在这种情况下，您无法删除该模块。

过程

步骤 1 禁用网络模块并保存配置。

netmod 2 disable

write memory

对于集群或故障转移，请在控制节点/主用设备上执行此步骤；模块状态被复制到其他节点。

示例：

```
ciscoasa(config)# netmod 2 disable
ciscoasa(config)# write memory
```

步骤 2 根据硬件安装指南删除网络模块。您可以在防火墙通电时删除网络模块。

对于集群或故障转移，请删除所有节点上的网络模块。

步骤 3 重新加载防火墙；请参阅 重新加载 ASA，第 39 页。

对于集群或故障转移，请重新加载所有节点。由于具有不同网络模块的节点无法加入集群/故障转移对，因此您需要重新加载不含该模块的所有节点，然后它们才能重组集群/故障转移对。

监控接口

请参阅以下命令。

注释 对于 Firepower 和 Cisco Secure Firewall 模型，某些统计信息未使用 ASA 命令显示。您必须使用 FXOS 命令查看更详细的接口统计信息。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

有关详细信息，请参阅 FXOS 故障排除指南。

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

基本接口示例

请参阅以下配置示例。

物理接口参数示例

以下示例在单模式下配置物理接口的参数：

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

多情景模式示例

以下示例在多情景模式下配置用于系统配置的接口参数，并将千兆以太网 0/1.1 子接口分配到 contextA：

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

基本接口配置的历史记录

表 *24:* 接口的历史记录

功能名称	版本	功能信息
支持 Cisco Secure Firewall 1200 系列	9.22(1)	支持流量控制、FEC、检测 SFP 和自动协商等功能。
Cisco Secure Firewall 3100 固定端口上的默认前向纠错 (FEC) 从第 74 条 FC-FEC 更改为第 108 条 RS-FEC，适用于 25 GB+ SR、CSR 和 LR 收发器。	9.18(3) / 9.19(1)	当您在 Cisco Secure Firewall 3100 固定端口上将 FEC 设置为自动时，对于 25 GB SR、CSR 和 LR 收发器，默认类型现在设置为 cl108-rs 而不是 cl74-fc。 新增/修改的命令：**fec**
为 Cisco Secure Firewall 3100 暂停流量控制的帧	9.18(1)	如果流量激增，数据包会在激增量超过 NIC 上的 FIFO 缓冲区的缓冲容量且接收环缓冲的情况下发生中断。启用暂停帧来进行流量控制可缓解此问题。 新增/修改的命令：**flowcontrol send on**
Cisco Secure Firewall 3130 和 3140 的分支端口	9.18(1)	您现在可以为 Cisco Secure Firewall 3130 和 3140 上的每个 40GB 接口配置四个 10GB 分支端口。 新增/修改的命令：**breakout**
支持热插拔 Cisco Secure Firewall 3100 的网络模块	9.17(1)	您可以在防火墙通电时在 Cisco Secure Firewall 3100 上添加或删除网络模块。要将某个模块替换为相同类型的另一个模块，则无需重新启动。初始启动后，添加模块、永久删除模块或用新类型替换模块都需要重新启动。 新增/修改的命令：**netmod**
支持 Cisco Secure Firewall 3100 的前向纠错	9.17(1)	Cisco Secure Firewall 3100 25 Gbps 接口支持前向纠错 (FEC)。FEC 默认为启用并会设为“自动”(Auto)。 新增/修改的命令：**fec**
支持基于 SFP 为 Cisco Secure Firewall 3100 设置速度	9.17(1)	Cisco Secure Firewall 3100 支持基于安装的 SFP 的接口速度检测。检测 SFP 默认为启用。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。 新增/修改的命令：**speed sfp-detect**
可以为 1Gigabit 及更高版本的接口启用或禁用 Cisco Secure Firewall 3100 自动协商。	9.17(1)	Cisco Secure Firewall 3100 自动协商功能可与千兆位及以上接口的速度分开启用或禁用。 新增/修改的命令： **negotiation-auto**

功能名称	版本	功能信息
在 Firepower 1100 和 2100 的光纤接口上可禁用速度自动协商	9.14(1)	现在，您可以配置 Firepower 1100 或 2100 光纤接口以禁用自动协商。对于 10GB 接口，您可以将速度配置为 1GB 而无需自动协商；无法对速度设置为 10GB 的接口禁用自动协商。 新增/修改的命令：**speed nonegotiate**
ASA virtual的管理 0/0 接口上提供通过流量支持	9.6(2)	现在，您可以在 ASA virtual的管理 0/0 接口上允许通过流量。过去，仅 Microsoft Azure 上的 ASA virtual 支持通过流量；现在所有 ASA virtual都支持通过流量。您可以选择将此接口配置为仅管理接口，但默认情况下，没有进行此配置。 修改了以下命令：**management-only**
在千兆以太网接口上支持暂停帧以进行流量控制	8.2(5)/8.4(2)	您现在可以在所有 ASA 型号的千兆以太网接口上启用暂停 (XOFF) 帧以进行流量控制。 修改了以下命令：**flowcontrol**。
在 ASA 5580 的 10 千兆以太网接口上支持暂停帧以进行流量控制	8.2(2)	您现在可以为流量控制启用暂停 (XOFF) 帧。 ASA 5585-X 也支持此功能。 引入了以下命令：**flowcontrol**。
对 ASA 5580 的巨型数据包支持	8.1(1)	ASA 5580 支持巨帧。巨帧是指大于标准最大字节数（1518 字节）的以太网数据包（包括第 2 层报头和 FCS），最大可达 9216 字节。您可以通过增加用于处理以太网帧的内存量对所有接口启用巨型帧支持。为巨型帧分配较多内存可能会有碍于最大限度地利用其他功能（例如 ACL）。 ASA 5585-X 也支持此功能。 引入了以下命令：**jumbo-frame reservation**。
对于 ASA 5510 增强型安全许可证的千兆以太网支持	7.2(3)	现在，ASA 5510 通过增强型安全许可证为端口 0 和 1 提供 GE（千兆以太网）支持。如果从基础许可证升级至增强型安全许可证，则外部 Ethernet 0/0 和 Ethernet0/1 端口的容量将从原始的 FE（快速以太网）(100 Mbps) 增加到 GE (1000 Mbps)。接口名称将仍为 Ethernet 0/0 和 Ethernet 0/1。使用 **speed** 命令可更改接口上的速度，使用 **show interface** 命令可查看为每个接口当前配置的速度。
ASA 5510 上的基础许可证增加了接口数	7.2(2)	对于 ASA 5510 上的基础许可证，最大接口数从 3 加管理接口数增加到无限个。

第 15 章

Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口的基本接口配置

可以将各 Firepower 1010 或 Cisco Secure Firewall 1210/1220 接口配置为作为常规防火墙接口或第 2 层硬件交换机端口运行。本章节包括用于启动交换机端口配置的任务，包括启用或禁用交换模式以及创建 VLAN 接口和将它们分配给 VLAN。本章节还介绍如何在受支持接口上自定义以太网供电 (PoE)。

- 关于 Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口，第 675 页
- 交换机端口准则和限制，第 676 页
- 配置交换机端口和以太网供电，第 678 页
- 监控交换机端口，第 686 页
- 交换机端口示例，第 687 页
- 交换机端口的历史记录，第 691 页

关于 Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口

本节介绍 Firepower 1010 和 Cisco Secure Firewall 1210/1220的交换机端口。

了解交换机端口和接口

端口和接口

对于各物理 Firepower 1010 或 Cisco Secure Firewall 1210/1220 接口，可以将其操作设置为防火墙接口或交换机端口。请参阅以下有关物理接口和端口类型的信息，以及为其分配交换机端口的逻辑 VLAN 接口：

- 物理防火墙接口 - 在路由模式下，这些接口使用已配置的安全策略在第 3 层网络之间转发流量，以应用防火墙和 VPN 服务。 在透明模式下，这些接口是桥接组成员，用于在第 2 层同一网络上的接口之间转发流量，使用已配置的安全策略应用防火墙服务。在路由模式下，还可以将集

成路由和桥接与某些接口一起用作桥接组成员，将其他接口用作第 3 层接口。默认情况下，以太网 1/1 接口配置为防火墙接口。

- 物理交换机端口 - 交换机端口使用硬件中的交换功能在第 2 层转发流量。同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受 ASA安全策略的限制。接入端口仅接受未标记流量，可以将其分配给单个VLAN。中继端口接受未标记和已标记流量，且可以属于多个VLAN。默认情况下，以太网 1/2 至 1/8 (1010 和 1210) 或以太网 1/2 至 1/10 (1220) 配置为 VLAN 1 上的接入交换机端口。不能将 管理接口配置为交换机端口。
- 逻辑 VLAN 接口 - 这些接口的运行方式与物理防火墙接口相同，但不同的是，无法创建子接口或 EtherChannel 接口。如果交换机端口需要与另一个网络进行通信，则 ASA 设备将安全策略应用至 VLAN 接口，并路由至另一个逻辑 VLAN 接口或防火墙接口。甚至可以将集成路由和桥接与 VLAN 接口一起用作桥接组成员。同一 VLAN 上的交换机端口之间的流量不受安全策略 ASA 的限制，但桥接组中 VLAN 之间的流量会受到安全策略的限制，因此，可以选择将桥接组和交换机端口进行分层，以在某些分段之间实施安全策略。

以太网供电

Firepower 1010 支持以太网接口 1/7 和 1/8 上的增强型以太网供电+ (PoE+)。

Auto-MDI/MDIX 功能

如果是所有交换机口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

交换机端口准则和限制

情景模式

- Firepower 1010 不支持多情景模式。
- Cisco Secure Firewall 1210/1220 不支持多情景模式。

故障转移和集群

- 无集群支持。
- 仅支持主用/备用故障转移。
- 使用故障转移时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备 和备用设备上传输流量。故障转移旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常 故障转移网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN 接口可通过故障转移监控，而交换机端口无

法通过故障转移监控。理论上，您可以将单个交换机端口置于VLAN上并成功使用 故障转移，但更简单的设置是改用物理防火墙接口。

- 仅可使用防火墙接口作为故障转移链路。

逻辑 VLAN 接口 (SVI)

- 您可以创建多达 60 个 VLAN 接口。
- 如果还在防火墙接口上使用 VLAN 子接口，则无法使用与逻辑 VLAN 接口相同的 VLAN ID。
- MAC 地址：
  - 路由防火墙模式 - 所有 VLAN 接口共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一MAC地址，可手动分配MAC地址。请参阅手动配置 MAC 地址，第 791 页。
  - 透明防火墙模式 - 每个 VLAN 接口都有唯一的 MAC 地址。如有需要，您可通过手动分配 MAC 地址覆盖生成的 MAC 地址。请参阅手动配置 MAC 地址，第 791 页。

网桥组

您不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个网桥组中。

VLAN 接口和交换机端口不支持的功能

VLAN 接口和交换机端口不支持：

- 动态路由
- 组播路由
- 基于策略的路由
- 等价多路径路由 (ECMP)
- VXLAN
- EtherChannel
- 故障转移和状态链路
- 流量区域
- 安全组标记 (SGT)

其他准则和限制

- 您最多可以在 Firepower 1010 和 Cisco Secure Firewall 1210/1220上配置 60 个命名接口。
- 不能将 管理接口配置为交换机端口。

默认设置

- 以太网 1/1 是一个防火墙接口。
- 在 Firepower 1010 和 Cisco Secure Firewall 1210，以太网 1/2 至以太网 1/8 是分配给 VLAN 1 的交换机端口。
- 在 Cisco Secure Firewall 1220，以太网 1/2 至以太网 1/8 交换机端口会被分配给 VLAN 1。
- 默认速度和复用 - 默认情况下，速度和复用设置为自动协商。

配置交换机端口和以太网供电

要配置交换机端口和 PoE，请完成以下任务。

启用或禁用交换机端口模式

您可以将每个接口单独设置为防火墙接口或交换机端口。默认情况下，以太网 1/1 是防火墙接口，而剩余的以太网接口则配置为交换机端口。

过程

步骤 1 进入接口配置模式。

interface ethernet1/端口

- 端口，用于设置端口号，从 1 到 8。

您无法将 Management 1/1 接口设置为交换机端口模式。

示例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

步骤 2 启用交换机端口模式。

switchport

如果此接口已处于交换机端口模式，系统会提示您输入交换机端口参数，而不是更改模式。

```
ciscoasa(config-if)# switchport
ciscoasa(config-if)# switchport ?
interface mode commands/options:
  access         Set access mode characteristics of the interface
  mode           Set trunking mode of the interface
  monitor        Monitor another interface
  protected      Configure an interface to be a protected port
  trunk          Set trunking characteristics of the interface
<cr>
```

```
ciscoasa(config-if)#
```

步骤 3 禁用交换机端口模式。

no switchport

```
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# switchport ?

interface mode commands/options:
<cr>
```

示例

以下示例将以太网 1/3 和 1/4 设置为防火墙模式：

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)#
```

配置 VLAN 接口

本节介绍如何配置 VLAN 接口 (SVI) 以用于关联交换机端口。您最多可以创建 60 个与交换机端口相关联的 VLAN 接口。

过程

步骤 1 添加 VLAN 接口。

interface vlan *id*

- *id* - 设置此接口的 VLAN ID（介于 1 和 4070 之间），不包括 3968 到 4047 范围内的ID（保留供内部使用）。

示例：

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)#
```

步骤 2 （可选） 禁用转发到另一个 VLAN。

no forward interface *vlan_id*

- *vlan_id* - 为不能发起到其它 VLAN 流量的 VLAN 接口的 VLAN ID。

例如，您有一个 VLAN 分配给外部以供互联网访问，另一个 VLAN 分配给内部企业网络，第三个 VLAN 分配给您的家庭网络。家庭网络无需访问企业网络，因此，您可以使用 **no forward interface** 命令来选择家庭 VLAN；企业网络可以访问家庭网络，但家庭网络不能访问企业网络。

示例：

```
ciscoasa(config-if)# no forward interface 200
ciscoasa(config-if)#
```

将交换机端口配置为接入端口

要将交换机端口分配给单个 VLAN，请将其配置为接入端口。接入端口仅接受未标记流量。默认情况下，以太网 1/2 至以太网 1/8 交换机端口会被启用并分配给 的 VLAN 1。在 Cisco Secure Firewall 1220 上，以太网 1/2 至以太网 1/10 交换机端口会被默认启用并分配给 VLAN 1。

注释 设备不支持在网络中进行环路检测的生成树协议。因此，您必须确保与ASA的任何连接均不会在网络环路中结束。

过程

步骤 1 进入接口配置模式。

interface ethernet1/端口

- 端口，用于设置端口号，从 1 到 8。

示例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

步骤 2 将此交换机端口分配给 VLAN。

switchport access vlan编号

- *number* - 设置介于 1 和 4070 之间的 VLAN ID。默认值为 VLAN 1。

示例：

```
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)#
```

步骤 3 （可选） 将此交换机端口设置为受保护端口， 因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

switchport protected

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；如出现病毒感染或其他安全漏洞，则需要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，则在您将 **switchport protected** 命令应用于各交换机端口后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

示例：

```
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)#
```

步骤 4 （可选） 设置速度。

speed {**auto** | **10** | **100** | **1000**}

默认值为 **auto**。

示例：

```
ciscoasa(config-if)# speed 100
ciscoasa(config-if)#
```

步骤 5 （可选） 设置双工。

duplex {**auto** | **full** | **half**}

默认值为 **auto**。

示例：

```
ciscoasa(config-if)# duplex half
ciscoasa(config-if)#
```

步骤 6 启用交换机端口。

no shutdown

要禁用此交换机端口，请输入 **shutdown** 命令。

示例：

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

示例

以下示例将以太网 1/3、以太网 1/4 和以太网 1/5 的比例分配给 VLAN 101，并将以太网 1/3 和以太网 1/4 的比例设置为受保护：

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/4
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/5
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# no shutdown
```

将交换机端口配置为中继端口

此程序介绍如何创建可以使用 802.1 Q 标记传输多个 VLAN 的中继端口。中继端口接受未标记和标记流量。允许的 VLAN 上的流量通过中继端口保持不变。

中继端口接收未标记流量后将其标记为本地 VLAN ID，以便 ASA 可以将流量转发至正确交换机端口，或可以将流量路由至另一个防火墙接口。如果 ASA 从中继端口发送本地 VLAN ID 流量，则会删除 VLAN 标记。请务必在另一台交换机上的中继端口上设置相同的本地 VLAN，以便将未标记流量标记至同一 VLAN。

过程

步骤 1 进入接口配置模式。

interface ethernet1/端口

- 端口，用于设置端口号，从 1 到 8。

示例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

步骤 2 使此交换机端口成为中继端口。

switchport mode trunk

要将此端口恢复为接入模式，请输入 **switchport mode access** 命令。

示例：

```
ciscoasa(config-if)# switchport mode trunk
```

```
ciscoasa(config-if)#
```

步骤 3 将 VLAN 分配给此中继。

switchport trunk allowed vlan *vlan_range*

- *vlan_range* - 设置介于 1 和 4070 之间的 VLAN ID。您可以通过以下方式之一识别最多 20 个ID：
  - 单一编号 (n)
  - 范围 (n-x)
  - 用逗号将编号和范围隔开，例如：

    5,7-10,13,45-100

可以用空格代替逗号，但此命令保存到配置中后，其中的空格将会变成逗号。

如果在此命令中包含本地 VLAN，则将忽略该本地 VLAN；从端口发送本地 VLAN 流量时，中继端口始终会删除 VLAN 标记。此外，不会接收仍具有 VLAN 标记的流量。

示例：

```
ciscoasa(config-if)# switchport trunk allowed vlan 100,200,300
ciscoasa(config-if)#
```

步骤 4 设置本地 VLAN。

switchport trunk native vlan *vlan_id*

- *vlan_range* - 设置介于 1 和 4070 之间的 VLAN ID。默认值为 VLAN 1。

每个端口只能有一个本地 VLAN，但各端口的本地 VLAN 可以相同也可以不同。

示例：

```
ciscoasa(config-if)# switchport trunk native vlan 2
ciscoasa(config-if)#
```

步骤 5 （可选） 将此交换机端口设置为受保护端口， 因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

switchport protected

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；如出现病毒感染或其他安全漏洞，则需要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，则在您将 **switchport protected** 命令应用于各交换机端口后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

示例：

```
ciscoasa(config-if)# switchport protected
```

```
ciscoasa(config-if)#
```

步骤 6 （可选） 设置速度。

speed {**auto** | **10** | **100** | **1000**}

默认值为 **auto**。

示例：

```
ciscoasa(config-if)# speed 100
ciscoasa(config-if)#
```

步骤 7 （可选） 设置双工。

duplex {**auto** | **full** | **half**}

默认值为 **auto**。

示例：

```
ciscoasa(config-if)# duplex half
ciscoasa(config-if)#
```

步骤 8 启用交换机端口。

no shutdown

要禁用此交换机端口，请输入 **shutdown** 命令。

示例：

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

示例

以下示例将以太网 1/6 设置为 VLAN 为 20 到 30 的中继端口，并将本地 VLAN 设置为 4：

```
ciscoasa(config)# interface ethernet1/6
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 20-30
ciscoasa(config-if)# switchport trunk native vlan 4
ciscoasa(config-if)# no shutdown
```

配置以太网供电

在 Firepower 1010， 以太网 1/7 和以太网 1/8 支持 IP 电话或无线接入点等设备的以太网供电 (PoE)。在 Cisco Secure Firewall 1210CP 上，以太网 1/5-1/8 支持 PoE。Firepower 1010 和 Cisco Secure Firewall

1210CP 支持 IEEE 802.3af (PoE) 和 802.3at (PoE+)。PoE+ 使用链路层发现协议 (LLDP) 来协商功率级别。PoE+ 可以为受电设备提供 30 瓦的功率。仅在需要时提供功率。

如果关闭接口，则会禁用设备电源。

在 Firepower 1010， 在以太网 1/7 和以太网 1/8 上启用 PoE。在 Cisco Secure Firewall 1210CP 上，以太网 1/5-1/8 上的 PoE 默认启用。此过程介绍如何禁用和启用 PoE 以及如何设置可选参数。

过程

步骤 1 进入接口配置模式。

interface ethernet1/5（仅限 1210CP）|（仅限 1210CP）**6**（仅限 1210CP）**7** | **8**}

示例：

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)#
```

步骤 2 启用或禁用 PoE+。

power inline {**auto** | **never** | **consumption wattage** *milliwatts*}

- **auto** - PoE 使用适合受电设备类别的瓦数将电源自动传送至受电设备。Firepower 1010 和 Cisco Secure Firewall 1210CP 使用 LLDP 进一步协商正确的瓦数。
- **never** - 禁用 PoE。
- **consumption wattage***millipowers* - 手动指定以瓦为单位的瓦数，范围为 4000 至 30000。如果要手动设置瓦数并禁用 LLDP 协商，请使用此命令。

使用 **show power inline** 命令查看当前 PoE+ 状态。

示例：

```
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)# show power inline
Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

示例

以下示例为以太网 1/7 手动设置功率，为以太网 1/8 设置功率为自动：

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)# power inline consumption wattage 10000
ciscoasa(config-if)# interface ethernet1/8
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)#
```

监控交换机端口

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

- **show switch vlan**

  显示 VLAN 到交换机端口的关联。

```
ciscoasa# show switch vlan
VLAN Name                 Status    Ports
---- -------------------- --------- --------------------
1    -                     down      Ethernet1/3,
                                     Ethernet1/4,
                                     Ethernet1/5,
                                     Ethernet1/6
                                     Ethernet1/7,
                                     Ethernet1/8
10   inside                up        Ethernet1/1
20   outside               up        Ethernet1/2
```

- **show switch mac-address-table**

  显示静态和动态 MAC 地址条目。

```
ciscoasa# show switch mac-address-table
Legend: Age - entry expiration time in seconds
  Mac Address  | VLAN |       Type       | Age | Port
-----------------------------------------------------
0c75.bd11.c504 | 0010 |     dynamic      | 330 | In0/0
885a.92f6.c6e3 | 0010 |     dynamic      | 330 | Et1/1
0c75.bd11.c504 | 0020 |     dynamic      | 330 | In0/0
885a.92f6.c45b | 0020 |     dynamic      | 330 | Et1/2
```

- **show arp**

显示动态、静态和代理 ARP 条目。动态 ARP 条目包括 ARP 条目时限（秒）。静态 ARP 条目以短划线 (-) 取代时限，代理 ARP 条目则显示“别名”。以下是 **show arp** 命令的输出示例。第一个条目是时限为 2 秒的动态条目。第二个条目是静态条目，第三个条目来自代理 ARP。

```
ciscoasa# show arp
outside 10.86.194.61 0011.2094.1d2b 2
outside 10.86.194.1 001a.300c.8000 -
outside 10.86.195.2 00d0.02a8.440a alias
```

- **show power inline**

  显示 PoE+ 状态。

```
ciscoasa# show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

交换机端口示例

以下主题提供在路由和透明模式下配置交换机端口的示例。

路由模式示例

以下示例创建两个 VLAN 接口，并将两个交换机端口分配给内部接口，一个分配给外部接口。

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Vlan20
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
```

```
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

透明模式示例

以下示例在网桥组 1 中创建两个 VLAN 接口，并将两个交换机端口分配给内部接口，一个分配给外部接口。

```
firewall transparent
!
interface BVI1
ip address 10.20.20.1 255.255.255.0
!
interface Vlan11
bridge-group 1
nameif inside
security-level 100
no shutdown
!
interface Vlan20
bridge-group 1
nameif outside
security-level 0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

混合防火墙接口/交换机端口示例

以下示例为内部接口创建一个 VLAN 接口，为外部和 dmz 创建两个防火墙接口。

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
```

```
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/4
nameif outside
security-level 0
ip address 10.12.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/5
nameif dmz
security-level 50
ip address 10.13.11.1 255.255.255.0
no shutdown
```

集成的路由和桥接示例

以下示例创建两个网桥组，其中两个VLAN接口（inside_1和inside_2）在网桥组1中，一个（外部）在网桥组2中。第四个VLAN接口不属于网桥组，而是常规路由接口。同一VLAN上交换机端口之间的流量不受ASA的安全策略限制。但网桥组中VLAN之间的流量会受到安全策略的限制，因此，可以选择将网桥组和交换机端口进行分层，以在某些分段之间实施安全策略。

```
interface BVI1
nameif inside_bvi
security-level 100
ip address 10.30.1.10 255.255.255.0
!
interface BVI2
nameif outside_bvi
security-level 0
ip address 10.40.1.10 255.255.255.0
!
interface Vlan10
bridge-group 1
nameif inside_1
security-level 100
no shutdown
!
interface Vlan20
bridge-group 2
nameif outside
security-level 0
no shutdown
!
interface Vlan30
bridge-group 1
nameif inside_2
security-level 100
no shutdown
```

```
!
interface Vlan 100
nameif dmz
security-level 0
ip address 10.1.1.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 10
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/4
switchport
switchport access vlan 20
security-level 100
no shutdown
!
interface Ethernet1/5
switchport
switchport access vlan 100
no shutdown
!
interface Ethernet1/6
switchport
switchport access vlan 10
no shutdown
!
interface Ethernet1/7
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/8
switchport
switchport access vlan 100
no shutdown
```

故障转移示例

以下示例将以太网 1/3 配置为故障转移接口。

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0 standby 10.11.11.2
no shutdown
!
interface Vlan20
nameif outside
```

```
security-level 0
ip address 10.20.20.1 255.255.255.0 standby 10.20.20.2
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
description LAN/STATE Failover Interface
no shutdown
!
failover
failover lan unit primary
failover lan interface folink Ethernet1/3
failover replication http
failover link folink Ethernet1/3
failover interface ip folink 10.90.90.1 255.255.255.0 standby 10.90.90.2
```

交换机端口的历史记录

表 *25:* 交换机端口的历史记录

功能名称	版本	功能信息
Cisco Secure Firewall 1210/1220 硬件交换机支持	9.22(1)	Cisco Secure Firewall 1210/1220 支持将各以太网接口设置为交换机端口或防火墙接口。
以太网端口 1/5-1/8 上的 Cisco Secure Firewall 1210CP PoE+ 支持	9.22(1)	Cisco Secure Firewall 1210CP 在以太网端口 1/5-1/8 上支持以太网供电+ (PoE+)。
Firepower 1010 硬件交换机支持	9.13(1)	Firepower 1010 支持将各以太网接口设置为交换机端口或防火墙接口。 新增/修改的命令：forward interface、interface vlan、show switch mac-address-table、show switch vlan、switchport、switchport access vlan、switchport mode、switchport trunk allowed vlan
Firepower 1010 PoE + 支持以太网 1/7 和以太网 1/8	9.13(1)	Firepower 1010 支持以太网接口 1/7 和 1/8 上的增强型以太网供电+ (PoE+)。 新增/修改的命令：**power inline**、**show power inline**

第 16 章

EtherChannel 接口

本章介绍如何配置 EtherChannel 接口。

注释 在多情景模式下，请在系统执行空间中完成本节所述的所有任务。 要从情景更改到系统执行空间，请输入 **changeto system** 命令。

有关具有特殊要求的 ASA 集群接口，请参阅为 Cisco Secure Firewall 3100/4200部署 ASA 集群，第 333 页。

注释 对于平台模式下的 Firepower 4100/9300 机箱，EtherChannel 接口是在 FXOS 操作系统中配置。有关详细信息，请参阅机箱的配置或快速入门指南。

- 关于 EtherChannels，第 693 页
- EtherChannel 的准则，第 696 页
- EtherChannel 的默认设置，第 698 页
- 配置 EtherChannel，第 698 页
- 监控 EtherChannels，第 702 页
- EtherChannel 示例，第 703 页
- EtherChannels的历史记录，第 704 页

关于 EtherChannels

本节介绍 EtherChannel 。

关于 EtherChannel

802.3ad EtherChannel 是逻辑接口（称为端口通道接口），该接口由一组单独的以太网链路（通道组）组成，以便可以提高单个网络的带宽。配置接口相关功能时，可以像使用物理接口一样来使用端口通道接口。

最多可以配置 48 个 Etherchannel，具体取决于型号支持的接口数量。

通道组接口

各信道组最多可以有 8 个活动接口，但 ISA 3000 除外，支持 16 个活动接口。对于仅支持 8 个主用接口的交换机，您最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。

通道组中的所有接口都必须属于同一类型且具有相同速度。添加到通道组的第一个接口确定正确的类型和速度。

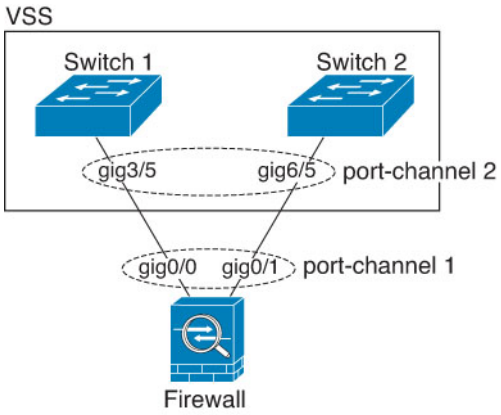
EtherChannel 汇聚通道中所有可用活动接口上的流量。系统根据源或目标 MAC 地址、IP 地址、TCP 端口号、UDP 端口号和 VLAN 编号使用专有散列算法来选择接口。

连接到其他设备上的 EtherChannel

ASAEtherChannel 连接到的设备还必须支持 802.3ad EtherChannel；例如，可以连接到 Catalyst 6500 交换机或 Cisco Nexus 7000。

如果交换机属于虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 的一部分，则可以将同一 EtherChannel 内的 ASA接口连接到 VSS/vPC 中的单独交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台单独的交换机的行为就像一台交换机一样。

图 *66:* 连接至 *VSS/vPC*

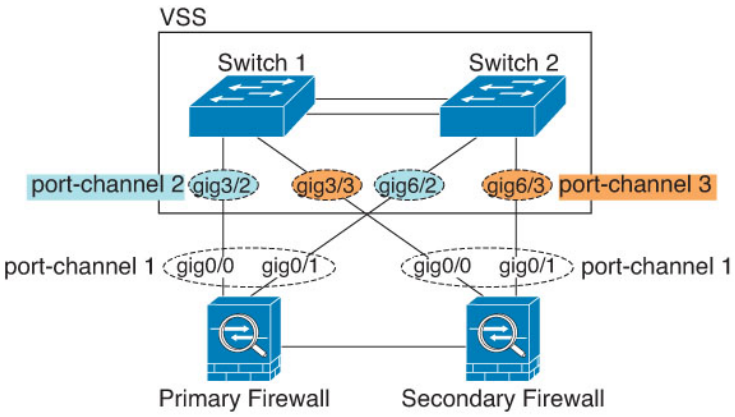


注释 如果 ASA 设备处于透明防火墙模式下，并且将 ASA 设备置于两组 VSS/vPC 交换机之间，请确保在使用 EtherChannel 连接到 ASA 设备的所有交换机端口上禁用单向链路检测 (UDLD)。如果启用 UDLD，则交换机端口可能会接收来自另一个 VSS/vPC 对中的两台交换机的 UDLD 数据包。接收交换机会将接收接口置于关闭状态，原因是“UDLD 邻居不匹配”。

如果您在主用/备用故障转移部署中使用 ASA 设备，则需要在 VSS/vPC 中的交换机上创建单独的 EtherChannel，为每个 ASA 设备创建一个。在每个 ASA 设备上，单个 EtherChannel 连接至两台交换机。即使您可以将所有的交换机接口分组到连接两个 ASA 设备的一个 EtherChannel 中（在这种情况

下，将不会建立 EtherChannel，因为 ASA 系统 ID 是单独的），但单个 EtherChannel 并不可取，因为您不希望将流量发送到备用 ASA 设备。

图 *67:* 主用/备用故障转移和 *VSS/vPC*



链路聚合控制协议

链路聚合控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

您可以将 EtherChannel 中的每个物理接口配置为：

- Active - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- 被动 - 接收 LACP 更新。备用 EtherChannel 只能与主用 EtherChannel 建立连接。在硬件型号上不受支持。
- 开启 - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

负载均衡

ASA 设备通过对数据包的源 IP 地址和目标 IP 地址进行散列处理来将数据包分发给 EtherChannel 中的接口（此条件可配置）。在模数运算中，将得到的散列值除以主用链路数，得到的余数确定哪个接口拥有流量。*hash_value* **mod** *active_links* 结果为 0 的所有数据包都发往 EtherChannel 中的第一个接口，结果为 1 的发往第二个接口，结果为 2 的数据包发往第三个接口，依此类推。例如，如果您有 15 个主用链路，则模数运算的值为 0 到 14。如果有 6 个主用链路，则值为 0 到 5，依此类推。

对于集群中的跨网络 EtherChannel，会逐个 ASA进行负载均衡。例如，如果 8 个 ASA之间的跨网络 EtherChannel 中有 32 个主用接口，而 EtherChannel 中的每个 ASA又有 4 个接口，则仅会在 ASA上的 4 个接口之间进行负载均衡。

如果主用接口发生故障且未由备用接口替代，则流量会在剩余的链路之间重新均衡。该故障会在第 2 层的生成树和第 3 层的路由表中被屏蔽，因此故障转移对其他网络设备是透明的。

相关主题

自定义 EtherChannel（ISA 3000），第 701 页

EtherChannel MAC 地址

属于通道组一部分的所有接口都共享同一 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。

Firepower 和 Cisco Secure Firewall 硬件

端口通道接口使用内部接口 Internal-Data 0/1 的 MAC 地址。或者，您可以为端口通道接口手动配置 MAC 地址。在多情景模式下，您可以将唯一 MAC 地址自动分配给共享接口，包括一个 EtherChannel 端口接口。机箱上的所有 EtherChannel 接口都使用相同的 MAC 地址，因此请注意，例如，如果使用 SNMP 轮询，则多个接口将具有相同的 MAC 地址。

注释 成员接口仅在重新启动后使用内部数据 0/1 MAC 地址。在重新启动之前，成员接口使用自己的 MAC 地址。如果在重新启动后添加新的成员接口，则必须再次重新启动以更新其 MAC 地址。

EtherChannel 的准则

桥接组

在路由模式下，不支持将 ASA-定义的 EtherChannel 接口作为桥接组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。

故障转移

- 如果要将 EtherChannel 接口用作 故障转移 链路，则必须在 故障转移 对中的两台设备上预配置要使用的接口；不能在主设备上配置该接口并期望它会复制到辅助设备，因为复制需要 故障转移链路本身。
- 如果要将 EtherChannel 接口用于状态链路，则无需特殊配置；可以照常从主设备复制配置。Firepower 4100/9300 机箱 的所有接口（包括 EtherChannel）均需在两台设备上进行预配置。
- 可以使用 **monitor-interface** 命令监控 EtherChannel 接口 (故障转移)。如果主用成员接口故障转移到备用接口，则此活动不会在监控设备级故障转移时导致 EtherChannel 接口出现故障。仅在所有物理接口都出现故障的情况下，EtherChannel 接口或 EtherChannel 接口才会出现故障（对于 EtherChannel 接口，可配置允许出现故障的成员接口数量）。
- 如果将 EtherChannel 接口用于故障转移或状态链路，然后防止无序数据包，则仅会使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。

您不能在 EtherChannel 配置用作故障转移链路时对其进行修改。要修改配置，您需要暂时禁用故障转移，以防止在此期间发生故障转移。

型号支持

- 对于 Firepower 4100/9300 或 ASA virtual，不能在 ASA 中添加 EtherChannels。Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。
- 无法在 Etherchannel 中使用 Firepower 1010 或 Cisco Secure Firewall 1210/1220 交换机端口或 VLAN 接口。

集群

- 如果要将 EtherChannel 接口用作集群控制链路，您必须在该集群中的所有设备上预配置要使用的接口；不能在主设备上配置该接口并期望它会复制到成员设备，因为复制 需要使用集群控制链路本身。
- 要配置跨网络 EtherChannel 或单个集群接口，请参阅有关集群的章节。

通用 EtherChannel 准则

- 最多可以配置 48 个 Etherchannel，具体取决于型号可用的接口数量。
- 各信道组最多可以有 8 个活动接口，但 ISA 3000 除外，支持 16 个活动接口。对于仅支持 8 个主用接口的交换机，您最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。
- 通道组中的所有接口都必须具有相同的介质类型和速度能力，并且必须设置为相同的速度和复用模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在较大容量的接口上将速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口），但 Cisco Secure Firewall 1200/3100/4200除外，它支持不同的接口容量，只要速度设置为检测 SFP；在此情况下会使用较低的常见速度。
- ASAEtherChannel 连接到的设备还必须支持 802.3ad EtherChannel。
- ASA 设备不支持带有 VLAN 标记的 LACPDU。如果使用 Cisco IOS **vlan dot1Q tag native** 命令在相邻交换机上启用本地 VLAN 标记，则 ASA 设备将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。在多情景模式下，在数据包捕获中不包含这些消息，因此您无法轻易对问题进行诊断。
- LACP 值取决于型号。设置速率（正常或快速）时，设备会向连接的交换机请求该速率。作为回报，设备将按照连接的交换机请求的速率进行发送。我们建议您在两端设置相同的速率。
  - Firepower 4100/9300 - LACP 速率在 FXOS 中默认设置为“快速”，但您可以将其配置为“正常”（也称为“慢速”）。
  - Cisco Secure Firewall 3100/4200 - 默认情况下，LACP 速率设置为正常（慢速），但您可以在设备上将其配置为快速。

- 所有型号-LACP 速率设置为正常（慢），并且不可配置，这意味着设备将始终从连接的交换机请求慢速速率。我们建议将交换机上的速率设置为慢速，以便两端以相同的速率发送 LACP 消息。

- 在低于 15.1(1)S2 的 Cisco IOS 软件版本中， ASA 不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆叠连接 ASA EtherChannel，则当主要交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。
- 所有 ASA 配置均引用 EtherChannel 接口，而不是成员物理接口。
- 您必须先从端口通道成员身份中删除分支端口，然后才能删除具有分支端口的端口通道。否则，在删除端口通道后，分支端口将显示为未关联。如果端口通道只有固定端口且没有分支端口，则此选项不适用。

EtherChannel 的默认设置

本节列出了接口的默认设置（如果没有出厂默认配置）。

接口的默认状态

接口的默认状态取决于类型和情景模式。

在多情景模式下，默认启用所有已分配的接口，而不考虑接口在系统执行空间中的状态。但是，要使流量通过该接口，还必须在系统执行空间中启用该接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

在单模式下或在系统执行空间中，接口具有以下默认状态：

- 物理接口 - 已禁用。
- EtherChannel 端口通道接口 - 已启用。但是，要使流量通过 EtherChannel 接口，还必须启用通道组物理接口。

配置 EtherChannel

本节介绍如何创建 EtherChannel 端口通道接口，如何向 EtherChannel 分配接口，以及如何自定义 EtherChannel。

将接口添加到 EtherChannel

本节介绍如何创建 EtherChannel 端口通道接口并向 EtherChannel 分配接口。默认情况下，端口通道接口已启用。

开始之前

- 最多可以配置 48 个 Etherchannel，具体取决于型号具有的接口数量。
- 各信道组最多可以有 8 个活动接口，但 ISA 3000 除外，支持 16 个活动接口。对于仅支持 8 个主用接口的交换机，您最多可以将 16 个接口分配给一个通道组：但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。
- 要为集群配置跨网络 EtherChannel，请参阅有关集群的章节而不是此程序。
- 通道组中的所有接口都必须具有相同的介质类型和容量，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在较大容量的接口上将速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口），但 Cisco Secure Firewall 3100/4200除外，它支持不同的接口容量，只要速度设置为检测 SFP；在此情况下会使用较低的常见速度。 。
- 如果已为物理接口配置了名称，则不能将该物理接口添加到通道组。您必须先中使用 **no nameif** 命令删除该名称。
- 对于多情景模式，请在系统执行空间中完成本程序。要从情景切换到系统执行空间，请输入 **changeto system** 命令。

注意 如果使用的是配置中已有的物理接口，则删除名称将会清除引用该接口的任何配置。

过程

步骤 1 指定要添加到通道组的接口：

interface *physical_interface*

示例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID 包含类型、插槽和端口号，格式为 type[slot/]port。通道组中的第一个接口决定了该组中所有其他接口的类型和速度。

在透明模式下，如果使用多个管理接口创建通道组，则可以将 EtherChannel 用作管理专属接口。

步骤 2 将此物理接口分配到 EtherChannel：

channel-group *channel_id* **mode** {**active** | **passive** | **on**}

示例：

```
ciscoasa(config-if)# channel-group 1 mode active
```

channel_id 是一个介于 1 和 48 之间的证书（1~8 用于 Firepower 1010 和 1210，介于 1 和 10 用于 1220）。如果此通道 ID 的端口通道接口尚未存在于配置中，则将添加一个端口通道接口：

interface port-channel *channel_id*

我们建议使用 **active** 模式。**被动**模式仅适用于 ISA 3000。

步骤 3 （可选）（仅限 Cisco Secure Firewall 3100/4200）设置通道组中物理接口的 LACP 数据单元接收速率。

lacp rate {**normal** | **fast**}

默认值为 **normal**（慢，每 30 秒）。**fast** 选项每秒接收一次 LACP 数据单元。应与所连接开关的设置相匹配。

步骤 4 （可选）（仅 ISA 3000 型号）为通道组中的物理接口设置优先级。

lacp port-priority 编号

示例：

```
ciscoasa(config-if)# lacp port-priority 12345
```

优先级 *number* 是介于 1 和 65535 之间的整数。默认值为 32768。数字越大，优先级越低。如果分配的接口多于可用的接口，则ASA将使用此设置决定哪些接口是主用接口，哪些是备用接口。如果所有接口的端口优先级设置都相同，则优先级由接口 ID（插槽/端口）确定。最低的接口 ID 具有最高优先级。例如，千兆以太网 0/0 的优先级高于千兆以太网 0/1 的优先级。

如果要将某个接口优先确定为主用接口（即使它具有较高的接口ID也如此），请将此命令设置为具有较低的值。例如，要在千兆以太网 0/7 之前将千兆以太网 1/3 设为主用，请在 1/3 接口上将 **lacp port-priority** 值设置为 12345；在 0/7 接口上设置为默认值 32768。

如果 EtherChannel 另一端的设备端口存在优先级冲突，则会使用系统优先级来确定使用哪些端口优先级。请参阅 **lacp system-priority** 命令。

步骤 5 （可选）将端口通道接口的以太网属性设置为覆盖各个接口上设置的属性。

interface port-channel *channel_id*

有关以太网命令，请参阅启用物理接口和配置以太网参数，第 662 页。此方法提供了设置这些参数的快捷方式，因为通道组中所有接口的这些参数都必须匹配。

步骤 6 对于要添加到通道组中的每个接口，请重复步骤 1 至步骤 3。

通道组中的每个接口都必须具有相同的类型和速度。不支持半双工。如果添加不匹配的接口，则该接口将处于暂停状态。

步骤 7 （可选）（仅限 Cisco Secure Firewall 3100/4200）设置通道组中物理接口的 LACP 数据单元接收速率。

a) 点击 **Interfaces** 表中的物理接口，然后点击 **Edit**。

系统将显示 **Edit Interface** 对话框。

b) 点击 **Advanced** 选项卡。

c) 在 **EtherChannel** 区域中，从**速率 (Rate)** 下拉列表选择**正常 (Normal)** 或**快速 (Fast)**。

默认设置为**正常 (Normal)**（慢速，每 30 秒）。**快速 (Fast)** 选项每秒接收一次 LACP 更新。应与所连接开关的设置相匹配。

相关主题

链路聚合控制协议，第 695 页
自定义 EtherChannel（ISA 3000），第 701 页

自定义 EtherChannel（ISA 3000）

本节介绍如何设置 EtherChannel 中的最大接口数，用于使 EtherChannel 成为主用接口所需的最小操作接口数、负载均衡算法以及其他可选参数。这些参数仅适用于 ISA 3000。

过程

步骤 1 指定端口通道接口：

interface port-channel *channel_id*

示例：

```
ciscoasa(config)# interface port-channel 1
```

在将接口添加到通道组时，将自动创建此接口。如果尚未添加接口，则此命令会创建端口通道接口。

您需要先向端口通道接口添加至少一个成员接口，然后才能为其配置逻辑参数（例如名称）。

步骤 2 指定通道组中允许的最大主用接口数：

lacp max-bundle 编号

示例：

```
ciscoasa(config-if)# lacp max-bundle 6
```

number 介于 1 和 16 之间。默认值为 16。如果交换机不支持 16 个主用接口，请务必将此命令设置为 8 或更小的值。

步骤 3 指定使端口通道接口变成主用接口所需的最小主用接口数：

port-channel min-bundle 编号

示例：

```
ciscoasa(config-if)# port-channel min-bundle 2
```

number 介于 1 和 16 之间。默认值为 1。如果通道组中的主用接口数小于此值，则端口通道接口将会发生故障，并可能会触发设备级故障转移。

步骤 4 配置负载均衡算法：

port-channel load-balance {**dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port**}

示例：

```
ciscoasa(config-if)# port-channel load-balance src-dst-mac
```

默认情况下，ASA 根据数据包的源 IP 地址和目标 IP 地址 (**src-dst-ip**) 来均衡接口上的数据包负载。要更改数据包分类所依据的属性，请使用此命令。例如，如果流量严重偏向于相同的源 IP 地址和目标 IP 地址，则分配给 EtherChannel 中的接口的流量将失去平衡。更改为其他算法可使流量分布更均匀。

步骤 5 设置 LACP 系统优先级：

lacp system-priority 编号

示例：

```
ciscoasa(config)# lacp system-priority 12345
```

number 介于 1 和 65535 之间。默认值为 32768。数字越大，优先级越低。对于 ASA 而言，此命令是全局命令。

如果 EtherChannel 另一端的设备端口存在优先级冲突，则会使用系统优先级来确定使用哪些端口优先级。有关 EtherChannel 内的接口优先级，请参阅 **lacp port-priority** 命令。

相关主题

负载均衡，第 695 页
将接口添加到 EtherChannel，第 698 页

监控 EtherChannels

请参阅以下命令：

注释 对于 Firepower 和 Cisco Secure Firewall 模型，某些统计信息未使用 ASA 命令显示。您必须使用 FXOS 命令查看更详细的接口统计信息。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

有关详细信息，请参阅 FXOS 故障排除指南。

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

- (ISA 3000 only) **show lacp** {[*channel_group_number*] {**counters** | **internal** | **neighbor**} | **sys-id**}

  对于 EtherChannel，显示 LACP 信息，例如流量统计信息、系统标识符和邻居详细信息。

- (ISA 3000 only) **show port-channel** [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

  对于 EtherChannel，以详细的单行摘要形式显示 EtherChannel 信息。此命令还显示端口和端口通道信息。

- (ISA 3000 only) **show port-channel** *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **l4port** | **mac** | **mixed** | **vlan-only**} *parameters*]

  对于 EtherChannel，显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

EtherChannel 示例

以下示例将三个接口配置为 EtherChannel 的一部分。此示例还将系统优先级设置为较高的优先级，并在 EtherChannel 分配有超过 8 个接口的情况下将千兆以太网 0/2 的优先级设置为高于其他接口。

```
lacp system-priority 1234
interface GigabitEthernet0/0
  channel-group 1 mode active
interface GigabitEthernet0/1
  channel-group 1 mode active
interface GigabitEthernet0/2
  lacp port-priority 1234
  channel-group 1 mode passive
interface Port-channel1
  lacp max-bundle 4
  port-channel min-bundle 2
  port-channel load-balance dst-ip
```

EtherChannels的历史记录

表 *26: EtherChannels*的历史记录

功能名称	版本	功能信息
EtherChannel 支持	8.4(1)	您可以为八个主用接口各配置多达 48 个 802.3ad EtherChannel。 引入了以下命令：**channel-group**、**lacp port-priority**、**interface port-channel**、**lacp max-bundle**、**port-channel min-bundle**、**port-channel load-balance**、**lacp system-priority**、**clear lacp counters**、**show lacp**、**show port-channel**。 注释 ASA 5505 不支持 EtherChannel。
一个 EtherChannel 中支持 16 个主用链路	9.2(1)	现在，一个 EtherChannel 中最多可以配置 16 个主用链路。以前，可以有 8 个主用链路和 8 个备用链路。确保交换机可以支持 16 个主用链路（例如，可使用带有 F2 系列 10 千兆以太网模块的思科 Nexus 7000）。 注释 如果从早期 ASA 版本进行升级，则为了实现兼容，可将最大主用接口数设置为 8（**lacp max-bundle** 命令）。 修改了以下命令：**lacp max-bundle** 和 **port-channel min-bundle**。

第 17 章

环回接口

本部分介绍如何配置环回接口。

- 关于环回接口， 第 705 页
- 环回接口准则， 第 706 页
- 配置环回接口， 第 706 页
- 对流向环回接口的流量进行速率限制， 第 706 页
- 监控环回接口， 第 708 页
- 环回接口的历史记录， 第 708 页

关于环回接口

环回接口是一种会模拟物理接口的纯软件接口。此接口可通过多个物理接口在IPv4和IPv6上访问。环回接口有助于克服路径故障；它可以从任何物理接口访问，因此，如果其中一个接口发生故障，您可以从另一个接口访问环回接口。

环回接口可用于：

- AAA
- BGP
- DNS
- HTTP
- ICMP
- SNMP
- SSH
- 静态和动态 VTI 隧道
- 系统日志
- Telnet

ASA可以使用动态路由协议分发环回地址，也可以在对等设备上配置静态路由，以通过ASA的物理接口之一到达环回 IP 地址。不能在指定环回接口的 ASA 上配置静态路由。

环回接口准则

故障转移和集群

- 无集群支持。

情景模式

- VTI 仅支持单情景模式。在多情景模式下支持其他环回用途。

其他准则和限制

- 对于从物理接口到环回接口的流量，TCP 序列随机化始终处于禁用状态。

配置环回接口

添加环回接口。

过程

步骤 1 创建环回接口：

interface loopback 编号

数字可以介于 0 和 10413 之间。

示例：

```
ciscoasa(config)# interface loopback 10
```

步骤 2 配置名称和 IP 地址。请参阅路由模式接口和透明模式接口，第 749 页。

步骤 3 配置环回的速率限制。请参阅对流向环回接口的流量进行速率限制，第 706 页。

对流向环回接口的流量进行速率限制

您应该对流向环回接口 IP 地址的流量进行速率限制，以防止系统负载过大。您可以向全局服务策略添加连接限制规则。此程序会显示添加到默认全局策略 (global_policy)。

过程

步骤 1 创建用于识别流向环回接口 IP 地址的流量的访问列表。

access-list *name* **extended permit ip any host** *loopback_ip*

为每个环回接口 IP 地址创建 ACE。您还可以通过指定源 IP 地址而不是 **任何**来缩小此访问列表的范围。

示例：

```
ciscoasa(config)# access-list loop extended permit ip any host 10.1.1.1
ciscoasa(config)# access-list loop extended permit ip any host 10.2.1.1
```

步骤 2 创建可标识访问列表的类映射。

class-map 名称

match access-list *acl_name*

示例：

```
ciscoasa(config)# class-map rate-limit-loopback
ciscoasa(config-cmap)# match access-list loop
```

步骤 3 将最大连接数和最大初期连接数作为全局策略映射的一部分应用于类映射。

policy-map global_policy

class *class_map_name*

set connection conn-max *conns* **embryonic-conn-max** *conns*

将最大连接数设置为环回接口的预期连接数，并将初期 连接数设置为较低的数字。例如，您可以将其设置为 5/2、10/5 或 1024/512，具体取决于所需的预期环回接口会话。

设置初期连接限制触发 TCP 拦截，从而防止系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。

示例：

```
ciscoasa(config-cmap)# policy-map global_policy
ciscoasa(config-pmap)# class rate-limit-loopback
ciscoasa(config-pmap-c)# set connection conn-max 5 embryonic-conn-max 2
```

示例

以下示例将默认全局策略的最大连接数和初期连接数设为 10.1.1.1 和 10.2.1.1 处的两个环回接口。

```
ciscoasa(config)# interface loopback 1
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nameif loop1
ciscoasa(config-if)# interface loopback 2
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# nameif loop2
ciscoasa(config-if)# access-list loop extended permit ip any host 10.1.1.1
ciscoasa(config)# access-list loop extended permit ip any host 10.2.1.1
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match access-list loop
ciscoasa(config-cmap)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
ciscoasa(config-pmap-c)# set connection conn-max 10 embryonic-conn-max 5
```

监控环回接口

请参阅以下命令：

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

环回接口的历史记录

表 *27:* 环回接口的历史记录

功能名称	版本	功能信息
环回接口支持 DNS、HTTP、ICMP 和 IPsec 分流	9.20(1)	您现在可以添加环回接口并用于： • DNS • HTTP • ICMP • IPsec 流分流
VTI 的环回接口支持	9.19(1)	环回接口提供静态和动态 VTI VPN 隧道的冗余。现在，您可以将环回接口设置为 VTI 的源接口。VTI 接口可以从环回接口继承 IP 地址，而不是静态配置的 IP 地址。环回接口有助于克服路径故障。如果接口发生故障，您可以通过环回接口的 IP 地址来访问所有接口。 新增/修改的命令：**tunnel source interface**、**ip unnumbered**、**ipv6 unnumbered**

功能名称	版本	功能信息
支持环回接口	9.18(2)	您现在可以添加环回接口并用于： • BGP • AAA • SNMP • 系统日志 • SSH • Telnet 新增/修改的命令：**interface loopback**、**logging host**、**neighbor update-source**、**snmp-server host**、**ssh**、**telnet**

第 18 章

VLAN 子接口

本章说明如何配置 VLAN 子接口。

注释 在多情景模式下，请在系统执行空间中完成本节所述的所有任务。要从该情景更改到系统执行空间，请输入 **changeto system** 命令。

- 关于 VLAN 子接口，第 711 页
- VLAN 子接口的许可，第 711 页
- VLAN 子接口的准则和限制，第 712 页
- VLAN 子接口的默认设置，第 713 页
- 配置 VLAN 子接口和 802.1Q 中继，第 713 页
- 监控 VLAN 子接口，第 715 页
- VLAN 子接口示例，第 715 页
- VLAN 子接口的历史记录，第 716 页

关于 VLAN 子接口

通过 VLAN 子接口，您可以将物理接口或 EtherChannel 接口划分为标记有不同 VLAN ID 的多个逻辑接口。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 允许您在特定物理接口上将流量分开，所以您可以增加网络中可用的接口数量，而无需增加物理接口或 ASA。此功能对多情景模式尤其有用，使得可以向每个情景分配唯一的接口。

可以配置主 VLAN，以及一个或多个辅助 VLAN。当 ASA 接收到辅助 VLAN 上的流量时，它会将该流量映射到主 VLAN。

VLAN 子接口的许可

型号	许可证要求
Firepower 1010	基础 许可证：60

型号	许可证要求
Firepower 1120	基础 许可证：512
Firepower 1140 和 1150	基础 许可证：1024
Cisco Secure Firewall 1210、1220	基础 许可证：1024
Cisco Secure Firewall 3100	基础 许可证：1024
Firepower 4100	基础 许可证：1024
Cisco Secure Firewall 4200	基础 许可证：1024
Firepower 9300	基础 许可证：1024
ASA Virtual	吞吐量： 100 Mbps：25 1 Gbps：50 2 Gbps：200 10 Gbps：1024
ISA 3000	基础 许可证：5 增强型安全许可证：100

注释 对于根据 VLAN 限制计数的接口，您必须向其分配 VLAN。 例如：

```
interface gigabitethernet 0/0.100
  vlan 100
```

VLAN 子接口的准则和限制

型号支持

- Firepower 1010 和 Cisco Secure Firewall 1210/1220 - 交换机端口和 VLAN 接口不支持 VLAN 接口。
- 对于 ASA 型号，您无法在管理接口上配置子接口。请参阅 管理插槽/端口接口，第 660 页 了解子接口支持。

其他准则

- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常表明也不希望物理接口传递流量，因为物理接口会传递未标记的数据包。此属性的主用物理接口以及 EtherChannel 链路同样适用。由于必须启用物理 接口或 EtherChannel 接口才能使子接口传递流量，请通过不传递流量。如果要使物理接口或 EtherChannel 接口传递未标记的数据包，您可以照常配置**nameif** 命令。
- 同一父接口上的所有子接口必须为网桥组成员或路由接口；您无法混合搭配。
- ASA 不支持动态中继协议 (DTP)，因此您必须无条件地将连接的交换机端口配置到中继上。
- 您可能想要为 ASA 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。您可以自动生成唯一的MAC地址；请参阅自动分配 MAC 地址，第 792 页。

VLAN 子接口的默认设置

本节列出了接口的默认设置（如果没有出厂默认配置）。

接口的默认状态

接口的默认状态取决于类型和情景模式。

在多情景模式下，默认启用所有已分配的接口，而不考虑接口在系统执行空间中的状态。但是，要使流量通过该接口，还必须在系统执行空间中启用该接口。如果您在系统执行空间中关闭了一个接口，则该接口在所有共享它的情景中都会关闭。

在单模式下或在系统执行空间中，接口具有以下默认状态：

- 物理接口 - 已禁用。
- VLAN 子接口 - 已启用。但是，要使流量通过子接口，还必须启用物理接口。

配置 VLAN 子接口和 802.1Q 中继

向物理接口或 EtherChannel 接口添加 VLAN 子接口。

开始之前

对于多情景模式，请在系统执行空间中完成本程序。要从该情景更改到系统执行空间，请输入**changeto system** 命令。

过程

步骤 1 指定新的子接口：

interface {*physical_interface* | **port-channel** *number*}.*subinterface*

示例：

```
ciscoasa(config)# interface gigabitethernet 0/1.100
```

port-channel *number* 参数是 EtherChannel 接口 ID，例如 **port-channel 1**。

subinterface ID 是介于 1 和 4294967293 之间的整数。

步骤 2 指定子接口的 VLAN：

vlan *vlan_id* [**secondary** *vlan_range*]

示例：

```
ciscoasa(config-subif)# vlan 101 secondary 52 64,66-74
```

vlan_id 是介于 1 和 4094 之间的整数。某些 VLAN ID 可能是连接的交换机中的保留 VLAN ID，因此请查看交换机文档以了解详细信息。

可以使用空格、逗号和连字符（适用于连续范围）分隔辅助 VLAN。当 ASA 接收到辅助 VLAN 的流量时，它会将流量映射到主 VLAN。

不能将同一 VLAN 分配给多个子接口。您无法将 VLAN 分配给物理接口。每个子接口必须有一个 VLAN ID，然后才能传递流量。要更改 VLAN ID，您无需使用 **no** 选项删除旧 VLAN ID；您可以输入带有不同 VLAN ID 的 **vlan** 命令，ASA 会更改旧的 ID。要从列表中删除某些辅助 VLAN，可以使用 **no** 命令，并仅列出要删除的 VLAN。可以仅有选择地删除列出的 VLAN；例如，不能删除某一范围中的单个 VLAN。

示例

以下示例将一组辅助 VLAN 映射到 VLAN 200：

```
interface gigabitethernet 0/6.200
   vlan 200 secondary 500 503 600-700
```

以下 示例将从列表中删除辅助 VLAN 503：

```
no vlan 200 secondary 503
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
 vlan 200 secondary 500 600-700
```

```
no nameif
no security-level
no ip address
```

相关主题

VLAN 子接口的许可，第 711 页

监控 VLAN 子接口

请参阅以下命令：

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

- **show vlan mapping**

  显示接口以及接口映射到的辅助 VLAN 和主 VLAN。

VLAN 子接口示例

以下示例在单模式下配置子接口的参数：

```
interface gigabitethernet 0/1
  no nameif
  no security-level
  no ip address
  no shutdown
interface gigabitethernet 0/1.1
  vlan 101
  nameif inside
  security-level 100
  ip address 192.168.6.6 255.255.255.0
  no shutdown
```

以下示例显示 VLAN 映射如何与 Catalyst 6500 配合使用。请查看 Catalyst 6500 配置指南，了解如何将节点连接到 PVLANS。

ASA Configuration

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
  no shutdown
!
```

```
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

Catalyst 6500 Configuration

```
vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

VLAN 子接口的历史记录

表 *28: VLAN* 子接口的历史记录

功能名称	版本	功能信息
增加了 VLAN 数量	7.0(5)	提高了以下限制： • ASA5510 基础许可证的 VLAN 数量从 0 增加到 10。 • ASA5510 增强型安全许可证 VLAN 数量从 10 增加到 25。 • ASA5520 VLAN 数量从 25 增加到 100。 • ASA5540 VLAN 数量从 100 增加到 200。
增加了 VLAN 数量	7.2(2)	提高了以下型号的 VLAN 限制：ASA 5510（对于基础许可证，从 10 提高到 50；对于增强型安全许可证，从 25 提高到 100）、ASA 5520（从 100 提高到 150）、ASA 5550（从 200 提高到 250）。
增加了 ASA 5580 的 VLAN 数量	8.1(2)	在 ASA 5580 上支持的 VLAN 数量从 100 增加到 250。

功能名称	版本	功能信息
支持将辅助 VLAN 映射到主 VLAN	9.5(2)	现在您可以为一个子接口配置一个或多个辅助 VLAN。当 ASA 接收到辅助 VLAN 的流量时，它会将流量映射到主 VLAN。 引入或修改了以下命令：**vlan secondary**、**show vlan mapping**
为 ISA 3000 增加了 VLAN	9.13(1)	拥有增强型安全许可证的 ISA 3000 的最大 VLAN 数量从 25 增加到 100。

第 19 章

VXLAN 接口

本章介绍如何配置虚拟可扩展局域网 (VXLAN) 接口。VXLAN 作为第 3 层物理网络之上的第 2 层虚拟网络，可对第 2 层网络进行扩展。

- 关于 VXLAN 接口， 第 719 页
- VXLAN 接口的要求和前提条件， 第 728 页
- VXLAN 接口准则， 第 728 页
- VXLAN 接口默认设置， 第 729 页
- 配置 VXLAN 接口， 第 729 页
- 配置 Geneve 接口， 第 736 页
- 允许网关负载均衡器运行状况检查， 第 739 页
- 监控 VXLAN 接口， 第 740 页
- VXLAN 接口示例， 第 743 页
- VXLAN 接口的历史记录， 第 746 页

关于 VXLAN 接口

VXLAN 提供与 VLAN 相同的以太网第 2 层网络服务，但其可扩展性和灵活性更为出色。与 VLAN 相比，VXLAN 提供以下优势：

- 可在整个数据中心中灵活部署多租户网段。
- 更高的可扩展性可提供更多的第 2 层网段，最多可达 1600 万个 VXLAN 网段。

本节介绍 VXLAN 如何工作。有关 VXLAN 的详细信息，请参阅 RFC 7348。有关 Geneve 的详细信息，请参阅 RFC 8926。

封装

ASA 支持两种类型的 VXLAN 封装：

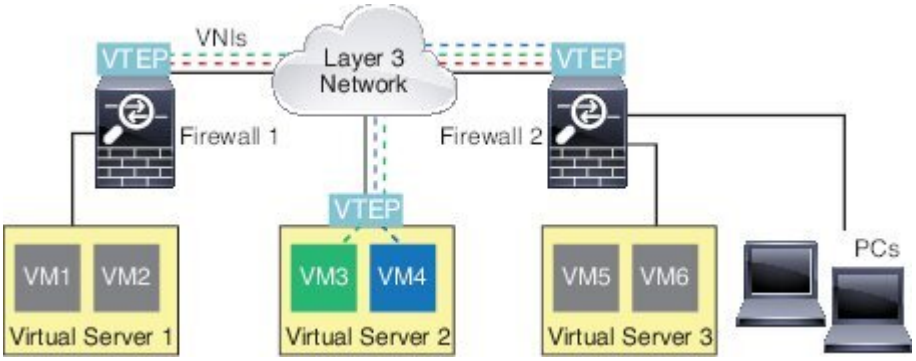
- VXLAN（所有型号）- VXLAN 使用 MAC Address-in-User 数据报协议 (MAC-in-UDP) 的封装方式。原始第 2 层帧已添加 VXLAN 报头，然后放入 UDP-IP 数据包中。

- Geneve（仅限 ASA virtual）- Geneve 具有不限于 MAC 地址的灵活内部报头。要在 Amazon Web 服务 (AWS) 网关负载均衡器和设备之间透明路由数据包，以及发送额外信息，则需要使用 Geneve 封装。

VXLAN 隧道端点

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口，您可以向其应用安全策略；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

下图显示第 3 层网络范围内用作 VTEP 的两个 ASA 和虚拟服务器 2，扩展了站点之间的 VNI 1、2 和 3 网络。ASA 可用作 VXLAN 与非 VXLAN 网络之间的网桥或网关。



VTEP 之间的底层 IP 网络与 VXLAN 重叠无关。封装的数据包根据外部 IP 地址报头路由，该报头具有初始 VTEP（用作源 IP 地址）和终止 VTEP（作为目标 IP 地址）。对于 VXLAN 封装：当远程 VTEP 未知时，目标 IP 地址可以是组播组。在使用 Geneve 时，ASA 仅支持静态对等体。默认情况下， VXLAN 的目标端口是 UDP 端口 4789（用户可配置）。Geneve 的目的端口是 6081。

VTEP 源接口

VTEP 源接口是一个计划要与所有 VNI 接口相关联的常规 ASA 接口（物理EtherChannel 接口，甚至 VLAN 接口）。每个 ASA/安全情景可以配置一个 VTEP 源接口。 由于只能配置一个 VTEP 源接口，因此不能在同一设备上同时配置 VXLAN 和 Geneve 接口。AWS或 Azure上的集群有一个例外，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，一个 Geneve (AWS) 或 VXLAN (Azure) 接口可用于 AWS 网关负载均衡器。

尽管并未将 VTEP 源接口限制为全部用于传输 VXLAN 流量，但是可以实现该用途。如果需要，可以使用该接口传输常规流量，并将一个安全策略应用于传输此类流量的该接口。但是，对于 VXLAN 流量，必须对 VNI 接口应用所有安全策略。VTEP 接口仅作为物理端口。

在透明防火墙模式下，VTEP 源接口不是 BVI 的一部分，并且类似于对待管理接口的方式，不为该源接口配置 IP 地址。

VNI 接口

VNI 接口类似于 VLAN 接口：它们是虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。将安全策略直接应用于每个 VNI 接口。

您智能添加一个 VTEP 接口，并且所有 VNI 接口都与同一 VTEP 接口相关联。 AWS 或 Azure上的 ASA Virtual 集群例外。对于 AWS 集群，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，一个 Geneve 接口可用于 AWS 网关负载均衡器。对于 Azure 集群，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，第二个 VXLAN 接口可用于 Azure 网关负载均衡器。

VXLAN 数据包处理

VXLAN

进出 VTEP 源接口的流量取决于 VXLAN 处理，特别是封装或解封。

封装处理包括以下任务：

- VTEP 源接口通过 VXLAN 报头封装内部 MAC 帧。
- UDP 校验和字段设置为零。
- 外部帧源 IP 设置为 VTEP 接口 IP。
- 外部帧目标 IP 通过远程 VTEP IP 查找确定。

解封；ASA 仅在以下条件下解封 VXLAN 数据包：

- VXLAN 数据包是目标端口设置为 4789（用户可配置该值）的 UDP 数据包。
- 入口接口是 VTEP 源接口。
- 入口接口 IP 地址与目标 IP 地址相同。
- VXLAN 数据包格式符合标准。

Geneve

进出 VTEP 源接口的流量取决于 Geneve 处理，特别是封装或解封。

封装处理包括以下任务：

- VTEP 源接口通过 Geneve 报头封装内部 MAC 帧。
- UDP 校验和字段设置为零。
- 外部帧源 IP 设置为 VTEP 接口 IP。
- 外部帧目标 IP 会被设置为您配置的对等体 IP 地址。

解封；ASA 仅在以下条件下解封 Geneve 数据包：

- VXLAN 数据包是目标端口设置为 6081（用户可配置该值）的 UDP 数据包。
- 入口接口是 VTEP 源接口。
- 入口接口 IP 地址与目标 IP 地址相同。
- Geneve 数据包格式符合标准。

对等体 VTEP

ASA 向对等体 VTEP 后的设备发送数据包时，ASA 需要两条重要信息：

- 远程设备的目标 MAC 地址
- 对等体 VTEP 的目标 IP 地址

ASA 维护目标 MAC 地址到 VNI 接口的远程 VTEP IP 地址的映射。

VXLAN 对等体

ASA 可以通过两种方式找到这些信息：

- 单个对等体 VTEP IP 地址可以在 ASA 上静态配置。

  无法手动定义多个对等体。

  对于 IPv4: 然后，ASA 设备将已封装 VXLAN 的 ARP 广播发送到 VTEP，以获取终端节点 MAC 地址。

  对于 IPv6：然后，ASA 将 IPv6 邻居请求消息发送到 IPv6 被请求节点的组播地址。对等体 VTEP 以具有其链路本地地址的 IPv6 邻居通告消息作为响应。

- 可以在每个 VNI 接口（或者总的来说，在 VTEP 上）配置组播组。

注释 Geneve 不支持此选项。

  对于 IPv4： ASA 将通过 VTEP 源接口在 IP 组播数据包内发送一个 VXLAN 封装的 ARP 广播数据包。对此 ARP 请求的响应使 ASA 可以获悉远程 VTEP IP 地址以及远程结束节点的目标 MAC 地址。

  对于 IPv6：ASA 通过 VTEP 源接口发送组播侦听程序发现 (MLD) 报告消息，以指示 ASA 正在 VTEP 接口上侦听组播地址流量。

Geneve 对等体

ASA virtual 仅支持静态定义的对等设备。您可以在 AWS 网关负载均衡器上定义 ASA virtual 对等体 IP 地址。由于 ASA virtual 绝不会向网关负载均衡器发起流量，因此您也不必在 ASA virtual 上指定网关负载均衡器 IP 地址；它会在收到 Geneve 流量时获知对等体 IP 地址。Geneve 不支持组播组。

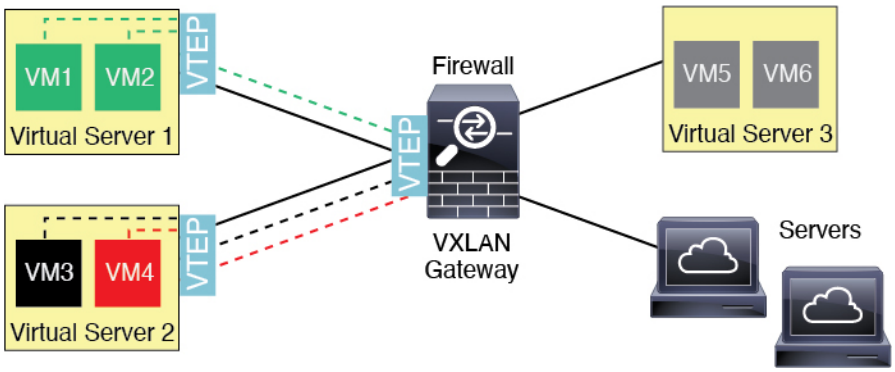
VXLAN 使用案例

本部分介绍在 ASA 上实施 VXLAN 的使用案例。

VXLAN 网桥或网关概述

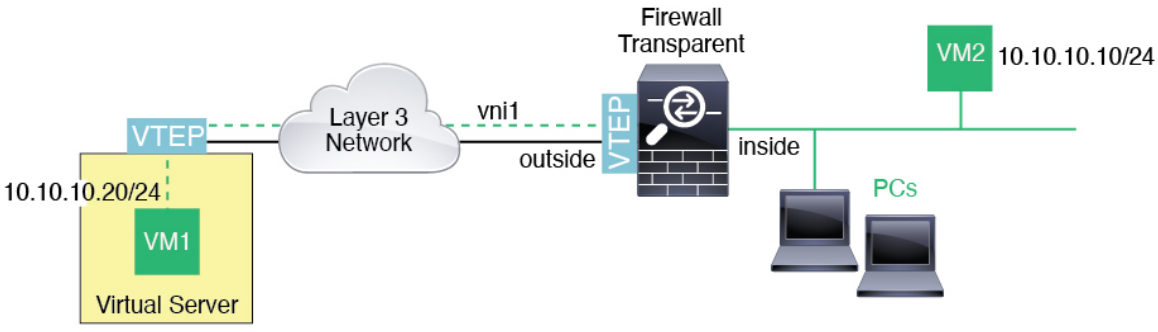
每个 ASA VTEP 都可作为终端节点（例如 VM、服务器和 PC）和 VXLAN 重叠网络之间的网桥或网关。对于通过 VTEP 源接口借助 VXLAN 封装接收的传入帧，ASA 去掉 VXLAN 报头，并基于内部以太网帧的目标 MAC 地址，将传入帧转发到连接非 VXLAN 网络的物理接口。

ASA 始终会处理 VXLAN 数据包；而不仅仅是在两个其他 VTEP 之间转发未处理的 VXLAN 数据包。



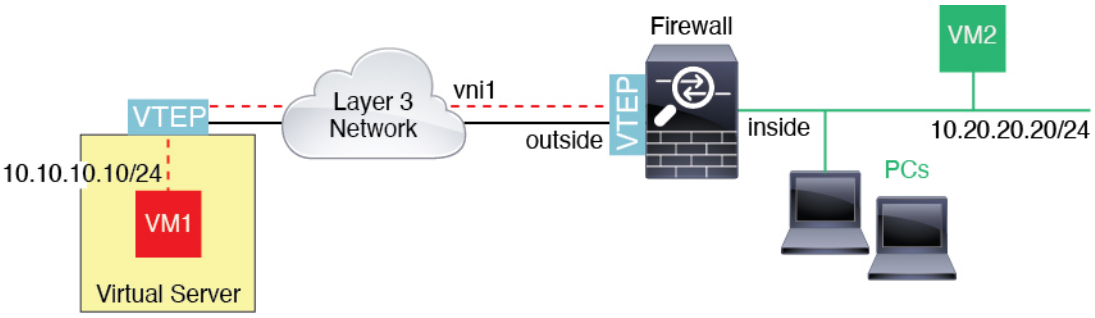
VXLAN 网桥

在使用网桥组（透明防火墙模式或可选的路由模式）时，ASA 可以用作 VXLAN 网段与本地网段之间的 VXLAN 网桥（远程），其中二者均位于同一网络中。在这种情况下，网桥组的一个成员是常规接口，而另一个成员是 VNI 接口。



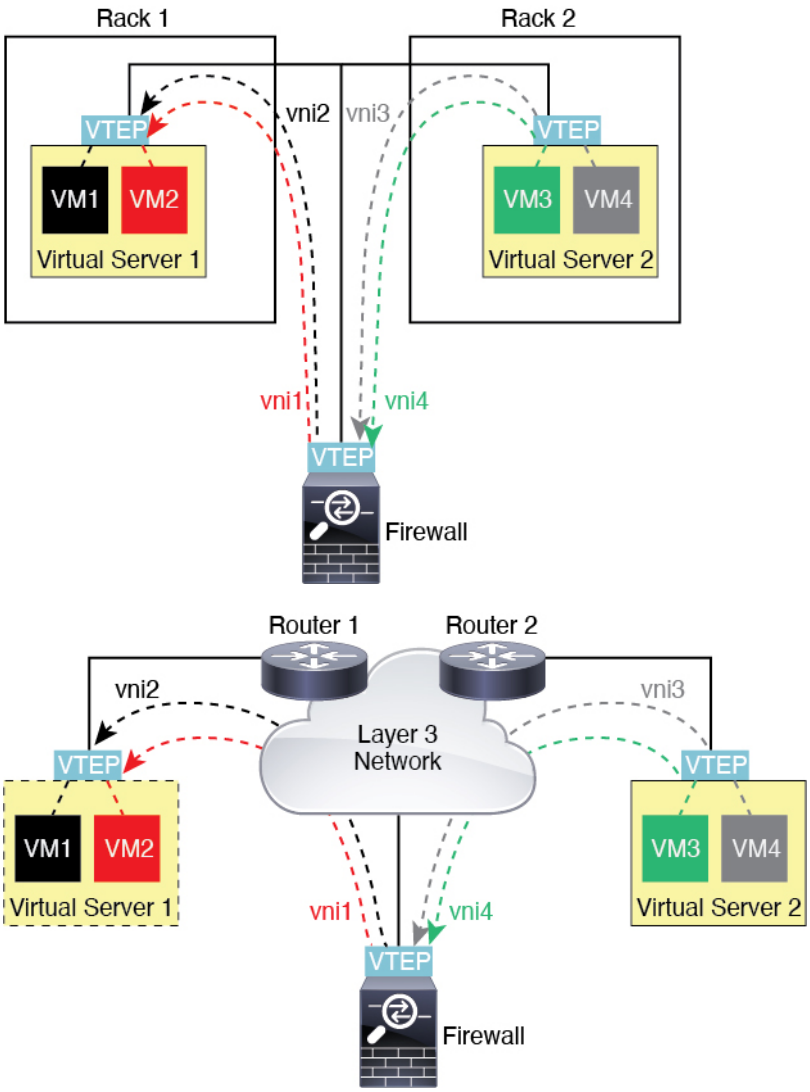
VXLAN 网关（路由模式）

ASA 可充当 VXLAN 和非 VXLAN 域之间的路由器，用于连接不同网络上的设备。



VXLAN 域之间的路由器

借助通过 VXLAN 扩展的第 2 层域，虚拟机可以指向一个 ASA 作为其网关，即使 ASA 位于不同机架中，甚至当 ASA 位于第 3 层网络上很远的位置也是如此。



请参阅有关此场景的以下注释：

1. 对于从 VM3 到 VM1 的数据包，目标 MAC 地址为 ASA MAC 地址，因为 ASA 是默认网关。
2. 虚拟服务器 2 上的 VTEP 源接口接收来自 VM3 的数据包，然后使用 VNI 3 的 VXLAN 标签封装数据包，并将数据包发送到 ASA。
3. 当 ASA 接收数据包时，会解封数据包以获得内部帧。
4. ASA 使用内部帧进行路由查找，然后发现目标位于 VNI 2 上。如果尚不具有 VM1 的映射，ASA 会在 VNI 2 上的组播组 IP 上发送封装的 ARP 广播。

注释 ASA 必须使用动态 VTEP 对等体发现，因为 ASA 在此场景下有多个 VTEP 对等体。

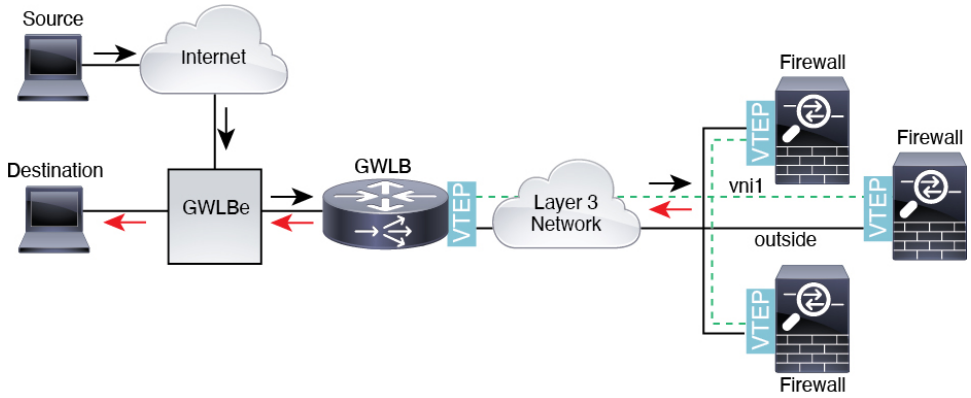
5. ASA 再次使用 VXLAN 标签为 VNI 2 封装数据包，并且将数据包发送到虚拟服务器 1。在封装之前，ASA 将内部帧目标 MAC 地址更改为 VM1 的 MAC 地址（ASA 可能需要组播封装的 ARP，以获取 VM1 MAC 地址）。
6. 当虚拟服务器 1 接收 VXLAN 数据包时，该虚拟服务器会解封数据包并向 VM1 提供内部帧。

AWS 网关负载均衡器和 Geneve 单臂代理

注释 这是 Geneve 接口当前唯一支持的使用案例。

AWS网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。ASA virtual支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示了从网关负载均衡器终端转发到网关负载均衡器的流量。网关负载均衡器会在多个流量之间进行均衡，这些流量在丢弃流量或将其发送回网关负载均衡器之前对其进行检查（掉头流量）。ASA virtual然后，网关负载均衡器会将流量发送回网关负载均衡器终端和目的地。

图 *68: Geneve* 单臂代理



AWS 网关负载均衡器和 Geneve 双臂代理

注释 这是 Geneve 接口当前唯一支持的使用案例。

ASA virtual 在单臂和双臂模式下，支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示直接转发到目标（互联网）的出站流量（由ASA virtual检查的流量），无需流量跃点到 GWLB 和 GWLB 终端。 ASA virtual 检查出站流量并对流量执行 NAT，然后丢弃流量或通过 NAT 网关将流量发送回互联网。双臂代理为多 VPC 部署提供通用出口路径。防火墙检查来自多个VPC的出站流量，并从单点退出到互联网，使其成为具有成本效益的基础设施解决方案。

图 *69: Geneve* 双臂代理 - 来自单 *VPC* 的出口流量

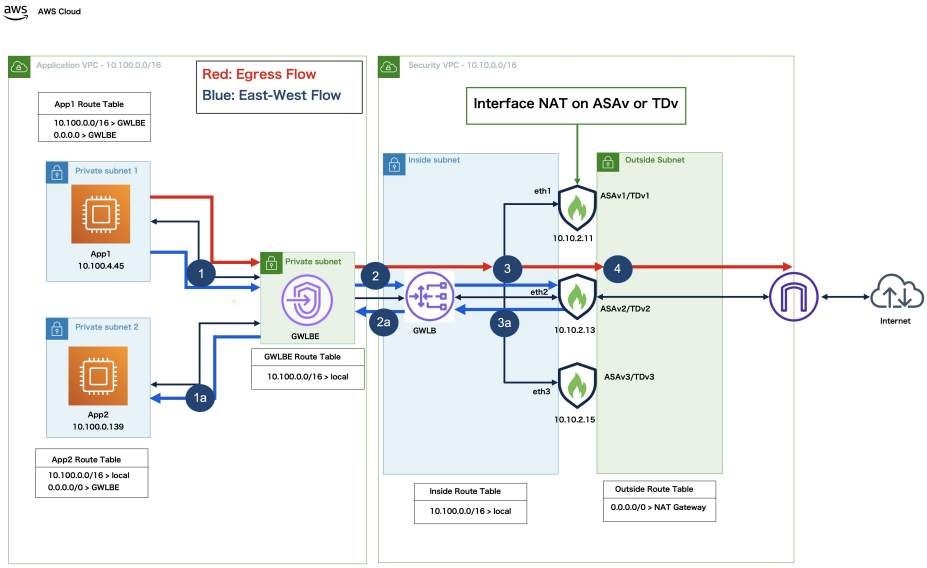
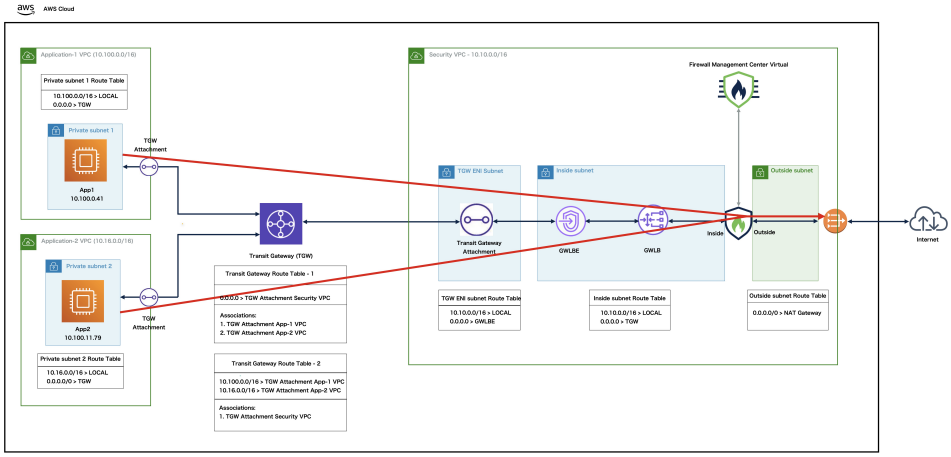


图 *70: Geneve* 双臂代理 - 来自多个 *VPC* 的出口流量

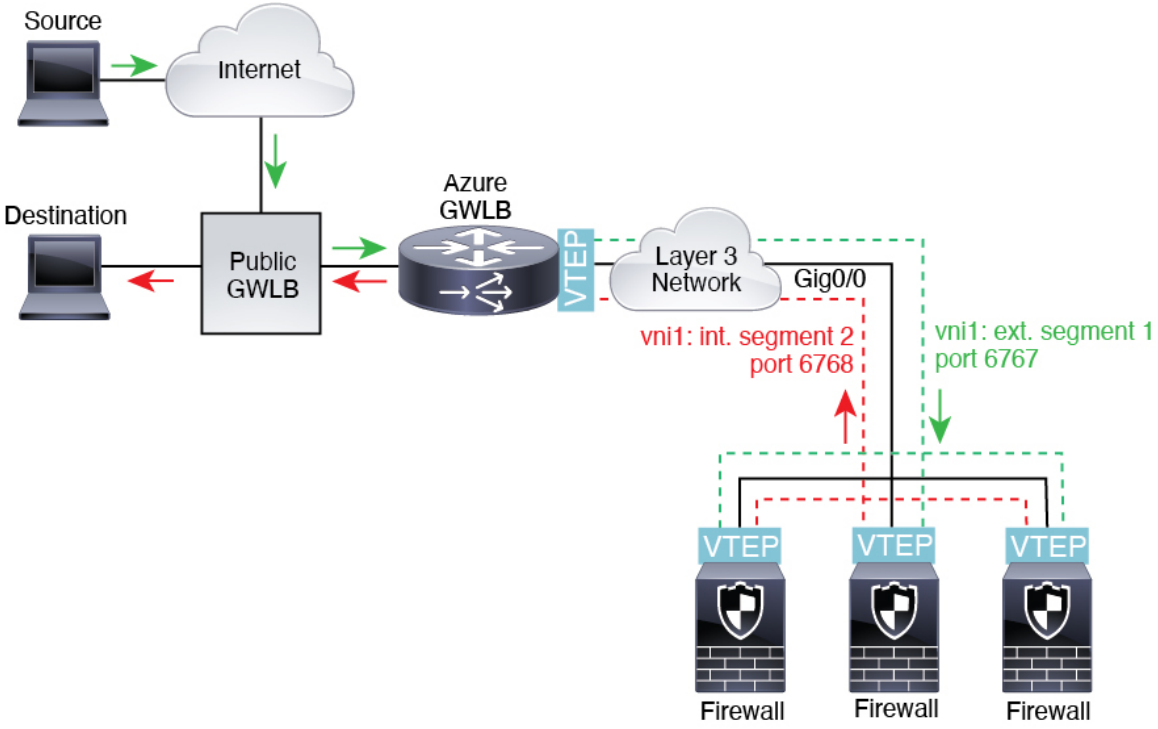


Azure 网关负载均衡器和配对代理

在 Azure 服务链中， ASA virtual充当可以拦截互联网和客户服务之间的数据包的透明网关。 ASA virtual 通过已配对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

下图显示了从外部 VXLAN 网段上的公共网关负载均衡器转发到 Azure 门户负载均衡器的流量。网关负载均衡器会在多个 ASA virtual流量之间进行均衡 ， 这些流量在丢弃流量或将其发送回在内部 VXLAN 部分的网关负载均衡器之前对其进行检查。然后，Azure 网关负载均衡器会将流量发送回公共网关负载均衡器和目的地。

图 *71: Azure* 网关负载均衡器和配对代理



VXLAN 接口的要求和前提条件

型号要求

- 不支持将 Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口和 VLAN 接口用作 VTEP 接口。
- 以下型号支持 Geneve 封装：Amazon Web Services (AWS) 上的 ASAv30、ASAv50、ASAv100
- 以下型号支持配对代理模式下的 VXLAN：
  - Azure 中的 ASA Virtual

VXLAN 接口准则

防火墙模式

- Geneve 接口仅在路由防火墙模式下支持。
- 配对代理 VXLAN 接口仅在路由防火墙模式下支持。

IPv6

- VNI 接口支持 IPv4 和 IPv6 流量。
- 对于 VXLAN 封装，VTEP 源接口同时支持 IPv4 和 IPv6。 ASA virtual 集群控制链路 VTEP 源接口仅支持 IPv4。

  对于 Geneve，VTEP 源接口仅支持 IPv4。

集群和多情景模式

- 集群在单个接口模式 下不支持 VXLAN，但集群控制链路除外（仅限ASA virtual ）。仅跨区以太网通道模式支持 VXLAN。

  AWS 上的 ASA virtual例外，它可以使用额外的 Geneve 接口与 GWLB 配合使用，而 Azure 可以使用额外的成对代理 VXLAN 接口与 GWLB配合使用。
- Geneve 接口仅在独立的单情景模式下受支持。 多情景模式不支持它们。

路由

- VNI 接口上仅支持静态路由或基于策略的路由；动态路由协议不受支持。

MTU

- VXLAN 封装-如果源接口 MTU 少于 1554 个字节 (IPv4) 或 1574 个字节 (IPv6)，则 ASA 会自动将 MTU 提高到 1554 个字节或 1574 字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。如果其他设备使用的 MTU 更大，则您应 为 IPv4 将源接口 MTU 设置为网络 MTU + 54 个字节，或者为 IPv6 设置为 +64 个字节。此 MTU 需要您在一些型号上启用巨帧预留；请参阅 启用巨帧支持（ASA Virtual、ISA 3000），第 665 页。
- Geneve 封装- 如果源接口 MTU 少于 1806 个字节，ASA 会自动将 MTU 提高到 1806 个字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的MTU。如果其他设备使用的 MTU 更大，您应将源接口 MTU 设置为网络 MTU + 306 个字节。此 MTU 需要您在一些型号上启用巨帧预留；请参阅 启用巨帧支持（ASA Virtual、ISA 3000），第 665 页。

VXLAN 接口默认设置

默认启用 VNI 接口。

配置 VXLAN 接口

要配置 VXLAN，请执行下列步骤：

注释 您可以配置 VXLAN 或 Geneve（仅限 ASA virtual）。有关 Geneve 接口，请参阅配置 Geneve 接口，第 736 页。

过程

步骤 1 配置 VTEP 源接口，第 730 页。

步骤 2 配置 VNI 接口，第 732 页

步骤 3 （可选）更改 VXLAN UDP 端口，第 735 页。

步骤 4 (Azure GWLB) 允许网关负载均衡器运行状况检查，第 739 页。

配置 VTEP 源接口

每个 ASA 或安全情景可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)。在 Azure 中，ASA virtual 上的集群是个例外，您可以使用一个 VTEP 源接口作为集群控制链路，将另一个 VTEP 源接口用于连接到 Azure GWLB 的数据接口。

开始之前

对于多情景模式，请在情景执行空间完成本节所述的任务。输入 **changeto context** *name* 命令以更改为要配置的情景。

过程

步骤 1 （透明模式）将源接口指定为仅 NVE：

interface *id*

nve-only

示例：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

可以通过此设置配置接口的 IP 地址。在路由模式下，此设置限制此接口上仅允许流向 VXLAN 的流量和常见的管理流量，这种情下此命令是可选的。

步骤 2 配置源接口名称和 IPv4 和/或 IPv6 地址。

ASA virtual 集群控制链路不支持 IPv6。

示例：

（路由模式）

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64
```

示例：

（透明模式）

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64
```

步骤 3 指定 NVE 实例：

nve 1

只能指定一个 NVE 实例，其中 ID 为 1。

示例：

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)#
```

步骤 4 指定 VXLAN 封装。

encapsulation vxlan

示例：

```
ciscoasa(cfg-nve)# encapsulation vxlan
```

步骤 5 指定您在第 2 步配置的源接口名称：

source-interface *interface-name*

示例：

```
ciscoasa(cfg-nve)# source-interface outside
```

注释
如果 VTEP 接口 MTU 少于 1554 个字节 (IPv4) 或 1574 个字节 (IPv6)，则 ASA 会自动将 MTU 提高到 1554 个字节 或 1574 字节。

步骤 6 （多情景模式；对于单情景模式为可选）手动指定对等体 VTEP IP 地址：

peer ip *ip_address*

示例：

IPv4 对等体

```
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

示例：

IPv6 对等体：

```
ciscoasa(cfg-nve)# peer ip 2001:0DB8:BA98::1234
```

如果指定对等体 IP 地址，则无法使用组播组发现。在多情景模式中不支持组播，因此只能选择手动配置。只能为 VTEP 指定一个对等体。

步骤 7 （可选；仅限单情景模式）为所有关联的 VNI 接口指定默认组播组：

default-mcast-group *mcast_ip*

示例：

IPv4 组

```
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

示例：

IPv6 组

```
ciscoasa(cfg-nve)# default-mcast-group ff0e::100
```

如果每个 VNI 接口未配置组播组，则使用该组。如果配置一个 VNI 接口级别的组，则该组将覆盖此设置。

配置 VNI 接口

添加 VNI 接口，将其与 VTEP 源接口相关联，并配置基本的接口参数。

对于 Azure 中的 ASA Virtual，您可以配置常规 VXLAN 接口，也可以配置配对代理模式 VXLAN 接口，以便与 Azure GWLB 配合使用。配对代理模式是唯一支持的集群模式。

过程

步骤 1 创建 VNI 接口：

interface vni *vni_num*

示例：

```
ciscoasa(config)# interface vni 1
```

将 ID 设置为 1 和 10000 之间的整数。此 ID 仅为内部接口标识符。

步骤 2 (Regular VXLAN) 指定 VXLAN 网段 ID：

segment-id *id*

示例：

```
ciscoasa(config-if)# segment-id 1000
```

将 ID 设置为 1 和 16777215 之间的整数。网段 ID 用于 VXLAN 标记。

步骤 3 （Azure GWLB 的已配对代理 VXLAN）启用代理配对模式并设置所需的参数。

a) 启用代理配对模式。

proxy paired

示例：

```
ciscoasa(config-if)# proxy paired
```

b) 设置内部端口。

internal-port *port_number*

其中 *port_number* 介于 1024 和 65535 之间。

示例：

```
ciscoasa(config-if)# internal-port 2000
```

c) 设置内部网段 ID。

internal-segment-id *id_number*

其中 *id_number* 介于 1 和 16777215 之间。

示例：

```
ciscoasa(config-if)# internal-segment-id 101
```

d) 设置外部端口。

external-port *port_number*

其中 *port_number* 介于 1024 和 65535 之间。

示例：

```
ciscoasa(config-if)# external-port 2001
```

e) 设置外部网段 ID。

external-segment-id *id_number*

其中 *id_number* 介于 1 和 16777215 之间。

示例：

```
ciscoasa(config-if)# external-segment-id 102
```

f) 允许流量进出同一接口。

same-security-traffic permit intra-interface

示例：

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

步骤 4 （透明模式下需要）指定要将此接口关联至的网桥组：

bridge-group 编号

示例：

```
ciscoasa(config-if)# bridge-group 1
```

请参阅 配置网桥组接口，第 757 页 配置 BVI 接口并将普通接口关联至此 网桥组。

步骤 5 将此接口与 VTEP 源接口相关联：

vtep-nve 1

步骤 6 为接口命名：

nameif *vni_interface_name*

示例：

```
ciscoasa(config-if)# nameif vxlan1000
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 7 （路由模式）分配 IPv4 和/或 IPv6 地址：

ip address {*ip_address* [*mask*] [**standby** *ip_address*] | **dhcp** [**setroute**] | **pppoe** [**setroute**]}

{| ipv6-address / prefix-length [ipv6-address]} **ipv6 addressautoconfigstandby**

示例：

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

步骤 8 设置安全级别：

security-level 级别

示例：

```
ciscoasa(config-if)# security-level 50
```

其中 *number* 为 0（最低）到 100（最高）之间的整数。

步骤 9 （单情景模式）设置组播组地址：

mcast-group *multicast_ip*

示例：

IPv4 组：

```
ciscoasa(config-if)# mcast-group 236.0.0.100
```

示例：

IPv6 组：

```
ciscoasa(config-if)# mcast-group ff0e::101
```

如果没有为 VNI 接口设置组播组，请使用源自 VTEP 源接口配置的默认组（如果有）。如果手动设置 VTEP 源接口的 VTEP 对等体 IP，则无法为 VNI 接口指定组播组。多情景模式下不支持组播。

（可选）更改 VXLAN UDP 端口

默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。如果网络使用非标准端口，可以对其进行更改。

开始之前

对于多情景模式，请在系统执行空间中完成此任务。要从该情景切换到系统执行空间，请输入**changeto system** 命令。

过程

设置 VXLAN UDP 端口：

vxlan 端口号

示例：

```
ciscoasa(config)# vxlan port 5678
```

配置 Geneve 接口

要为 ASA virtual 配置 Geneve 接口，请执行以下步骤：

注释 您可以配置 VXLAN 或 Geneve。有关 VXLAN 接口的信息，请参阅配置 VXLAN 接口，第 729 页。

过程

步骤 1 为 Geneve 配置 VTEP 源接口，第 736 页。

步骤 2 为 Geneve 配置 VNI 接口，第 737 页

步骤 3 允许网关负载均衡器运行状况检查，第 739 页。

为 Geneve 配置 VTEP 源接口

每个 ASA virtual 设备可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)。

过程

步骤 1 （可选）将源接口指定为仅限 NVE。

interface *id*

nve-only

示例：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

此设置限制此接口上仅允许流向 VXLAN 的流量和常见的管理流量，这种情下此设置是可选的。

步骤 2 配置源接口名称和 IPv4 地址。

示例：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
```

```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

步骤 3 指定 NVE 实例：

nve 1

只能指定一个 NVE 实例，其中 ID 为 1。

示例：

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)#
```

步骤 4 指定 Geneve 封装。

encapsulation geneve

请勿更改 Geneve 端口；AWS 需要使用端口 6081。

示例：

```
ciscoasa(cfg-nve)# encapsulation geneve
```

步骤 5 指定您在第 2 步配置的源接口名称：

source-interface *interface-name*

示例：

```
ciscoasa(cfg-nve)# source-interface outside
```

注释
如果源接口 MTU 少于 1806 个字节，ASA 会自动将 MTU 提高到 1806 个字节。

为 Geneve 配置 VNI 接口

添加 VNI 接口，将其与 VTEP 源接口相关联，并配置基本的接口参数。

过程

步骤 1 创建 VNI 接口：

interface vni *vni_num*

示例：

```
ciscoasa(config)# interface vni 1
```

将 ID 设置为 1 和 10000 之间的整数。此 ID 仅为内部接口标识符。

步骤 2 将此接口与 VTEP 源接口相关联：

vtep-nve 1

步骤 3 为接口命名：

nameif *vni_interface_name*

示例：

```
ciscoasa(config-if)# nameif geneve1000
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 4 分配 IPv4 和/或 IPv6 地址：

ip address {*ip_address* [*mask*] [**standby** *ip_address*]}

{| ipv6-address / prefix-length [ipv6-address]} **ipv6 addressautoconfigstandby**

Geneve 仅支持静态 IP 地址。

示例：

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

步骤 5 设置安全级别：

security-level 级别

级别 为 0（最低）到 100（最高）之间的整数。

示例：

```
ciscoasa(config-if)# security-level 50
```

步骤 6 启用单臂代理或双臂代理。

proxy single-arm

示例：

```
ciscoasa(config-if)# proxy single-arm
```

proxy dual-arm

示例：

```
ciscoasa(config-if)# proxy single-arm | dual-arm
```

其中，

`Proxy` 是指定 VNI 接口将运行的模式的关键字。

`single-arm` 或 `dual-arm` 是用于指定 AWS 单臂或双臂部署模式的关键字。

步骤 7 允许流量进出同一接口。

same-security-traffic permit intra-interface

示例：

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

允许网关负载均衡器运行状况检查

AWS 或 Azure 网关负载均衡器要求设备对运行状况检查进行正确应答。AWS 网关负载均衡器只会将流量发送到被视为正常的设备。

您必须将 ASA virtual 配置为响应 SSH、Telent、HTTP 或 HTTPS 运行状况检查。

SSH 连接

对于 SSH，允许来自网关负载均衡器的 SSH。网关负载均衡器将尝试与 ASA virtual 建立连接，而 ASA virtual 的登录提示将被视为运行状况的证明。

注释 SSH 登录尝试会在 1 分钟后超时。为了适应此超时，您需要在网关负载均衡器上配置更长的运行状况检查间隔。

示例

```
! Allow SSH connections from GWLB network: 10.0.1.0/24
ssh 10.0.1.0 255.255.255.0 outside
```

Telnet 连接

对于 Telnet，允许来自网关负载均衡器的 Telnet。网关负载均衡器将尝试与 ASA virtual 建立连接，而 ASA virtual 的登录提示将被视为运行状况的证明。

注释 您无法通过 Telnet 连接到最低安全级别的接口，因此此方法可能不实用。

示例

```
! Allow Telnet connections from GWLB network: 10.0.1.0/24
telnet 10.0.1.0 255.255.255.0 outside
```

HTTP(S) 直通代理

您可以将 ASA 配置为提示网关负载均衡器进行 HTTP(S) 登录。

示例

```
! Identify health probe HTTP traffic from GWLB nw 10.0.1.0/24 to ASAv interface 10.2.2.2
access-list gwlb extended permit tcp 10.0.1.0 255.255.255.0 host 10.2.2.2 eq www
! Enable HTTP authentication
aaa authentication http console LOCAL
! Require authentication for the health probe traffic
aaa authentication match gwlb outside LOCAL
! Use an HTTP login page on the ASA
aaa authentication listener http outside port www
```

使用支持端口转换的静态接口 NAT 的 HTTP(S) 重定向。

您可以将 ASA virtual 配置为将运行状况检查重定向到元数据 HTTP(S) 服务器。对于 HTTP(S) 运行状况检查，HTTP(S) 服务器必须使用 200 到 399 范围内的状态代码来回复网关负载均衡器。由于 ASA virtual 对同时管理连接的数量存在限制，因此您可以选择将运行状况检查分流到外部服务器。

支持端口转换的静态接口 NAT 允许您将某个端口（例如端口 80）的连接重定向到其他 IP 地址。例如，将来自网关负载均衡器的 HTTP 数据包转换为 ASA virtual 外部接口的目标，使其看起来像是来自目标为 HTTP 服务器的 ASA virtual 外部接口。ASA virtual 随后会将数据包转发到映射的目标地址。HTTP 服务器会响应 ASA virtual 外部接口，然后 ASA virtual 会将响应转发回网关负载均衡器。您需要允许从网关负载均衡器到 HTTP 服务器的流量的访问规则。

示例

```
! Permit HTTP traffic from GWLB nw 10.0.1.0/24 to HTTP server 10.2.2.3
access-list gwlb-health extended permit tcp 10.0.1.0 255.255.255.0 host 10.2.2.3 eq www
access-group gwlb-health in interface outside

! Create network objects
object network gwlb-subnet
 subnet 10.0.1.0 255.255.255.0
object-group network gwlb
    network-object object gwlb-subnet
object-group network http-server
    network-object host 10.2.2.3
object service http80
    service tcp destination eq www

! For HTTP, translate src GWLB IP to outside IP; translate dest of outside IP to HTTP Server
 IP
nat (outside,outside) source static gwlb interface destination static interface http-server
 service http80 http80
```

监控 VXLAN 接口

参阅以下命令，以监控 VTEP 和 VNI 接口。

- **show nve** [*id*] [**summary**]

此命令显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。使用 **summary** 选项，此命令仅显示 NVE 接口的状态、NVE 接口后 VNI 的数量，以及所发现的 VTEP 数量。

请参阅以下所示的 **show nve 1** 命令输出：

```
ciscoasa# show nve 1
ciscoasa(config-if)# show nve
nve 1, source-interface "inside" is up
IP address 15.1.2.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
6701004 packets input, 3196266002 bytes
6700897 packets output, 3437418084 bytes
1 packets dropped
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 15.1.2.3
Number of VNIs attached to nve 1: 2
VNIs attached:
vni 2: segment-id 5002, mcast-group 239.1.2.3
vni 1: segment-id 5001, mcast-group 239.1.2.3
```

请参阅以下所示的 **show nve 1 summary** 命令输出：

```
ciscoasa# show nve 1 summary
nve 1, source-interface "inside" is up
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Default multicast group: 239.1.2.3
Number of VNIs attached to nve 1: 2
```

- **show interface vni** *id* [**summary**]

  此命令显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。**summary** 选项仅显示 VNI 接口参数。

  请参阅以下所示的 **show interface vni 1** 命令输出：

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
235 packets input, 23606 bytes
524 packets output, 32364 bytes
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 bytes/sec
1 minute drop rate, 0 pkts/sec
```

```
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
```

请参阅以下所示的 **show interface vni 1 summary** 命令输出：

```
ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured
```

- **show vni vlan-mapping**

  此命令显示 VNI 网段 ID 和 VLAN 接口或物理接口之间的映射。此命令仅在透明防火墙模式下有效，因为在路由模式下，VXLAN 和 VLAN 之间的映射可能会显示过多的值。

  请参阅以下所示的 **show vni vlan-mapping** 命令输出：

```
ciscoasa# show vni vlan-mapping
vni1: segment-id: 6000, interface: 'g0110', vlan 10, interface: 'g0111', vlan 11
vni2: segment_id: 5000, interface: 'g01100', vlan 1, interface: 'g111', vlan 3, interface:
 'g112', vlan 4
```

- **show arp vtep-mapping**

  此命令可显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。

  请参阅以下所示的 **show arp vtep-mapping** 命令输出：

```
ciscoasa# show arp vtep-mapping
vni-outside 192.168.1.4 0012.0100.0003 577 15.1.2.3
vni-inside 192.168.0.4 0014.0100.0003 577 15.1.2.3
```

- **show mac-address-table vtep-mapping**

  此命令将使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。

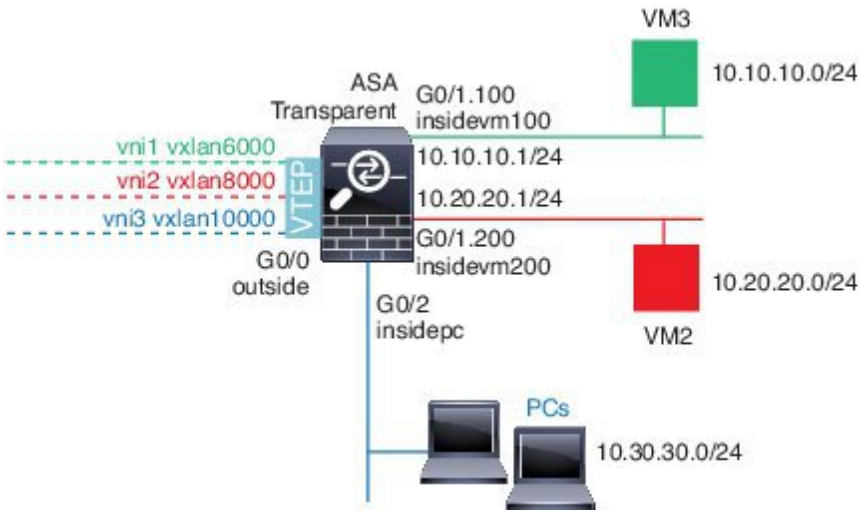
  请参阅以下所示的 **show mac-address-table vtep-mapping** 命令输出：

```
ciscoasa# show mac-address-table vtep-mapping
interface                  mac  address       type     Age(min)   bridge-group    VTEP
-------------------------------------------------------------------------------------------
vni-outside               00ff.9200.0000      dynamic      5         1        10.9.1.3
vni-inside                 0041.9f00.0000      dynamic      5         1      10.9.1.3
```

VXLAN 接口示例

请参阅以下所示的 VXLAN 配置示例。

透明 VXLAN 网关示例



请参见以下有关此示例的说明：

- GigabitEthernet 0/0 上的外部接口用作 VTEP 源接口，并且连接到第 3 层网络。
- GigabitEthernet 0/1.100 上的 insidevm100 VLAN 子接口连接到 VM3 所在的 10.10.10.0/24 网络。当 VM3 与 VM1（未显示；两者均有 10.10.10.0/24 IP 地址）通信时，ASA 使用 VXLAN 标签 6000。
- GigabitEthernet 0/1.200 上的 insidevm200 VLAN 子接口连接到 VM2 所在的 10.20.20.0/24 网络。当 VM2 与 VM4（未显示；两者均有 10.20.20.0/24 IP 地址）通信时，ASA 使用 VXLAN 标签 8000。
- GigabitEthernet 0/2 上的 insidepc 接口连接到若干 PC 所在的 10.30.30.0/24 网络。当这些 PC 与属于同一网络（全部具有 10.30.30.0/24 IP 地址）的远程 VTEP 后面的 VM/PC（未显示）进行通信时，ASA 使用 VXLAN 标签 10000。

ASA 配置

```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
```

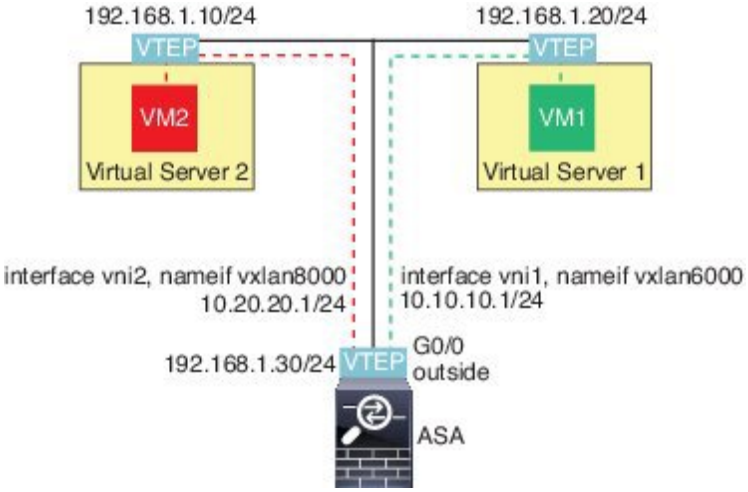
```
nve 1
  encapsulation vxlan
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  vtep-nve 1
  mcast-group 235.0.0.100
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  bridge-group 2
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface vni3
  segment-id 10000
  nameif vxlan10000
  security-level 0
  bridge-group 3
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface gigabitethernet0/1.100
  nameif insidevm100
  security-level 100
  bridge-group 1
!
interface gigabitethernet0/1.200
  nameif insidevm200
  security-level 100
  bridge-group 2
!
interface gigabitethernet0/2
  nameif insidepc
  security-level 100
  bridge-group 3
!
interface bvi 1
  ip address 10.10.10.1 255.255.255.0
!
interface bvi 2
  ip address 10.20.20.1 255.255.255.0
!
interface bvi 3
  ip address 10.30.30.1 255.255.255.0
```

备注

- 对于 VNI 接口 vni1 和 vni2，在封装过程中将删除内部 VLAN 标签。
- VNI 接口 vni2 和 vni3 通过组播共享封装的 ARP 的同一组播 IP 地址。系统允许此共享。
- ASA 基于以上 BVI 和网桥组配置，将 VXLAN 流量桥接到非 VXLAN 支持的接口。对于每个扩展的第 2 层网段（10.10.10.0/24、10.20.20.0/24 和 10.30.30.0/24），ASA 充当网桥。

- 在网桥组中允许有多个 VNI 或多个常规接口（VLAN 或仅物理接口）。VXLAN 网段 ID 与 VLAN ID（或物理接口）之间的转发或关联，由目标 MAC 地址和连接到目标的接口决定。
- VTEP 源接口是透明防火墙模式下，由接口配置中的 **nve-only** 所指示的第 3 层接口。VTEP 源接口不是 BVI 接口或管理接口，但是具有 IP 地址，并且使用路由表。

VXLAN 路由示例



请参见以下有关此示例的说明：

- VM1 (10.10.10.10) 通过虚拟服务器 1 进行托管，VM2 (10.20.20.20) 通过虚拟服务器 2 进行托管。
- VM1 的默认网关是 ASA，它不与虚拟服务器 1 位于同一个 pod 上，但 VM1 对此并不知晓。VM1 只知道其默认网关 IP 地址为 10.10.10.1。同样，VM2 只知道其默认网关 IP 地址为 10.20.20.1。
- 虚拟服务器 1 和 2 上的支持 VTEP 的虚拟机监控程序可以通过相同的子网或第 3 层网络（未显示；不管是哪种情况，ASA 和虚拟服务器的上行链路都具有不同的网络地址）与 ASA 进行通信。
- VM1 的数据包将通过其虚拟机监控程序的 VTEP 进行封装，并通过 VXLAN 隧道发送到其默认网关。
- 当 VM1 将数据包发送到 VM2 时，对数据包而言，它将通过默认网关 10.10.10.1 进行发送。虚拟服务器 1 知道 10.10.10.1 不是本地地址，因此 VTEP 会通过 VXLAN 封装数据包，并将其发送至 ASA 的 VTEP。
- 在 ASA 上，对数据包进行解封。在解封过程中可获取 VXLAN 网段 ID。然后，ASA 会基于 VXLAN 网段 ID 将内部帧重新注入到对应的 VNI 接口 (vni1)。ASA 然后会执行路由查找，并通过 VNI 接口 vni2 发送内部数据包所有通过 vni2 的传出数据包都使用 VXLAN 网段 8000 进行封装，并通过 VTEP 发送到外部。
- 最终，虚拟服务器 2 的 VTEP 接收封装的数据包、解封数据包，并将数据包转发到 VM2。

ASA 配置

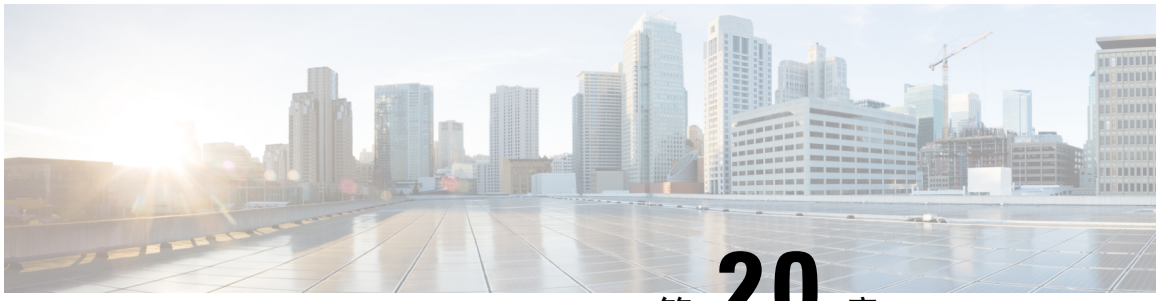
```
interface gigabitethernet0/0
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
  default-mcast-group 235.0.0.100
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  vtep-nve 1
  ip address 10.20.20.1 255.255.255.0
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  vtep-nve 1
  ip address 10.10.10.1 255.255.255.0
!
```

VXLAN 接口的历史记录

表 *29: VXLAN* 接口的历史记录

功能名称	版本	功能信息
VXLAN VTEP IPv6 支持	9.20(1)	现在，您可以为 VXLAN VTEP 接口指定 IPv6 地址。 ASA virtual 集群控制链路或 Geneve 封装不支持 IPv6。 新增/修改的命令：**default-mcast-group**、**mcast-group**、**peer ip**
ASA Virtual 用于 Azure 网关负载均衡器的已配对代理 VXLAN	9.19(1)	您可以在 Azure 中为 ASA Virtual 配置配对代理模式 VXLAN 接口，以便与 Azure 网关负载均衡器 (GWLB) 配合使用。ASA Virtual 通过利用成对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。 新增/修改的命令： **external-port**、**external-segment-id**、**internal-port**、**internal-segment-id**、**proxy paired**
AWS 网关负载均衡器对 AWS 上 ASA virtual 的 Geneve 支持	9.17(1)	添加了 Geneve 封装支持，以支持 ASAv30、ASAv50 和 ASAv100 网关负载均衡器的单臂代理。 新增/修改的命令： 调试 **geneve**、 调试 **nve**、 调试 **vxlan**、 封装、 数据包跟踪器 **geneve**、 代理单臂、 显示 **asp drop**、 显示捕获、 显示接口、 显示 **nve**、

功能名称	版本	功能信息
VXLAN 支持	9.4(1)	增加了 VXLAN 支持，包括 VXLAN 隧道终端 (VTEP) 支持。每个 ASA 或安全情景可以定义一个 VTEP 源接口。 引入了以下命令：**debug vxlan**、**default-mcast-group**、**encapsulation vxlan**、**inspect vxlan**、**interface vni**、**mcast-group**、**nve**、**nve-only**、**peer ip**、**segment-id**、**show arp vtep-mapping**、**show interface vni**、**show mac-address-table vtep-mapping**、**show nve**、**show vni vlan-mapping**、**source-interface**、**vtep-nve**、**vxlan port**



第 20 章

路由模式接口和透明模式接口

本章介绍在路由或透明防火墙模式下为所有型号完成接口配置的相关任务。

注释 对于多情景模式，请在情景执行空间完成本节所述的任务。输入 **changeto context** *name* 命令以更改为要配置的情景。

- 关于路由和透明模式接口，第 749 页
- 路由和透明模式接口准则和限制，第 751 页
- 配置路由模式接口，第 753 页
- 配置网桥组接口，第 757 页
- 配置 IPv6 寻址，第 763 页
- 监控路由模式和透明模式接口，第 774 页
- 路由和透明模式接口示例，第 780 页
- 路由模式和透明模式接口的历史记录，第 783 页

关于路由和透明模式接口

ASA支持两种类型的接口：路由和桥接。

每个第 3 层路由接口都需要唯一子网上的一个 IP 地址。

桥接接口属于桥接组，且所有接口都在同一网络上。桥接组由在网桥网络上有 IP 地址的桥接虚拟接口 (BVI) 表示。路由模式支持路由和桥接接口，您可以在路由接口和 BVI 之间路由。透明防火墙模式仅支持桥接组和 BVI 接口。

安全级别

每个接口都必须有一个0（最低）到100（最高）的安全级别，包括网桥组成员接口。例如，应将最安全的网络（如内部主机网络）分配至级别100。而连接到互联网的外部网络可分配至级别0。其他网络（例如 DMZ）可指定为介于中间的级别。您可以将多个接口分配至同一安全级别。

是否为 BVI 分配安全级别取决于防火墙模式。在透明模式下，BVI 接口没有安全级别，因为它没有参与接口之间的路由。在路由模式下，如果您选择在 BVI 和其他接口之间路由，则 BVI 接口就有安全级别。对于路由模式，网桥组成员接口的安全级别仅适用于网桥组内部的通信。类似地，BVI 安全级别仅适用于 BVI 间/第 3 层接口通信。

级别控制以下行为：

- 网络访问 - 默认情况下，默许从安全级别较高的接口访问安全级别较低的接口（出站）。较高安全级别接口上的主机可以访问较低安全级别接口上的任何主机。您可以通过将 ACL 应用于接口来限制访问。

  如果为相同安全级别的接口启用通信，那么就会隐式许可这些接口访问处于同一安全级别或更低安全级别的其他接口。

- 检测引擎 - 某些应用检测引擎依赖于安全级别。对于同一安全级别的接口，检测引擎适用于任意方向的流量。
  - NetBIOS 检测引擎 - 仅应用于出站连接。
  - SQL*Net 检测引擎 - 如果 SQL*Net（之前称为 OraServ）端口的控制连接存在于主机对之间，则只有入站数据连接允许通过 ASA。

双 IP 堆栈（IPv4 和 IPv6）

ASA在接口上同时支持 IPv6 和 IPv4 地址。请确保配置一条同时适用于 IPv4 和 IPv6 的默认路由。

31 位子网掩码

对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。31 位子网只包含 2 个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 ASA 之间的故障转移链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行 SNMP 或系统日志的一个直连管理站。

31 位子网和集群

您可以在跨集群模式下使用 31 位子网掩码用于，但管理接口和集群控制链路除外。

在单集群模式下，在任何接口上都不能使用 31 位子网掩码。

31 位子网和故障转移

进行故障转移时，如果为 ASA 接口 IP 地址使用 31 位子网，则无法为该接口配置备用 IP 地址，因为没有足够的地址。通常，用于进行故障转移的接口应有一个备用 IP 地址，以便主设备可以执行接口测试来确保备用接口正常运行。如果没有备用 IP 地址，ASA 无法执行任何网络测试；只能跟踪链路状态。

对于故障转移和可选的独立状态链路（点对点连接），也可以使用 31 位子网。

31 位子网和管理

如果您有直接连接的管理工作站，则对于 ASA 的 SSH 或 HTTP，或管理工作站上的 SNMP 或 Syslog，可使用点对点连接。

31 位子网不支持的功能

以下功能不支持 31 位子网：

- 网桥组的 BVI 接口 - 网桥组需要至少 3 个主机地址：BVI 和连接到两个网桥组成员接口的两台主机。您必须使用 /29 子网或更小的子网。
- 组播路由

路由和透明模式接口准则和限制

情景模式

- 在多情景模式下，您只能配置已根据配置多情景，第 228 页分配给系统配置中的情景的情景接口。
- 在多情景模式下不支持 PPPoE。
- 对于透明模式下的多情景模式，每个情景必须使用不同的接口；不能跨情景共享接口。
- 对于透明模式下的多情景模式，每个情景通常使用不同子网。您可以使用重叠子网，但是从路由角度而言，需要路由器和 NAT 配置才能实现网络拓扑。
- 多情景模式不支持 DHCPv6 和前缀委派选项。
- 在路由防火墙模式下，多情景模式中不支持网桥组接口。

故障转移、 集群

- 请勿采用本章中的程序配置故障转移接口。有关详细信息，请参阅故障转移。
- 对于集群接口，请参阅“集群”一章了解要求。
- 在使用故障转移时，则必须为数据接口手动设置 IP 地址和备用地址；不支持 DHCP 和 PPPoE。

IPv6

- 所有接口上都支持 IPv6。
- 只能在透明模式下手动配置 IPv6 地址。
- ASA 不支持 IPv6 任播地址。
- 多情景模式、透明模式、集群或故障转移不支持 DHCPv6 和前缀委派选项。

型号准则

- 对于 ASAv50，在透明或路由模式不支持桥接组。

透明模式和网桥组准则

- 您可以创建最多 250 个桥接组，每个桥接组 64 个接口。
- 各个直连网络必须在同一子网上。
- ASA不支持辅助网络上的流量；只有与 BVI IP 地址相同的网络上的流量才受支持。
- 每个桥接组都需要 BVI 的 IP 地址，以用于管理往返设备的流量和使流量通过 ASA。对于 IPv4 流量，请指定 IPv4 地址。对于 IPv6 流量，请指定 IPv6 地址。
- 您仅可手动配置 Ipv6 地址。
- BVI IP 地址必须与已连接网络位于同一子网上。您不能将该子网设置为主机子网 (255.255.255.255)。
- 不支持将管理接口作为桥接组成员。
- 对于具有桥接 ixgbevf 接口的 VMware 上的 ASAv50，透明模式不受支持，在路由模式中网桥组不受支持。
- 对于 Firepower 1010 和 Cisco Secure Firewall 1210/20，不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个桥接组中。
- 在透明模式下，必须至少使用 1 个桥接组；数据接口必须属于桥接组。
- 在透明模式下，请勿将 BVI IP 地址指定为所连接设备的默认网关；设备需要将位于 ASA另一端的路由器指定为默认网关。
- 在透明模式下，默认路由（为管理流量提供返回路径所需的路由）仅适用于来自一个桥接组网络的管理流量。这是因为默认路由会指定网桥组中的接口以及网桥组网络上的路由器 IP 地址，而您只能定义一个默认路由。如果您具有来自多个桥接组网络的管理流量，则需要指定常规静态路由来确定预期会发出管理流量的网络。
- 在透明模式下，管理接口不支持 PPPoE。
- 在路由模式下，要在桥接组和其他路由接口之间路由，您必须指定 BVI。
- 在路由模式下，ASA - 不支持将 EtherChannel 和 VNI 接口定义为网桥组成员。 Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。
- 使用网桥组成员时，不允许双向转发检测 (BFD) 回应数据包通过 ASA。如果 ASA 的一端有两个邻居运行 BFD，则 ASA 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。

默认安全级别

默认安全级别为0。如果将一个接口命名为“inside”，且未明确设置安全级别，则ASA将安全级别设置为 100。

注释 如果更改接口的安全级别，且不希望等待现有连接超时后才使用新安全信息，则可使用 **clear conn** 命令清除连接。

其他准则和要求

- ASA 仅支持数据包中的一个 802.1Q 报头，不支持的多个报头（称为 QinQ 支持）。
- 接口问题（例如频繁的启动/关闭状态更改）会导致浮动连接计时器无法正确应用于通过接口的连接。如果接口状态有问题，可考虑在状态稳定后清除所有连接，以清除无效连接。

配置路由模式接口

要配置路由模式接口，请执行以下步骤：

配置常规路由模式接口参数

此程序介绍如何设置名称、安全级别、IPv4 地址和其他选项。

开始之前

在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入 **changeto context** *name* 命令。

过程

步骤 1 进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

接口 ID 可以是：

- **port-channel**
- *physical* - 例如，**ethernet**、**gigabitethernet**、**tengigabitethernet**、**management**。请参阅您的型号的硬件安装指南以获取接口名称。

- *physical*.*subinterface* - 例如，**gigabitethernet0/0.100**。
- **vni**
- **vlan**
- 环回
- *mapped_name* - 适用于多情景模式。

注释
对于 Firepower 1010，不能将交换机端口配置为路由模式接口。

步骤 2 为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 3 使用以下其中一种方法设置 IP 地址。

要用于故障转移和集群，以及用于环回接口，您必须手动设置 IP 地址；不支持 DHCP 和 PPPoE。

- 手动设置 IP 地址：

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  备用 *ip_address* 参数用于故障转移。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

  ip_address 和 *mask* 参数分别用于设置接口 IP 地址和子网掩码。对于点对点连接，可以指定 31 位子网掩码 (255.255.255.254)。在这种情况下，不会为网络或广播地址预留 IP 地址。在此情况下，无法设置备用 IP 地址。

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.0 255.255.255.254
  ```

- 从 DHCP 服务器获取 IP 地址。

  ip address dhcp [**setroute**]

  示例：

```
ciscoasa(config-if)# ip address dhcp
```

setroute 关键字允许 ASA 使用 DHCP 服务器提供的 默认路由。

重新输入此命令，以重置 DHCP 租用并请求新的租用。

注释
如果在输入 **ip address dhcp** 命令之前没有使用 **no shutdown** 命令启用接口，某些 DHCP 请求可能无法发送。

- 从 PPPoE 服务器获取 IP 地址：

  ip address pppoe [**setroute**]

  示例：

  ```
  ciscoasa(config-if)# ip address pppoe setroute
  ```

  您可以通过手动输入 IP 地址 来选择启用 PPPoE。

  ip address *ip_address mask* **pppoe**

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.78 255.255.255.0 pppoe
  ```

  Setroute 选项设置 PPPoE 客户端尚未建立连接时的默认路由。使用 **setroute** 选项时，无法在配置中使用 静态定义的路由。

  注释
  如果在两个接口（例如主用接口和备用接口）上都启用了 PPPoE，但未配置双重 ISP 支持，则 ASA 只能通过第一个接口发送流量来获取 IP 地址。

步骤 4 设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 为介于 0（最低）到 100（最高）之间的整数。

注释
对于环回接口，不要设置安全级别，因为该接口仅支持进出设备的流量。

步骤 5 （可选）将接口设置为管理专属模式，以便其不允许流量通过。

management-only

默认情况下，管理接口配置为管理专属。

注释
对于环回接口，不要设置管理模式，因为该接口仅支持传入/传出设备的流量。

示例

以下示例为 VLAN 101 配置参数：

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

以下示例在多情景模式下为情景配置进行参数配置。接口 ID 是一个映射名称。

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

相关主题

配置 IPv6 寻址，第 763 页
启用物理接口和配置以太网参数，第 662 页
配置 PPPoE，第 756 页

配置 PPPoE

如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，请配置以下参数。

过程

步骤 1 定义您选择的虚拟专用拨号网络 (VPDN) 组名称来表示此连接：

vpdn group *group_name* **request dialout pppoe**

示例：

```
ciscoasa(config)# vpdn group pppoe-sbc request dialout pppoe
```

步骤 2 如果 ISP 要求身份验证，请选择身份验证协议：

vpdn group *group_name* **ppp authentication** {**chap** | **mschap** | **pap**}

示例：

```
ciscoasa(config)# vpdn group pppoe-sbc ppp authentication chap
```

针对 ISP 所使用的身份验证类型输入相应的关键字：

使用 CHAP 或 MS-CHAP 时，用户名可能是指远程系统名称，而密码可能是指 CHAP 密钥。

步骤 3 将 ISP 分配的用户名关联到 VPDN 组：

vpdn group *group_name* **localname** *username*

示例：

```
ciscoasa(config)# vpdn group pppoe-sbc localname johncrichton
```

步骤 4 为 PPPoE 连接创建用户名和密码对：

vpdn username *username* **password** *password* [**store-local**]

示例：

```
ciscoasa(config)# vpdn username johncrichton password moya
```

store-local 选项可在 ASA 上 NVRAM 的特殊位置存储用户名和密码。如果自动更新服务器向 ASA 发送 **clear config** 命令，然后连接中断，ASA 可从 NVRAM 读取用户名和密码并重新进行身份验证来连接访问集中器。

配置网桥组接口

网桥组是指 ASA 网桥（而非路由）的接口组。 网桥组在透明和路由防火墙模式下受支持。有关网桥组的详细信息，请参阅 关于网桥组，第 191 页。

要配置网桥组和关联接口，请执行以下步骤。

配置网桥虚拟接口 (BVI)

每个网桥组都需要一个您应为其配置 IP 地址的 BVI。ASA 使用该 IP 地址作为源自网桥组的数据包的源地址。BVI IP 地址必须与所连接的网络位于同一子网。对于 IPv4 流量，任何流量的传递都需要使用 BVI IP。对于 IPv6 流量，您必须至少配置链路本地地址以传递流量，但要实现完整功能（包括远程管理和其他管理操作），建议采用全局管理地址。

对于路由模式，如果为 BVI 提供一个名称，则 BVI 将参与路由。如果不提供名称，网桥组在透明防火墙模式下将保持隔离状态。

某些型号的默认配置中包括一个网桥组和 BVI。您可以创建其他网桥组和 BVI，并可以在组之间重新分配成员接口。

注释 对于透明模式（适用于受支持的型号）下单独的管理接口，系统会向您的配置自动添加一个不可配置的网桥组 (ID 301)。此网桥组未包含在网桥组限制中。

过程

步骤 1 创建 BVI：

interface bvi *bridge_group_number*

示例：

```
ciscoasa(config)# interface bvi 2
```

bridge_group_number 是介于 1 和 250 之间的整数。稍后，您会将物理接口分配给此网桥组编号。

步骤 2 （透明模式）为 BVI 指定 IP 地址：

ip address *ip_address* [*mask*] [**standby** *ip_address*]

示例：

```
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

请勿为 BVI 分配主机地址（/32 或 255.255.255.255）。此外，也不要使用所含主机地址数小于 3（上游路由器、下游路由器和 BVI 各一个）的其他子网，例如 /30 子网 (255.255.255.252)。ASA 会丢弃传入子网中第一个和最后一个地址或从其传出的所有 ARP 数据包。因此，如果您使用 /30 子网，并从该子网中为上游路由器分配了一个预留地址，那么ASA将丢弃从下游路由器发送至上游路由器的 ARP 请求。

standby 关键字和地址用于故障转移。

步骤 3 （路由模式）使用以下方法之一设置 IP 地址：

要用于故障转移和集群，您必须手动设置 IP 地址；不支持 DHCP。

- 手动设置 IP 地址：

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  备用 *ip_address* 参数用于故障转移。

  ip_address 和 *mask* 参数分别用于设置接口 IP 地址和子网掩码。

- 从 DHCP 服务器获取 IP 地址。

ip address dhcp [**setroute**]

示例：

```
ciscoasa(config-if)# ip address dhcp
```

setroute 关键字允许 ASA 使用 DHCP 服务器提供的 默认路由。

重新输入此命令，以重置 DHCP 租用并请求新的租用。

如果在输入 **ip address dhcp** 命令之前没有使用 no shutdown 命令启用接口，某些 DHCP 请求可能无法发送。

步骤 4 （路由模式）为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside
```

如果要在网桥组成员之外路由流量，例如路由到外部接口或其他网桥组的成员，则必须为 BVI 命名。*name* 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 5 （路由模式）设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 为 0（最低）到 100（最高）之间的整数。

示例

以下示例设置 BVI 2 地址和备用地址：

```
ciscoasa(config)# interface bvi 2
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

配置常规网桥组成员接口参数

此程序描述如何为每个网桥组成员接口设置名称、安全级别和网桥组。

开始之前

- 同一网桥组可以包括不同类型的接口：物理接口、VLAN 子接口、VNI 接口和 EtherChannel 接口。管理接口不受支持。 在路由模式下，不支持 EtherChannels 和 VNI。
- 在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入**changeto context** *name* 命令。
- 对于透明模式，请勿为管理接口使用此程序；请参阅为透明模式配置管理接口，第 761 页配置管理接口。

过程

步骤 1 进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

接口 ID 可以是：

- **port-channel**
- *physical*—For example, **ethernet**, **gigabitethernet**, **tengigabitethernet**. 管理接口不受支持。请参阅您的型号的硬件安装指南以获取接口名称。
- *physical_or_port-channel.subinterface* - 例如，**gigabitethernet0/0.100**或 **port-channel1.100**。
- **vni**
- **vlan**
- *mapped_name* - 适用于多情景模式。

注释
对于 Firepower 1010，不能将交换机端口配置为网桥组成员。

您不能将逻辑 VLAN 接口和物理路由器接口混合在同一个网桥组中。

注释
在路由模式下，不支持将 **port-channel**和 **VNI** 接口作为网桥组成员。

步骤 2 向网桥组分配接口：

bridge-group 编号

示例：

```
ciscoasa(config-if)# bridge-group 1
```

编号为 1 到 250 之间的整数，必须与 BVI 接口编号匹配。最多可将 64 个接口分配到网桥组。您不能将同一接口分配至多个网桥组。

步骤 3 为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif inside1
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 4 设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 50
```

number 为介于 0（最低）到 100（最高）之间的整数。

相关主题

配置、MTU和 TCP MSS，第 793 页

为透明模式配置管理接口

在透明防火墙模式下，所有接口必须属于网桥组。唯一例外的是管理接口（物理接口、子接口（如果您的型号支持）或由管理接口组成的 EtherChannel 接口（如果您有多个管理接口）），您可以将其配置为单独的管理接口；对于 Firepower 4100/9300 机箱，管理接口 ID 取决于分配给 ASA 逻辑设备的管理类型接口。您不能将任何其他接口类型用作管理接口。您可以在单模式下或为每个情景配置一个管理接口。有关详细信息，请参阅透明模式下的管理接口，第 661 页。

开始之前

- 请勿将此接口分配给网桥组；不可配置的网桥组 (ID 301) 将自动添加到您的配置中。此网桥组未包含在网桥组限制中。
- 对于 Firepower 4100/9300 机箱，管理接口 ID 取决于分配给 ASA 逻辑设备的管理类型接口。
- 在多情景模式下，您无法跨情景共享任何接口，包括管理接口。您必须连接到数据接口。
- 在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请在。

过程

步骤 1 进入接口配置模式：

interface {{**port-channel** *number* | **management** *slot*/*port* | *mgmt-type_interface_id* }[**.** *subinterface*] | *mapped_name*}

示例：

```
ciscoasa(config)# interface management 0/0.1
```

port-channel *number* 参数是 EtherChannel 接口 ID，例如 **port-channel 1**。EtherChannel 接口只能拥有管理成员接口。

在多情景模式下，如已使用 **allocate-interface** 命令分配一个接口，请输入 *mapped_name* 命令。

对于 Firepower 4100/9300 机箱，指定分配给 ASA 逻辑设备的管理类型接口（单独或 EtherChannel）的接口 ID。

步骤 2 为接口命名：

nameif *name*

示例：

```
ciscoasa(config-if)# nameif management
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 3 使用以下其中一种方法设置 IP 地址。

- 手动设置 IP 地址：

  要用于故障转移，您必须手动设置 IP 地址和备用地址；不支持 DHCP。

  ip_address 和 *mask* 参数分别用于设置接口 IP 地址和子网掩码。

  备用 *ip_address* 参数用于故障转移。

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  示例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

- 从 DHCP 服务器获取 IP 地址。

  ip address dhcp [**setroute**]

  示例：

```
ciscoasa(config-if)# ip address dhcp
```

setroute 关键字允许 ASA 使用 DHCP 服务器提供的 默认路由。

重新输入此命令，以重置 DHCP 租用并请求新的租用。

如果在输入 **ip address dhcp** 命令之前没有使用 no shutdown 命令启用接口，某些 DHCP 请求可能无法发送。

步骤 4 设置安全级别：

security-level *number*

示例：

```
ciscoasa(config-if)# security-level 100
```

number 为 0（最低）到 100（最高）之间的整数。

配置 IPv6 寻址

此部分介绍如何配置 IPv6 寻址。

关于 IPv6

本节包括关于 IPv6 的信息。

IPv6 寻址

您可以为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。对于网桥组，需要为 BVI（而不必为每个成员接口）配置此地址。还可以为透明模式下的管理接口配置全局 IPv6 地址。
- 链路本地 - 链路本地地址是只能在直连网络上使用的专用地址。路由器不使用链路本地地址转发数据包；它们仅用于在特定物理网段上通信。链路本地地址可用于地址配置或邻居发现功能，例如地址解析。在网桥组中，只有成员接口具有链路本地地址；BVI 没有链路本地地址。

至少需要配置链路本地地址，IPv6 才会起作用。如果配置全局地址，则接口上会自动配置链路本地地址，因此无需另外专门配置链路本地地址。对于网桥组成员接口，在 BVI 上配置全局地址时，ASA 将为成员接口自动生成链路本地地址。如果不配置全局地址，则需要自动或手动配置链路本地地址。

注释 如果希望仅配置链路本地地址，请参阅命令参考中的**ipv6 enable**（自动配置）或**ipv6 address link-local**（手动配置）命令。

修改的 EUI-64 接口 ID

RFC 3513：互联网协议第 6 版 (IPv6) 寻址架构要求所有单播 IPv6 地址（以二进制值 000 开头的地址除外）的接口标识符部分的长度为 64 位，并以修改的 EUI-64 格式进行构造。ASA 可为连接到本地链路的主机执行该要求。

在接口上启用此功能时，该接口接收的 IPv6 数据包源地址根据源 MAC 地址进行验证，以确保接口标识符使用修改的 EUI-64 格式。如果 IPv6 数据包不将修改的 EUI - 64 格式用于接口标识符，则会丢弃数据包并生成以下系统日志消息：

```
325003: EUI-64 source address check failed.
```

只有在创建流量时才会执行地址格式验证。不检查来自现有流量的数据包。此外，只能对本地链路上的主机执行地址验证。

配置 IPv6 前缀代理客户端

ASA 可以作为 DHPCv6 前缀授权客户端，以便客户端接口（例如连接到电缆调制解调器的外部接口）可以接收一个或多个 IPv6 前缀，然后 ASA 可以将这些前缀通过子网分配到其内部接口。

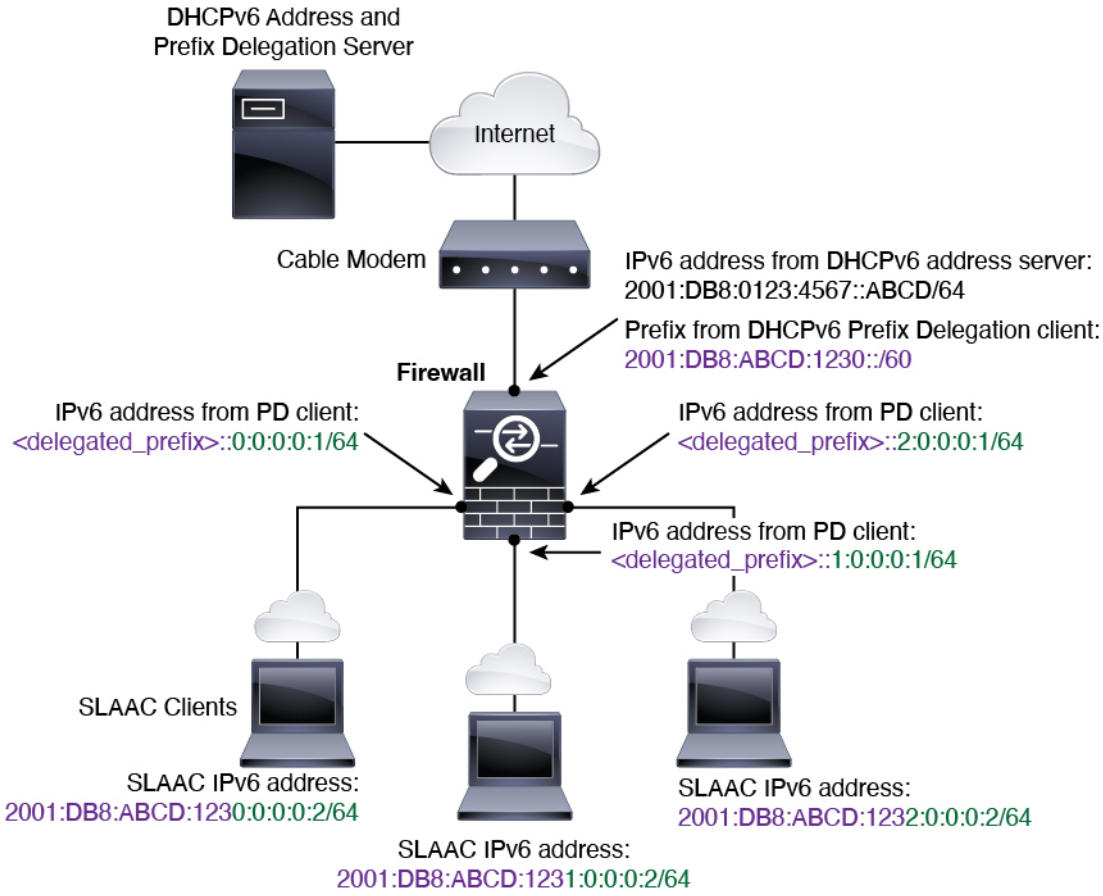
关于 IPv6 前缀授权

ASA 可以作为 DHPCv6 前缀授权客户端，以便客户端接口（例如连接到电缆调制解调器的外部接口）可以接收一个或多个 IPv6 前缀，然后 ASA 可以将这些前缀通过子网分配到其内部接口。然后，连接到内部接口的主机可以使用无状态地址自动配置 (SLAAC) 获取全局 IPv6 地址。请注意，内部 ASA 接口不会依次充当前缀授权服务器；ASA 只能向 SLAAC 客户端提供全局 IP 地址。例如，如果路由器连接到 ASA，它可以作为 SLAAC 客户端获取其 IP 地址。但是，如果您要为路由器后的网络使用授权的前缀的子网，则必须在路由器的内部接口上手动配置这些地址。

ASA 中包括一个轻型 DHCPv6 服务器，以便 SLAAC 客户端在向 ASA 发送信息请求 (IR) 数据包时，ASA 可以向这些客户端提供 DNS 服务器和域名等信息。ASA 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 ASA 的前缀。

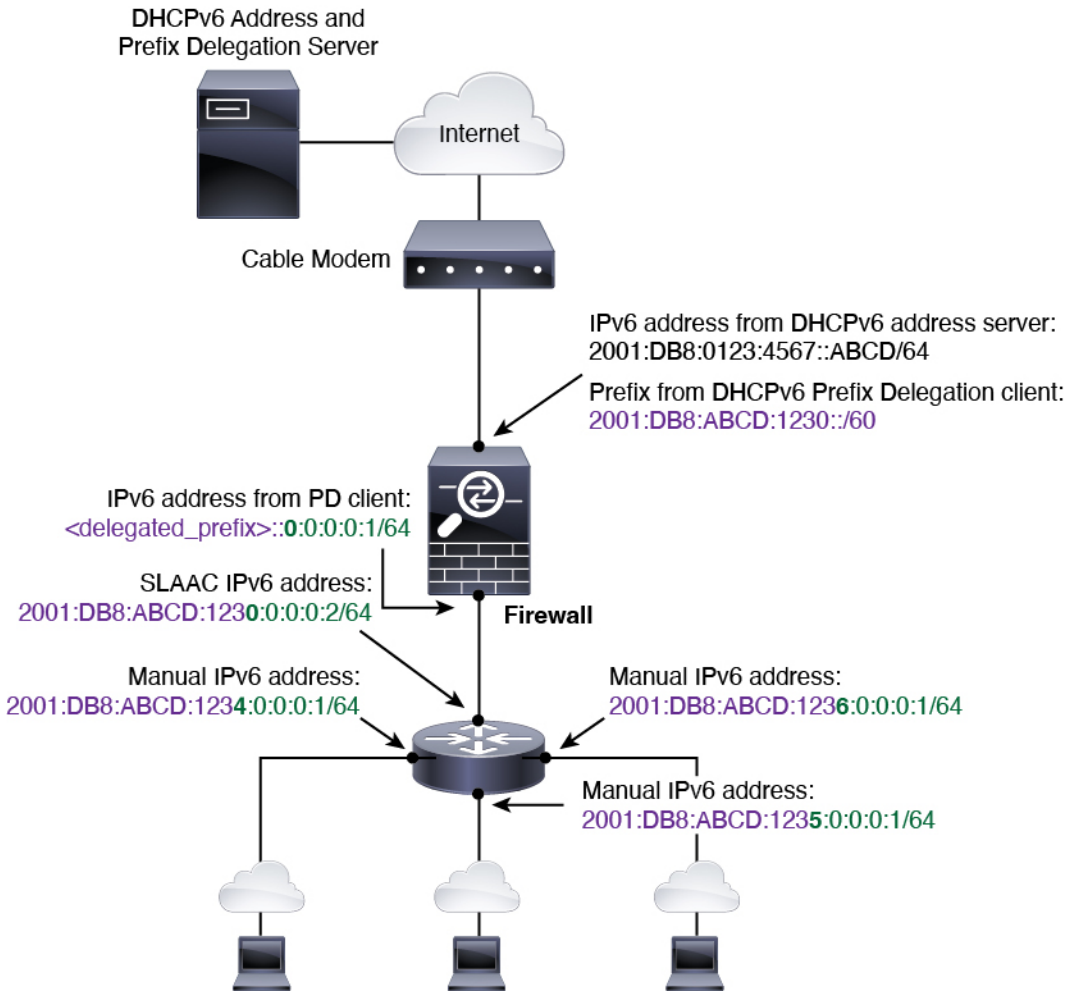
IPv6 前缀授权 /64 子网示例

以下示例显示使用 DHCPv6 地址客户端在外部接口上接收 IP 地址的 ASA。此外，它还会使用 DHCPv6 前缀授权客户端获得一个授权的前缀。ASA 将授权的前缀编入 /64 网络的子网，并使用授权的前缀以及手动配置的子网（::0、::1 或 ::2）和每个接口上的 IPv6 地址 (0:0:0:1) 为其内部接口动态分配全局 IPv6 地址。连接至这些内部接口的 SLAAC 客户端将获得每个 /64 子网上的 IPv6 地址。



IPv6 前缀委派 /62 子网示例

以下示例显示了 ASA 将前缀子网划分到 4 个 /62 子网中:2001:DB8:ABCD:123**0**::/62、2001:DB8:ABCD:123**4**::/62、2001:DB8:ABCD:123**8**::/62 和 2001:DB8:ABCD:123**C**::/62。ASA 将 2001:DB8:ABCD:1230::/62 上 4 个可用 /64 子网之一用于其内部网络 (::0)。随后您可以手动将其他 /62 子网用于下游路由器。所示的路由器将 2001:DB8:ABCD:1234::/62 上 4 个可用 /64 子网中的 3 个用于其内部接口（::4、::5 和 ::6）。在此情况下，内部路由器接口无法动态获取委派的前缀，因此您需要在 ASA 上查看委派的前缀，然后将该前缀用于您的路由器配置。通常，当租约到期时，ISP 会将同一前缀委派给指定客户端，但如果 ASA 收到新前缀，则您必须修改路由器配置以使用该新前缀。DHCP 唯一标识符 (DUID) 在重新启动时会保持不变。



启用 IPv6 前缀授权客户端

在一个或多个接口上启用 DHCPv6 前缀代理客户端。ASA 可获取一个或多个可设置子网和分配给内部网络的 IPv6 前缀。通常，在其上启用前缀代理客户端的接口使用 DHCPv6 地址客户端获取其 IP 地址，只有其他 ASA 接口才能使用代理前缀衍生的地址。

开始之前

- 此功能仅支持路由防火墙模式。
- 此功能不支持多情景模式。
- 此功能不支持集群。
- 无法在仅管理接口上配置此功能。
- 当您使用前缀代理时，必须将 ASA IPv6 邻居发现路由器通告间隔设置为远低于 DHCPv6 服务器分配的前缀的首选有效期，以防 IPv6 流量中断。例如，如果 DHCPv6 服务器将首选前缀代理有效期设置为 300 秒，则您应将 ASA RA 间隔设置为 150 秒。要设置首选有效期，请使用 **show**

ipv6 general-prefix 命令。要设置 ASA RA 间隔，请参阅配置 IPv6 邻居发现，第 770 页；默认值为 200 秒。

过程

步骤 1 对于连接到 DHCPv6 服务器网络的接口，请进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

步骤 2 启用 DHCPv6 前缀代理客户端，并为在此接口上获取的前缀命名：

ipv6 dhcp client pd 名称

示例：

```
ciscoasa(config-if)# ipv6 dhcp client pd Outside-Prefix
```

name 最长为 200 个字符。

步骤 3 提供有关要接收的代理前缀的一项或多项提示：

ipv6 dhcp client pd hint *ipv6_prefix/prefix_length*

示例：

```
ciscoasa(config-if)# ipv6 dhcp client pd hint 2001:DB8:ABCD:1230::/60
```

通常，您需要请求特定的前缀长度（例如 ::/60），或者如果您以前收到过特定前缀并希望确保在租用到期后重新获取该前缀，可以作为提示输入整个前缀。如果输入了多个提示（不同的前缀或长度），则由 DHCP 服务器来决定要尊重的提示或是否尊重提示。

步骤 4 请参阅配置全局 IPv6 地址，第 768 页为 ASA 接口分配作为全局 IP 地址的前缀子网。

步骤 5 （可选） 请参阅配置 DHCPv6 无状态服务器，第 847 页为 SLAAC 客户端提供域名和服务器参数。

步骤 6 （可选） 请参阅配置 IPv6 网络设置，第 1004 页通告包含 BGP 的前缀。

示例

以下示例在 GigabitEthernet 0/0 上配置 DHCPv6 地址客户端和前缀代理客户端，然后在 GigabitEthernet 0/1 和 0/2 上分配包含该前缀的地址：

```
interface gigabitethernet 0/0
  ipv6 address dhcp default
```

```
  ipv6 dhcp client pd Outside-Prefix
  ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

配置全局 IPv6 地址

要为任何路由模式接口和透明或路由模式 BVI 配置全局 IPv6 地址，请执行以下步骤。

多情景模式不支持 DHCPv6 和前缀代理选项。

注释 配置全局地址将自动配置链路本地地址，因此无需单独对其进行配置。对于网桥组，在 BVI 上配置全局地址会自动在所有成员接口上配置链路本地地址。

对于子接口，建议您同样手动设置 MAC 地址，这是因为它们使用父接口上相同的固化 MAC 地址。由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一的 MAC 地址分配给子接口会允许唯一的 IPv6 链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。请参阅 手动配置 MAC 地址，第 791 页。

开始之前

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入 **changeto context** *name* 命令。

过程

步骤 1 进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

在透明模式或路由模式下，为网桥组指定 BVI：

示例：

```
ciscoasa(config)# interface bvi 1
```

在透明模式下，除了 BVI 之外，您还可以指定管理接口：

示例：

```
ciscoasa(config)# interface management 1/1
```

步骤 2 （路由接口）使用以下方法之一设置 IP 地址。

要用于故障转移和集群，以及用于环回接口，您必须手动设置 IP 地址。对于集群，不支持手动配置链路本地地址。

- 在接口上启用无状态自动配置：

  ipv6 address autoconfig [**default trust** {**dhcp** | **ignore**}]

  在接口上启用无状态自动配置时，将基于 Router Advertisement 消息中接收到的前缀来配置 IPv6 地址。启用无状态自动配置时，将基于修改的 EUI-64 接口 ID 自动生成接口的链路本地地址。

  注释
  尽管 RFC 4862 指定为无状态自动配置所配置的主机不会发送路由器通告消息，但这种情况下，ASA 会发送路由器通告消息。要抑制消息，请参阅 **ipv6 nd suppress-ra** 命令。

  如果要安装默认路由，请指定 **default trust dhcp** 或 **ignore**。**dhcp** 指定 ASA 仅使用源自受信任源（即源自提供 IPv6 地址的同一台服务器）的路由器通告的默认路由。**ignore** 指定路由器通告可以源自其他网络，这种方法风险可能要高一些。

- 使用 DHCPv6 获取地址：

  ipv6 address dhcp [**default**]

  示例：

  ```
  ciscoasa(config-if)# ipv6 address dhcp default
  ```

  default 关键字从路由器通告获取默认路由。

- 手动为接口分配全局地址：

  ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

  示例：

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
  ```

  分配全局地址时，将为接口自动创建 链路本地地址。

  standby 指定辅助设备或故障转移对中的故障转移组 使用的接口地址。

- 通过将指定前缀与使用 Modified EUI-64 格式从接口 MAC 地址生成的接口 ID 配合使用，来为接口分配全局地址。

  ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

  示例：

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
  ```

分配全局地址时，将为接口自动创建 链路本地地址。

您不需要指定备用接口；接口 ID 将会自动生成。

- 使用授权的前缀：

  ipv6 address *prefix_name ipv6_address/prefix_length*

  示例：

  ```
  ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ```

  此功能要求 ASA 在不同接口上启用 DHCPv6 前缀授权客户端。请参阅 启用 IPv6 前缀授权客户端，第 766 页。通常情况下，授权的前缀将为 /60 或更小，因此您可以将其作为多个 /64 网络的子网。如果希望连接的客户端支持 SLAAC，则 /64 是受支持的子网长度。您应指定可以完成 /60 子网的地址，例如 ::1:0:0:0:1。在地址前输入 ::，以免前缀小于 /60。例如，如果授权的前缀是 2001:Db8:1234:5670::/60，则分配给该接口的全局 IP 地址是 2001:DB8:1234:5671::1/64。在路由器通告中通告的前缀是 2001:DB8:1234:5671::/64。在本例中，如果前缀小于 /60，则前缀剩余的位将是 0，就如前导 :: 所指示的那样。例如，如果前缀是 2001:DB8:1234::/48，则 IPv6 地址将为 2001:DB8:1234::1:0:0:0:1/64。

步骤 3 （BVI 接口）为 BVI 手动分配全局地址。对于透明模式下的管理接口，也请使用此方法。

ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

示例：

```
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

分配全局地址时，将为接口自动创建 链路本地地址。

standby 指定辅助设备或故障转移对中的故障转移组 使用的接口地址。

步骤 4 （可选）在本地链路上的 IPv6 地址中，强制使用修改的 EUI-64 格式的接口标识符。

ipv6 enforce-eui64 *if_name*

示例：

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

if_name 参数是 **nameif** 命令所指定的接口的名称，您将在此接口上启用地址格式执行。

配置 IPv6 邻居发现

IPv6 邻居发现过程使用 ICMPv6 消息和请求节点组播地址，确定同一网络（本地链路）中邻居的链路层地址、验证邻居的可读性及跟踪相邻路由器。

节点（主机）使用邻居发现确定已知驻留在连接的链路上邻居的链路层地址并快速清除变为无效的缓存值。主机还使用邻居发现查找愿意代表自己转发数据包的邻居路由器。此外，节点使用协议主动跟踪哪些邻居可访问及哪些邻居不可访问，并检测已更改的链路层地址。当路由器或路由器的路径发生故障时，主机会主动搜索起作用的替代项。

过程

步骤 1 指定要配置的 IPv6 接口。

interface *name*

示例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)#
```

步骤 2 指定重复地址检测 (DAD) 尝试的次数 。

ipv6 nd dad attempts *value*

value 参数的有效值范围为 0 至 600。0 值可在指定的接口上禁用 DAD 处理。默认值为 1 条消息。

DAD 确保新的单播 IPv6 地址在分配之前的唯一性，并确保按链路检测网络中的重复 IPv6 地址。ASA 使用邻居请求消息来执行 DAD。

识别出重复地址后，该地址的状态会设置为 DUPLICATE，且不会使用该地址并生成以下错误消息：

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。

示例：

```
ciscoasa(config-if)# ipv6 nd dad attempts 20
```

步骤 3 设置 IPv6 邻居请求重新传输的间隔时间。

ipv6 nd ns-interval *value*

value 参数的值范围为 1000 到 3600000 毫秒。

邻居请求消息（ICMPv6 类型 135）由尝试发现本地链路上其他节点的链路层地址的节点在本地链路上发送。在收到邻居请求消息后，目标节点通过在本地链路上发送邻居通告消息（ICPMv6 类型 136）作出应答。

源节点接收邻居通告后，源节点与目标节点即可通信。识别邻居的链路层地址后，邻居请求消息也用于验证邻居的可访问性。当节点要验证邻居的可访问性时，邻居请求消息中的目标地址是邻居的单播地址。

本地链路中一个节点的链路层地址发生变化时，也会发送邻居通告消息。

示例：

```
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

步骤 4 设置远程 IPv6 节点可访问的时间量。

ipv6 nd reachable-time *value*

value 参数的值范围为 0 到 3600000 毫秒。当该值为 0 时，将发送未确定的可访问时间。由接收设备来设置和跟踪可访问时间的值。

邻居可访问时间可启用检测不可用邻居。配置时间越短，检测不可用邻居的速度就越快，但是，时间缩短却在所有 IPv6 网络设备中占用了更多的 IPv6 网络带宽和处理资源。在正常 IPv6 操作中不建议设置很短的配置时间。

示例：

```
ciscoasa config-if)# ipv6 nd reachable-time 1700000
```

步骤 5 设置 IPv6 路由器通告传输之间的时间间隔。

ipv6 nd ra-interval [**msec**] *value*

msec 关键字指示提供的值以毫秒为单位。如果此关键字不存在，则提供的值以秒为单位。*value* 参数的有效值范围介于 3 到 1800 秒之间；如果提供了 **msec** 关键字，则范围介于 500 到 1800000 毫秒之间。默认值为 200 秒。

时间间隔值包括在发送出此接口的所有 IPv6 路由器通告中。

如果将 ASA 配置为默认路由器，则传输之间的时间间隔应小于或等于 IPv6 路由器通告有效期。为防止与其他 IPv6 节点的同步，请将所用的实际值随机调整为所需值的 20% 以内。

示例：

```
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

步骤 6 指定本地链路上的节点应将 ASA 视为链路上默认路由器的时间长度。

ipv6 nd ra-lifetime [**msec**] *value*

可选的 **msec** 关键字指示提供的值以毫秒为单位。如未指定，则该值以秒为单位。*value* 参数的值范围为 0 到 9000 秒。输入 0 表示不应将 ASA 视为选定接口的默认路由器。

路由器有效期值包括在发送出接口的所有 IPv6 路由器通告中。此值表示 ASA 作为此接口的默认路由器的益处。

示例：

```
ciscoasa(config-if)# ipv6 nd ra-lifetime 2000
```

步骤 7 抑制路由器通告。

ipv6 nd suppress-ra

路由器通告消息（ICMPv6 类型 134）会自动发送，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

在不希望 ASA 提供 IPv6 前缀的所有接口（例如，外部接口）上，您可能想要禁用这些消息。

输入此命令会导致 ASA 显示为链路上的常规 IPv6 邻居，而不是显示为 IPv6 路由器。

步骤 8 添加标志到 IPv6 路由器通告，以通知 IPv6 自动配置客户端使用 DHCPv6 获取 IPv6 地址以及派生的无状态自动配置地址。

ipv6 nd managed-config-flag

此选项在 IPv6 路由器通告数据包中设置托管地址配置标志。

步骤 9 添加标志到 IPv6 路由器通告，以通知 IPv6 自动配置客户端使用 DHCPv6 获取 DNS 服务器地址或其他信息。

ipv6 nd other-config-flag

此选项在 IPv6 路由器通告数据包中设置其他地址配置标志。

步骤 10 配置包含在 IPv6 路由器通告中的 IPv6 前缀：

ipv6 nd prefix {*ipv6_prefix*/*prefix_length* | **default**} [*valid_lifetime preferred_lifetime* | **at** *valid_date preferred_date*] [**no-advertise**] [**no-autoconfig**] [ ] [**off-link**]

前缀通告可供邻居设备用于自动配置其接口地址。无状态自动配置使用路由器通告消息中提供的IPv6前缀从链路本地地址创建全局单播地址。

默认情况下，接口上使用 **ipv6 addres** 命令配置为地址的前缀在路由器通告中通告。如果使用 **ipv6 nd prefix** 命令为通告配置前缀，则仅通告这些前缀。

为使无状态自动配置正常运行，路由器通告消息中通告的前缀长度必须始终为 64 位。

- **default**- 表示使用默认前缀。
- *valid_lifetime preferred_lifetime* - 指定通告指定的 IPv6 前缀为有效前缀和首选前缀的时间量。地址在首选的有效期内没有任何限制。首选的有效期到期后，该地址会进入已弃用状态；对于已弃用状态的地址，虽然不推荐使用，但并未严格禁止。有效的有效期到期后，地址将变为无效状态，且无法使用。有效的有效期必须大于或等于首选的有效期。值范围为 0 秒至 4294967295 秒。最大值代表无穷大，也可以使用 **infinite** 关键字指定。有效的有效期默认值为 2592000（30 天）。首选的有效期默认值为 604800（7 天）。
- **at** *valid_date preferred_date* - 指示前缀到期的具体日期和时间。指定日期格式为 *month_name day hh*:*mm*。例如，输入 **dec 1 13:00**。
- **no-advertise**- 禁用前缀通告。
- **no-autoconfig** - 指定前缀不能用于 IPv6 自动配置。
- **off-link**- 将指定的前缀配置为关闭链路。该前缀将在通告时清除 L-位。该前缀将不会作为已连接前缀插入到路由表。

在链路上打开（默认情况下）时，指定的前缀会分配给该链路。向包含指定前缀的此类地址发送流量的节点会将目标视为在链路上本地可访问。

示例：

```
ciscoasa(config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

步骤 11 在 IPv6 邻居发现缓存中配置静态条目。

ipv6 neighbor *ipv6_address if_name mac_address*

以下准则和限制适用于配置静态 IPv6 邻居：

- **ipv6 neighbor** 命令类似于 **arp** 命令。如果指定 IPv6 地址的条目在邻居发现缓存中已存在（已通过 IPv6 邻居发现过程获悉），则该条目会自动转换为静态条目。当使用复制命令存储配置时，这些条目存储在配置中。
- 使用 **show ipv6 neighbor** 命令可查看 IPv6 邻居发现缓存中的静态条目。
- **clear ipv6 neighbor** 命令可删除 IPv6 邻居发现缓存中除静态条目之外的所有条目。**no ipv6 neighbor** 命令可从邻居发现缓存中删除指定的静态条目；该命令不会从缓存中删除动态条目，这些条目从 IPv6 邻居发现过程中获悉。使用 **no ipv6 enabl** 命令在接口上禁用 IPv6 可删除为该接口配置的所有 IPv6 邻居发现缓存条目，静态条目（条目的状态更改为 INCMP [Incomplete]）除外。
- 邻居发现过程不会修改 IPv6 邻居发现缓存中的静态条目。
- **clear ipv6 neighbor** 命令不会从 IPv6 邻居发现缓存中删除静态条目；仅会清除动态条目。
- IPv6 邻居条目的定期刷新生成了 ICMP 系统日志。IPv6 邻居条目的 ASA 默认计时器为 30 秒，因此，ASA 将大约每 30 秒生成 ICMPv6 邻居发现和响应数据包。如果 ASA 拥有用 IPv6 地址配置的故障转移 LAN 和状态接口，则 ASA 将每 30 秒为配置的和链路本地的 IPv6 地址生成 ICMPv6 邻居发现和响应数据包。此外，由于每个数据包将生成多个系统日志（ICMP 连接和本地主机创建或拆卸），因此，似乎一直在不断生成 ICMP 系统日志。可以在常规数据接口上配置 IPv6 邻居条目的刷新时间，但是，不可在故障转移接口上配置。但是，此 ICMP 邻居发现流量对 CPU 的影响最小。

示例：

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

监控路由模式和透明模式接口

您可以监控接口统计信息、状态、PPPoE 。

注释 对于 Firepower 和 Cisco Secure Firewall 模型，某些统计信息未使用 ASA 命令显示。您必须使用 FXOS 命令查看更详细的接口统计信息。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

有关详细信息，请参阅 FXOS 故障排除指南。

接口统计信息和信息

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

- **show bridge-group**

  显示网桥组信息，如分配的接口、MAC 地址和 IP 地址。

DHCP 信息

- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  show ipv6 dhcp interface 命令用于显示所有接口的 DHCPv6 信息。如果接口配置用于 DHCPv6 无状态服务器配置（请参阅配置 DHCPv6 无状态服务器，第 847 页），则此命令将列出该服务器正在使用的 DHCPv6 池。如果接口包含 DHCPv6 地址客户端或前缀委派客户端配置，则此命令将显示各个客户端的状态，以及从该服务器收到的值。对于特定接口，可以显示 DHCP 服务器或客户端的消息统计信息。以下示例显示此命令提供的信息：

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
```

```
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
        IA NA: IA ID 0x00030001, T1 250, T2 400
          Address: 2004:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
        DNS server: 2004:abcd:abcd:abcd::2
        DNS server: 2004:abcd:abcd:abcd::4
        Domain name: relay.com
        Domain name: server.com
        Information refresh time: 0
    Prefix name: Sample-PD

Management1/1 is in client mode
    Prefix State is IDLE
    Address State is OPEN
    Renew for address will be sent in 11:26:44
    List of known servers:
      Reachable via address: fe80::4e00:82ff:fe6f:f6f9
      DUID: 000300014C00826FF6F8
      Preference: 0
      Configuration parameters:
        IA NA: IA ID 0x000a0001, T1 43200, T2 69120
          Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
        Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
```

```
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp client [pd] statistics**

  show ipv6 dhcp client statistics 命令用于显示 DHCPv6 客户端统计信息，并显示已发送和已接收的消息数量的输出结果。**show ipv6 dhcp client pd statistics** 命令显示前缀委派客户端统计信息。以下示例显示此命令提供的信息：

```
ciscoasa(config)# show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                   8
  Total number of Message Validation errors in received messages: 0


ciscoasa(config)# show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:


 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:


 Total number of Re-transmission messages sent:                  1
 Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

  show ipv6 dhcp ha statistics 命令用于显示故障转移设备之间的事务处理统计信息，包括在 DUID 信息各个设备之间的同步次数。以下示例显示了此命令提供的信息。

  在主用设备上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

在备用设备上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

- **show ipv6 general-prefix**

  show ipv6 general-prefix 命令显示 DHCPv6 前缀委派客户端获得的所有前缀，该前缀到其他进程的 ASA 分发（“消费端列表”）。以下示例显示此命令提供的信息：

```
ciscoasa(config)# show ipv6 general-prefix
IPv6 Prefix Sample-PD, acquired via DHCP PD
  2005:abcd:ab03::/48 Valid lifetime 524, preferred lifetime 424
   Consumer List                Usage count
    BGP network command         1
    inside (Address command)    1
```

PPPoE

- **show ip address** *interface_name* **pppoe**

  显示当前 PPPoE 客户端配置信息。

- **debug pppoe** {**event** | **error** | **packet**}

  启用调试 PPPoE 客户端。

- **show vpdn session** [**l2tp** | **pppoe**] [**id** *sess_id* | **packets** | **state** | **window**]

  查看 PPPoE 会话的状态。

  以下示例显示此命令提供的信息：

```
ciscoasa# show vpdn

Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
     6 packets sent, 6 received, 84 bytes sent, 0 received
```

```
Remote Internet Address is 10.0.0.1
     Session state is SESSION_UP
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
```

IPv6 邻居发现

要监控 IPv6 邻居发现参数，请输入以下命令：

- **show ipv6 interface**

  此命令显示为 IPv6 配置的接口的可用性状态（包括接口名称，例如“outside”），并显示指定接口的设置。但是，它会从命令中排除名称并显示已启用 IPv6 的所有接口的设置。命令输出显示以下信息：

  - 接口的名称和状态。
  - 链路本地和全局单播地址。
  - 接口所属的组播组。
  - ICMP 重新定向和错误消息设置。
  - 邻居发现设置。
  - 命令设置为 0 时的实际时间。
  - 正在使用的邻居发现可访问时间。

路由和透明模式接口示例

包括 2 个网桥组的透明模式示例

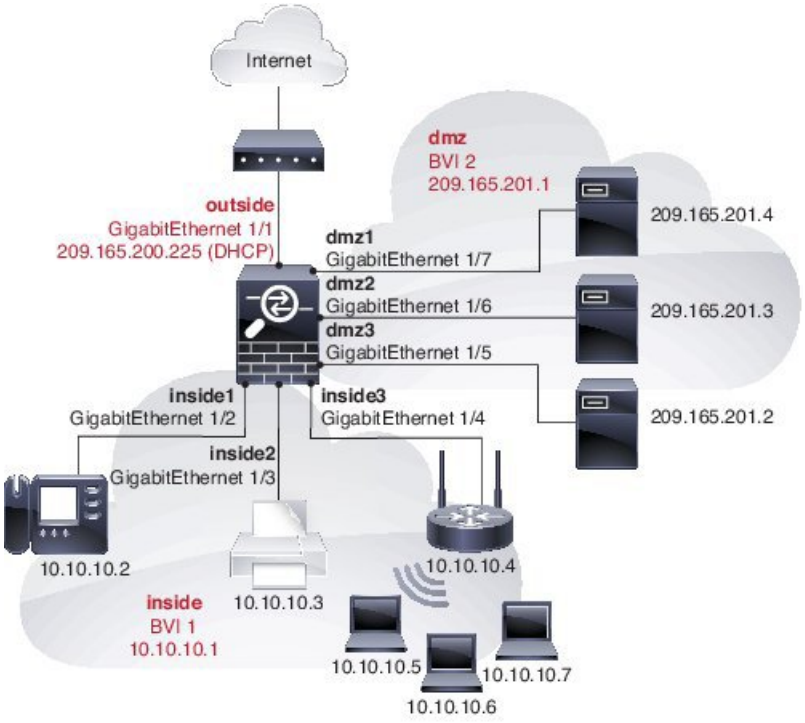
以下透明模式示例包括两个网桥组（每组三个接口）以及一个管理专属接口：

```
interface gigabitethernet 0/0
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

与 2 个网桥组的交换 LAN 网段示例

以下示例配置 2 个网桥组（每个网桥组包含 3 个接口）和一个用于 outside 的普通路由接口。在公共 Web 服务器中，网桥组 1 为 inside，网桥组 2 为 dmz。由于网桥组的每个成员属于同一安全级别，而且我们已启用同一安全通信，所以网桥组成员接口在网桥组内可以自由通信。虽然 inside 成员的安全级别为 100，dmz 成员的安全级别也是 100，但这些安全级别不适用于 BVI 间通信；只有 BVI

安全级别才会影响 BVI 间的流量。BVI 和 outside（100、50 和 0）的安全级别隐式允许 inside 到 dmz、inside 到 outside 以及 dmz 到 outside 的流量。向 outside 应用访问规则以允许流量流入 dmz 上的服务器。




```
interface gigabitethernet 1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface gigabitethernet 1/2
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/3
  nameif inside2
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/4
  nameif inside3
  security-level 100
  bridge-group 1
  no shutdown
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 10.10.10.1 255.255.255.0
!
interface gigabitethernet 1/5
  nameif dmz1
```

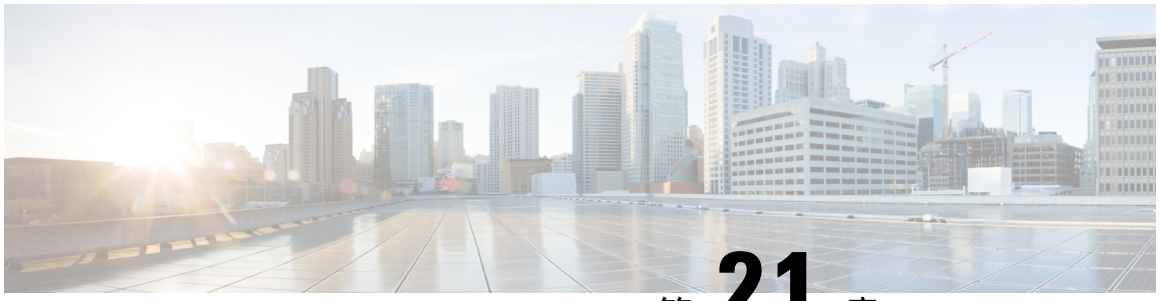
```
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/6
  nameif dmz2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/7
  nameif dmz3
  security-level 100
  bridge-group 2
  no shutdown
!
interface bvi 2
  nameif dmz
  security-level 50
  ip address 209.165.201.1 255.255.255.224
!
same-security-traffic permit inter-interface
!
# Assigns IP addresses to inside hosts
dhcpd address 10.10.10.2-10.10.10.200 inside
dhcpd enable inside
!
# Applies interface PAT for inside traffic going outside
nat (inside1,outside) source dynamic any interface
nat (inside2,outside) source dynamic any interface
nat (inside3,outside) source dynamic any interface
!
# Allows outside traffic to each server for specific applications
object network server1
  host 209.165.201.2
object network server2
  host 209.165.201.3
object network server3
  host 209.165.201.4
!
# Defines mail services allowed on server3
object-group service MAIL
  service-object tcp destination eq pop3
  service-object tcp destination eq imap4
  service-object tcp destination eq smtp
!
# Allows access from outside to servers on the DMZ
access-list SERVERS extended permit tcp any object server1 eq www
access-list SERVERS extended permit tcp any object server2 eq ftp
access-list SERVERS extended permit tcp any object server3 object-group MAIL
access-group SERVERS in interface outside
```

路由模式和透明模式接口的历史记录

功能名称	平台版本	功能信息
IPv6 邻居发现	7.0(1)	引入了此功能。 引入了以下命令：**ipv6 nd ns-interval**、**ipv6 nd ra-lifetime**、**ipv6 nd suppress-ra**、**ipv6 neighbor**、**ipv6 nd prefix**、**ipv6 nd dad-attempts**、**ipv6 nd reachable-time**、**ipv6 address**、**ipv6 enforce-eui64**。
透明模式的 IPv6 支持	8.2(1)	为透明防火墙模式引入了 IPv6 支持。
透明模式的网桥组	8.4(1)	如果您不希望产生安全情景开销，或者希望最大限度地利用安全情景，则可以将接口一起集合到网桥组中，然后配置多个网桥组，每个网络一个组。网桥组流量相互分隔。在单情景模式或每个情景中最多可配置八个网桥组，每组四个接口。 引入了以下命令：**interface bvi** 和 **show bridge-group**
IPv6 DHCP 中继的地址配置标志	9.0(1)	引入了以下命令：**ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag**。
透明模式的网桥组最大数量增加到 250	9.3(1)	网桥组最大数量从 8 个增加到 250 个网桥组。在单情景模式和多情景模式的每个情景中，最多可配置 250 个网桥组，每组最多 4 个接口。 修改了以下命令：**interface bvi**、**bridge-group**
每个桥接组的透明模式最大接口数增加到 64	9.6(2)	每个网桥组的最大接口数量已从 4 增加到 64。 未修改任何命令。

功能名称	平台版本	功能信息
IPv6 DHCP	9.6(2)	ASA 现在支持 IPv6 寻址的以下功能： • DHCPv6 地址客户端 - ASA 从 DHCPv6 服务器获取 IPv6 全局地址和可选默认路由。 • DHCPv6 前缀代理客户端 - ASA 从 DHCPv6 服务器获取指定的前缀。然后，ASA 可使用这些前缀来配置其他 ASA 接口地址，以使无状态地址自动配置 (SLAAC) 客户端可在同一网络上自动配置 IPv6 地址。 • BGP 路由器通告指定的前缀 • DHCPv6 无状态服务器 - 当 SLAAC 客户端向 ASA 发送信息请求 (IR) 数据包时，ASA 会向它们提供域名等其他信息。ASA 仅接受 IR 数据包，不向客户端分配地址。 引入或修改了以下命令：**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address autoconfig**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address**
集成的路由与桥接	9.7(1)	集成路由和桥接提供了在网桥组和路由接口之间路由的功能。网桥组指 ASA 桥接（而非路由）的接口组。ASA 并非真正的网桥，因为 ASA 仍继续充当防火墙：控制接口之间的访问控制，并执行所有常规防火墙检查。以前，您只能在透明防火墙模式下配置网桥组，而无法在网桥组之间路由。通过此功能，可以在路由防火墙模式下配置网桥组，并在网桥组之间以及网桥组与路由接口之间进行路由。网桥组使用网桥虚拟接口 (BVI) 作为网桥组的网关，由此参与路由。如果 ASA 上还有额外接口可分配给网桥组，集成路由和桥接可提供替代使用外部第 2 层交换机的其他方案。在路由模式下，BVI 可以是已命名接口，并可独立于成员接口参与某些功能，例如访问规则和 DHCP 服务器。 路由模式不支持透明模式下支持的以下功能：多情景模式、ASA 集群。以下功能在 BVI 上也不受支持：动态路由和组播路由。 修改了以下命令：**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn**

功能名称	平台版本	功能信息
31 位子网掩码	9.7(1)	对于路由接口，您可以在 31 位子网上为点对点连接配置 IP 地址。31 位子网只包含 2 个地址；通常，该子网中的第一个和最后一个地址预留用于网络和广播，因此，不可使用包含 2 个地址的子网。但是，如果您有点对点连接，并且不需要网络或广播地址，则 31 位子网是在 IPv4 中保留地址的有用方式。例如，2 个 ASA 之间的故障转移链路只需要 2 个地址；该链路一端传输的任何数据包始终由另一端接收，无需广播。您还可以拥有运行 SNMP 或系统日志的一个直连管理站。网桥组或组播路由的 BVI 不支持此功能。 修改了以下命令：**ip address**、**http**、**logging host**、**snmp-server**、**ssh**



第 21 章

高级接口配置

本章介绍如何为接口配置 MAC 地址，如何设置最大传输单元 (MTU)，如何设置最大 TCP 分片大小 (TCP MSS)，以及如何允许相同安全级别通信。设置正确的 MTU 和最大 TCP 分片大小是实现最佳网络性能的关键。

- 关于高级接口配置， 第 787 页
- 手动配置 MAC 地址， 第 791 页
- 自动分配 MAC 地址， 第 792 页
- 配置、MTU和 TCP MSS， 第 793 页
- 允许同一安全级别的通信， 第 794 页
- 高级接口配置的历史记录， 第 795 页

关于高级接口配置

本节介绍高级接口设置。

关于 MAC 地址

您可以手动分配 MAC 地址以覆盖默认值。对于多情景模式，您可以自动生成唯一的 MAC 地址（适用于分配给情景的所有接口）和单情景模式（适用于子接口）。.

注释 您可能想要为 ASA 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。

默认 MAC 地址

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。

- VLAN 接口 (Firepower 1010 和 Cisco Secure Firewall 1210/1220) - 路由防火墙模式：所有 VLAN 接口均共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一 MAC 地址，可手动分配 MAC 地址。请参阅手动配置 MAC 地址，第 791 页。

  透明防火墙模式：各 VLAN 接口均有唯一的 MAC 地址。如有需要，您可通过手动分配 MAC 地址覆盖生成的 MAC 地址。请参阅手动配置 MAC 地址，第 791 页。

- EtherChannels（Firepower 型号） - 对于 EtherChannel，属于通道组的所有接口均共享同一 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。

- EtherChannel（ASA 型号）- 端口通道接口使用编号最小的通道组接口 MAC 地址作为端口通道 MAC 地址。或者，您可以为端口通道接口配置 MAC 地址。我们建议在组通道接口成员身份更改时，配置唯一的 MAC 地址。如果删除提供端口通道 MAC 地址的接口，则端口通道 MAC 地址会更改为下一个编号最小的接口，从而导致流量中断。

- 子接口- 物理接口的所有子接口都使用同一个烧录 MAC 地址。您可能想为子接口分配唯一的 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。

自动 MAC 地址

在多情景模式下，自动生成会为分配给情景的所有接口分配唯一的 MAC 地址。

如果您手动分配 MAC 地址，并且同时启用自动生成，则会使用手动分配的 MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址（如果已启用）。

在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，您可以为接口手动设置 MAC 地址。

由于自动生成的地址（使用前缀时）以 A2 开头，因此如果您同时希望使用自动生成，则不能使用以 A2 开头的手动 MAC 地址。

ASA 使用以下格式生成 MAC 地址：

A2*xx.yyzz.zzzz*

其中，*xx.yy* 是用户定义的前缀或根据接口 MAC 地址的最后两个字节自动生成的前缀，*zz.zzzz* 是由 ASA 生成的内部计数器。对于备用 MAC 地址，地址完全相同，但内部计数器会加 1。

如何使用前缀的示例如下：如果将前缀设置为 77，则 ASA 会将 77 转换为十六进制值 004D (*yyxx*)。在 MAC 地址中使用时，该前缀会反转 (*xxyy*)，以便与 ASA 的本地形式匹配：

A2**4D.00***zz.zzzz*

对于前缀 1009 (03F1)，MAC 地址为：

A2**F1.03***zz.zzzz*

注释 没有前缀的MAC地址格式是旧式版本。有关传统格式的详细信息，请参阅命令参考中的**mac-address auto** 命令。

关于 MTU

MTU 指定 ASA 在给定以太网接口上传输的最大帧负载大小。MTU 值是没有以太网报头、VLAN 标记或其他系统开销情况下的帧大小。例如，将 MTU 设置为 1500 时，预期帧大小为 1518 字节（含报头）或 1522 字节（使用 VLAN）。请勿为容纳这些报头而将 MTU 的值设得过高。

对于 VXLAN 或 Geneve，帧中会封装整个以太网数据报，因此新的 IP 数据包更大，需要更大的 MTU：您应该将 ASA VTEP 源接口 MTU 设置为网络 MTU + 54 字节 (对于 VXLAN) 或 + 306 字节 (Geneve)。

路径 MTU 发现

ASA 支持路径 MTU 发现（如 RFC 1191 中所定义），从而使两个主机之间的网络路径中的所有设备均可协调 MTU，以便它们可以标准化路径中的最低 MTU。

默认 MTU

ASA 上的默认 MTU 为 1500 字节。该值不包括 18-22 字节的以太网报头、VLAN 标记和其他开销。

如果在 VTEP 接口上启用 VXLAN，当 MTU 小于 1554 字节时，ASA 会自动将 MTU 提高到 1554 字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的MTU。一般来说，应将 ASA 源接口 MTU 设置为网络 MTU + 54 字节。

MTU 和分段

对于IPv4，如果传出IP数据包大于指定MTU，则该数据包将分为2帧或更多帧。片段在目标处（有时在中间跃点处）重组，而分片可能会导致性能下降。对于 IPv6，通常不允许对数据包进行分段。因此，IP 数据包大小应在 MTU 大小范围内，以避免分片。

对于 TCP 数据包，终端通常使用它们的 MTU 来确定 TCP 最大报文段长度（例如，MTU-40）。如果之后添加额外的 TCP 报头，例如对于站点间的 VPN 隧道，则 TCP MSS 可能需要由隧道传输实体向下调整。请参阅关于 TCP MSS，第 790 页。

对于 UDP 或 ICMP，应用应将 MTU 考虑在内，以避免分段。

注释 只要有内存空间，ASA 就可接收大于所配置的 MTU 的帧。

MTU 和巨型帧

MTU 越大，您能发送的数据包越大。加大数据包可能有利于提高网络效率。请参阅以下准则：

- 与流量路径上的MTU相匹配 - 我们建议将所有ASA接口以及流量路径的其他设备接口上的MTU设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧 - 在启用巨型帧时，MTU 可设置为 9000 字节或更高。最大值取决于型号。

关于 TCP MSS

TCP 最大报文段长度 (MSS) 是 TCP 负载在添加任何 TCP 和 IP 报头前的大小。UDP 数据包不会受到影响。建立连接时，客户端和服务器会在三次握手期间交换 TCP MSS 值。

您可以使用 FlexConfig中的 Sysopt_Basic 对象在 ASA威胁防御 FlexConfig 策略#unique_1025 ；默认情况下，最大 TCP MSS 设置为 1380 字节。当 ASA 需要增加数据包长度以执行 IPsec VPN 封装时，此设置非常有用。不过，对于非 IPsec 终端，应在 ASA 上禁用最大 TCP MSS。

如果设置了 TCP MSS 的最大值，当连接的任一终端请求的 TCP MSS 大于 ASA 中设定的值时，ASA 会使用 ASA 最大值覆盖请求数据包中的 TCP MSS。如果主机或服务器没有请求 TCP MSS，ASA 会假定采用 RFC 793 的默认值 536 字节 (IPv4) 或 1220 字节 (IPv6)，但不会修改数据包。例如，可以将默认 MTU 保留为 1500 字节。如果主机请求的 MSS 为 1500 减去 TCP 和 IP 报头长度，这会将 MSS 设置为 1460。如果 ASA 上的最大 TCP MSS 为 1380（默认值），ASA 会将 TCP 请求数据包中的 MSS 值改为 1380。然后，服务器会发送 1380 字节负载的数据包。然后，ASA 可向数据包中增加最多 120 字节的报头，并且仍然符合 1500 的 MTU 大小。

您还可以配置最小 TCP MSS；如果主机或服务器请求一个非常小的 TCP MSS，则 ASA 可将该值调高。默认情况下，最小 TCP MSS 未启用。

对于流向设备的流量，包括用于 SSL VPN 连接的流量，此设置不适用。ASA 使用 MTU 来推导 TCP MSS：MTU - 40 (IPv4) 或 MTU - 60 (IPv6)。

默认 TCP MSS

默认情况下，ASA 上的最大 TCP MSS 是 1380 字节。此默认值符合 VPN 连接的要求（在 VPN 连接中，报头最多可达到 120 字节）；此值在默认 MTU（1500 字节）范围内。

建议的最大 TCP MSS 设置

默认 TCP MSS 假定 ASA作为 IPv4 IPsec VPN 终端，并且 MTU 为 1500。当 ASA用作 IPv4 IPsec VPN 终端时，它需要为 TCP 和 IP 报头容纳最多 120 个字节。

如果您要更改 MTU 值、使用 IPv6，或者不使用 ASA作为 IPsec VPN 终端，则应更改 TCP MSS 设置（。

请参阅以下准则：

- 正常流量 - 禁用TCP MSS限制，并接受在连接终端之间建立的值。由于连接终端一般是从MTU获得 TCP MSS，因此非 IPsec 数据包通常符合此 TCP MSS。
- IPv4 IPsec 终端流量 - 将最大 TCP MSS 设置为 MTU - 120。例如，如果使用巨帧并将 MTU 设置为 9000，则需要将 TCP MSS 设置为 8880，以利用新 MTU。
- IPv6 IPsec 终端流量 - 将最大 TCP MSS 设置为 MTU - 140。

接口间通信

允许同一安全级别的接口之间相互通信具有以下优势：

- 您可以配置超过 101 个通信接口。

  如果您为每个接口使用不同级别，而且不将任何接口分配到同一安全等级，则仅可以为每个级别（0 到 100）配置一个接口。

- 您希望流量能够在同一安全级别的各接口之间自由流动而无需 ACL。

如果启用同一安全级别接口通信，则仍可以照常配置不同安全级别的接口。

接口内通信（路由防火墙模式）

接口间通信可能对从某一接口流入、却从同一接口流出的 VPN 流量有用。这种情况下，VPN 流量可能未加密，也可能被重新加密以用于另一个 VPN 连接。例如，如果您有一个中心和辐射 VPN 网络，其中 ASA 是中心，远程 VPN 网络是辐射，一个辐射与另一个辐射进行通信，则流量必须流入 ASA，然后再流出，进入另一个辐射。

注释 此功能允许的所有流量仍将受到防火墙规则的制约。务必要小心，不要造成不对称的路由情景，否则可能会导致流量不会流经 ASA。

手动配置 MAC 地址

如果需要手动分配 MAC 地址，可以使用本程序完成。

您可能想要为 ASA 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。

开始之前

在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入 **changeto context** *name* 命令。

过程

步骤 1 进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

步骤 2 向此接口分配专用 MAC 地址：

mac-address*mac_address* [**standby** *mac_address*]

示例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

mac_address 的格式为 H.H.H，其中 H 是 16 位十六进制数字。例如， MAC 地址 00-0C-F1-42-4C-DE 以 000C.F142.4CDE 的形式输入。不得为 MAC 地址设置组播位，即左起第二个十六进制数字不能是奇数。

如果您还要使用自动生成的 MAC 地址，则手动 MAC 地址的前两个字节不能为 A2。

如需与故障转移配合使用，请设置**备用** MAC 地址。如果主用设备发生故障转移，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

自动分配 MAC 地址

本节介绍如何配置 MAC 地址的自动生成。对于多情景模式，此功能将向所有已分配至情景的接口类型分配唯一 MAC 地址。 对于单模式，此功能将向 VLAN 子接口分配唯一 MAC 地址。

开始之前

- 为接口配置**nameif** 命令时，会立即生成新 MAC 地址。如果在配置接口后启用此功能，则在启用之后，会立即为所有接口生成 MAC 地址。如果禁用此功能，则每个接口的 MAC 地址会恢复为默认 MAC 地址。例如，GigabitEthernet0/1 的子接口恢复为使用 GigabitEthernet0/1 的 MAC 地址。
- 在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，您可以为接口手动设置 MAC 地址。
- 对于多情景模式，请在系统执行空间中完成本程序。要从情景更改到系统执行空间，请输入 **changeto system** 命令。

过程

自动向每个接口分配专用 MAC 地址：

mac-address auto [**prefix** *prefix*]

如果未输入前缀， 则 ASA 将根据接口 MAC 地址的最后两个字节自动生成前缀。

如果您手动输入前缀，则 *prefix* 是介于 0 和 65535 之间的十进制值。此前缀会转换为一个四位数的十六进制数字，并用作 MAC 地址的一部分。

示例：

```
ciscoasa(config)# mac-address auto prefix 19
```

配置、MTU和 TCP MSS

开始之前

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入**changeto context** *name* 命令。
- 要将 MTU 增加到 1500 以上，请按照启用巨帧支持（ASA Virtual、ISA 3000），第 665 页启用巨型帧。

过程

步骤 1 设置 MTU。最小值和最大值取决于您的平台。

mtu *interface_name bytes*

示例：

```
ciscoasa(config-if)# mtu inside ?

configure mode commands/options:
  <64-9198>  MTU bytes
ciscoasa(config)# mtu inside 9000
```

默认值为 1500 字节。

注释
为端口通道接口设置 MTU 时，ASA 将设置应用于所有成员接口。

对于支持巨型帧的某些型号，如果为任何接口输入的值大于 1500，则需启用巨型帧支持。请参阅启用巨帧支持（ASA Virtual、ISA 3000），第 665 页。

步骤 2 以字节为单位设置 TCP 最大分片大小，范围在 48 和任何最大值之间：

sysopt connection tcpmss [**minimum**] *bytes*

示例：

```
ciscoasa(config)# sysopt connection tcpmss 8500
```

```
ciscoasa(config)# sysopt connection tcpmss minimum 1290
```

默认值为 1380 字节。您可以禁用此功能，只需将字节数设置为 **0**。

对于 **minimum** 关键字，请将最大分片大小设置为不小于 48 和 65535 之间的字节数。默认情况下，minimum 功能已禁用（设置为 0）。

步骤 3 配置未处理的 TCP 数据段的最大数量。

sysopt connection tcp-max-unprocessed-seg 未处理的网段

示例：

```
ciscoasa(config)# sysopt connection tcp-max-unprocessed-seg 7
```

默认值为 6。范围为 6 到 24。

示例

以下示例将启用巨型帧、增加所有接口上的 MTU 并为非 VPN 流量禁用 TCP MSS（将 TCP MSS 设置为 0，表示无限制）：

```
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 0
```

以下示例将启用巨型帧、增加所有接口上的 MTU，并将 VPN 流量的 TCP MSS 更改为 9078（MTU 减去 120）：

```
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 9078
```

允许同一安全级别的通信

默认情况下，同一个安全级别的接口不能相互通信，而且数据包无法进入和退出同一接口。本节介绍当接口为同一安全级别时如何启用接口间通信。

过程

步骤 1 启用同一安全级别的接口，使接口间可以互相通信：

same-security-traffic permit inter-interface

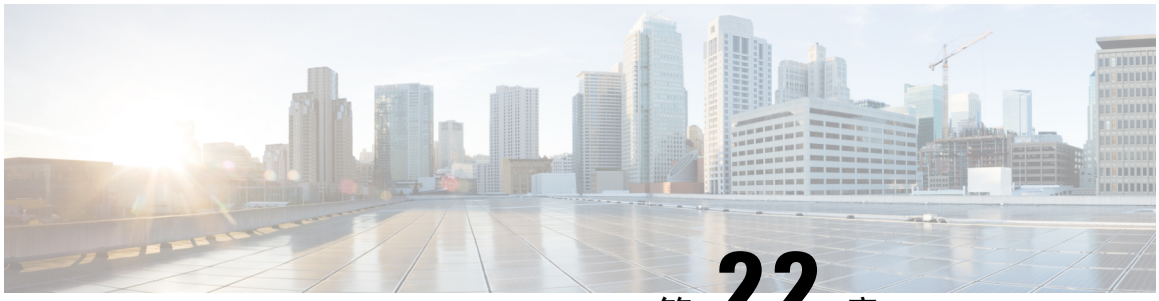
步骤 2 启用连接到同一接口的主机之间的通信：

same-security-traffic permit intra-interface

高级接口配置的历史记录

表 *30:* 高级接口配置的历史记录

功能名称	版本	功能信息
最大 MTU 现为 9198 字节	9.1(6)、9.2(1)	ASA 可使用的最大 MTU 为 9198 字节（通过 CLI 帮助可检查型号的确切限制）。此值不包括第 2 层报头。以前，ASA 允许您将最大 MTU 指定为 65535 字节，这不准确，并可能引发问题。如果您的 MTU 设置为高于 9198 的值，则升级后 MTU 会自动降低。在某些情况下，这种 MTU 变化可能导致 MTU 不匹配；请务必将连接的所有设备设置为使用新的 MTU 值。 修改了以下命令：**mtu**
增加了 Firepower 4100/9300 机箱 上 ASA 的 MTU 大小	9.6(2)	可以在 Firepower 4100 和 9300 上将最大 MTU 设置为 9184 字节；以前，最大值为 9000 字节。FXOS 2.0.1.68 及更高版本中支持此 MTU。 修改了以下命令：**mtu**
单情景模式下的唯一 MAC 地址生成	9.8(3), 9.8(4), 9.9(2)	现在，您可以在单情景模式下启用 VLAN 子接口的唯一 MAC 地址生成。正常情况下，子接口与主接口共享同一 MAC 地址。由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此，此功能将允许唯一的 IPv6 链路本地地址。 新增或修改的命令：**mac-address auto**
可以为 1Gigabit 及更高版本的接口启用或禁用 Cisco Secure Firewall 3100 自动协商。	9.17(1)	可以为 1Gigabit 及更高版本的接口启用或禁用 Cisco Secure Firewall 3100 自动协商。对于其他型号的 SFP 端口， **no speed nonegotiate** 选项将速度设置为 1000 Mbps；新命令意味着您可以独立设置自动协商和速度。 新增/修改的命令： **negotiation-auto**



第 22 章

流量区域

可以向流量区域分配多个接口，流量区域允许现有数据流的流量在该区域内的任何接口上进出ASA。此功能允许 ASA 上的等价多路径 (ECMP) 路由以及对多个接口分担流向 ASA 的外部流量进行负载均衡。

- 关于流量区域， 第 797 页
- 流量区域的前提条件， 第 803 页
- 流量区域准则， 第 804 页
- 配置流量区域， 第 806 页
- 监控流量区域， 第 807 页
- 流量区域示例， 第 809 页
- 流量区域的历史记录， 第 812 页

关于流量区域

本节介绍应如何使用网络中的流量区域。

未分区行为

自适应安全算法在决定是允许还是拒绝流量时会考虑数据包的状态。流量的执行参数之一是流入和流出同一端口的流量。任何流入其他接口的现有流量都将被 ASA 丢弃。

通过流量区域，您可以将多个接口集合在一起，这样流入或流出区域的任意接口的流量都将执行自适应安全算法安全检查。

相关主题

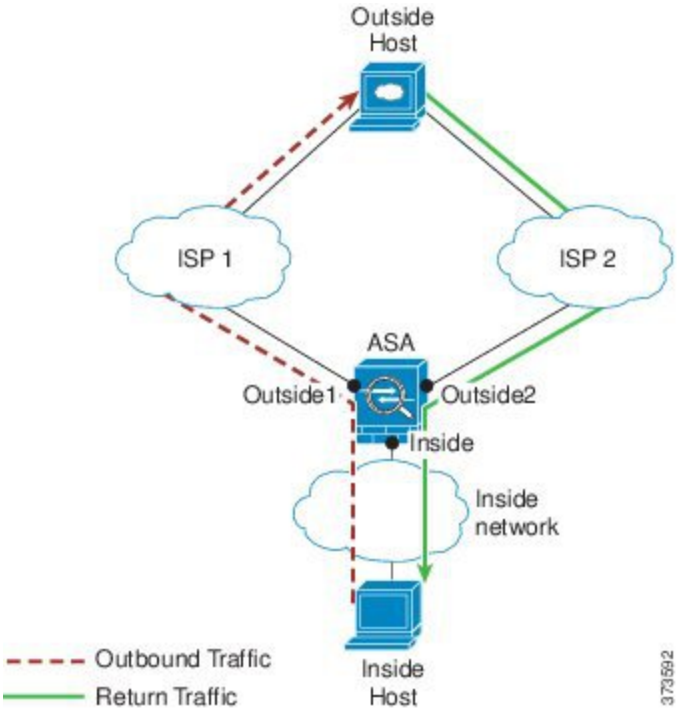
状态监测概述， 第 6 页

为什么使用区域？

您可以使用区域来支持几种路由情景。

非对称路由

在以下场景中，通过 Outside1 接口上的 ISP 1 在内部主机和外部主机之间建立了连接。由于目标网络上的非对称路由，从 Outside2 接口上的 ISP 2 返回已到达的流量。

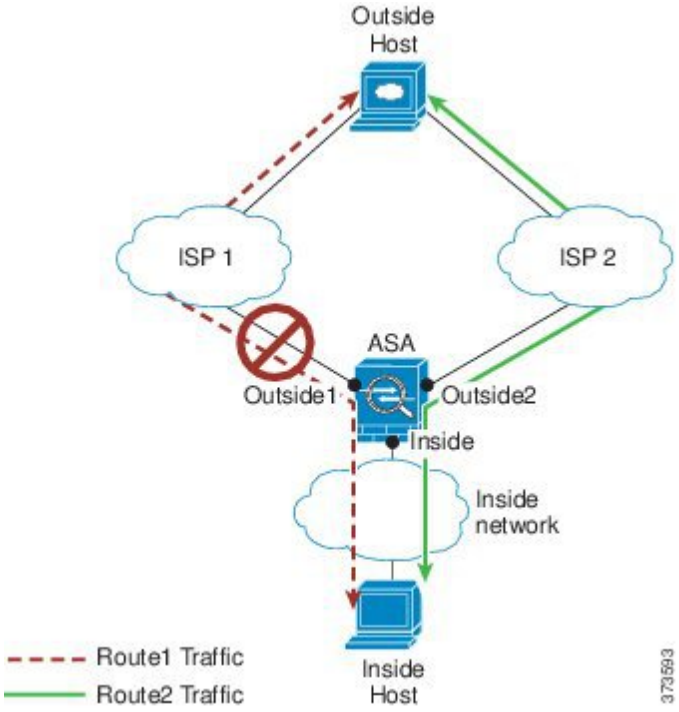


非区域问题：ASA 将为每个接口维护连接表。返回到达 Outside2 的流量时，它不会匹配连接表，并且将被丢弃。对于ASA集群，如果集群包含至同一路由器的多个邻接，则非对称路由可能会造成无法接受的流量损失。

通过划分区域解决问题：ASA 针对每个区域维护连接表。如果您将 Outside1 和 Outside2 集合到一个区域中，当返回到达 Outside2 的流量时，它将匹配每区域连接表，并且允许连接。

丢失的路由

在以下场景中，通过 Outside1 接口上的 ISP 1 在内部主机和外部主机之间建立了连接。由于 Outside1 和 ISP 1 之间的路由已丢失或移动，流量需要通过 ISP 2 采取不同的路由。

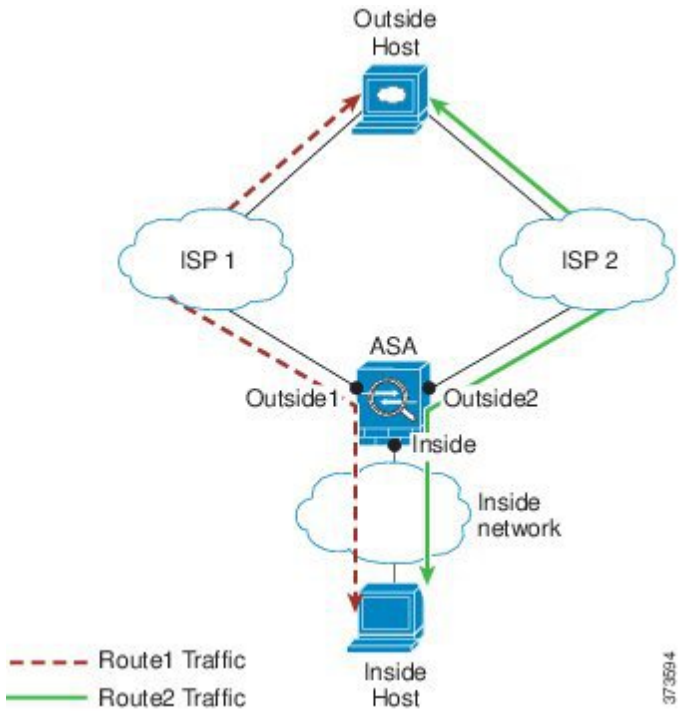


因未划分区域出现的问题：内部主机和外部主机之间的连接将被删除；您必须使用新的次优路由建立新连接。对于 UDP，新路由将在单次丢包之后使用；但对于 TCP，需要重新建立新连接。

区域解决方案：ASA 将检测丢失的路由并通过 ISP 2 切换至新路径的流量。流量将被无缝转发，无任何丢包现象。

负载均衡

在以下场景中，通过 Outside1 接口上的 ISP 1 在内部主机和外部主机之间建立了连接。借助通过 Outside2 上的 ISP 2 的等价路由建立了第二个连接。



因未划分区域出现的问题：无法进行跨接口负载均衡；您只能在一个接口上通过等价路由进行负载均衡。

区域解决方案：ASA 将跨区域内所有接口上的多达八个成本相同的路由实施连接负载均衡。

每区域连接和路由表

ASA维护每区域连接表，使流量能够到达任何一个区域接口。此外，ASA还维护每区域路由表，提供 ECMP 支持。

ECMP 路由

ASA 支持等开销多路径 (ECMP) 路由。

未划分区域的 ECMP 支持

如果没有区域，每个接口最多支持 8 个等价静态或动态路由。例如，您可以在外部接口上配置三个默认路由，指定不同的网关：

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

在这种情况下，流量在外部接口上的 10.1.1.2、10.1.1.3 和 10.1.1.4 之间进行负载均衡。流量基于散列源和目标 IP 地址、传入接口、协议、源与目标端口的算法在 指定网关之间进行分发。

不支持跨多个接口执行 ECMP，因此您不能在不同接口上定义到同一目标的路由。使用上述任一路由配置时，不允许使用以下路由：

```
route outside2 0 0 10.2.1.1
```

划分区域的 ECMP 支持

如果有区域，在一个区域中最多可以跨 8 个接口配置最多 8 个等价静态或动态路由。例如，您可以在区域中跨三个接口配置三个默认路由：

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同样，动态路由协议可以 自动配置等价路由。ASA 使用更稳健的负载均衡机制 跨接口对流量进行负载均衡。

当某条路由丢失时，ASA 将流量无缝 移至其他路由。

如何对连接进行负载均衡

ASA 可以使用数据包六元组（源和目标 IP 地址、源和目标端口、协议和入口接口）构成的散列跨等价路由对连接进行负载均衡。除非路由丢失，否则连接将在其持续时间内在所选接口上保持不中断的状态。

连接中的数据包不会跨路由进行负载均衡；连接只使用一个路由，除非此路由丢失。

ASA 执行负载均衡时，不考虑接口带宽或其他参数。您应确保同一区域中的所有接口都有相同的特性，例如 MTU、带宽等。

用户不能配置负载均衡算法。

回退到另一区域中的路由

当路由在某个接口上丢失时，如果区域中没有其他路由可用，则 ASA 将使用来自其他接口/区域的路由。如果使用此备用路由，可能会发生丢包现象，就像使用未划分区域的路由支持一样。

基于接口的安全策略

区域允许流量进出区域中的任何接口，但安全策略（访问规则、NAT 等）本身仍然应用于每个接口，而非每个区域。如果为区域中的所有接口配置相同的安全策略，则可对该流量成功实施 ECMP 和负载均衡。有关所需并行接口配置的详细信息，请参阅流量区域的前提条件，第 803 页。

流量区域支持的服务

区域支持以下服务：

- 访问规则

- NAT
- 服务规则，QoS 流量管制除外。
- 路由

虽然没有完整的划分区域支持，但您还可以配置流入流量和流出流量，第 802 页中列出的流向设备服务和流出设备服务。

请勿为流量区域中的接口配置其他服务（例如，VPN 或 Botnet 流量过滤器）；它们可能不会按预期运行或扩展。

注释 有关如何配置安全策略的详细信息，请参阅流量区域的前提条件，第 803 页。

安全级别

添加到区域的第一个接口决定区域的安全级别。所有其他接口必须具有相同的安全级别。要更改区域中接口的安全级别，除了一个接口之外，所有其他接口都必须删除，然后更改安全级别，再重新添加接口。

流量的主接口和当前接口

每个连接流都是在初始入口和出口接口的基础上构建的。这些接口是主接口。

如果由于路由更改或非对称路由而使用新的出口接口，则新接口为当前接口。

加入或离开区域

将接口分配到区域时，该接口上的所有连接都会删除。必须重新建立连接。

如果从区域删除某个接口，以该接口为主接口的连接都会删除。必须重新建立连接。如果该接口是当前接口，ASA 会将连接移回主接口。区域路由表也会刷新。

区域内流量

要允许流量进入一个接口，并且从同一区域内的另一接口退出，请启用 **same-security permit intra-interface** 命令（允许流量进出同一接口）以及 **same-security permit inter-interface** 命令（允许流量在同一安全级别的接口之间传送）。否则，流量不能在同一区域中的两个接口之间路由。

流入流量和流出流量

- 您不能向区域添加管理专用接口或管理访问接口。
- 对于区域中常规接口上的管理流量，仅支持对现有流量进行非对称路由；无 ECMP 支持。

- 您只能在一个区域接口上配置管理服务，但要利用非对称路由支持，需要在所有接口上配置管理服务。即使所有接口上的配置是并行的，也不支持 ECMP。
- ASA 在一个区域中支持以下流入服务和流出服务：
  - Telnet
  - SSH
  - HTTPS
  - SNMP
  - 系统日志

区域内重叠的 IP 地址

对于非区域接口，只要正确配置了 NAT，ASA 在接口上使用重叠的 IP 地址网络。但是，不支持同一区域中的接口上的重叠网络。

流量区域的前提条件

- 配置所有接口参数，包括名称、IP 地址和安全级别。注意，安全级别必须匹配区域中的所有接口。您应根据带宽和其他第 2 层属性计划同类接口的集合。
- 配置以下服务以便在所有区域接口上匹配：
  - 访问规则 - 将同一访问规则应用到所有区域成员接口，或者使用全局访问规则。

    例如：

    ```
    access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
    access-group ZONE1 in interface outside1
    access-group ZONE1 in interface outside2
    access-group ZONE1 in interface outside3
    ```

  - NAT - 在区域的所有成员接口上配置相同的 NAT 策略，或者使用全局 NAT 规则（换句话说，使用“any”表示 NAT 规则中的区域接口）。

    不支持接口 PAT。

    例如：

    ```
    object network WEBSERVER1
      host 10.9.9.9 255.255.255.255
      nat (inside,any) static 209.165.201.9
    ```

注释 使用接口特定 NAT 和 PAT 池时，ASA 无法在原始接口发生故障的情况下切换连接。

如果使用的是接口特定 PAT 池，则来自同一主机的多个连接可能会对不同接口进行负载均衡，并使用不同的映射 IP 地址。在此情况下，使用多个并发连接的互联网服务或许无法正确工作。

- 服务规则 - 使用全局服务策略，或向区域中的每个接口分配相同策略。

  不支持 QoS 流量管制。

  例如：

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```

注释 对于 VoIP 检测，区域负载均衡会造成无序数据包增加。发生这种情况的原因是，后面的数据包可能先于前面的采用不同路径的数据包到达ASA。无序数据包的特征包括：

- 中间节点（防火墙和 IDS）和接收端节点（如果使用查询）上的内存利用率更高。
- 视频或语音质量差。

为减少这些影响，我们建议 IP 地址仅用于 VoIP 流量的负载分配。

- 配置路由时着眼于 ECMP 区域功能。

流量区域准则

防火墙模式

仅支持路由防火墙模式。不支持透明防火墙模式或路由模式下的网桥组接口。

故障转移

- 您不能将故障转移或状态链路添加到区域。
- 在主用/主用故障转移模式下，您可以在每个情景中将接口分配给非对称路由 (ASR) 组。此服务允许在对等设备上的类似接口返回的流量恢复到原始设备。您无法在一个情景中同时配置 ASR

组和流量区域。如果在情景中配置一个区域，任何情景接口都不能属于 ASR 组。有关 ASR 组的详细信息，请参阅配置非对称路由数据包支持（主用/主用模式），第 297 页。

- 仅将每个连接的主接口复制到备用设备；不复制当前接口。如果备用设备变为主用状态，它将根据需要分配一个新的当前接口。

集群

- 您不能将集群控制链路添加到区域。

型号准则

不能将 Firepower 1010 和 Cisco Secure Firewall 1210/1220 交换机端口和 VLAN 接口添加到区域。

其他准则

- 您最多可以创建 256 个区域。
- 您可以将以下类型的接口添加到区域：
  - 物理
  - VLAN
  - EtherChannel
- 您不能添加以下类型的接口：
  - 管理专用
  - 管理访问
  - 故障转移或状态链路
  - 集群控制链路
  - EtherChannel中的成员接口
  - VNI；此外，如果常规数据接口被标记为 nve-only，它不能成为区域的成员。
  - BVI，或网桥组成员接口。
- 接口只能是一个区域的成员。
- 每个区域最多可包含 8 个接口。
- 对于 ECMP，在所有区域接口上，每个区域最多可以添加 8 个等价路由。您也可以将单个接口上的多个路由配置为 8 路由限制的一部分。
- 在向区域添加接口时，将删除这些接口的所有静态路由。
- 不能在流量区域内的接口上启用 DHCP 中继。
- 对于负载均衡到单独接口的片段，ASA 不支持分段的数据包重组；这些片段将被丢弃。

- 区域中的接口上不支持 PIM/IGMP 组播路由。

配置流量区域

配置已命名区域，并向该区域分配接口。

过程

步骤 1 添加区域：

zone *name*

示例：

```
zone outside
```

区域名称的最大长度为 48 个字符。

步骤 2 向区域添加接口：

interface *id* **zone-member** *zone_name*

示例：

```
interface gigabitethernet0/0
  zone-member outside
```

步骤 3 向区域添加更多接口；确保它们与您添加的第一个接口具有相同的安全级别。

示例：

```
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

示例

以下示例配置具有 4 个成员接口的外部区域：

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
```

```
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

监控流量区域

本节介绍如何监控流量区域。

区域信息

- **show zone** [*name*]

  显示区域 ID、情景、安全级别和成员。

  请参阅以下所示的 **show zone** 命令的输出：

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

- **show nameif zone**

  显示接口名称和区域名称。

  请参阅以下所示的 **show nameif zone** 命令的输出：

```
ciscoasa# show nameif zone
Interface                Name                   zone-name      Security
GigabitEthernet0/0       inside-1               inside-zone     100
GigabitEthernet0/1.21    inside                 inside-zone     100
GigabitEthernet0/1.31    4                                        0
GigabitEthernet0/2       outside                outside-zone   0
Management0/0            lan                                      0
```

区域连接

- **show conn** [**long** | **detail**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

  show conn zone 命令可显示区域的连接。**long** 和 **detail** 关键字显示建立连接的主接口，括号中的是当前用于转发流量的接口或最后一个数据包来自的接口。因此，在连接来自多个接口的情况下，当前接口会在不同时间显示不同的接口，这取决于 show conn 命令是何时发出的。

  请参阅以下所示的 **show conn long zone** 命令的输出：

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

  显示用于调试的加速安全路径表。

- **show local-host** [**zone** *zone_name* [**zone** *zone_name*] [...]]

  显示区域内本地主机的网络状态。

  请参阅以下所示的 **show local-host zone** 命令的输出。首先列出的是主接口，当前接口用括号括起来。

```
ciscoasa# show local-host zone outside-zone

Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
 TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

区域路由

- **show route zone**

  显示区域接口的路由。

  请参阅以下所示的 **show route zone** 命令的输出：

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

- **show asp table routing**

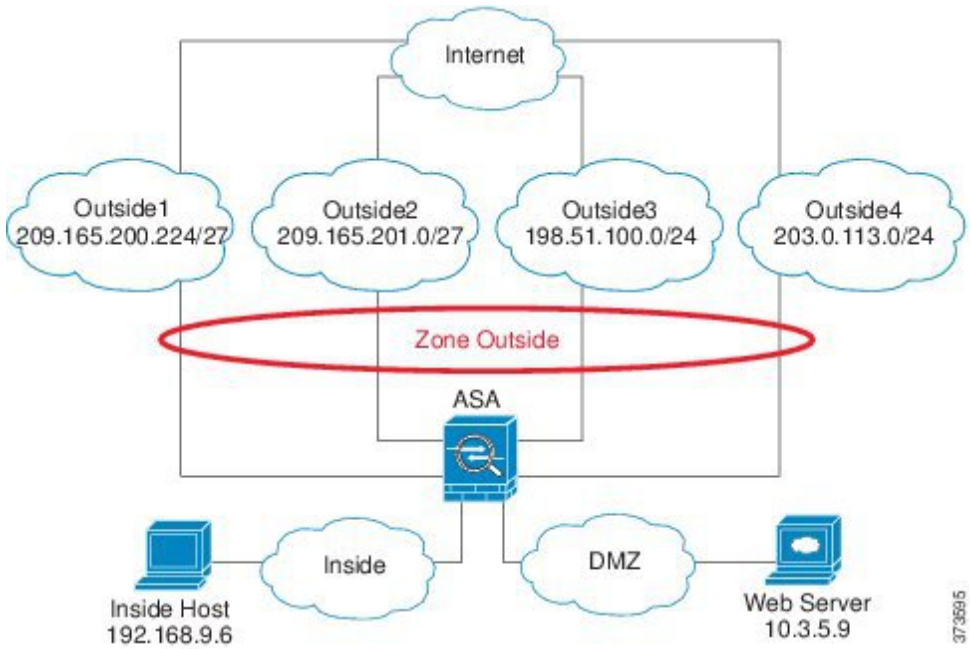
  显示用于调试的加速安全路径表，并显示与每个路由关联的区域。

  请参阅以下所示的 **show asp table routing** 命令的输出：

```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1       255.255.255.255 identity
in   10.2.0.1       255.255.255.255 identity
in   10.6.6.4         255.255.255.255 identity
in   10.4.4.4         255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in   172.0.0.67       255.255.255.255 identity
in   172.0.0.0       255.255.255.0   wan-zone:outside2
in   10.85.43.0      255.255.255.0   via 10.4.0.3 (unresolved, timestamp: 50)
in   10.85.45.0      255.255.255.0   via 10.4.0.20 (unresolved, timestamp: 51)
in   192.168.0.0        255.255.255.0   mgmt
in   192.168.1.0       255.255.0.0     lan-zone:inside
out  255.255.255.255 255.255.255.255 mgmt
out  172.0.0.67       255.255.255.255 mgmt
out  172.0.0.0        255.255.255.0   mgmt
out  10.4.0.0       240.0.0.0       mgmt
out  255.255.255.255 255.255.255.255 lan-zone:inside
out  10.1.0.1       255.255.255.255 lan-zone:inside
out  10.2.0.0       255.255.0.0     lan-zone:inside
out  10.4.0.0       240.0.0.0       lan-zone:inside
```

流量区域示例

以下示例将 4 个 VLAN 接口分配给了外部区域，并且配置了 4 个默认等价路由。为内部接口配置了 PAT，Web 服务器在使用静态 NAT 的 DMZ 接口上可用。




```
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch

zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown
```

```
interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99

# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
```

```
    inspect rtsp
    inspect skinny
    inspect esmtp _default_esmtp_map
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
service-policy global_policy global
```

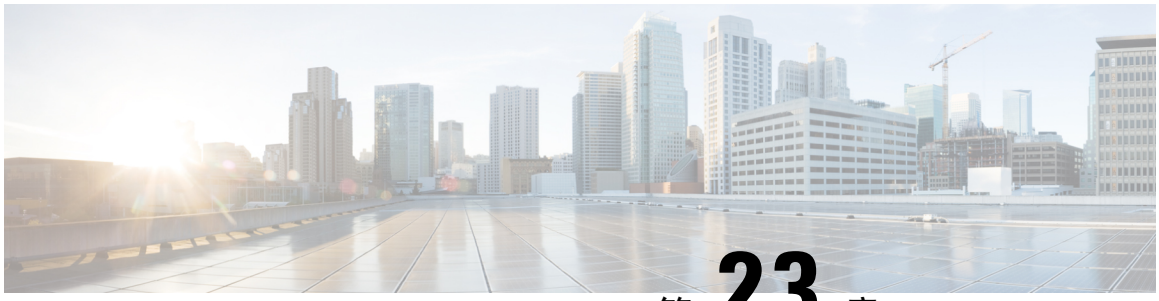
流量区域的历史记录

功能名称	平台版本	说明
流量区域	9.3(2)	您可以将接口集合到一个流量区域以实现流量负载均衡（使用等价多路径 (ECMP) 路由）、路由冗余以及多个接口之间的非对称路由。 注释 您不能将安全策略应用于已命名的区域；安全策略是基于接口的策略。当区域中的接口配置了相同的访问规则、NAT 和服务策略时，负载均衡和非对称路由将能够正常工作。 引入或修改了以下命令：**zone**, **zone-member**、**show running-config zone**、**clear configure zone**、**show zone**、**show asp table zone**、**show nameif zone**、**show conn long**、**show local-host zone**、**show route zone**、**show asp table routing**、**clear conn zone**、**clear local-host zone**。
clear local-host 命令	9.14(1)	已弃用 **clear local-host** 命令及其所有属性和关键字。将会在未来的版本中删除。

第 IV 部分

基本设置

- 基本设置， 第 815 页
- DHCP 和 DDNS 服务， 第 839 页
- 数字证书， 第 865 页
- 的 ARP 检测和 MAC 地址表， 第 905 页



第 23 章

基本设置

本章介绍如何在 ASA 上配置有效配置通常所需的基本设置。

- 设置主机名、域名及启用密码和 Telnet 密码，第 815 页
- 设置日期和时间，第 817 页
- 配置主密码，第 824 页
- 配置 DNS 服务器，第 828 页
- 配置硬件旁路和双重电源（思科 ISA 3000），第 830 页
- 调整 ASP（加速安全路径）性能和行为，第 832 页
- 监控 DNS 缓存，第 834 页
- 基本设置的历史记录，第 834 页

设置主机名、域名及启用密码和 Telnet 密码

要设置主机名、域名及启用密码和 Telnet 密码，请执行以下步骤。

开始之前

在设置主机名、域名及启用密码和 Telnet 密码之前，请检查以下需求：

- 在多情景模式下，可在系统和情景执行空间中配置主机名和域名。
- 启用密码和 Telnet 密码可在每个情景中设置；此类密码在系统中不可用。
- 要从系统切换至情景配置，请输入 **changeto context** *name* 命令。

过程

步骤 1 为 ASA 或情景指定主机名。默认主机名为“asa”。

hostname *name*

示例：

```
ciscoasa(config)# hostname myhostnamexample12345
```

此名称最多可包含63个字符。主机名必须以字母或数字开头和结尾，并且只能包含字母、数字或连字符。

为ASA设置主机名时，该名称将显示在命令行提示符中。如果建立与多台设备的会话，则该主机名有助于跟踪命令输入位置。

对于多情景模式，在系统执行空间中设置的主机名显示在所有情景的命令行提示符中。在情景内选择性设置的主机名不会显示在命令行中，但可供 **banner** 命令 **$(hostname)** 令牌使用。

步骤 2 为 ASA 指定域名。默认域名为 default.domain.invalid。

domain-name *name*

示例：

```
ciscoasa(config)# domain-name example.com
```

ASA会将域名作为后缀追加到不受限定的名称。例如，如果您将域名设置为“example.com”并通过不受限定的名称“jupiter”来指定系统日志服务器，则ASA会将名称限定为“jupiter.example.com”。

步骤 3 更改启用密码。默认情况下，启用密码为空，但第一次输入 **enable** 命令时，系统会提示您更改密码。

enable password *password*

示例：

```
ciscoasa(config)# enable password Pa$$w0rd
```

如果没有配置启用身份验证，则可使用启用密码进入特权 EXEC 模式。如果没有配置 HTTP 身份验证，还可使用启用密码以空白用户名登录 ASDM。

密码 参数是一个区分大小写的密码，长度为 8 到 127 个字符，可以任意组合使用 ASCII 可打印字符（字符代码 32-126），但是以下除外。

- 无空格
- 没有问号
- 不能使用三个或三个以上连续或重复的 ASCII 字符。例如，以下密码将被拒绝：
  - **abc**user1
  - 用户**543**
  - 用户**aaaa**
  - 用户2**666**

该命令可更改最高权限级别 (15) 的密码。如果配置本地命令授权，则可使用以下语法，为从 0 到 15 的每个权限级别设置启用密码：

enable password *password* **level** *number*

encrypted 关键字（在 9.6 和早期版本中，用于 32 个字符或以下的密码）或 **pbkdf2** 关键字（在 9.6 和更高版本中，用于长度超过 32 个字符的密码；在 9.7 和更高版本中，用于所有长度的密码）表示密码已被加密（使用基于 MD5 的散列或 PBKDF2（基于密码的密钥派生功能 2）使用 SHA-512 散列）。请注意，现有密码将继续使用基于 MD5 的散列方法，除非您输入新的密码。当您在 **enable password** 命令中定义密码后，出于安全目的，ASA 会在将其保存到配置时进行加密。输入 **show running-config** 命令后，**enable password**命令不会显示实际密码；它将显示加密的密码，后跟 **encrypted** 或 **pbkdf2** 关键字。例如，如果输入密码“test”，则 **show running-config** 命令输出内容将与以下内容类似：

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

只有在您剪切和粘贴配置文件，以便 在另一 ASA 中使用，而且您使用相同的密码时， 才会真的在 CLI 上输入 **encrypted** 或 **pbkdf2** 关键字。

您无法将密码重置为空值。

步骤 4 为 Telnet 访问设置登录密码。没有默认密码。

未配置 Telnet 身份验证时，登录密码可用于 Telnet 访问。

passwd *password* [**encrypted**]

示例：

```
ciscoasa(config)# passwd cisco12345
```

password 是一个区分大小写的密码，最多由 16 个字母数字和特殊字符组成。可以在密码中使用除问号和空格以外的任意字符。

密码以加密形式保存在配置中，因此在输入原始密码后无法查看原始密码。如果出于某种原因需要将密码复制到另一个 ASA，但不知道原始密码，则可随加密密码和 **encrypted** 关键字一起输入 **passwd** 命令。通常，只能在输入 **showing running-config passwd** 命令时查看该密码。

设置日期和时间

注释 请勿为 Firepower 4100/9300 设置日期和时间；ASA 会从机箱接收这些设置。

设置时区和夏令时日期

要设置时区和夏令时日期范围，请执行以下步骤：

过程

步骤 1 设置时区。默认时区为 UTC。

- Firepower 和 Cisco Secure Firewall 模型：

  clock timezone *zone*

  - *zone* - 输入 **clock timezone ?** 命令以查看可接受的时区名称列表。

  示例：

```
ciscoasa(config)# clock timezone ?
Available timezones:
CET
CST6CDT
Cuba
EET
Egypt
Eire
EST
EST5EDT
Factory
GB
GB-Eire
GMT
GMT0
GMT-0
GMT+0
Greenwich
Hongkong
HST
Iceland
Iran
Israel
Jamaica
Japan
[...]

ciscoasa(config)# clock timezone US/?

configure mode commands/options:
  US/Alaska          US/Aleutian    US/Arizona    US/Central
  US/East-Indiana    US/Eastern     US/Hawaii     US/Indiana-Starke
  US/Michigan        US/Mountain    US/Pacific

ciscoasa(config)# clock timezone US/Mountain
```

- 所有其他型号：

  clock timezone *zone* [-]*hours* [*minutes*]

  - *zone* - 以字符串形式指定时区，例如 PST 表示太平洋标准时间。
  - [-]*hours* - 设置与 UTC 偏离的小时数。例如，PST 为 -8 小时。
  - *minutes* - 设置与 UTC 偏离的分钟数。

示例：

```
ciscoasa(config)# clock timezone PST -8
```

步骤 2 (ASA virtual和 ISA 3000) 输入以下命令之一，以更改夏令时日期范围的默认值。默认的循环日期范围是从三月第二个星期日的凌晨 2:00 到十一月第一个星期日的凌晨 2:00。

- 设置夏令时开始和结束日期，作为特定年份中的特定日期。如果使用此命令，则需要每年重置日期。

  clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]

  - *zone* - 以字符串形式指定时区， 例如 PDT 表示太平洋夏令时。
  - *day* - 设置一月中的第几天，从 1 到 31。例如，日期和月份也可输入为“April 1 或 1 April，具体取决于标准日期格式。
  - *month* - 以字符串形式设置月份。例如，日期和月份也可输入为“April 1 或 1 April，具体取决于标准日期格式。
  - *year* - 以四位数字格式设置年份，例如，2004。年份范围为 1993 至 2035。
  - *hh:mm* - 以 24 小时制设置小时和分钟。
  - *offset* - 设置要为夏令时更改的分钟数。默认情况下，该值为 60 分钟。

  示例：

  ```
  ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60
  ```

- 以某月某日某一时间，而非某年中的特定日期这种形式，指定夏令时的开始和结束日期。此命令可供您设置循环日期范围，无需每年更改。

  clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

  - *zone* - 以字符串形式指定时区， 例如 PDT 表示太平洋夏令时。
  - *week* - 用 1 到 4 之间的整数或“first”或“last”这样的词指定某月中的第几周。例如，如果某天刚好跨在第五周，则用“last”来指定。
  - *weekday* - 指定星期几：星期一、星期二、星期三等等。
  - *month* - 以字符串形式设置月份。
  - *hh:mm* - 以 24 小时制设置小时和分钟。
  - *offset* - 设置要为夏令时更改的分钟数。默认情况下，该值为 60 分钟。

  示例：

```
ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60
```

使用 NTP 服务器设置日期和时间

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，例如验证CRL，其包括精确时间戳。可配置多个NTP服务器。ASA选择层级最低的服务器，作为衡量数据可靠性的方式。

NTP 服务器生成的时间将覆盖手动设置的任何时间。

ASA 支持 NTPv4。

开始之前

在多情景模式下，只能在系统配置中设置时间。

过程

步骤 1 （可选） 启用 服务器身份验证。

a) 启用身份验证。

ntp authenticate

示例：

```
ciscoasa(config)# ntp authenticate
```

在启用 NTP 身份验证时，还必须在 **ntp trusted-key** 命令中指定一个密钥 ID，并使用 **ntp server key** 命令将该密钥与服务器关联起来。使用 **ntp authentication-key** 命令为该 ID 配置实际密钥。如果您有多台服务器，请为每台服务器配置一个单独的 ID。

b) 指定要作为受信任密钥的身份验证密钥 ID，通过 NTP 服务器进行身份验证必须执行此操作。

ntp trusted-key *key_id*

示例：

```
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
```

key_id 参数为介于 1 和 4294967295 之间的值。可输入多个受信任密钥，供多台服务器使用。

c) 设置 NTP 服务器身份验证密钥。

ntp authentication-key *key_id* {**md5** | **sha1** | **sha256** | **sha512** | **cmac**} *key*

示例：

```
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey1
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
```

- *key_id* - 使用 **ntp trusted-key** 命令设置您设置的 ID。
- {**md5** | **sha1** | **sha256** | **sha512** | **cmac**} - 设置算法。
- *key* - 将 密钥设置为最长 32 个字符的字符串。

步骤 2 标识 NTP 服务器。

ntp server {*ipv4_address* | *ipv6_address* }[**key** *key_id*] [**source** *interface_name*] [**prefer**]

示例：

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp server 2001:DB8::178 key 3
ciscoasa(config)# ntp server 2001:DB8::8945:ABCD key 4
```

如果您启用了 NTP 身份验证 (**ntp authenticate**)，则必须使用通过 **ntp trusted-key** 命令设定的 ID 指定 **key***key_id* 参数。

source *interface_name* 关键字参数对标识 NTP 数据包的传出接口（如果不想使用路由表中的默认接口）。由于在多情景模式下系统不包含任何接口，请指定在管理情景中定义的接口名称。

如果多台服务器的准确度相似，**prefer** 关键字将此 NTP 服务器设置为首选服务器。NTP 使用一种算法确定最准确的服务器，然后与该服务器同步。如果多台服务器的准确度相似，**prefer** 关键字将指定使用这些服务器中的哪台服务器。但是，如果某台服务器的准确度明显高于首选服务器，则 ASA 将使用这台更准确的服务器。例如，ASA 使用 2 层服务器，而不使用作为首选服务器的 3 层服务器。

可确定多台服务器；ASA 会使用最准确的服务器。

手动设置日期和时间

要手动设置日期和时间，请执行以下步骤：

开始之前

在多情景模式下，只能在系统配置中设置时间。

过程

手动设置日期时间。

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

示例：

```
ciscoasa# clock set 20:54:00 april 1 2004
```

hh:::参数以 24 小时制设置小时、分钟和秒。例如，输入 20:54:00 表示下午 8:54。

day 值设置月中的日期，范围为 1 到 31。例如，可用 april 1 或 1 april 形式输入月份和日期，具体取决于标准日期格式。

month 值设置月份。根据标准日期格式，可用 april 1 或 1 april 形式输入月份和日期。

year 值使用四位数字设置年份，例如 2004。有效范围为 1993 到 2035。

默认时区为 UTC。如果在输入 **clock set** 命令后使用 **clock timezone** 命令更改时区，时间将自动调整为新的时区。

此命令将时间设置在硬件芯片中，不在配置文件中保存时间。该时间保持至重新启动为止。与其他 **clock** 命令不同，此命令为特权 EXEC 命令。要重置时钟，您需要使用 clock set 命令设置新的时间。

配置精确时间协议 (ISA 3000)

精确时间协议 (PTP) 是一种时间同步协议，用于在基于数据包的网络中同步各种设备的时钟。这些设备时钟通常具有不同的精度和稳定性。该协议专为工业联网测量和控制系统设计，而且最适合用于分布式系统，因为其需要极少的带宽和处理开销。

PTP 系统是一个分布式联网系统，包含 PTP 设备和非 PTP 设备的组合。PTP 设备包含常见的时钟、边界时钟和透明时钟。非 PTP 设备包含网络交换机、路由器和其他基础设施设备。

可以将 ASA 设备配置为透明时钟。ASA 设备不会将其时钟与 PTP 时钟同步。ASA 设备将使用 PTP 默认配置文件，如 PTP 时钟上所定义。

当您配置 PTP 设备时，需要为要一起运行的设备定义一个域编号。因此，您可以配置多个 PTP 域，然后将每个非 PTP 设备配置为使用一个特定域的 PTP 时钟。

开始之前

- 此功能在 ISA 3000 上不可用。
- 仅在单情景模式下支持使用 PTP。
- 思科 PTP 仅支持组播 PTP 消息。

- 默认情况下，在透明模式下对所有 ISA 3000 接口启用 PTP。在路由模式下，必须添加必要的配置以确保允许 PTP 数据包通过设备。
- PTP 仅可用于 IPv4 网络，不可用于 IPv6 网络。
- 物理以太网接口支持 PTP 配置，无论是独立式还是网桥组成员。它在以下对象上不受支持：
  - 管理接口。
  - 子接口、EtherChannel、BVI 或任何其他虚拟接口。
- 假如父接口上具有适当的 PTP 配置，则支持 VLAN 子接口上的 PTP 流。
- 必须确保允许 PTP 数据包通过设备。在透明防火墙模式下，默认会配置访问列表以允许 PTP 流量。PTP 流量由 UDP 端口 319 和 320 以及目标 IP 地址 224.0.1.129 标识，因此在路由防火墙模式下，允许此流量的任何 ACL 都可接受。
- 在路由防火墙模式下，您还必须为 PTP 组播组启用组播路由：
  - 进入全局配置模式命令 **multicast-routing**。
  - 对于在其上启用了 PTP，且不是网桥组成员的每个接口，请输入接口配置命令 **igmp join-group 224.0.1.129** 以静态启用 PTP 组播组成员身份。桥接组成员不支持或不需要使用此命令。

过程

步骤 1 指定 设备的所有端口的域编号：

ptp domain *domain_num*

示例：

```
ciscoasa(config)# ptp domain 54
```

domain_num 参数是设备上所有端口的域编号。在其他域中接收的数据包将像正常组播数据包一样处理，不会进行任何 PTP 处理。该值可以从 0 到 255；默认值为 0。输入在网络中的 PTP 设备上配置的域编号。

步骤 2 （可选）在设备上配置 PTP 时钟模式：

ptp mode e2etransparent

示例：

```
ciscoasa(config)# ptp mode e2etransparent
```

此命令可在所有启用 PTP 的接口上启用端到端透明模式。

步骤 3 在接口上启用 PTP：

ptp enable

在系统可用于联系至配置的域中 PTP 时钟的每个接口上启用 PTP。

示例：

```
ciscoasa(config)# interface gigabitethernet1/2
ciscoasa(config-if)# ptp enable
```

配置主密码

主密码可供您用加密格式安全地存储纯文本密码，并提供一个对所有密码进行加密或掩蔽的通用密钥，而无需更改任何功能。使用主密码的功能包括：

- OSPF
- EIGRP
- VPN 负载均衡
- VPN（远程访问和站点间）
- 故障转移
- AAA 服务器
- 日志记录
- 共享许可证

添加或更改主密码

如要添加或更改主密码，请执行以下步骤。

开始之前

- 该程序只能在安全会话中进行，例如通过控制台、SSH 或通过 HTTPS 连接 ASDM。
- 如果已启用故障转移，但未设置故障转移共享密钥，则在更改主密码时会显示错误消息，通知您必须输入故障转移共享密钥，以防主密码更改以纯文本形式发送。
- 在主用/备用故障转移中启用或更改密码加密会导致 **write standby**，这会将主用配置复制到备用设备。如果不进行此复制操作，即使主用设备和备用设备使用相同的密码，备用设备上经过加密的密码也不会不同；配置复制可确保两者的配置相同。对于主用/主用故障转移，您必须手动输入 **write standby**。**write standby** 可能导致主用/主用模式下出现流量中断，因为辅助设备上的配置在同步新配置之前已被清除。您应该使用 **failover active group 1** 和 **failover active group 2** 命令激活主 ASA 上的所有情景，输入 **write standby**，然后使用 **no failover active group 2** 命令将第 2 组情景还原到辅助设备。

过程

步骤 1 设置用于生成加密密钥的密码。密码的长度必须介于 8 和 128 个字符之间。除退格符号和双引号之外的所有字符都可用于密码。如果未在命令中输入新密码，则系统会提示您输入。要更改密码，必须输入原密码。

key config-key password-encryption [*new_passphrase* [*old_passphrase*]]

示例：

```
ciscoasa(config)# key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
```

注释
使用交互式提示用户输入密码，以避免密码被记录在命令历史缓冲区。

请谨慎使用 **no key config-key password-encrypt** 命令，因为该命令会将加密密码更改为纯文本密码。降级至不支持密码加密的软件版本时，可使用该命令的 **no** 形式。

步骤 2 启用密码加密。

password encryption aes

示例：

```
ciscoasa(config)# password encryption aes
```

只要启用密码加密且有可用的主密码，所有用户密码均将被加密。运行的配置将以加密格式显示密码。

如果启用密码加密时未配置密码，则该命令将预期该密码在未来可用。

如果稍后使用 **no password encryption aes** 命令禁用密码加密，所有现有加密密码将保持不变，并且只要主密码存在，加密密码就会根据应用要求被解密。

步骤 3 保存主密码的运行时值和生成的配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

如果未输入此命令，启动配置中的密码可能仍然可见（如果此前未加密保存）。此外，在多情景模式下，主密码在系统情景配置中将被更改。因此，所有情景中的密码都将受到影响。如果未在系统情景模式中输入 write memory 命令，但也未在所有用户情景中输入该命令，则用户情景中的加密密码可能会过期。或者，在系统情景中使用 write memory all 命令以保存所有配置。

示例

以下示例显示不存在上一个密钥：

```
ciscoasa(config)# key config-key password-encryption 12345678
```

以下示例显示已存在密钥：

```
ciscoasa(config)# key config-key password-encryption 23456789
Old key: 12345678
```

在以下示例中，输入不包含参数的命令，以便系统提示您输入密钥。由于密钥已经存在，系统将提示您输入。

```
ciscoasa(config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

在以下示例中，因为不存在密钥，所以系统不会提示您提供密钥。

```
ciscoasa(config)# key config-key password-encryption
New key: 12345678
Confirm key: 12345678
```

禁用主密码

禁用主密码可将加密密码恢复为纯文本密码。如果降级为不支持加密密码的以前软件版本，移除密码可能十分有用。

开始之前

- 只有知道当前主密码才能禁用该主密码。请查看删除主密码，第827页，看看是否不知道密码。
- 此程序只能在安全会话中进行；即可通过 Telnet、SSH，或通过 HTTPS 连接 ASDM。

要禁用主密码，请执行以下步骤：

过程

步骤 1 删除主密码。如果未在命令中输入密码，则系统将提示您输入。

no key config-key password-encryption [*old_passphrase*]]

示例：

```
ciscoasa(config)# no key config-key password-encryption

Warning! You have chosen to revert the encrypted passwords to plain text.
This operation will expose passwords in the configuration and therefore
exercise caution while viewing, storing, and copying configuration.

Old key: bumblebee
```

步骤 2 保存主密码的运行时值和生成的配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

包含密码的非易失存储器将被 0xFF 模式擦除并覆盖。

在多情景模式下，主密码在系统情景配置中将被更改。因此，所有情景中的密码都将受到影响。如果未在系统情景模式下输入 write memory 命令，但也未在所有用户情景中输入该命令，则用户情景中的加密密码可能会过期。或者，在系统情景中使用 write memory all 命令以保存所有配置。

删除主密码

无法恢复主密码。如果主密码丢失或未知，则可删除该主密码。

要删除主密码，请执行以下步骤：

过程

步骤 1 删除主密钥和包括加密密码的配置。

write erase

示例：

```
ciscoasa(config)# write erase
```

步骤 2 使用启动配置重新加载 ASA，而不使用任何主密钥或加密密码。

reload

示例：

```
ciscoasa(config)# reload
```

配置 DNS 服务器

需要配置 DNS 服务器，以便 ASA 能够将主机名解析为 IP 地址。还必须配置 DNS 服务器，以在访问规则中使用完全限定域名 (FQDN) 网络对象。

某些ASA功能需要使用DNS服务器按域名访问外部服务器。通过其他功能，例如 **ping** 或 **traceroute** 命令，可输入要 ping 或 traceroute 的名称，而且 ASA 能够通过与 DNS 服务器进行通信来解析名称。许多 SSL VPN 和证书命令也支持名称。

默认情况下，有一个名为 DefaultDNS 的默认 DNS 服务器组。您可以创建多个 DNS 服务器组： 一个组是默认组，而其他组可以与特定域相关联。与 DNS 服务器组关联的域匹配的 DNS 请求将使用该组。例如，如果您希望发往内部 eng.cisco.com 服务器的流量使用内部 DNS 服务器，则可以将 eng.cisco.com 映射到内部 DNS 组。与域映射不匹配的所有 DNS 请求都将使用没有关联域的默认 DNS 服务器组。例如，DefaultDNS 组可以包括外部接口上可用的公共 DNS 服务器，。可为 VPN 隧道组配置其他 DNS 服务器组。有关详细信息，请参阅命令参考中的 **tunnel-group** 命令。

注释 ASA 有限支持使用 DNS 服务器，具体取决于功能。例如，大多数命令要求您输入 IP 地址，只有当手动配置 **name** 命令以将名称与 IP 地址相关联，并使用 names 命令启用名称后，才能够使用名称。

开始之前

确保为启用DNS域名查找所在的任何接口配置合适的路由和访问规则，以便能够到达DNS服务器。

过程

步骤 1 启用 ASA 能够发送 DNS 请求至 DNS 服务器，以对受支持的命令执行名称查找。

dns domain-lookup *interface_name*

如果不在接口上启用 DNS 查找，则 ASA 将不会与该接口上的 DNS 服务器通信。确保在将用于访问 DNS 服务器的所有接口上启用 DNS 查找。

示例：

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns domain-lookup outside
```

步骤 2 创建一个或多个 DNS 服务器组并将服务器添加到组。

a) DNS 服务器组的名称。

dns server-group *name*

要配置默认的 DefaultDNS 服务器组，请指定 DefaultDNS 作为名称。

示例：

```
ciscoasa(config)# dns server-group DefaultDNS
```

b) 为组指定一个或多个 DNS 服务器。

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*] *[interface_name]*

可将六个 IP 地址全部输入同一命令中，用空格分隔，或者也可单独输入每个命令。

（可选）指定 ASA 与服务器通信时使用的 *interface_name*。如果未指定接口，ASA 将检查数据路由表；如果没有匹配项，则会检查仅管理路由表。

ASA 按顺序尝试每台 DNS 服务器，直至收到响应。

示例：

```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6 outside
```

c) （仅对于默认组） 配置附加到主机名的域名（如果主机名不是完全限定名称）。

domain-name *name*

示例：

```
ciscoasa(config-dns-server-group)# domain-name example.com
```

d) （可选） 配置 DNS 服务器组的其他属性。

如果默认设置不适合您的网络，请使用以下命令更改组特征。

- **timeout***seconds* - 尝试下一个 DNS 服务器之前等待的秒数，从 1 到 30 秒。默认值为 2 秒。每次 ASA 重试服务器列表，此超时将加倍。
- **retries***number* - 当 ASA 收不到响应时，重试 DNS 服务器列表的次数，从 0 到 10 次。
- number-DNS条目的最小TTL，以分钟为单位。**expire-entry-timer minutes** 如果到期计时器长于条目的TTL，则TTL增加到到期条目时间值。如果TTL比到期计时器长，则将忽略到期条目时间值：在这种情况下，不会向TTL添加额外时间。到期后，该条目将从DNS查找表中删除。删除条目要求重新编译表，使频繁删除能够增加设备上的处理负载。因为某些 DNS 条目可以有非常短的 TTL（短至 3 秒），所以您能够使用此设置实际上延长 TTL。默认值为1分钟（即，所有分辨率的最小TTL为1分钟）。范围为 1 至 65535 分钟。仅解析 FQDN 网络对象时使用此选项。
- **poll-timer minutes***number* - 将 FQDN 网络/主机对象解析为 IP 地址时使用的轮询周期时间（按分钟计）。仅在防火墙策略中使用 FQDN 对象时才解析这些对象。定时器确定解析的最长时间间隔；DNS 条目的生存时间 (TTL) 值也用于确定更新 IP 地址解析的时间，使各个 FQDN 可以比轮询周期更加频繁地解析。默认设置为 240（4 个小时）。范围为 1 至 65535 分钟。

e) 重复上述步骤添加其他 DNS 服务器组。

步骤 3 （可选） 将域映射到特定 DNS 服务器组。

dns-group-map

dns-to-domain *dns_group_name domain*

您最多可以映射 30 个域。不能将同一域映射到多个 DNS 服务器组，但可以将多个域映射到同一服务器组。请勿将任何域映射到要用于默认值的组（例如，DefaultDNS）。

示例：

```
ciscoasa(config)# dns-group-map
ciscoasa(config-dns-group-map)# dns-to-domain group1 eng.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group1 hr.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group2 example.com
```

步骤 4 指定默认 DNS 组。

dns-group *name*

默认情况下，已指定 DefaultDNS。如果配置了其他组，则可以使用此命令指定其他默认组。默认组的 DNS 组映射中不能有任何关联的域。

示例：

```
ciscoasa(config)# dns-group new_default_group
```

配置硬件旁路和双重电源（思科 ISA 3000）

您可以启用硬件旁路，以使流量在断电期间继续在接口对之间流动。支持的接口对为铜缆 GigabitEthernet 1/1 和 1/2 以及 GigabitEthernet 1/3 和 1/4。当硬件旁路处于活动状态时，不会实施防火墙功能，因此请确保您了解允许流量通过的风险。请参阅以下硬件旁路准则：

- 此功能仅可用于思科 ISA 3000 设备。
- 如果您使用的是光纤以太网型号，则只有铜缆以太网对（GigabitEthernet 1/1 和 1/2）支持硬件绕行。
- 当 ISA 3000 断电并进入硬件旁路模式时，只有支持的接口对可以通信；当使用默认配置时，inside1 <---> inside2 和 outside1 <---> outside2 无法再进行通信。这些接口之间的所有现有连接将会丢失。
- 我们建议您禁用 TCP 序列随机化（如本程序中所述）。如果启用随机化（默认设置），则在激活硬件旁路时需要重新建立 TCP 会话。默认情况下，ISA 3000 会将通过其的 TCP 连接的初始序列号 (ISN) 重写为随机编号。激活硬件旁路时，ISA 3000 不再位于数据路径中，也不会转换序列号；接收客户端会收到意外的序列号并丢弃该连接。即便禁用 TCP 序列随机化后，某些 TCP 连接将也需要重新建立，因为链路在切换期间会临时终止。
- 激活硬件旁路时，硬件旁路接口上的思科 TrustSec 连接会被丢弃。当 ISA 3000 开启及停用硬件旁路时，会重新协商这些连接。

- 当停用硬件旁路及流量恢复通过ISA 3000数据路径时，需要重新建立某些现有的TCP会话，因为链路在切换期间会临时终止。
- 当硬件旁路处于活动状态时，以太网 PHY 会断开连接，因此 ASA 无法确定接口状态。接口可能显示为关闭状态。

对于 ISA 3000 中的双电源，可在 ASA OS 中将双电源建立为预期配置。如果其中一个电源发生故障，ASA会发出报警。默认情况下，ASA需要单一电源，只要其中有一个电源正常工作，它就不会发出报警。

开始之前

- 必须将硬件旁路接口连接到交换机的接入端口。不能将它们连接到中继端口。

过程

步骤 1 配置在断电期间要激活的硬件旁路：

hardware-bypass GigabitEthernet {**1/1-1/2** | **1/3-1/4**} [**sticky**]

示例：

```
ciscoasa(config)# hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
```

sticky 关键字会在电源恢复和设备启动后使设备保持处于硬件旁路模式。在这种情况下，您需要在准备就绪后手动关闭硬件旁路；此选项允许您控制流量何时短暂中断。

步骤 2 手动激活或停用硬件旁路：

[**no**] **hardware-bypass manual GigabitEthernet** {**1/1-1/2** | **1/3-1/4**}

示例：

```
ciscoasa# hardware-bypass manual GigabitEthernet 1/1-1/2
ciscoasa# no hardware-bypass manual GigabitEthernet 1/1-1/2
```

步骤 3 （可选） 将硬件旁路配置为保持活动状态，直到 ASA FirePOWER 模块启动后：

hardware-bypass boot-delay module-up sfr

启用硬件旁路时必须不带 **sticky** 选项，才能运行启动延迟。没有 **hardware-bypass boot-delay** 命令，硬件旁路可能会在 ASA FirePOWER 模块完成启动前处于不活动状态。例如，如果将该模块配置为故障关闭，此情景可能会导致流量被丢弃。

步骤 4 禁用 TCP 序列随机化。此示例显示如何通过向默认配置中添加设置来对所有流量禁用随机化。

policy-map global_policy

class sfrclass

set connection random-sequence-number disable

如果稍后决定将其打开，请将“disable”替换为 **enable**。

步骤 5 作为预期配置建立双重电源：

power-supply dual

步骤 6 保存配置。

write memory

系统启动后硬件旁路的行为由启动配置中的配置设置决定，因此您必须保存运行配置。

调整 ASP（加速安全路径）性能和行为

ASP 是实现层，在此使策略和配置付诸实施。除了在通过思科技术支持中心进行故障排除期间，其他操作均与该层无直接关系。但是，可以调整几项与性能和可靠性相关的行为。

选择规则引擎交易提交模式

默认情况下，当更改基于规则的策略（例如访问规则）时，更改会立即生效。但是，这种即时性将稍微降低性能。在每秒有大量连接的环境下，大型规则列表的性能成本更加明显，例如当ASA每秒处理 18,000 个连接时更改包含 25,000 个规则的策略。

由于规则引擎要编译规则以实现更快的规则查找，所以性能会受到影响。默认情况下，系统在评估连接尝试时也搜索未编译规则，以便能够应用新规则；由于规则未编译，因此搜索需要更长时间。

您可以更改此行为，以便规则引擎在实施规则更改时使用交易模式，并在新规则编译并可用之前继续使用旧规则。通过交易模式，在规则编译期间性能应不会下降。下表解释了行为差异。

模型	编译前	编译中	编译后
默认	匹配原规则。	匹配新规则。 （每秒连接速率降低。）	匹配新规则。
事务性	匹配原规则。	匹配原规则。 （每秒连接速率不受影响。）	匹配新规则。

交易模式的另一个优势是，当替换接口上的 ACL 时，在删除旧的 ACL 和应用新的 ACL 之间没有间隙。该功能减少了可接受连接在操作期间被断开的可能性。

开始之前

- 如果使用 FQDN 对象来处理解析经常变化的主机名，则不建议使用事务提交来处理访问控制规则，因为访问组编译可能会由于DNS的变化而永远无法完全解析。如果仍想使用事务提交，请考虑延长 DNS 失效时间。

- 如果为某种规则类型启用交易模式，则将生成系统日志以标记编译的开始和结束。这些系统日志的编号从 780001 到 780004。

过程

为规则引擎启用交易提交模式：

asp rule-engine transactional-commit *option*

其中，选项包括：

- **access-group** - 全局应用或应用于接口的访问规则。
- **nat** - 网络地址转换规则。

示例：

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

启用 ASP 负载均衡

ASP 负载均衡机制有助于避免以下问题：

- 因偶发的流量高峰而造成溢出
- 因大量流量过度订用特定接口接收环而造成溢出
- 单核无法承受负载的相对严重过载接口接收环造成溢出。

ASP 负载均衡允许多个核心在从单个接口接收环接收的数据包上同步工作。如果系统丢弃数据包，并且 **show cpu** 命令输出远小于 100%，此功能可能在数据包属于许多不相关的连接时有助于提高您的吞吐量。

注释 在 ASA virtual上禁用 ASP 负载均衡。将 DPDK（数据平面开发套件）集成到 ASA virtual的加速安全路径（ASP）中， ASA virtual 在禁用此功能的情况下表现出更好的性能。

过程

步骤 1 启用 ASP 负载均衡的自动打开和关闭：

asp load-balance per-packet auto

步骤 2 手动启用 ASP 负载均衡：

asp load-balance per-packet

ASP 负载均衡在您手动将其禁用之前一直保持启用状态，即使您启用了 **auto** 命令亦是如此。

步骤 3 手动禁用 ASP 负载均衡：

no asp load-balance per-packet

仅当您手动启用了 ASA 负载均衡时，才可以使用此命令。如果您也启用了 **auto** 命令，则系统将恢复为自动启用或禁用 ASP 负载均衡。

监控 DNS 缓存

ASA 提供 DNS 信息的本地缓存，这些信息来自于为某些无客户端 SSL VPN 和证书命令而发送的外部 DNS 查询。首先在本地缓存中查找每个 DNS 转换请求。如果本地缓存中有该信息，则将返回生成的 IP 地址。如果本地缓存无法解析该请求，则将 DNS 查询发送至已配置的各个 DNS 服务器。如果外部 DNS 服务器解析请求，则生成的 IP 地址与其相应的主机名一起存储在本地缓存中。

如需监控 DNS 缓存，请参阅以下命令：

- **show dns-hosts**

  此命令显示 DNS 缓存，其中包括从 DNS 服务器动态获悉的条目以及使用 name 命令手动输入的名称和 IP 地址。

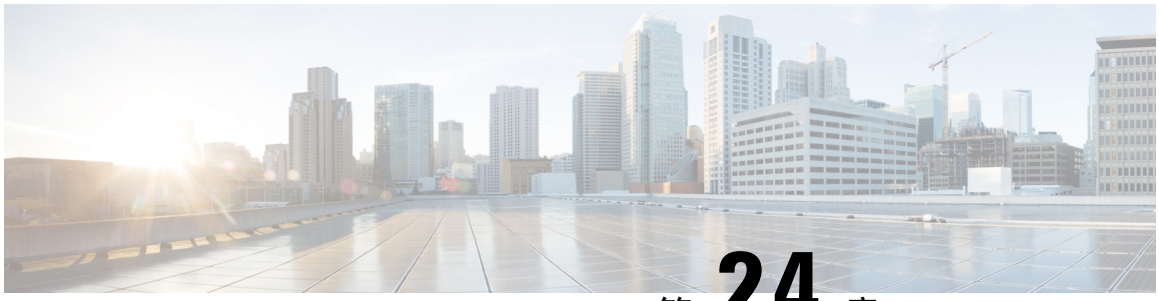
基本设置的历史记录

功能名称	平台版本	说明
多个 DNS 服务器组	9.18(1)	您现在可以使用多个 DNS 服务器组：一个组是默认值，而其他组可以与特定域相关联。与 DNS 服务器组关联的域匹配的 DNS 请求将使用该组。例如，如果您希望发往内部 eng.cisco.com 服务器的流量使用内部 DNS 服务器，则可以将 eng.cisco.com 映射到内部 DNS 组。与域映射不匹配的所有 DNS 请求都将使用没有关联域的默认 DNS 服务器组。例如，DefaultDNS 组可以包括外部接口上可用的公共 DNS 服务器。 新增/修改的命令： **dns-group-map**、**dns-to-domain**
用于网络服务对象域解析的受信任 DNS 服务器。	9.17(1)	您可以指定在解析网络服务对象中的域名时系统应信任的 DNS 服务器。此功能可确保任何 DNS 域名解析都从受信任的来源获取 IP 地址。 新增/修改的命令： **dns trusted-source**、**show dns trusted-source**

功能名称	平台版本	说明
DNS 条目 TTL 行为的更改	9.17(1)	以前，配置的值会添加到每个条目的现有 TTL 中（默认值为 1 分钟）。现在，如果到期计时器长于条目的TTL，则TTL增加到到期条目时间值。如果TTL比到期计时器长，则将忽略到期条目时间值：在这种情况下，不会向TTL添加额外时间。 新增/修改的命令：**expire-entry-timer minutes**
更强的本地用户和启用密码要求	9.17(1)	对于本地用户和启用密码，添加了以下密码要求： • 密码长度 - 至少为 8 个字符。以前，最小值为 3 个字符。 • 重复和连续字符 - 不允许使用三个或三个以上连续的连续或重复 ASCII 字符。例如，以下密码将被拒绝： • **abc**user1 • 用户**543** • 用户**aaaa** • 用户2**666** 新增/修改的命令： **enable password**、**username**
NTPv4 支持	9.14(1)	ASA 现在支持 NTPv4。 未修改任何命令。
额外 NTP 身份验证算法：	9.13(1)	以前，NTP 身份验证仅支持 MD5。现在 ASA 支持以下加密算法： • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC 新增/修改的命令：**ntp authentication-key**
NTP 支持使用 IPv6	9.12(1)	现在，您在设置 NTP 服务器时可以使用 IPv6 地址。 新增/修改的命令：**ntp server**

功能名称	平台版本	说明
现在登录时需要更改 **enable** 密码	9.12(1)	**enable** 默认密码为空。现在，如果您尝试在 ASA 上进入特权 EXEC 模式，系统会要求您将密码改为一个至少包含 3 到 127 个字符的值。而不能将密码留空。**no enable password** 命令今后将不受支持。 在 CLI 中，您可以使用 **enable** 命令、**login** 命令（用户权限级别应在 2 级以上）或者 SSH 或 Telnet 会话（如果启用 **aaa authorization exec auto-enable**）来进入特权 EXEC 模式。无论使用哪种方法，您都必须设置密码。 但是在登录 ASDM 时，则没有这项更改密码的要求。默认情况下，在 ASDM 中，您无需使用用户名和 **enable** 密码即可登录。 新增/修改的命令：**enable password**
在 ASA virtual上禁用 ASP 负载均衡	9.10(1)	将 DPDK（数据平面开发套件）最近集成到 ASA virtual的加速安全路径（ASP）中，ASA virtual 在禁用此功能的情况下表现出更好的性能。
ASA virtual现在支持自动 ASP 负载均衡	9.8(1)	过去只能手动启用和禁用 ASP 负载均衡。 修改了以下命令：**asp load-balance per-packet auto**
对所有本地 **username** 和 **enable** 密码使用 PBKDF2 散列算法	9.7(1)	配置中存储的所有长度的本地 **username** 和 **enable** 密码都将使用 PBKDF2 (基于密码的密钥派生函数 2)使用 SHA-512 的散列算法。以前，32 个字符或以下的密码使用基于 MD5 的哈希处理方法。已经存在的密码仍将继续使用基于 MD5 的哈希值，但您输入的新密码除外。如需下载准则，请参阅一般操作配置指南中的“软件和配置”一章。 修改了以下命令：**enable**、**username**
ISA 3000 支持双电源	9.6(1)	对于 ISA 3000 中的双电源，可在 ASA OS 中将双电源建立为预期配置。如果其中一个电源发生故障，ASA 会发出报警。默认情况下，ASA 需要单一电源，只要其中有一个电源正常工作，它就不会发出报警。 引入了以下命令：**power-supply dual**
本地 **username** 和 **enable** 密码支持更长的密码（最多 127 个字符）	9.6(1)	您现在可以创建最多 127 个字符的本地 **username** 和 **enable** 密码（过去的限制为 32 个字符）。在创建长度超过 32 个字符的密码时，它将使用 PBKDF2（基于密码的密钥派生功能 2）散列存储在配置中。较短的密码将继续使用基于 MD5 的散列处理方法。 修改了以下命令：**enable**、**username**
ISA 3000 硬件旁路	9.4(1.225)	ISA 3000 支持硬件旁路功能，以便在发生断电时允许流量继续通过设备流动。 引入了以下命令：**hardware-bypass**、**hardware-bypass manual**、**hardware-bypass boot-delay**、**show hardware-bypass** *9.5(1)* 版本不提供此功能。

功能名称	平台版本	说明
自动 ASP 负载均衡	9.3(2)	现在可以启用自动开启和关闭 ASP 负载均衡功能。 注释 ASA virtual不支持该自动功能；仅支持手动启用和禁用。 引入了以下命令：**asp load-balance per-packet auto**。
删除默认 Telnet 密码	9.0(2)、9.1(2)	为了提高 ASA 管理访问的安全性，已删除 Telnet 的默认登录密码；使用 Telnet 登录之前必须手动设置密码。 注释 如果不配置 Telnet 用户身份验证，登录密码仅用于 Telent（**aaa authentication telnet console** 命令）。 过去，当清除了密码时，ASA 恢复默认设置“cisco”。现在，当清除密码时，密码也被删除。 登录密码还用于从交换机到 ASASM 的 Telnet 会话（请参阅 **session** 命令）。对于初始 ASASM 访问，必须使用 **service-module session** 命令，直到设置登录密码。 修改了以下命令：**password**
密码加密可见性	8.4(1)	已修改了 **show password encryption** 命令。
主密码	8.3(1)	引入了此功能。主密码可供您用加密格式安全地存储纯文本密码，并提供一个对所有密码进行加密或掩蔽的通用密钥，而无需更改任何功能。 引入了以下命令：**key config-key password-encryption**、**password encryption aes**、**clear configure password encryption aes**、**show running-config password encryption aes**、**show password encryption**



第 24 章

DHCP 和 DDNS 服务

本章介绍如何配置 DHCP 服务器和 DHCP 中继以及动态 DNS (DDNS) 更新方法。

- 关于 DHCP 和 DDNS 服务，第 839 页
- DHCP 和 DDNS 服务准则，第 841 页
- 配置 DHCP 服务器，第 843 页
- 配置 DHCP 中继代理，第 849 页
- 配置动态 DNS，第 852 页
- 监控 DHCP 和 DDNS 服务，第 857 页
- DHCP 和 DDNS 服务的历史记录，第 862 页

关于 DHCP 和 DDNS 服务

以下主题介绍 DHCP 服务器、DHCP 中继代理和 DDNS 更新。

关于 DHCPv4 服务器

DHCP 为 DHCP 客户端提供网络配置参数，如 IP 地址。ASA 可以为连接到 ASA 接口的 DHCP 客户端提供 DHCP 服务器。DHCP 服务器直接为 DHCP 客户端提供网络配置参数。

IPv4 DHCP 客户端使用广播而非组播地址到达服务器。DHCP 客户端侦听 UDP 端口 68 上的消息；DHCP 服务器侦听 UDP 端口 67 上的消息。

DHCP 选项

DHCP 提供用于将配置信息传递至 TCP/IP 网络中主机的标准。配置参数在存储于 DHCP 消息的 Options 字段中的标记项目中携带，数据也称为选项。供应商信息也存储在 Options 中，并且所有供应商信息扩展均可用作 DHCP 选项。

例如，思科 IP 电话从 TFTP 服务器下载其配置。当思科 IP 电话启动时，如果其不让 IP 地址和 TFTP 服务器 IP 地址均得以预配置，则其将向 DHCP 服务器发送带有选项 150 或 66 的请求以获取此信息。

- DHCP 选项 150 提供 TFTP 服务器列表的 IP 地址。
- DHCP 选项 66 提供单一 TFTP 服务器的 IP 地址或主机名。

- DHCP 选项 3 设置默认路由。

单一请求可能同时包括选项 150 和 66。在此情况下，如在 ASA 上已配置这两个选项，则 ASA DHCP 服务器将在响应中为两个选项提供值。

您可以使用高级 DHCP 选项向 DHCP 客户端提供 DNS、WINS 和域名参数；DHCP 选项 15 用于 DNS 域名后缀。也可以使用 DHCP 自动配置设置获得这些值或手动定义这些值。如果使用多种方法定义此信息，则按以下序列将其传递给 DHCP 客户端：

1. 手动配置的设置。
2. 高级 DHCP 选项设置。
3. DHCP 自动配置设置。

例如，可以手动定义要 DHCP 客户端接收的域名，然后启用 DHCP 自动配置。尽管 DHCP 自动配置要结合 DNS 和 WINS 服务器来发现域，但手动定义的域名将与已发现的 DNS 和 WINS 服务器名称一起传递到 DHCP 客户端，因为手动定义的域名将取代通过 DHCP 自动配置过程发现的域名。

关于 DHCPv6 无状态服务器

对于结合前缀授权功能 (启用 IPv6 前缀授权客户端，第 766 页) 使用无状态地址自动配置 (SLAAC) 的客户端，可以来配置 ASA，以便在它们向 ASA 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。ASA 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 ASA 的前缀。

关于 DHCP 中继代理

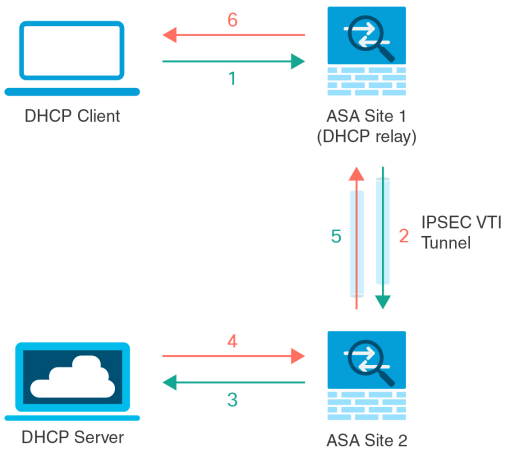
您可以配置 DHCP 中继代理以向一个或多个 DHCP 服务器转发接口上收到的 DHCP 请求。DHCP 客户端使用 UDP 广播发送其初始 DHCPDISCOVER 消息，因为它们没有与其所连接网络有关的信息。如果客户端位于不包含服务器的网段，则通常 UDP 广播不会由 ASA 进行转发，因为它不转发广播流量。DHCP 中继代理可用于配置用来接收广播的 ASA 的接口，以将 DHCP 请求转发至另一接口上的 DHCP 服务器。

VTI 上的 DHCP 中继服务器支持

您可以在 ASA 接口上配置 DHCP 中继代理，以在 DHCP 客户端和 DHCP 服务器之间接收和转发 DHCP 消息。但是，不支持通过逻辑接口转发消息的 DHCP 中继服务器。

下图显示了通过 VTI VPN 使用 DHCP 中继的 DHCP 客户端和 DHCP 服务器的发现过程。在 ASA 站点 1 的 VTI 接口上配置的 DHCP 中继代理从 DHCP 客户端接收 DHCPDISCOVER 数据包，并通过 VTI 隧道发送数据包。ASA 站点 2 将 DHCPDISCOVER 数据包转发到 DHCP 服务器。DHCP 服务器使用 DHCPOFFER 向 ASA 站点 2 进行回复。ASA 站点 2 将其转发到 DHCP 中继（ASA 站点 1），后者将其转发到 DHCP 客户端。

图 *72:* 通过 *VTI* 的 *DHCP* 中继服务器



DHCPREQUEST 和 DHCPACK/NACK 要求遵循相同的程序。

DHCP 和 DDNS 服务准则

本节介绍在配置 DHCP 和 DDNS 服务之前应检查的准则和限制。

情景模式

- 多情景模式下不支持 DHCPv6 无状态服务器。

防火墙模式

- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DHCP 中继。
- 在网桥组成员接口上的透明防火墙模式下，支持 DHCP 服务器。 在路由模式下，在 BVI 接口（而非网桥组成员接口）上支持 DHCP 服务器。BVI 必须具有名称，DHCP 服务器才能运行。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DDNS。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下，不支持 DHCPv6 无状态服务器。

集群

- 集群不支持 DHCPv6 无状态服务。

IPv6

支持 IPv6 用于 DHCP 无状态服务器和 DHCP 中继。

DHCPv4 服务器

- 最大可用 DHCP 池为 256 个地址。
- 您可以在具有名称和 IP 地址的任何接口（例如物理接口、子接口或路由模式下的 BVI）上配置 DHCP 服务器。
- 只能在每个接口上配置一个 DHCP 服务器。每个接口均可使用其自己的地址池。但是，其他 DHCP 设置（如 DNS 服务器、域名、选项、ping 超时和 WINS 服务器）以全局方式配置，且供 DHCP 服务器在所有接口上使用。
- 如果某个接口也启用了 DHCP 服务器，则不能将该接口配置为 DHCP 客户端；您必须使用静态 IP 地址。
- 不能在同一设备上同时配置 DHCP 服务器和 DHCP 中继，即使要在不同接口上启用它们也是如此；只能配置一种类型的服务。
- 您可以为接口保留 DHCP 地址。根据客户端的 MAC 地址，ASA 从地址池中将一个具体的 IP 地址分配给 DHCP 客户端。
- ASA 不支持 QIP DHCP 服务器与 DHCP 代理服务组合使用。
- DHCP 服务器不支持 BOOTP 请求。

DHCPv6 服务器

在已配置 DHCPv6 地址、前缀委派客户端或 DHCPv6 中继的接口上，无法配置 DHCPv6 无状态服务器。

DHCP 中继

- ，其中每个接口最多允许 4 台服务器。
- 最多可以配置 10 台 DHCPv6 中继服务器。不支持 IPv6 的接口专用服务器。
- 不能在同一设备上同时配置 DHCP 服务器和 DHCP 中继，即使要在不同接口上启用它们也是如此；只能配置一种类型的服务。
- 在透明防火墙模式下，或在 BVI 或网桥组成员接口上的路由模式下 DHCP 中继服务不可用。但是，可以通过使用访问规则允许 DHCP 流量通过。要允许 DHCP 请求和回复通过 ASA，需要配置两条访问规则，一条允许从内部接口到外部接口（UDP 目标端口 67）的 DCHP 请求，另一条允许来自其他方向（UDP 目标端口 68）的服务器的回复。
- 对于 IPv4，客户端必须直接连接到 ASA 且不能通过另一个中继代理或路由器发送请求。对于 IPv6，ASA支持来自另一个中继服务器的数据包。
- DHCP 客户端必须与 ASA 中继请求的 DHCP 服务器位于不同接口。
- 不能在流量区域内的接口上启用 DHCP 中继。

DDNS 服务

防火墙的 DDNS 仅支持 DynDNS 服务。因此，请确保使用以下语法中的更新 URL 配置 DDNS：

https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**.

配置 DHCP 服务器

本部分介绍如何配置 ASA 提供的 DHCP 服务器。

过程

步骤 1 启用 DHCPv4 服务器，第 843 页。
步骤 2 配置高级 DHCPv4 选项，第 845 页。
步骤 3 配置 DHCPv6 无状态服务器，第 847 页。

启用 DHCPv4 服务器

要在 ASA 接口上启用 DHCP 服务器，请执行以下步骤：

过程

步骤 1 为接口创建一个 DHCP 地址池。ASA 会向客户端分配此池中的一个地址，以供给定时间段内使用。这些地址属于直接连接网络的本地未转换地址。

dhcpd address *ip_address_start-ip_address_end if_name*

示例：

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
```

该地址池必须与 ASA 接口位于同一子网中。在透明模式下，指定桥接组成员接口。在路由模式下，请指定一个路由接口或 BVI；不要指定桥接组成员接口。

步骤 2 （可选）（路由模式）自动配置从运行 DHCP 或 PPPoE 客户端的接口或从 VPN 服务器获取的 DNS、WINS 和域名值。

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

示例：

```
ciscoasa(config)# dhcpd auto_config outside interface inside
```

如果使用以下命令指定 DNS、WINS 或域名参数，则它们将覆盖自动配置获取的参数。

步骤 3 （可选）为客户端保留 DHCP 地址。根据客户端的 MAC 地址，ASA 从配置的地址池中将一个具体的 IP 地址分配给 DHCP 客户端。

dhcpd reserve-address *ip_address mac_address if_name*

示例：

```
ciscoasa(config)# dhcpd reserve-address 10.0.1.109 030c.f142.4cde inside
```

保留的地址必须来自配置的地址池，并且地址池必须与ASA接口位于同一子网上。在透明模式下，指定桥接组成员接口。在路由模式下，请指定一个路由接口或 BVI；不要指定桥接组成员接口。

步骤 4 （可选）指定 DNS 服务器的 IP 地址。

dhcpd dns *dns1* [*dns2*]

示例：

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

步骤 5 （可选）指定 WINS 服务器的 IP 地址。最多可指定两台 WINS 服务器。

dhcpd wins *wins1* [*wins2*]

示例：

```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

步骤 6 （可选）更改要授予客户端的租用时间。租用时间等于租赁到期之前客户端可以使用向其分配的 IP 地址的时间（以秒为单位）。输入一个介于 0 和 1,048,575 之间的值。默认值为 3600 秒。

dhcpd lease *lease_length*

示例：

```
ciscoasa(config)# dhcpd lease 3000
```

步骤 7 （可选）配置域名。

dhcpd domain *domain_name*

示例：

```
ciscoasa(config)# dhcpd domain example.com
```

步骤 8 （可选）配置 ICMP 数据包的 DHCP ping 超时值。为了避免地址冲突，ASA 在将某个地址分配至 DHCP 客户端之前会向该地址发送两个 ICMP ping 数据包。默认值为 50 毫秒。

dhcpd ping timeout *milliseconds*

示例：

```
ciscoasa(config)# dhcpd ping timeout 20
```

步骤 9 定义被发送到 DHCP 客户端的默认网关。对于路由模式，如果未使用 **dhcpd option 3 ip** 命令，ASA 会作为默认网关发送启用 DHCP 服务器的接口 IP 地址。对于透明模式，如果要设置默认网关，必须设置 **dhcpd option 3 ip**；ASA 本身不能用作默认网关。

dhcpd option 3 ip *gateway_ip*

示例：

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

步骤 10 在 ASA 内启用 DHCP 后台守护程序，以在启用的接口上侦听 DHCP 客户端请求。

dhcpd enable *interface_name*

示例：

```
ciscoasa(config)# dhcpd enable inside
```

指定与 **dhcpd address** 范围相同的接口。

配置高级 DHCPv4 选项

ASA 支持 RFC 2132、RFC 2562 和 RFC 5510 中所列的 DHCP 选项以发送信息。所有 DHCP 选项 (1-255) 均受支持，但 1、12、50 – 54、58 – 59、61、67 和 82 除外。

过程

步骤 1 配置返回一个或两个 IP 地址的 DHCP 选项：

dhcpd option *code* **ip** *addr_1* [*addr_2*]

示例：

```
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1
ciscoasa(config)# dhcpd option 3 ip 10.10.1.10
```

选项 150 可为一台或两台 TFTP 服务器提供 IP 地址或名称，以用于思科 IP 电话。选项 3 可为思科 IP 电话设置默认路由。

步骤 2 配置返回文本字符串的 DHCP 选项：

dhcpd option 代码**ascii**文本

示例：

```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

选项 66 可提供 TFTP 服务器的 IP 地址或名称，以用于思科 IP 电话。

步骤 3 配置返回十六进制值的 DHCP 选项。

dhcpd option code hex 值

示例：

```
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11
```

注释
ASA 不验证您提供的选项类型和值是否与 RFC 2132 中定义的选项代码的预期类型和值匹配。例如，可输入 **dhcpd option 46 ascii hello** 命令，尽管 RFC 2132 中定义的选项 46 期望一位数十六进制值，但 ASA 仍将接受配置。有关选项代码及其关联的类型和期望值的详细信息，请参阅 RFC 2132。

下表显示 **dhcpd option** 命令不支持的 DHCP 选项。

表 *31*: 不受支持的 *DHCP* 选项

选项代码	说明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

配置 DHCPv6 无状态服务器

对于配合使用无状态地址自动配置 (SLAAC) 及前缀代理功能 (启用 IPv6 前缀授权客户端，第 766 页) 的客户端，可以将 ASA 配置为在客户端向 ASA 发送信息请求 (IR) 数据包时提供 DNS 服务器或域名等信息。ASA 仅接受 IR 数据包，不向客户端分配地址。您将通过在客户端上启用 IPv6 自动配置来配置客户端，以便生成自己的 IPv6 地址。在客户端上启用无状态自动配置时，将基于路由器通告消息中接收到的前缀来配置 IPv6 地址；换句话说，根据使用前缀授权收到 ASA 的前缀。

开始之前

此功能仅支持单一路由模式。此功能不支持集群。

过程

步骤 1 配置包含您希望 DHCPv6 服务器提供的信息的 IPv6 DHCP 池：

ipv6 dhcp pool *pool_name*

示例：

```
ciscoasa(config)# ipv6 dhcp pool Inside-Pool
ciscoasa(config)#
```

如果需要，可以为每个接口配置单独的池，也可以在多个接口上使用相同的池。

步骤 2 配置以下要提供给客户端的一个或多个参数以响应 IR 消息：

dns-server *dns_ipv6_address*

domain-name *domain_name*

nis address *nis_ipv6_address*

nis domain-name *nis_domain_name*

nisp address *nisp_ipv6_address*

nisp domain-name *nisp_domain_name*

sip address *sip_ipv6_address*

sip domain-name *sip_domain_name*

sntp address *sntp_ipv6_address*

{[] [] [] [] [] [] [] [] []} **importdns-serverdomain-namenis addressnis domain-namenisp addressnisp domain-namesip addresssip domain-namesntp address**

示例：

```
ciscoasa(config-dhcpv6)# domain-name example.com
ciscoasa(config-dhcpv6)# import dns-server
```

import 命令使用 ASA 在前缀代理客户端接口上从 DHCPv6 服务器获取的一个或多个参数。您可以混合搭配手动配置的参数与导入的参数；但是手动配置的参数与使用 **import** 命令配置的参数不能相同。

步骤 3 对于您希望 ASA 在其上侦听 IR 消息的接口，进入接口配置模式：

interface *id*

示例：

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

步骤 4 启用 DHCPv6 服务器：

ipv6 dhcp server *pool_name*

示例：

```
ciscoasa(config-if)# ipv6 dhcp server Inside-Pool
ciscoasa(config-if)#
```

步骤 5 配置路由器通告以通知 SLAAC 客户端有关 DHCPv6 服务器的信息：

ipv6 nd other-config-flag

此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。

示例

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
  domain-name eng.example.com
  import dns-server
ipv6 dhcp pool IT-Pool
  domain-name it.example.com
  import dns-server
interface gigabitethernet 0/0
  ipv6 address dhcp setroute default
  ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ipv6 dhcp server Eng-Pool
  ipv6 nd other-config-flag
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
  ipv6 dhcp server IT-Pool
  ipv6 nd other-config-flag
```

配置 DHCP 中继代理

在 DHCP 请求进入接口后，ASA 中继将请求转发到的 DHCP 服务器取决于您的配置。您可以配置以下类型的服务器：

- 接口专用 DHCP 服务器 - DHCP 请求进入特定接口后，ASA 仅向接口专用服务器中继请求。
- 全局 DHCP 服务器 - DHCP 请求进入未让接口专用服务器得以配置的接口后，ASA 将向所有全局服务器中继请求。如果接口有接口专用服务器，则将不使用全局服务器。

配置 DHCPv4 中继代理

当 DHCP 请求进入接口时，ASA 将向所有 DHCP 服务器中继该请求。

过程

步骤 1 执行以下两项操作或其中之一：

- 指定一个全局 DHCP 服务器 IP 地址及到达该地址所经过的接口。

  dhcprelay server *ip_address if_name*

  示例：

```
ciscoasa(config)# dhcprelay server 209.165.201.5 outside
ciscoasa(config)# dhcprelay server 209.165.201.8 outside
ciscoasa(config)# dhcprelay server 209.165.202.150 it
```

- 指定连接到 DHCP 客户端网络的接口 ID 以及要用于进入该接口的 DHCP 请求的 DHCP 服务器 IP 地址。

```
interface interface_id
  dhcprelay server ip_address
```

  示例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config)# dhcprelay server 209.165.201.6
ciscoasa(config)# dhcprelay server 209.165.201.7
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config)# dhcprelay server 209.165.202.155
ciscoasa(config)# dhcprelay server 209.165.202.156
```

  请注意，您没有使用全局 **dhcprelay server** 命令为这些请求指定出口接口；而 ASA 使用路由表确定出口接口。

步骤 2 在与 DHCP 客户端相连的接口上启用 DHCP 中继服务。您可以在多个接口上启用 DHCP 中继。

dhcprelay enable 接口

示例：

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# dhcprelay enable dmz
ciscoasa(config)# dhcprelay enable eng1
ciscoasa(config)# dhcprelay enable eng2
ciscoasa(config)# dhcprelay enable mktg
```

步骤 3 （可选）设置为 DHCP 中继地址处理预留的秒数。

dhcprelay timeout 秒

示例：

```
ciscoasa(config)# dhcprelay timeout 25
```

步骤 4 （可选）更改从 DHCP 服务器发送至 ASA 接口地址的数据包中的第一个默认路由器地址。

dhcprelay setroute *interface_name*

示例：

```
ciscoasa(config)# dhcprelay setroute inside
```

此操作允许客户端将其默认路由器设置为指向 ASA，即使 DHCP 服务器指定了其他路由器亦是如此。

如果数据包中没有默认的路由器选项，则 ASA 会添加一个包含接口地址的路由器选项。

步骤 5 （可选）将接口配置为受信任接口。执行以下操作之一：

- 指定您要信任的 DHCP 客户端接口：

  ```
  interface interface_id
    dhcprelay information trusted
  ```

  示例：

  ```
  ciscoasa(config)# interface gigabitethernet 0/0
  ciscoasa(config-if)# dhcprelay information trusted
  ```

  您可以将接口配置为受信任接口以保留 DHCP Option 82。下游交换机和路由器使用 DHCP 选项 82 进行 DHCP 探听和 IP 源保护。通常，如果 ASA DHCP 中继代理收到已设置选项 82 的 DHCP 数据包，但 giaddr 字段（指定在向服务器转发数据包之前由中继代理设置的 DHCP 中继代理地址）设置为 0，则 ASA 默认将丢弃该数据包。现在可以保留选项 82 并通过将接口标识为受信任接口而转发数据包。

- 将所有客户端接口配置为受信任接口。

dhcprelay information trust-all

示例：

```
ciscoasa(config)# dhcprelay information trust-all
```

配置 DHCPv6 中继代理

当 DHCPv6 请求进入接口时，ASA 将向所有 DHCPv6 全局服务器中继该请求。

过程

步骤 1 指定客户端消息转发到的 IPv6 DHCP 服务器目标地址。

ipv6 dhcprelay server *ipv6_address* [*interface*]

示例：

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
```

ipv6-address 参数可以是链路范围的单播、组播、站点范围单播或全局 IPv6 地址。不允许将未指定、环回和本地节点组播地址用作中继目标。可选 *interface* 参数为目标指定输出接口。客户端消息通过输出接口连接的链路转发到目标地址。如果指定地址属于链路范围地址，则必须指定接口。

步骤 2 在接口上启用 DHCPv6 中继服务。

ipv6 dhcprelay enable 接口

示例：

```
ciscoasa(config)# ipv6 dhcprelay enable inside
```

步骤 3 （可选）指定响应通过中继地址处理中继绑定从 DHCPv6 服务器传递至 DHCPv6 客户端所允许的时间量（以秒为单位）。

ipv6 dhcprelay timeout 秒

示例：

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

seconds 参数的有效值范围为 1 到 3600。默认值为 60 秒。

配置动态 DNS

当接口使用 DHCP IP 寻址时，分配的 IP 地址可以在续约 DHCP 租用时更改。当需要使用完全限定域名 (FQDN) 访问接口时，更改 IP 地址可能导致 DNS 服务器资源记录 (RR) 失效。动态 DNS (DDNS) 提供一种机制，会在 IP 地址或主机名更改时更新 DNS RR。您还可以将 DDNS 用于静态或 PPPoE IP 寻址。

DDNS 在 DNS 服务器上更新以下 RR：A RR 包括名称到 IP 地址的映射，而 PTR RR 将地址映射到名称。

ASA 支持以下 DDNS 更新方法：

- 标准 DDNS，即标准 DDNS 更新方法由 RFC 2136 定义。

  通过此方法，ASA 和 DHCP 服务器使用 DNS 请求更新 DNS RR。ASA 或 DHCP 服务器向其本地 DNS 服务器发送 DNS 请求以获取有关主机名的信息，并根据响应确定拥有 RR 的主 DNS 服务器。然后，ASA 或 DHCP 服务器直接向主 DNS 服务器发送更新请求。请参阅以下典型场景。

  - ASA 更新 A RR，而 DHCP 服务器更新 PTR RR。

    通常情况下，ASA“拥有”A RR，而 DHCP 服务器“拥有”PTR RR，因此两个实体需要单独请求更新。当 IP 地址或主机名更改时，ASA 将向 DHCP 服务器发送 DHCP 请求（包括 FQDN 选项），以通知它需要请求 PTR RR 更新。

  - DHCP 服务器既更新 A，也更新 PTR RR。

    如果 ASA 无权更新 A RR，请使用此场景。当 IP 地址或主机名更改时，ASA 将向 DHCP 服务器发送 DHCP 请求（包括 FQDN 选项），以通知它需要请求 A 和 PTR RR 更新。

  您可以根据安全需求和主 DNS 服务器的要求配置不同的所有权。例如，对于静态地址，ASA 应拥有两个记录的更新。

- Web - Web 更新方法使用使用 DynDNS 远程 API 规范 (https://help.dyn.com/remote-access-api/) 的任何 DDNS 服务器。

  使用此方法，当 IP 地址或主机名更改时，ASA 会直接向您拥有帐户的 DNS 提供商发送 HTTP 请求。

注释 BVI 或网桥组成员接口上不支持使用 DDNS。

开始之前

- 依次选择**配置** > **设备管理** > **DNS** > **DNS 客户端** 配置 DNS 服务器。请参阅 配置 DNS 服务器，第 828 页。
- 依次选择**配置** > **设备设置** > **设备名称/密码**，配置设备主机名和域名。请参阅 设置主机名、域名及启用密码和 Telnet 密码，第 815 页。如果未指定每个接口的主机名，则使用设备主机名。如

果未指定 FQDN，则对于静态或 PPPoE IP 寻址，系统域名或 DNS 服务器域名将附加到主机名之前。

过程

步骤 1 标准 DDNS 方法：配置 DDNS 更新方法以启用来自 ASA 的 DNS 请求。

如果 DHCP 服务器将执行所有请求，则无需配置 DDNS 更新方法。

a) 创建更新方法。

ddns update method 名称

示例：

```
ciscoasa(config)# ddns update method ddns1
ciscoasa(DDNS-update-method)#
```

b) 指定标准 DDNS 方法。

ddns [**both**]

默认情况下，ASA 仅更新A RR。如果您希望 DHCP 服务器更新 PTR RR，请使用此设置。如果希望 ASA 更新 A 和 PTR RR，请指定 **both**。使用 **both** 关键字进行静态或 PPPoE IP 寻址。

示例：

```
ciscoasa(DDNS-update-method)# ddns
```

c) （可选） 配置 DNS 请求之间的更新接口。

interval maximum *days hours minutes seconds*

默认情况下，当所有值都设置为 0 时，每当 IP 地址或主机名更改时，都会发送更新请求。要定期发送请求，请设置天数 (0-364)、小时、分钟和秒。

示例：

```
ciscoasa(DDNS-update-method)# interval maximum 0 0 15 0
```

d) 将此方法与接口关联。请参阅 步骤 3，第 855 页。

步骤 2 Web 方法：配置 DDNS 更新方法，启用来自 ASA 的 HTTP 更新请求。

a) 创建更新方法。

ddns update method 名称

示例：

```
ciscoasa(config)# ddns update method web1
ciscoasa(DDNS-update-method)#
```

b) 指定引用身份名称以验证 ddns 服务器证书身份。ASA 尝试查找主机名匹配项。解析主机失败或未找到匹配项时，连接将终止。

示例：

```
ciscoasa(DDNS-update-method)# web reference-identity dyndns
```

c) 指定 Web 方法和更新 URL。

web update-url https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**

在输入问号 (？) 字符之前，请同时按 Ctrl + V 键。这样，你就可以输入“?”，软件也不会将“?”解释为帮助查询。

示例：

```
ciscoasa(DDNS-update-method)#
web update-url
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
```

d) （可选） 指定要更新的地址类型（IPv4 或 IPv6）。

默认情况下，ASA 更新所有 IPv4 和 IPv6 地址。如果要限制地址，请输入以下命令。

web update-type {**ipv4** | **ipv6** [**all**] | **both** [**all**]}

- **both all**-（默认）更新所有 IPv4 和 IPv6 地址。
- **both** - 更新 IPv4 地址和最新的 IPv6 地址。
- **ipv4** - 仅更新 IPv4 地址。
- **ipv6** - 仅更新最新的 IPv6 地址。
- **ipv6 all** - 更新所有 IPv6 地址。

示例：

```
ciscoasa(DDNS-update-method)# web update-type ipv4
```

e) （可选） 配置 DNS 请求之间的更新接口。

interval maximum *days hours minutes seconds*

默认情况下，当所有值都设置为 0 时，每当 IP 地址或主机名更改时，都会发送更新请求。要定期发送请求，请设置天数 (0-364)、小时、分钟和秒。

示例：

```
ciscoasa(DDNS-update-method)# interval maximum 0 0 15 0
```

f) 将此方法与接口关联。请参阅 步骤 3，第 855 页。

g) DDNS 的 Web 类型方法还要求您识别 DDNS 服务器根证书，以验证 HTTPS 连接的 DDNS 服务器证书。请参见第 步骤 4，第 856 页 步。

步骤 3 配置 DDNS 的接口设置，包括为此接口设置更新方法、DHCP 客户端设置和主机名。

a) 进入接口配置模式。

interface *id*

示例：

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)#
```

b) 分配一个更新方法。

ddns update 名称

标准 DDNS 方法：如果您希望 DHCP 服务器执行所有更新，则无需分配方法。Web 更新方法需要执行此命令。

示例：

```
ciscoasa(config-if)# ddns update ddns1
```

c) 为该接口分配一个主机名。

ddns update hostname *hostname*

如果未设置主机名，则会使用设备主机名。如果未指定 FQDN，则会附加系统域名或 DNS 服务器组中的默认域（用于静态或 PPPoE IP 寻址），或附加来自 DHCP 服务器的域名（用于 DHCP IP 寻址）。

示例：

```
ciscoasa(config-if)# ddns update hostname asa1.example.com
```

d) 标准 DDNS 方法：确定您希望 DHCP 服务器更新哪些记录。

dhcp client update dns [**server** {**both** | **none**}]

ASA 将 DHCP 客户端请求发送到 DHCP 服务器。请注意，还必须将 DHCP 服务器配置为支持 DDNS。可以将该服务器配置为满足客户端请求，也可以覆盖客户端（在这种情况下，它将回复客户端，因此客户端也不会尝试执行服务器正在执行的更新）。即使客户端不请求DDNS更新，也可以将 DHCP 服务器配置为始终发送更新。

静态或 PPPoE IP 寻址，请忽略这些设置。

注释
您还可以使用 **dhcp-client update dns** 命令为所有接口全局设置这些值。每个接口的设置优先于全局设置。

- 默认（无关键字）- 请求 DHCP 服务器执行 PTR RR 更新。此设置与启用 **ddns** A 记录的 DDNS 更新方法配合使用。
- **server both** - 请求 DHCP 服务器同时执行 A 和 PTR RR 更新。此设置不需要将 DDNS 更新方法与接口关联。

- **server none** - 请求 DHCP 服务器不执行更新。此设置与启用 **ddns both** A 和 PTR 记录的 DDNS 更新方法配合使用。

示例：

```
ciscoasa(config-if)# ddns client update dns
```

步骤 4 DDNS 的 Web 方法还要求您识别 DDNS 服务器根证书，以验证 HTTPS 连接的 DDNS 服务器证书。请参阅 配置信任点，第 877 页。

示例：

```
crypto ca trustpoint DDNS_Trustpoint
  enrollment terminal
crypto ca authenticate DDNS_Trustpoint nointeractive
   MIIFWjCCA0KgAwIBAgIQbkepxUtHDA3sM9CJuRz04TANBgkqhkiG9w0BAQwFADBH
   MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
   [...]
   quit
```

静态 IP 地址的标准 DDNS 方法

以下示例显示如何配置用于静态 IP 地址的标准 DDNS 方法。请注意，此场景中不配置 DHCP 客户端设置。

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
 ddns both
interface gigabitethernet1/1
 ip address 209.165.200.225
! Associate the method with the interface:
 ddns update ddns-2
 ddns update hostname asa1.example.com
```

示例：标准 DDNS 方法；ASA 更新 A RR，DHCP 服务器更新 PTR RR

以下示例将 ASA 配置为更新 A RR，将 DHCP 服务器配置为更新 PTR RR。

```
! Define the DDNS method to update the A RR:
ddns update method ddns-1
 ddns
interface gigabitethernet1/1
  ip address dhcp
! Associate the method with the interface:
  ddns update ddns-1
  ddns update hostname asa
! Set the client to update the A RR, and the server to update the PTR RR:
  dhcp client update dns
```

示例：标准 DDNS 方法；RR 没有 DHCP 服务器更新

以下示例将 ASA 配置为同时更新 A 和 PTR RR，同时请求 DHCP 服务器更新无 RR。

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
  ddns both
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update ddns-2
  ddns update hostname asa1.example.com
! Set the client to update both RRs, and the server to update none:
  dhcp client update dns server none
```

示例：标准 DDNS 方法；DHCP 服务器更新所有 RR

以下示例将 DHCP 客户端配置为请求 DHCP 服务器同时更新 A 和 PTR RR。由于服务器执行所有更新，因此不需要将更新方法与接口关联。

```
interface gigabitethernet1/1
  ip address dhcp
  ddns update hostname asa
! Configure the DHCP server to update both RRs:
  dhcp client update dns server both
```

示例：Web 类型

以下示例配置 Web 类型方法。

```
! Define the web type method:
ddns update method web-1
  web update-url https://captainkirk:enterpr1s3@domains.cisco.com/ddns?hostname=<h>&myip=<a>
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update web-1
  ddns update hostname asa2.example.com
```

监控 DHCP 和 DDNS 服务

本节介绍监控 DHCP 和 DDNS 服务的程序。

监控 DHCP 服务

- **show dhcpd** {**binding** [*IP_address*] | **state** | **statistics**}

  此命令将显示当前 DHCP 服务器客户端绑定、状态和统计信息。

- **show dhcprelay** {**state** | **statistics**}

  此命令将显示 DHCP 中继状态和统计信息。

- **show ipv6 dhcprelay binding**

  此命令可显示中继代理创建的中继绑定条目。

- **show ipv6 dhcprelay statistics**

  此命令可显示 IPv6 的 DHCP 中继代理统计信息。

- **show ipv6 dhcp server statistics**

  此命令显示 DHCPv6 无状态服务器统计信息。以下示例显示了此命令提供的信息：

```
ciscoasa(config)# show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                  10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp pool** [*pool_name*]

- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  show ipv6 dhcp interface 命令用于显示所有接口的 DHCPv6 信息。如果接口配置用于 DHCPv6 无状态服务器配置（请参阅配置 DHCPv6 无状态服务器，第 847 页），则此命令将列出该服务器正在使用的 DHCPv6 池。如果接口包含 DHCPv6 地址客户端或前缀委派客户端配置，则此命令将显示各个客户端的状态，以及从该服务器收到的值。对于特定接口，可以显示 DHCP 服务器或客户端的消息统计信息。以下示例显示此命令提供的信息：

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
```

```
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                 preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
```

```
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

  show ipv6 dhcp ha statistics 命令用于显示故障转移设备之间的事务处理统计信息，包括在DUID信息各个设备之间的同步次数。以下示例显示了此命令提供的信息。

  在主用设备上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

  在备用设备上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

故障排除 VTI 上的 DHCP 中继

如果 DHCP 客户端无法获取 IP 地址：

- 验证两个 ASA 站点中的隧道接口/ VTI配置。
- 使用 **show crypto ipsec sa** 命令验证站点之间传输的数据包：

  示例

```
ciscoasa(config)# show crypto ipsec sa
interface: outside
Crypto map tag: cmap, seq num: 10, local addr: 192.168.2.111
access-list CSM_IPSEC_ACL_0 extended permit ip any4 any4
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 192.168.2.110
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
```

启用调试命令

启用 DHCP 中继调试可帮助您了解 DISCOVER/REQUEST 数据包是否已转发到 DHCP 中继服务器：

- **debug dhcprelay event 255**

- **debug dhcprelay packet 255**
- **debug dhcprelay error 255**

示例

```
ciscoasa(config)# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
DHCP: Received a BOOTREQUEST from interface 2 (size = 548)
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPRA: setting giaddr to 192.168.1.111. dhcpd_forward_request: request from xxxx.xxxx.xxxx
forwarded to 192.168.3.112.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on vti interface
DHCP: Received a BOOTREPLY from relay interface 5 (size = 300, xid = xxxxxxxxx) at 04:40:52
UTC Tue Sep 10 2019
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPD/RA: creating ARP entry (192.168.1.88, xxxx.xxxx.xxxx).
DHCPRA: Adding rule to allow client to respond using offered address 192.168.1.95
DHCPRA: forwarding reply to client xxxx.xxxx.xxxx.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
```

监控 DDNS 状态

请参阅以下用于监控 DDNS 状态的命令。

- **show ddns update** {**interface** *if_name* | **method** [*name*]}

  此命令显示 DDNS 更新状态。

  以下示例显示有关 DDNS 更新方法的详细信息：

```
ciscoasa# show ddns update method ddns1

Dynamic DNS Update Method: ddns1
  IETF standardized Dynamic DNS 'A' record update
```

  以下示例显示有关 Web 更新方法的详细信息：

```
ciscoasa# show ddns update method web1

Dynamic DNS Update Method: web1
 Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
https://cdarwin:*****@ddns.cisco.com/update?hostname=<h>&myip=<a>
```

  以下示例显示有关 DDNS 接口的信息：

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available
```

  以下示例显示 Web 类型更新成功：

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
```

```
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : asa1.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

以下示例显示 Web 类型故障：

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

以下示例显示 DNS 服务器返回 Web 类型更新错误：

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

以下示例显示，由于 IP 地址未配置或 DHCP 请求失败，尚未尝试 Web 更新，例如：

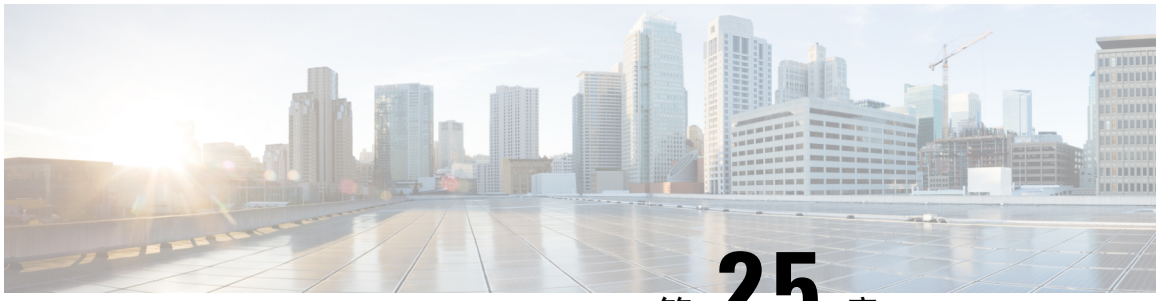
```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update Not attempted
```

DHCP 和 DDNS 服务的历史记录

功能名称	平台版本	说明
DDNS 支持 Web 更新方法	9.15(1)	您现在可以将接口配置为使用支持 Web 更新方法的 DDNS。 新增/修改的命令：**show ddns update interface**、**show ddns update method**、**web update-url**、**web update-type**
VTI 支持 DHCP 中继服务器	9.14(1)	现在，您可以在 VTI 上启用 DHCP 中继。 新增/修改的命令：**dhcprelay server** 。

功能名称	平台版本	说明
DHCP 预留	9.13(1)	ASA 支持 DHCP 预留。根据客户端的 MAC 地址从定义的地址池中将一个静态 IP 地址分配给 DHCP 客户端。 新增/修改的命令：**dhcpd reserve-address** 。
IPv6 DHCP	9.6(2)	ASA 现在支持 IPv6 寻址的以下功能： • DHCPv6 地址客户端 - ASA 从 DHCPv6 服务器获取 IPv6 全局地址和可选默认路由。 • DHCPv6 前缀代理客户端 - ASA 从 DHCPv6 服务器获取指定的前缀。然后，ASA 可使用这些前缀来配置其他 ASA 接口地址，以使无状态地址自动配置 (SLAAC) 客户端可在同一网络上自动配置 IPv6 地址。 • BGP 路由器通告指定的前缀 • DHCPv6 无状态服务器 - 当 SLAAC 客户端向 ASA 发送信息请求 (IR) 数据包时，ASA 会向它们提供域名等其他信息。ASA 仅接受 IR 数据包，不向客户端分配地址。 添加或修改了以下命令：**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address**
DHCPv6 监控	9.4(1)	现在，可以监控适用于 IPv6 的 DHCP 统计信息和适用于 IPv6 的 DHCP 绑定。
DHCP 中继服务器验证 DHCP 服务器标识符是否存在应答	9.4(3)	如果 ASA DHCP 中继服务器收到来自错误的 DHCP 服务器的应答，现在它会验证该应答是否来自正确的服务器，然后对应答做出反应。未引入或修改任何命令。未修改任何 ASDM 屏幕。 未引入或修改任何命令。
DHCP 重新绑定功能	9.1(4)	在 DHCP 重新绑定阶段，客户端会尝试重新绑定到隧道组列表中的其他 DHCP 服务器。在此版本之前，当 DHCP 租约未能更新时，客户端不会重新绑定到备用服务器。 未引入或修改任何命令。
DHCP 受信任接口	9.1(2)	现可将接口配置为受信任接口，以保留 DHCP 选项 82。下游交换机和路由器使用 DHCP 选项 82 进行 DHCP 探听和 IP 源保护。通常，如果 ASA DHCP 中继代理收到已设置选项 82 的 DHCP 数据包，但 giaddr 字段（指定在向服务器转发数据包之前由中继代理设置的 DHCP 中继代理地址）设置为 0，则 ASA 默认将丢弃该数据包。现在可以保留选项 82 并通过将接口标识为受信任接口而转发数据包。 引入或修改了以下命令：**dhcprelay information trusted**、**dhcprelay information trust-all**、**show running-config dhcprelay**。

功能名称	平台版本	说明
每个接口的 DHCP 中继服务器（仅限 IPv4）	9.1(2)	现在可以配置单个接口的 DHCP 中继服务器，因此仅将进入指定接口的请求中继给为该接口指定的服务器。每接口 DHCP 中继不支持 IPv6。 引入或修改了以下命令：**dhcprelay server**（接口配置模式）、**clear configure dhcprelay**、**show running-config dhcprelay**。
适用于 IPv6 的 DHCP 中继 (DHCPv6)	9.0(1)	添加了 DHCP 中继对 IPv6 的支持。 引入了以下命令：**ipv6 dhcprelay server**、**ipv6 dhcprelay enable**、**ipv6 dhcprelay timeout**、**clear config ipv6 dhcprelay**、**ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag**、**debug ipv6 dhcp**、**debug ipv6 dhcprelay**、**show ipv6 dhcprelay binding**、**clear ipv6 dhcprelay binding**、**show ipv6 dhcprelay statistics** 和 **clear ipv6 dhcprelay statistics**。
DDNS	7.0(1)	引入了此功能。 添加了下列命令：**ddns**、**ddns update**、**dhcp client update dns**、**dhcpd update dns**、**show running-config ddns** 和 **show running-config dns server-group**。
DHCP	7.0(1)	ASA 可向连接到 ASA 接口的 DHCP 客户端提供 DHCP 服务器或 DHCP 中继服务。 引入了以下命令： **dhcp client update dns**、 **dhcpd address**、 **dhcpd domain**、dhcpd enable、 **dhcpd lease**, **dhcpd option**、 **dhcpd ping timeout**、 **dhcpd update dns**、 **dhcpd wins**、 **dhcp-network-scope**、 **dhcprelay enable**、 **dhcprelay server**、 **dhcprelay setroute**、 **dhcp-server**、 **show running-config dhcpd**和 **show running-config dhcprelay**。



第 25 章

数字证书

本章介绍如何配置数字证书。

- 关于数字证书，第 865 页
- 数字证书准则，第 872 页
- 配置数字证书，第 875 页
- 如何设置特定整数类型，第 896 页
- 设置证书到期警报（对于身份或 CA 证书），第 898 页
- 监控数字证书，第 898 页
- 证书管理的历史记录，第 900 页

关于数字证书

数字证书是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或IP地址。CA 负责管理证书请求和颁发数字证书。CA 是负责“签署”证书以验证证书真实性的可信机构，旨在确保设备或用户的身份真实有效。

数字证书还包括用户或设备的公钥副本。CA 可以是可信的第三方（例如 VeriSign），也可以是组织内建立的私有（内部）CA。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。

如果使用数字证书进行身份验证，则 ASA 上必须存在至少一个身份证书及其颁发 CA 证书。此配置允许多个身份、根和证书层次结构。ASA 根据 CRL（也称为权限吊销列表）评估第三方证书，从身份证书一直到从属证书颁发机构链。

以下是几种不同类型的可用数字证书的说明：

- CA 证书用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。
- CA 还会颁发身份证书，这是特定系统或主机的证书。
- 代码签名证书是用于创建数字签名以签署代码的特殊证书，经过签署的代码会透露证书源。

在具有一个根 CA 和两个中间 CA 证书的层次结构中，当 ID 证书由一个中间 CA 签发，而 CRL 由另一个中间 CA 签发时，在运行 9.13 或更高版本的头端上远程访问的 CRL 验证会失败。即使头端信任由同一根节点签名的两个中间节点，也会发生该故障。

因此，每个签名者都必须维护自己的 CRL。然后，每个签名者将在其签名的每个证书的 url 列表中指定 CRL 的位置。或者，您可以在每个签名者的信任点中配置一个指向正确 CRL 位置的 url 覆盖。

本地 CA 在 ASA 上集成独立的证书颁发机构功能，并且会部署证书，对已颁发的证书提供安全的吊销检查。本地 CA 凭借通过网站登录页面进行的用户注册提供安全、可配置的内部机构进行证书身份验证。

注释 CA 证书和身份证书适用于站点间 VPN 连接和远程访问 VPN 连接。本文档中的程序是指 ASDM GUI 中使用的远程访问 VPN。

提示 有关包括证书配置和负载均衡的情景示例，请参阅以下 URL：https://supportforums.cisco.com/docs/DOC-5964。

公钥加密

通过公钥加密实现的数字签名为设备和用户提供了一种身份验证方法。在 RSA 加密系统等公钥加密中，每位用户都有一个包含公钥和私钥的密钥对。这一对密钥相互补充，用其中一个密钥加密的任何内容都可用另一个密钥解密。

简言之，使用私钥加密数据时会形成一个签名。此签名附加在数据中并发送给接收者。接收者对数据应用发送者的公钥。如果随数据一起发送的签名与对数据应用公钥的结果一致，就会确立消息的有效性。

此过程的前提是接收者拥有发送者的公钥副本而且非常确定此密钥属于发送者，而不是伪装成发送者的其他人。

获取发送方公钥通常是在外部处理或通过安装时执行的操作处理。例如，默认情况下，大多数 Web 浏览器都使用若干 CA 的根证书进行配置。对于 VPN，作为 IPsec 组件的 IKE 协议可使用数字签名在设置安全关联之前验证对等设备身份。

证书可扩展性

在没有数字证书的情况下，必须手动为每个与其通信的对等体配置各自的 IPSec 对等体；因此，每个添加到网络的新对等体都会要求对需要与其安全通信的每个对等体进行配置更改。

使用数字证书时，系统将向 CA 注册每个对等体。两个对等体试图进行通信时，它们将交换证书并以数字方式签署数据以进行相互身份验证。新对等体添加到网络时，会向 CA 注册该对等体，其他任何对等体都不需要修改。新对等体尝试进行 IPSec 连接时，证书将自动交换并且对等体可进行身份验证。

通过CA，对等体可将证书发送到远程对等体并执行一些公钥加密，从而自行向远程对等体进行身份验证。每个对等体发送由 CA 颁发的唯一证书。此过程之所以适用，是因为每个证书会封装关联对等体的公钥，每个证书由 CA 进行身份验证，且所有参与对等体都将 CA 视为身份验证机构。此过程称为带 RSA 签名的 IKE。

对等体可继续为多个 IPsec 会话发送其证书，并可向多个 IPSec 对等体发送证书，直到证书过期。证书过期后，对等体管理员必须从 CA 获取新的证书。

CA 还可以为不再参与 IPsec 的对等体吊销证书。已吊销的证书无法被其他对等体识别为有效证书。吊销的证书列在 CRL 中，在从其他对等体接收证书之前，每个对等体都可以对其进行检查。

某些 CA 在其实施过程中会使用 RA。RA 是一种用作 CA 的代理的服务器，以便 CA 功能可以在 CA 不可用时继续使用。

密钥对

密钥对包括 RSA 或椭圆曲线签名算法 (ECDSA) 密钥，具有以下特征：

- RSA 密钥可用于 SSH 或 SSL。
- SCEP 注册支持 RSA 密钥的认证。
- 最大 RSA 密钥大小为 4096，默认值为 2048。
- 最大 ECDSA 密钥长度为 521，默认值为 384。
- 您可以生成一个用于签名和加密的通用 RSA 密钥对，也可以为每种用途生成单独的 RSA 密钥对。单独的签名和加密密钥有助于减少密钥泄露，因为 SSL 使用密钥进行加密，但不签名。但是，IKE 使用密钥进行签名，但不加密。通过为每种用途使用单独的密钥，泄露密钥的风险降至最低。

信任点

通过信任点，您可以管理并跟踪 CA 和证书。信任点表示 CA 或身份对。信任点包括 CA 的身份、CA 特定配置参数，以及与一个注册的身份证书的关联。

定义信任点之后，您可以在要求指定CA的命令中根据名称对其进行引用。您可以配置多个信任点。

注释 如果 ASA 有多个共享同一个 CA 的信任点，则只有其中一个共享该 CA 的信任点可用来验证用户证书。要控制使用哪个共享 CA 的信任点来验证该 CA 颁发的用户证书，请使用 **support-user-cert-validation** 命令。

对于自动注册，信任点必须使用注册 URL 进行配置，并且信任点代表的 CA 必须在网络中可用且必须支持 SCEP。

您可以 PKCS12 格式导出和导入密钥对，以及与某个信任点关联的已颁发证书。此格式对于在其他 ASA 上手动复制信任点配置来说非常有用。

证书注册

ASA 的每个信任点都需要一个 CA 证书，自身需要一个或两个证书，具体取决于信任点所用的密钥配置。如果信任点使用单独的 RSA 密钥进行签名和加密，则 ASA 需要两个证书，每个任务一个。在其他密钥配置中，只需要一个证书。

ASA 支持使用 SCEP 自动注册，也支持手动注册，后者可让您将 base-64 编码的证书直接复制到终端。对于站点间 VPN，您必须注册每个 ASA。对于远程访问 VPN，则必须注册每个 ASA 以及每个远程访问 VPN 客户端。

SCEP 请求的代理

ASA 可以代理 Secure Client 和第三方 CA 之间的 SCEP 请求。如果 ASA 用作代理，则 CA 只需要允许它访问即可。为使 ASA 提供此服务，用户必须在 ASA 发送注册请求之前使用 AAA 支持的任何方法进行身份验证。您还可以使用主机扫描和动态访问策略执行注册资格规则。

ASA 仅对 Secure Client SSL 或 IKEv2 VPN 会话支持此功能。它支持所有符合 SCEP 的 CA，包括 Cisco IOS CS、Windows Server 2003 CA 和 Windows Server 2008 CA。

无客户端（基于浏览器）访问不支持 SCEP 代理，但 WebLaunch（无客户端启动的 Secure Client）则支持该代理。

ASA 不支持证书的轮询。

ASA 支持此功能的负载均衡。

撤销检查

颁发证书后，该证书在固定时期内有效。有时，CA 会在此时期到期前吊销证书，例如，因为安全问题、名称更改或关联。CA 会定期发布签署的已吊销证书列表。启用撤销检查会强制 ASA 检查每当它使用证书进行身份验证时，CA 都尚未撤销证书。

启用撤销检查后，ASA 会在 PKI 证书验证过程中检查证书撤销状态，可以使用 CRL 和/或 OCSP 检查。仅当第一种方法返回错误时（例如，指示服务器不可用时），才会使用 OCSP。

通过 CRL 检查，ASA 将检索、分析和缓存 CRL，从而提供包含其证书序列号的撤销（以及未撤销）证书完整列表。ASA 根据 CRL（也称为授权撤销列表）评估证书，从身份证书一直到从属证书颁发机构链。

OCSP 提供了一种更具可扩展性的吊销状态检查方法，此方法通过验证机构对证书状态进行本地化，而验证机构会查询特定证书的状态。

支持的 CA 服务器

ASA 支持以下 CA 服务器：

思科 IOS CS、ASA 本地 CA 和符合 X.509 标准的第三方 CA 供应商，包括但不限于：

- Baltimore Technologies
- Entrust

- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft 证书服务
- RSA Keon
- Thawte
- VeriSign

CRL

CRL 为 ASA 提供了一种方法来确定某个有效期内的证书是否已被证书颁发机构 (CA) 吊销。CRL 配置是信任点配置的一部分。

进行证书身份验证时，您可以使用 **revocation-check crl** 命令将 ASA 配置为强制进行 CRL 检查。您也可以使用 **revocation-check crl none** 命令将 CRL 检查设为可选检查，从而在 CA 无法提供更新后的 CRL 数据时，证书身份验证也会成功。

注释 恢复了在 9.13(1) 中删除的 **revocation-check crl none**。

ASA 可使用 HTTP、SCEP 或 LDAP 从 CA 检索 CRL。为每个信任点检索的 CRL 会在为每个信任点配置的时间内一直缓存。

注释 虽然 CRL 服务器使用 HTTP 标志“Connection：Keep-alive”进行响应以指示持久连接，但 ASA 不会请求支持持久连接。更改CRL服务器上的设置，以便在发送列表时以“Connection: Close”响应。

当ASA缓存CRL的时间超过配置的CRL缓存时间时，ASA会认为该CRL的版本过旧而不可靠（即“过时”）。下次证书身份验证要求检查过时 CRL 时，ASA 会尝试检索更新版本的 CRL。

如果超出 CRL 16MB 的大小限制，您可能收到针对用户连接/证书的 *revocation check* 故障。

ASA 缓存 CRL 的时间由以下两个因素确定：

- 使用 **cache-time** 命令指定的分钟数。默认值为 60 分钟。
- 检索到的 CRL 中的 NextUpdate 字段，CRL 中可能没有该字段。您可使用 **enforcenextupdate** 命令控制 ASA 是否需要和使用 NextUpdate 字段。

ASA 通过以下方式使用这两个因素：

- 如果不需要 NextUpdate 字段，则 会在经过由 **cache-time** 命令定义的时间长度后将 CRL 标记为过时。

- 如果需要 NextUpdate 字段，则 ASA 会在由 **cache-time** 命令和 NextUpdate 字段指定的两个时间中较早的那个时间将 CRL 标记为过时。例如，如果 **cache-time** 命令设置为 100 分钟，而 NextUpdate 字段指定下一次更新是在 70 分钟后，则 ASA 会将 CRL 标记为在 70 分钟内过时。

如果 ASA 的内存不足以存储为给定信任点缓存的所有 CRL，它将删除最近最少使用的 CRL 来为新检索的 CRL 腾出空间。大型 CRL 需要大量计算开销来进行解析。因此，为了获得更好的性能，请使用多个较小的 CRL，而不是几个大型 CRL，或者最好使用 OCSP。

请参阅以下缓存大小：

- 单情景模式 - 128MB
- 多情景模式 - 每个情景 16MB

OCSP

OCSP 为 ASA 提供了一种方法来确定某个有效期内的证书是否已被证书颁发机构 (CA) 吊销。OCSP 配置是信任点配置的一部分。

OCSP 在 ASA 查询特定证书状态的验证颁发机构（一台 OCSP 服务器，又称响应方）上本地化证书状态。相比 CRL 检查，此方法可提供更好的可扩展性和更新的吊销状态，并且可帮助组织进行大型 PKI 安装部署和扩展安全网络。

注释 ASA 会为 OCSP 响应留出 5 秒的时间偏差。

进行证书身份验证时，您可以使用 **revocation-check ocsp** 命令将 ASA 配置为强制进行 OCSP 检查。您也可以使用 **revocation-check ocsp none** 命令将 OCSP 检查设为可选检查，从而在验证机构无法提供更新后的 OCSP 数据时，证书身份验证也会成功。

注释 在 9.13(1) 中删除的 **revocation-check ocsp none** 已恢复。

OCSP 提供三种定义 OCSP 服务器 URL 的方法。ASA 按以下顺序使用这些服务器：

1. 使用 **match certificate** 命令在匹配证书覆盖规则中定义的 OCSP URL。
2. 使用 **ocsp url** 命令配置的 OCSP URL。
3. 客户端证书的 AIA 字段。

注释 要将信任点配置为验证自签名 OCSP 响应方证书，请将自签名响应方证书作为可信 CA 证书导入其自己的信任点。然后，在验证信任点的客户端证书中配置 **match certificate** 命令，以使用包括自签名 OCSP 响应方证书的信任点来验证响应器证书。使用同一程序配置客户端证书的验证路径外部配置验证响应方证书。

OCSP 服务器（响应方）证书通常会签署 OCSP 响应。收到响应后，ASA 会尝试验证响应方证书。CA 通常会将 OCSP 响应方证书的有效期设置为相对较短的时间以将受危害的可能性降至最低。CA 通常还会在响应方证书中包含 ocsp-no-check 扩展，表明此证书不需要进行吊销状态检查。但如此此扩展不存在，ASA 将尝试使用信任点中指定的相同方法检查吊销状态。如果响应方证书无法验证，则吊销检查失败。为了避免出现这种可能性，请使用 **revocation-check none** 命令来配置验证信任点的响应方证书，并使用 **revocation-check ocsp** 命令来配置客户端证书。

证书和用户登录凭证

下一节介绍使用证书和用户登录凭证（用户名和密码）进行身份验证和授权的不同方法。这些方法适用于 IPsec、 Secure Client和无客户端 SSL VPN。

在所有情况下，LDAP 授权都不会使用密码作为凭证。RADIUS 授权对所有用户使用公用密码或使用用户名作为密码。

用户登录凭证

身份验证和授权的默认方法是使用用户登录凭证。

- 身份验证
  - 通过隧道组（也称为 ASDM 连接配置文件）中的身份验证服务器组设置进行启用
  - 使用用户名和密码作为凭证
- 授权
  - 通过隧道组（也称为 ASDM 连接配置文件）中的授权服务器组设置进行启用
  - 使用用户名作为凭证

证书

如果配置了数字证书，ASA 首先会验证该证书。但是，它不会使用证书的任何 DN 作为用户名进行身份验证。

如果启用了身份验证和授权，ASA 会使用用户登录凭证进行用户身份验证和授权。

- 身份验证
  - 通过身份验证服务器组设置进行启用
  - 使用用户名和密码作为凭证

- 授权
  - 通过授权服务器组设置进行启用
  - 使用用户名作为凭证

如果禁用身份验证，但启用授权，ASA 将使用主 DN 字段进行授权。

- 身份验证
  - 通过身份验证服务器组设置进行禁用（设置为 None）
  - 未使用凭证
- 授权
  - 通过授权服务器组设置进行启用
  - 使用证书主 DN 字段的用户名值作为凭证

注释 如果证书中不存在主 DN 字段，ASA 将使用辅助 DN 字段值作为授权请求的用户名。

以包含以下 Subject DN 字段和值的用户证书为例：

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

如果主 DN = EA（邮件地址），辅助 DN = CN（公共名称），则授权请求中使用的用户名将为 anyuser@example.com。

数字证书准则

本节介绍在配置数字证书之前应检查的准则和限制。

情景模式准则

- 对于第三方 CA，仅在单情景模式下受支持。

故障转移准则

- 在有状态的故障转移中不支持复制会话。
- 对于本地 CA，不支持故障转移。
- 如果配置状态故障转移，证书会自动复制到备用设备。如果发现证书缺失，请在主用设备上使用**write standby**命令。

IPv6 准则

支持 IPv6 OCSP 和 CRL URL。您必须将 IPv6 地址括在方括号中，例如：*http://[0:0:0:0:0.18:0a01:7c16]*。

本地 CA 证书

- 确保已正确配置 ASA 以支持证书。ASA 配置不正确可能会导致注册失败或请求的证书包括错误信息。
- 确保 ASA 的主机名和域名配置正确。要查看当前配置的主机名和域名，请输入 **show running-config** 命令。
- 在配置 CA 之前，确保 ASA 时钟设置正确。证书具有生效日期和时间以及到期日期和时间。当 ASA 注册到 CA 并获取证书时，ASA 会检查当前时间是否在证书的有效范围内。如果超出范围，则注册失败。
- 在本地 CA 证书到期前 30 天，系统会生成一个滚动更新替代证书，并且系统日志消息将通知管理员到时间进行本地 CA 滚动更新。新的本地 CA 证书必须在当前证书到期前导入到所有必要的设备上。如果管理员未通过将滚动更新证书安装为新的本地 CA 证书作出响应，则验证可能会失败。
- 本地 CA 证书将在到期后使用相同的密钥对自动滚动更新。滚动更新证书可使用 base 64 格式导出。

  以下示例显示 base 64 编码的本地 CA 证书：

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

SCEP 代理支持

- 确保 ASA 和思科 ISE 策略服务节点使用相同的 NTP 服务器进行同步。
- Secure Client 终端上必须运行 3.0 或更高版本。
- 在组策略的连接配置文件中配置的身份验证方法必须设置为同时使用 AAA 身份验证和证书身份验证。
- 对于 IKEv2 VPN 连接，SSL 端口必须处于打开状态。
- CA 必须处于自动授予模式下。

其他准则

- 可以使用的证书类型受使用证书的应用支持的证书类型限制。使用证书的所有应用通常都支持RSA证书。但工作站操作系统，浏览器，ASDM 或 Secure Client可能不支持 EDDSA 证书。例如，您需要使用RSA证书进行远程访问VPN身份和身份验证。对于ASA是使用证书的应用的站点间VPN，支持EDDSA。
- 对于配置为 CA 服务器或客户端的 ASA，证书的有效期限制为小于建议的结束日期：2038 年 1 月 19 日 03:14:08 UTC。本准则还适用于从第三方供应商导入的证书。
- 仅当满足以下任一认证条件时，ASA 才会建立 LDAP/SSL 连接：
  - LDAP 服务器证书受信任（存在于信任点或 ASA 信任池中）且有效。
  - 来自服务器颁发链的 CA 证书是受信任的（存在于信任点或 ASA 信任池）中，链中的所有从属 CA 证书都已完成且有效。
- 证书注册完成后，ASA 将存储包含用户的密钥对和证书链的 PKCS12 文件，该文件每次注册需要约 2 KB 的闪存或磁盘空间。实际的磁盘空间容量取决于已配置的 RSA 密钥长度和证书字段。在可用闪存容量有限的 ASA 上添加大量待处理的证书注册时，请记住此准则，因为这些PKCS12文件在配置的注册检索超时期间存储在闪存中。我们建议使用至少 2048 位的密钥长度。
- 应将 ASA 配置为使用身份证书来保护传至管理接口的 ASDM 流量和 HTTPS 流量。每次重新启动后都会重新生成使用 SCEP 自动生成的身份证书，因此请确保手动安装您自己的身份证书。有关仅应用于 SSL 的此操作步骤的示例，请参阅以下 URL：http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml。
- ASA 和 Secure Client 只能验证其中 X520Serialnumber 字段（主题名称中的序列号）为 PrintableString 格式的证书。如果序列号格式使用编码（例如 UTF8），则证书授权将失败。
- 仅当在 ASA 上导入证书参数时，才对证书参数使用有效的字符和值。 在ASA中，对这些证书进行解码，以将其构建到内部数据结构中。具有空白字段的证书被解释为不符合解码标准，因此安装验证失败。但是，从版本9.16开始，可选字段的空白值不会影响解码和安装验证条件。
- 要使用通配符 (*) 符号，请确保在允许在字符串值中使用此字符的 CA 服务器上使用编码。虽然 RFC 5280 建议使用 UTF8String 或 PrintableString，但应使用 UTF8String，因为 PrintableString 无法将通配符识别为有效字符。如果在导入期间发现无效的字符或值，ASA 将拒绝导入的证书。例如：

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H÷ytes
 as CA certificate:0U0= \Ivr"phÕV°3é¼p0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
 mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

配置数字证书

以下主题介绍如何配置数字证书。

配置密钥对

要创建或删除密钥对，请执行以下步骤：

过程

步骤 1 生成一个默认、通用 RSA 密钥对。

crypto key generate rsa modulus 2048

示例：

```
ciscoasa(config)# crypto key generate rsa modulus 2048
```

默认密钥模块大小为2048，但是您应明确指定模块大小以确保要求。该密钥命名为Default-RSA-Key。

对于 RSA 密钥，模块大小可以是以下其中之一（位数）：2048或 4096。

如果还想要椭圆曲线签名算法 (ECDSA) 密钥，您可以生成 Default-ECDSA-Key。默认长度为 384，但您也可以使用 256 或 521。

crypto key generate ecdsa elliptic-curve 384

如果还想要椭圆曲线签名算法 (Edwards) 密钥，您可以生成 Default-ECDSA-Key。默认长度为 256 位。

注释
不支持使用类型为 EdDSA (Ed25519) 的密钥对的 ASA 上的 EST 注册。EST 注册只能使用 RSA 或 ECDSA 密钥。

crypto key generate eddsa edward-curve Ed25519

步骤 2 （可选）创建具有唯一名称的其他密钥。

crypto key generate rsa label *key-pair-label* **modulus** *size*

crypto key generate ecdsa label *key-pair-label* **elliptic-curve** *size*

示例：

```
ciscoasa(config)# crypto key generate rsa label exchange modulus 2048
```

该标签由使用密钥对的信任点引用。

步骤 3 验证已生成的密钥对。

show crypto key mypubkey {**rsa** | **ecdsa**}

示例：

```
ciscoasa/contexta(config)# show crypto mypubkey key rsa
```

步骤 4 保存已生成的密钥对。

write memory

示例：

```
ciscoasa(config)# write memory
```

步骤 5 如有必要，请删除现有密钥对，以便可以生成新的密钥对。

crypto key zeroize {**rsa** | **ecdsa**}

示例：

```
ciscoasa(config)# crypto key zeroize rsa
```

步骤 6 （可选）存档本地 CA 服务器证书和密钥对。

copy

示例：

```
ciscoasa# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/
```

此命令使用 FTP 或 TFTP 从 ASA 复制本地 CA 服务器证书和密钥对及所有文件。

注释
确保尽可能经常备份所有本地 CA 文件。

步骤 7 对于支持自动注册的注册方法，将在注册时自动生成密钥对，然后存储在闪存中。要启用此支持，请在信任点中指定以下关键参数：

以下示例显示 ECDSA 密钥对配置：

```
ciscoasa(config-ca-trustpoint)# keypair ?

crypto-ca-trustpoint mode commands/options:
  WORD < 129 char  Name of key pair
  ecdsa            Generate ECDSA keys
  eddsa            Generate EDDSA keys
  rsa              Generate RSA keys
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve ?

crypto-ca-trustpoint mode commands/options:
  256  256 bits
  384  384 bits
  521  521 bits
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve 521
ciscoasa(config-ca-trustpoint)#
```

以下示例显示 RSA 密钥对配置：

```
ciscoasa(config-ca-trustpoint)# keypair ?

crypto-ca-trustpoint mode commands/options:
  WORD < 129 char  Name of key pair
  ecdsa            Generate ECDSA keys
  eddsa            Generate EDDSA keys
  rsa              Generate RSA keys
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve ?

ciscoasa(config-ca-trustpoint)# keypair rsa modulus ?

crypto-ca-trustpoint mode commands/options:
  2048  2048 bits
  3072  3072 bits
  4096  4096 bits
ciscoasa(config-ca-trustpoint)# keypair rsa modulus 2048
ciscoasa(config-ca-trustpoint)#
```

步骤 8 运行以下命令即可删除密钥对：

crypto key zeroize rsa

以下示例显示如何删除密钥对：

示例：

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All device certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
```

配置信任点

要配置信任点，请执行以下步骤：

过程

步骤 1 创建与 ASA 需要从中接收证书的 CA 相对应的信任点。

crypto ca trustpoint *trustpoint-name*

示例：

```
ciscoasa/contexta(config)# crypto ca trustpoint Main
```

您可以进入 crypto ca trustpoint 配置模式，该模式控制可从步骤 3 开始配置的 CA 特定信任点参数。

步骤 2 指定用于 CA 认证的源接口：

enrollment interface *interface-name*

```
ciscoasa(config-ca-trustpoint)#  enrollment interface mgmt
```

步骤 3 选择以下选项之一：

- 运行以下命令，请求使用 SCEP 自动注册到指定信任点，并配置注册 URL。

  enrollment protocol scep *url*

  示例：

  ```
  ciscoasa/contexta(config-ca-trustpoint)# enrollment protocol scep url
  http://10.29.67.142:80/certsrv/mscep/mscep.dll
  ```

- 运行以下命令，请求使用 CMP 自动注册到指定信任点，并配置注册 URL。

  enrollment protocol cmp *url*

  示例

  ```
  ciscoasa/ contexta(config-ca-trustpoint)# enrollment protocol cmp url
  http://10.29.67.142:80/certsrv/mscep/mscep.dll
  ```

  注释
  必须包含运营商许可证才能注册 CMP。

- 通过运行以下命令，将从 CA 收到的证书粘贴到终端，请求使用指定信任点手动注册：

  enrollment terminal

  ```
  ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal
  ```

- 运行以下命令，请求自签名证书：

  enrollment self

- 运行以下命令，请求使用 EST 自动注册到指定信任点，并配置注册 URL。

  enrollment protocol est *url*

  示例

  ```
  asa(config-ca-trustpoint)# enrollment protocol est ?

  crypto-ca-trustpoint mode commands/options:
    url CA server enrollment URL
  asa(config-ca-trustpoint)# enrollment protocol est url ?
   crypto-ca-trustpoint mode commands/options:
    LINE < 477 char  URL
  asa(config-ca-trustpoint)# enrollment protocol est url https://xyz.com/est
  ```

步骤 4 如果信任点在以上步骤中被配置为使用CMP，可以选择性地启用自动请求证书的功能。输入需要自动注册前允许的绝对有效期百分比，并指定在更新证书时是否要生成新密钥。

```
[no] auto-enroll [<percent>] [regenerate]
```

步骤 5 指定可用的 CRL 配置选项。

revocation-check crl none

注释
恢复了在 9.13(1) 中删除的 **revocation-check crl none**。

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl
ciscoasa/contexta(config-ca-trustpoint)# revocation-check none
```

注释
要启用必需或可选的 CRL 检查，请确保在获得证书后为 CRL 管理配置信任点。

步骤 6 启用或禁用基本约束扩展和 CA 标志。

[**no**] **ca-check**

基本约束扩展标识证书主体是否为证书颁发机构 (CA)，这种情况下证书可用于签署其他证书。CA 标志是此扩展的一部分。证书中存在这些项目表明证书的公钥可用于验证证书签名。

ca-check 命令默认已启用，因此仅当您想要禁用基本约束和 CA 标志时，才需要输入此命令。

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# no ca-check
```

步骤 7 在注册过程中，要求 CA 在证书的 Subject Alternative Name 扩展中包含指定的邮件地址。

email *address*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# email example.com
```

步骤 8 （可选）指定重试周期（以分钟为单位），且仅应用于 SCEP 注册。

enrollment retry period

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5
```

步骤 9 （可选）指定允许的最大重试次数，且仅应用于 SCEP 注册。

enrollment retry count

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2
```

步骤 10 在注册过程中，要求 CA 在证书的 Subject Alternative Name 扩展中包含指定的完全限定域名。

fqdn *fqdn*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com
```

步骤 11 在注册过程中，请 CA 在证书或手动、SCEP、CMP、EST、 和自签名证书请求的 Subject Alternative Name 扩展名中包含多个完全限定域名值。FQDN 值的最大长度为 128 个字符。

alt-fqdn *fqdn*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# fqdn primary example.com
ciscoasa/contexta(config-ca-trustpoint)# alt-fqdn example1.com
ciscoasa/contexta(config-ca-trustpoint)# alt-fqdn example2.com
ciscoasa/contexta(config-ca-trustpoint)# alt-fqdn example3.com
```

步骤 12 在注册期间，要求 CA 在证书中包括 ASA 的 IP 地址。

ip-address *ip-address*

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1
```

步骤 13 指定要认证其公钥的密钥对。

keypair 名称

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# keypair exchange
```

步骤 14 当已为 CMP 配置信任点时，才能确定是否要为任何手动和自动注册生成 EDCSA 密钥、EDCSA 密钥，还是 RSA 密钥。

```
no keypair name | [rsa modulus 2048|4096] | [edcsa elliptic-curve 256|384|521] | [ eddsa edwards-curve Ed25519 ]
```

注释
不支持使用类型为 EDDSA (Ed25519) 的密钥对的 ASA 上的 EST 注册。EST 注册只能使用 RSA 和 ECDSA 密钥。不支持密钥对类型为 EDDSA 的 ACME 注册。

注释
使用 ECDHE_ECDSA 密码组时，请使用包含支持 ECDSA 的密钥的证书配置信任点。具有 RSA 密钥的证书与 ECDSA 密码不兼容。

步骤 15 配置 OCSP URL 覆盖和信任点以用于验证 OCSP 响应方证书。

match certificate map-name override ocsp

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp
```

步骤 16 配置 ASA 连接 OCSP 的源接口：

interface *nameif*

示例：

```
ciscoasa(config)# crypto ca trustpoint TP
ciscoasa(config-ca-trustpoint)# ocsp ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  interface      Configure Source interface
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp  interface
ciscoasa(config-ca-trustpoint)# ocsp interface ?

crypto-ca-trustpoint mode commands/options:
Current available interface(s):
  inside   Name of interface GigabitEthernet0/0.100
  inside1  Name of interface GigabitEthernet0/0.41
  mgmt     Name of interface Management0/0
  outside  Name of interface GigabitEthernet0/0.51
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt
```

步骤 17 在 OCSP 请求上禁用随机数扩展。随机数扩展以加密方式将请求与响应绑定以避免重放攻击。

ocsp disable-nonce

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce
```

步骤 18 为 ASA 配置 OCSP 服务器，以用于检查与信任点（而不是客户端证书的 AIA 扩展中指定的服务器）关联的所有证书。

ocsp url

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp url
```

ASA 支持 IPv4 和 IPv6 OCSP URL。将 IPv6 地址括在方括号中，例如：*http://[0:0:0:0:0.18:0a01:7c16]*。

步骤 19 指定在注册过程中向 CA 注册的质询短语。CA 通常使用此短语对随后的吊销请求进行身份验证。

password 字符串

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# password mypassword
```

步骤 20 设置一种或多种吊销检查方法：CRL、OCSP 和随机数。

注释
分配 OCSP URL 以进行吊销检查时，可以指定可从其访问 OCSP 的接口（包括管理接口）。此接口值确定路由决策。

revocation check

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# revocation check
```

步骤 21 在注册过程中，要求 CA 在证书中包含指定的使用者 DN。如果 DN 字符串包含逗号，可用双引号将值字符串引起来（例如，O=”Company, Inc.”）。

subject-name *X.500* 名称

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename
```

步骤 22 在注册期间，要求 CA 在证书中包括 ASA 序列号。

serial-number

示例：

```
ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7
```

步骤 23 保存运行配置。

write memory

示例：

```
ciscoasa/contexta(config)# write memory
```

为信任点配置 CRL

要在证书身份验证过程中使用强制或可选CRL检查，您必须为每个信任点配置CRL。要为信任点配置 CRL，请执行以下步骤：

过程

步骤 1 针对要修改其 CRL 配置的信任点进入 crypto ca trustpoint 配置模式。

crypto ca trustpoint *trustpoint-name*

示例：

```
ciscoasa (config)# crypto ca trustpoint Main
```

注释

确保在输入此命令之前已启用 CRL。此外，CRL 必须可用才能成功进行身份验证。

步骤 2 针对当前信任点进入 crl 配置模式。

crl configure

示例：

```
ciscoasa(config-ca-trustpoint)# crl configure
```

提示
要将所有 CRL 配置参数设置为默认值，请使用 **default** 命令。在 CRL 配置过程中，可以随时重新输入此命令来重新启动该程序。

步骤 3 选择下列其中一项来配置检索策略：

注释
ASA 支持基于 IPv4 或 IPv6 的 CDP 和静态 URL。将 IPv6 地址括在方括号中，例如：*http://[0:0:0:0:0.18:0a01:7c16]*。

- CRL 仅从已通过身份验证的证书中指定的 CRL 分发点 (CDP) URL 进行检索。

  policy cdp

  ```
  ciscoasa(config-ca-crl)# policy cdp
  ```

  注释
  证书中指定的分发点不支持 SCEP 检索。

- CRL 仅从您配置的认证映射匹配规则 中进行检索。

  policy static

  ```
  ciscoasa(config-ca-crl)# policy static
  ```

- CRL 仅从已通过身份验证的证书中指定的 CRL 分发点和您配置的认证映射匹配规则 中进行检索。

  policy both

  ```
  ciscoasa(config-ca-crl)# policy both
  ```

步骤 4 如果您在配置 CRL 策略时使用关键字 **static** 或 **both**，则必须为 CRL 检索配置认证映射匹配规则 。您现在可以将多个静态 CDP 配置到单个映射。

enrollment terminal

要删除特定实例，请在命令的**否定**形式中包含序列号或 URL。确保指定的值与配置的值匹配。要删除映射的所有条目，只需使用**否定**命令。

示例：

```
ciscoasa(crypto ca trustpoint)#enrollment terminal

ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  10 url http://192.0.2.10
ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  20 url http://192.0.2.12
ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  30 url http://192.0.2.13
```

步骤 5 指定 HTTP、LDAP 或 SCEP 作为 CRL 检索方法。

protocol http | **ldap** | **scep**

示例：

```
ciscoasa(config-ca-crl)# protocol http
```

步骤 6 配置 ASA 为当前信任点缓存 CRL 的时长。*refresh-time* 参数是 ASA 在认为 CRL 过时之前等待的时间（以分钟为单位）。

cache-time *refresh-time*

示例：

```
ciscoasa(config-ca-crl)# cache-time 420
```

步骤 7 选择以下其中一个选项：

- 要求 CRL 中有 NextUpdate 字段。这是默认设置。

  enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# enforcenextupdate
  ```

- 允许 CRL 中没有 NextUpdate 字段。

  no enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# no enforcenextupdate
  ```

步骤 8 如果 LDAP 被指定为检索协议，则向ASA 标识 LDAP 服务器。您可以按 DNS 主机名或按 IP 地址指定服务器。如果服务器侦听端口上的 LDAP 查询，则您还可以提供端口号，而不是使用默认端口号 389。

ldap-defaults *server*

示例：

```
ciscoasa (config-ca-crl)# ldap-defaults ldap1
```

注释
如果使用主机名而非 IP 地址来指定 LDAP 服务器，请确保已将 ASA 配置为使用 DNS。

步骤 9 如果 LDAP 服务器需要凭证，则允许 CRL 检索。

ldap-dn *admin-DN password*

示例：

```
ciscoasa (config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c00lRunZ
```

步骤 10 从指定信任点所代表的 CA 检索当前 CRL，并测试当前信任点的 CRL 配置。

crypto ca crl request 信任点

示例：

```
ciscoasa (config-ca-crl)# crypto ca crl request Main
```

步骤 11 保存运行配置。

write memory

示例：

```
ciscoasa (config)# write memory
```

导出或导入信任点配置

要导出和导入信任点配置，请执行以下步骤：

过程

步骤 1 以 PKCS12 格式导出带有所有关联密钥和证书的信任点配置。

crypto ca export 信任点

示例：

```
ciscoasa(config)# crypto ca export Main
```

ASA 将在终端显示 PKCS12 数据。您可以复制该数据。信任点数据受密码保护；但是，如果将信任点数据保存在文件中，请确保该文件处于安全位置。

步骤 2 导入与信任点配置关联的密钥对和已颁发证书。

crypto ca import *trustpoint* **pkcs12***passphrase*

示例：

```
ciscoasa(config)# crypto ca import Main pkcs12 ?
```

ASA 会提示您将文本以 base-64 格式粘贴到终端。系统将向与信任点一起导入的密钥对分配与所创建的信任点名称相匹配的标签。

注释
如果 ASA 的信任点共享同一个 Ca，您只能使用共享 CA 的其中一个信任点来验证用户证书。要控制使用哪个共享 CA 的信任点来验证该 CA 颁发的用户证书，请使用 **support-user-cert-validation** 关键字。

示例

以下示例显示使用密码 Wh0zits 导出信任点 Main 的 PKCS12 数据：

```
ciscoasa(config)# crypto ca export Main pkcs12 Wh0zits

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---
```

以下示例使用密码 Wh0zits 将 PKCS12 数据手动导入信任点 Main：

```
ciscoasa (config)# crypto ca import Main pkcs12 Wh0zits

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
```

以下示例手动导入信任点 Main 的证书：

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

配置 CA 证书映射规则

您可以根据证书的 Issuer 和 Subject 字段配置规则。使用您创建的规则，可以通过 **tunnel-group-map** 命令将 IPsec 对等体证书映射到隧道组。

要配置 CA 证书映射规则，请执行以下步骤：

过程

步骤 1 输入您要配置的规则的 CA 证书映射配置模式，并指定规则序列号。

crypto ca certificate map [*map_name*]*sequence-number*

示例：

```
ciscoasa(config)# crypto ca certificate map test-map 10
```

如果不指定映射名称，该规则将添加到默认映射：DefaultCertificateMap。对于每个规则编号，您可以指定一个或多个要匹配的字段。

步骤 2 指定发布者名称或主题名称：

{**issuer-name** | **subject-name**} [**attr** *attribute*] *operator string*

示例：

```
ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)# subject-name attr uid eq jcrichton
```

您可以匹配整个值，也可以指定要匹配的属性。以下为有效属性

- c - 国家/地区
- cn - 公用名
- dc - 域组件
- dnq - DN 限定符
- emailAddress - 邮件地址
- genq - 世代限定符
- gn - 名
- i - 首字母
- ip - IP 地址
- i - 位置
- n - 名称
- o - 组织名称
- ou - 组织单位
- ser - 序列号

注释
确保在subject-name中指定序列号属性。证书映射仅与subject-name中指定的序列号属性匹配。

- sn - 姓
- sp - 州/省
- t - 职务
- uid - 用户 ID
- uname - 非结构化名称

以下是有效的运算符：

- eq - 字段或属性必须与给定的值相同。
- ne - 字段或属性不能与给定的值相同。
- co - 部分或所有字段或属性必须与给定的值相匹配。
- nc - 字段或属性的任何部分都不能与给定的值相匹配。

步骤 3 指定备用主题名称：

alt-subject-name *operator string*

示例：

```
ciscoasa(config-ca-cert-map)# alt-subject-name eq happydays
```

以下是有效的运算符：

- eq - 字段必须与给定的值相同。
- ne - 字段不能与给定的值相同。
- co - 部分或所有字段或属性必须与给定的值相匹配。
- nc - 字段的任何部分都不能与给定的值相匹配。

步骤 4 指定扩展密钥的用法：

extended-key-usage *operator OID_string*

示例：

```
ciscoasa(config-ca-cert-map)# extended-key-usage nc clientauth
```

以下是有效的运算符：

- co - 部分或所有字段或属性必须与给定的值相匹配。
- nc - 字段的任何部分都不能与给定的值相匹配。

以下是有效的 OID 字符串：

- *string* - 用户定义的字符串。
- clientauth - 客户端身份验证 (1.3.6.1.5.5.7.3.2)
- codesigning - 代码签名 (1.3.6.1.5.5.7.3.3)
- emailprotection - 安全邮件保护 (1.3.6.1.5.5.7.3.4)
- ocspsigning - OCSP 签名 (1.3.6.1.5.5.7.3.9)
- serverauth - 服务器身份验证 (1.3.6.1.5.5.7.3.1)
- timestamping - 时间戳 (1.3.6.1.5.5.7.3.8)

配置引用标识

当 ASA 用作 TLS 客户端时，它将支持用于验证应用服务器标识是否符合 RFC 6125 中的定义的规则。此 RFC 将指定用于表示引用标识（在 ASA 上配置）并根据提供的标识（从应用服务器发送）验证它们的程序。如果提供的标识无法与配置的引用标识相匹配，则不会建立连接，并将记录错误。

服务器通过将一个或多个标识符包括在建立连接时提供给 ASA 的服务器证书中，来提供其标识。引用标识将在 ASA 上进行配置，以便在建立连接期间与服务器证书中提供的标识进行比较。这些标识符是 RFC 6125 中指定的四种标识符类型的特定实例。四种标识符类型包括：

- CN_ID：证书主题字段中的一个相对可分辨名称 (RDN)，它仅包含一个公用名称 (CN) 类型的属性类型和值对，其中值与域名的整体形式相匹配。CN 值不能是自由文本。CN-ID 引用标识符不会标识应用服务。
- DNS-ID：dNSName 类型的 subjectAltName 条目。这是一个 DNS 域名。DNS-ID 引用标识符不会标识应用服务。
- SRV-ID：otherName 类型的 subjectAltName 条目，根据 RFC 4985 中的定义，其名称形式为 SRVName。SRV-ID 标识符可以同时包含域名和应用服务类型。例如，SRV-ID“_imaps.example.net”可以拆分为 DNS 域名部分“example.net”和应用服务类型部分“imaps”。
- URI-ID：uniformResourceIdentifier 类型的 subjectAltName 条目，其值同时包括 (i)“scheme”和 (ii) 与 RFC 3986 中指定的“reg-name”规则相匹配的“host”组成部分（或其等效部分）。URI-ID 标识符必须包含 DNS 域名，而非 IP 地址，并且不仅是主机名。例如，URI-ID“sip:voice.example.edu”可以拆分为 DNS 域名部分“voice.example.edu”和应用服务类型“sip”。

在使用以前未使用的名称配置引用标识时，将创建一个引用标识。在创建引用标识后，可向或从引用标识中添加或删除四种类型的标识符及其相关联的值。引用标识符可以包含标识应用服务的信息，并且必须包含标识 DNS 域名的信息。

开始之前

- 当仅连接到系统日志服务器和智能许可服务器时，将使用引用标识。其他 ASA SSL 客户端模式连接目前都不支持配置或使用引用标识。
- ASA 将实施用于匹配 RFC 6125 中所述标识符的所有规则（除交互式客户端的已固定证书和回退以外）。
- 不会实施固定证书的功能。因此，不会出现 `No Match Found、Pinned Certificate`。此外，如果由于我们的实施并非交互式客户端而未找到匹配，则不会向用户提供固定证书的机会。

过程

步骤 1 在全局配置模式下输入 **[no] crypto ca reference-identity** 命令，以将 ASA 置于 ca-reference-identity 模式下。

[no] crypto ca reference-identity *reference-identity-name*

如果未找到包含此 *reference-identity-name* 的引用标识，将创建一个新引用标识。如果为仍在使用中的引用标识发布了该命令的 **no** 形式，则将显示一条警告，并且不会删除引用标识。

步骤 2 在处于 ca-reference-identity 模式下时输入引用标识。可向引用标识中添加多个任何类型的引用标识。

- **[no] cn-id** 值
- **[no] dns-id** 值
- **[no] srv-id** 值
- **[no] uri-id** 值

要删除引用标识，请使用该命令的 no 形式。

示例

为系统服务器的 RFC 6125 服务器证书验证配置引用标识：

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

下一步做什么

在配置系统日志和 Smart Call Home 服务器连接时，请使用引用标识。

手动获取证书

要手动获取证书，请执行以下步骤：

开始之前

您必须已从信任点代表的 CA 获取 base-64 编码的 CA 证书。

过程

步骤 1 导入已配置的信任点的 CA 证书。

crypto ca authenticate 信任点

示例：

```
ciscoasa(config)# crypto ca authenticate Main
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[ certificate data omitted ]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint:     24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

信任点是否要求手动获取证书由配置信任点时是否使用 **enrollment terminal** 命令而定。

步骤 2 使用信任点注册 ASA。

crypto ca enroll 信任点

示例：

```
ciscoasa(config)# crypto ca enroll Main
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: securityappliance.example.com

% Include the device serial number in the subject name? [yes/no]: n

Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:

MIIBoDCCAQkCAQAwIzEhMB8GCSqGSIb3DQEJAhYSRmVyYWxQaXguY2lzY28uY29t
[ certificate request data omitted ]
jF4waw68eOxQxVmdgMWeQ+RbIOYmvt8g6hnBTrd0GdqjjVLt

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: n
```

此命令生成用于签署数据和根据已配置的密钥类型加密数据的证书。如果对签署和加密使用不同的 RSA 密钥，则 **crypto ca enroll** 命令显示两个证书请求，每个密钥各一个。如果对签名和加密使用通用 RSA 密钥，则 **crypto ca enroll** 命令显示一个证书请求。

要完成注册，请从适用信任点所代表的CA 获取由 **crypto ca enroll** 命令生成的所有证书请求的证书。确保证书采用 base-64 格式。

步骤 3 在为 CMP 配置信任点时，可以指定共享密钥值 (ir)，或者指定包含将要签署请求的 (cr) 证书的信任点的名称，但不能同时指定两者。通过 CA提供带外值（用于确认与 ASA 交换的消息的真实性和完整性），或者提供包含过去颁发的设备证书的信任点的名称（用于签署CMP注册请求）。仅在将信任点注册协议设置为 CMP 时，共享密钥或签名证书关键字才可用。

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate <value>
```

步骤 4 确定是否应在建立注册请求之前生成新密钥对。

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate <value>
```

步骤 5 导入从 CA 收到的每个证书并确保以 base-64 格式将证书粘贴到终端。

crypto ca import 信任点 **certificate**

示例：

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

步骤 6 通过显示为 ASA 颁发的证书详细信息和信任点的 CA 证书，验证注册过程已成功。

show crypto ca certificate

示例：

```
ciscoasa(config)# show crypto ca  certificate Main
```

步骤 7 保存运行配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

步骤 8 对于为手动注册配置的每个信任点重复上述步骤。

使用 SCEP 自动获取证书

本节介绍如何使用 SCEP 自动获取证书。

开始之前

您必须已从信任点代表的 CA 获取 base-64 编码的 CA 证书。

过程

步骤 1 获取已配置的信任点的 CA 证书。

crypto ca authenticate 信任点

示例：

```
ciscoasa/contexta(config)# crypto ca authenticate Main
```

配置信任点时，使用 **enrollment url** 命令确定是否必须通过 SCEP 自动获取证书。

步骤 2 使用信任点注册 ASA。此命令检索用于签署数据和根据已配置的密钥类型加密数据的证书。在输入此命令前，请与 CA 管理员联系，其可能需要在 CA 授予证书之前手动对注册请求进行身份验证。

crypto ca enroll 信任点

示例：

```
ciscoasa/contexta(config)# crypto ca enroll Main
```

如果 ASA 未在发送证书请求后一分钟（默认值）内从 CA 收到证书，则会重新发送证书请求。ASA 会继续每分钟发送一次证书请求，直到收到证书。

如果为信任点配置的完全限定域名与ASA的完全限定域名（包括字符的大小写）不同，则系统将显示警告。要解决此问题，请退出注册过程，进行任何必要的更正，然后重新输入 **crypto ca enroll** 命令。

注释
如果 ASA 在您发出 **crypto ca enroll** 命令后但在收到证书前重新启动，请重新输入 **crypto ca enroll** 命令并通知 CA 管理员。

步骤 3 通过显示为 ASA 颁发的证书详细信息和信任点的 CA 证书，验证注册过程已成功。

show crypto ca certificate

示例：

```
ciscoasa/contexta(config)# show crypto ca certificate Main
```

步骤 4 保存运行配置。

write memory

示例：

```
ciscoasa/contexta(config)# write memory
```

为 SCEP 请求配置代理支持

要使用第三方 CA 配置 ASA 以对远程访问终端进行身份验证，请执行以下步骤：

过程

步骤 1 进入 tunnel-group ipsec-attributes 配置模式。

tunnel-group 名称 **ipsec-attributes**

示例：

```
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
```

步骤 2 启用客户端服务。

crypto ikev2 enable outside client-services port 端口号

示例：

```
ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services
```

默认端口号为 443。

注释
仅当支持 IKEv2 时，才需要此命令。

步骤 3 进入 tunnel-group general-attributes 配置模式。

tunnel-group 名称 **general-attributes**

示例：

```
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
```

步骤 4 为隧道组启用 SCEP 注册。

scep-enrollment enable

示例：

```
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this option.
```

步骤 5 进入 group-policy attributes 配置模式。

group-policy 名称 **attributes**

示例：

```
ciscoasa(config)# group-policy FirstGroup attributes
```

步骤 6 为组策略注册 SCEP CA。为每个组策略输入一次此命令，以支持第三方数字证书。

scep-forwarding-url value *URL*

示例：

```
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
```

URL 是 CA 上的 SCEP URL。

步骤 7 当证书不适用于 SCEP 代理的 WebLaunch 支持时，请提供通用辅助密码。

secondary-pre-fill-username clientless hide use-common-password 密码

示例：

```
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
use-common-password secret
```

您必须使用 **hide** 关键字支持 SCEP 代理。

例如，证书对于请求该证书的终端不可用。终端获得证书后，Secure Client 断开连接，然后重新连接到 ASA 以对提供内部网络资源访问权限的 DAP 策略进行限定。

步骤 8 隐藏 Secure Client VPN 会话的辅助预填写用户名。

secondary-pre-fill-username ssl-client hide use-common-password 密码

示例：

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-common-password secret
```

尽管从更早版本继承了 **ssl-client** 关键字，但此命令用于支持使用 IKEv2 或 SSL 的 Secure Client 会话。

您必须使用 **hide** 关键字支持 SCEP 代理。

步骤 9 当证书不可用时，请提供用户名。

secondary-username-from-certificate {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]

示例：

```
ciscoasa(config-tunnel-webvpn)# secondary-username-from-certificate CN no-certificate-fallback
```

```
cisco-secure-desktop machine-unique-id
```

如何设置特定整数类型

在您建立可信证书后，您就可以开始其他基础任务，如建立身份证书或更高级的配置，如建立本地 CA 或代码签名证书。

开始之前

阅读关于数字证书的信息，并建立可信证书。不含私钥的 CA 证书将供所有 VPN 协议和 webvpn 使用，并在信任点中配置，以验证传入客户端证书。同样，信任池是 webvpn 功能使用的可信证书的列表，该功能将使用这些证书验证通向 https 服务器的代理连接，以及验证 smart-call-home 证书。

过程

本地 CA 允许 VPN 客户端直接从 ASA 注册证书。这项高级配置会将 ASA 转换为 CA。要配置 CA，请参考CA 证书，第 896 页。

下一步做什么

设置证书到期警报或监控数字证书和证书管理历史。

CA 证书

在此页面中，可管理 CA 证书。以下主题介绍您可以执行的操作。

CA 服务器管理

管理用户证书

要更改证书状态，请执行以下步骤：

过程

步骤 1 在 **Manage User Certificates** 窗格中按用户名或按证书序列号选择特定证书。

步骤 2 选择以下其中一个选项：

- 如果用户证书有效期到期，请点击 **Revoke** 以删除用户访问。本地 CA 还会在证书数据库中将证书标记为已吊销，自动更新信息并重新发出 CRL。

- 选择已吊销证书并点击 **Unrevoke** 以恢复访问。本地 CA 还会在证书数据库中将证书标记为未吊销，自动更新证书信息并重新发出已更新的 CRL。

步骤 3 完成后点击 **Apply** 以保存更改。

配置信任池证书的自动导入

智能许可使用 Smart Call Home 基础设施。ASA 在后台配置 Smart Call Home 匿名报告时，ASA 会自动创建一个包含颁发 Call Home 服务器证书的 CA 的证书的信任点。现在，如果服务器的颁发层次结构发生变化，ASA 支持对证书进行验证，而无需客户来调整证书层次结构变化。您可以按照定期的间隔自动执行信任池捆绑包的更新，以便在 CA 服务器的自签名证书发生变化时 Smart Call Home 可以保持活动状态。此功能在多情景部署环境下不受支持。

信任池证书捆绑包的自动导入需要您指定 ASA 下载和导入捆绑包所用的 URL。使用以下命令，以便每天可以按照固定的间隔使用默认的思科 URL 和 22 小时的默认时间进行导入：

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

您还可以使用以下命令以自定义 URL 启用 自动导入：

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

为了能让您在非高峰时段或其他便利时间灵活地设置下载，请输入以下命令，以使用自定义时间启用导入：

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

使用自定义 URL 和自定义时间 设置自动导入需要使用以下 命令：

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

显示信任池策略的状态

使用以下命令查看 trustpool 策略的当前状态：

```
show crypto ca trustpool policy
```

此命令返回 如下信息：

```
0 trustpool certificates installed
Trustpool auto renewal statistics:
 State: Not in progress
 Last import result: Not attempted N/A
 Current Jitter: 0

Trustpool auto import statistics:
 Last import result: N/A
 Next schedule import at 22:00:00 Tues Jul 21 2015

Trustpool Policy

 Trustpool revocation checking is disabled.
 CRL cache time: 60 seconds
 CRL next update field: required and enforced
 Auto import of trustpool is enabled
 Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
 Download time: 22:00:00
```

```
Policy Overrides:
 None configured
```

清除 *CA* 信任池

要将 trustpool 策略重置为默认状态，请使用以下命令：

```
clear configure crypto ca trustpool
```

由于默认情况下会禁用 自动导入 trustpoint 证书，因此使用此命令 会禁用该功能。

设置证书到期警报（对于身份或 CA 证书）

ASA 每隔 24 小时检查一次信任点中的所有 CA 和 ID 证书是否到期。如果证书即将到期，则会将一条系统日志作为警报发出。

系统提供 CLI 来配置提醒和循环间隔。默认情况下，在到期前 60 天开始提醒并且每 7 天循环提醒一次。您可以通过使用以下命令配置提醒发送间隔和发送第一个提醒时的到期前天数：

```
[no] crypto ca alerts expiration [begin <days before expiration>] [repeat <days>]
```

不考虑警报配置， 在到期的最后一周内每天发送提醒。此外，还新增了 **show** 和 **clear** 命令，具体如下：

```
clear conf crypto ca alerts
show run crypto ca alerts
```

除了续签提醒之外，如果系统在配置中找到已到期证书，则每天会生成一次系统日志，以通过续签证书或删除已到期证书来调整配置。

例如，假设到期提醒配置为在到期前 60 天开始，此后每 6 天重复提醒一次。如果 ASA 在到期前 40 天重新启动，则系统当日会发送提醒，并在第 36 天发送下一个提醒。

注释 对于信任池证书不会执行到期检查。本地 CA 信任点会被视为也需要进行到期检查的普通信任点。

监控数字证书

请参阅以下命令来监控数字证书状态。

- **show crypto ca server**

  此命令显示本地 CA 配置和状态。

- **show crypto ca server cert-db**

  此命令显示由本地 CA 颁发的用户证书。

- **show crypto ca server certificate**

此命令以 base 64 格式显示控制台上的本地 CA 证书以及滚动更新证书（可用时），包括用于在新证书导入到其他设备时对其进行验证的滚动更新证书指纹。

- **show crypto ca server crl**

  此命令显示 CRL。

- **show crypto ca server user-db**

  此命令显示用户及其状态，可与以下限定符配合使用来减少显示的记录数：

  - allowed。仅显示当前允许注册的用户。
  - enrolled。仅显示已注册并持有有效证书的用户。
  - expired。仅显示持有已到期证书的用户。
  - on-hold。仅列出无证书且当前不允许注册的用户。

- **show crypto ca server user-db allowed**

  此命令显示符合注册条件的用户。

- **show crypto ca server user-db enrolled**

  此命令显示具有有效证书的已注册用户。

- **show crypto ca server user-db expired**

  此命令显示具有过期证书的用户。

- **show crypto ca server user-db on-hold**

  此命令显示无证书且不允许注册的用户。

- **show crypto key** *name of key*

  此命令显示您已生成的密钥对。

- **show running-config**

  此命令显示本地 CA 证书映射规则。

示例

以下示例显示 RSA 通用密钥：

```
ciscoasa/contexta(config)# show crypto key mypubkey rsa
Key pair was generated at: 16:39:47 central Feb 10 2010
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Storage: config
 Key Data:

  30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
  00ea2c38 df9c606e ddb7b08a e8b0a1a8 65592d85 0711cac5 fceddee1 fa494297
```

```
  525fffc0 90da8a4c e696e44e 0646c661 48b3602a 960d7a3a 52dae14a 5f983603
  e1f33e40 a6ce04f5 9a812894 b0fe0403 f8d7e05e aea79603 2dcd56cc 01261b3e
  93bff98f df422fb1 2066bfa4 2ff5d2a4 36b3b1db edaebf16 973b2bd7 248e4dd2
  071a978c 6e81f073 0c4cd57b db6d9f40 69dc2149 e755fb0f 590f2da8 b620efe6
  da6e8fa5 411a841f e72bb8ea cf4bdb79 f4e57ff3 a940ce3b 4a2c7052 56c1d17b
  af8fe2e2 e58718c6 ed1da0f0 1c6f36eb 79eb1aeb f098b5c4 79e07658 a52d8c7a
  51ceabfb f8ade096 7217cf2d 3728077e 89441d89 9bf5f875 c8d2db39 c858bb7a
  7d020301 0001
```

以下示例显示本地 CA CRL：

```
ciscoasa(config)# show crypto ca server crl
Certificate Revocation List:
    Issuer: cn=xx5520-1-3-2007-1
    This Update: 13:32:53 UTC Jan 4 2010
    Next Update: 13:32:53 UTC Feb 3 2010
    Number of CRL entries: 2
    CRL size: 270 bytes
Revoked Certificates:
    Serial Number: 0x6f
    Revocation Date: 12:30:01 UTC Jan 4 2010
    Serial Number: 0x47
    Revocation Date: 13:32:48 UTC Jan 4 2010
```

以下示例显示一个暂停用户：

```
ciscoasa(config)# show crypto ca server user-db on-hold
username: wilma101
email:    <None>
dn:       <None>
allowed:  <not allowed>
notified: 0
ciscoasa(config)#
```

以下示例显示 **show running-config** 命令的输出，其中会显示本地 CA 证书映射规则：

```
crypto ca certificate map 1
 issuer-name co asc
 subject-name attr ou eq Engineering
```

证书管理的历史记录

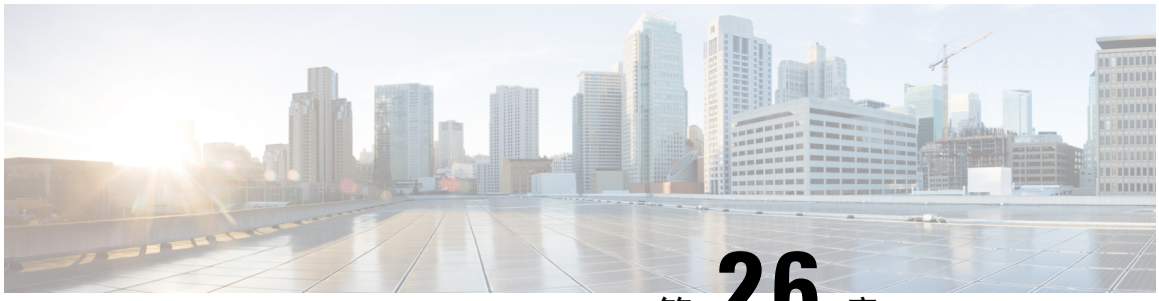
表 *32:* 证书管理的历史记录

功能名称	平台版本	说明
证书管理	7.0(1)	数字证书（包括 CA 证书、身份证书和代码签名者证书）是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或 IP 地址。CA 是“签署”证书以验证其真实性，从而确保设备或用户的身份的可信颁发机构。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。

功能名称	平台版本	说明
证书管理	7.2(1)	引入了以下命令： **issuer-name** *DN-string*、**revocation-check crl none**、**revocation-check crl**、**revocation-check none**。 废弃了以下命令：**crl** {**required** | **optional** | **nocheck**}。
证书管理	8.0(2)	引入了以下命令： **cdp-url**、**crypto ca server**、**crypto ca server crl issue**、**crypto ca server revoke** *cert-serial-no*、**crypto ca server unrevoke** *cert-serial-no*、**crypto ca server user-db add** *user* [**dn** *dn*] [**email** *e-mail-address*]、**crypto ca server user-db allow** {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**]、**crypto ca server user-db email-otp** {*username* | **all-unenrolled** | **all-certholders**}、**crypto ca server user-db remove** *username*、**crypto ca server user-db show-otp** {*username* | **all-certholders** | **all-unenrolled**}、**crypto ca server user-db write**、[**no**] **database path** *mount-name directory-path*、**debug crypto ca server** [*level*]、**lifetime** {**ca-certificate** | **certificate** | **crl**} *time*、**no shutdown**、**otp expiration** *timeout*、**renewal-reminder** *time*, **show crypto ca server**、**show crypto ca server cert-db** [**user** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial** *certificate-serial-number*]、**show crypto ca server certificate**、**show crypto ca server crl**、**show crypto ca server user-db** [**expired** | **allowed** | **on-hold** | **enrolled**]、**show crypto key** *name of key*、**show running-config**、**shutdown**。
SCEP 代理	8.4(1)	引入了此功能，可从第三方CA对设备证书进行安全部署。 引入了以下命令： **crypto ikev2 enable outside client-services port** *portnumber*、**scep-enrollment enable**, **scep-forwarding-url value** *URL*、**secondary-pre-fill-username clientless hide use-common-password** *password*、**secondary-pre-fill-username ssl-client hide use-common-password** *password*、**secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]。

功能名称	平台版本	说明
引用标识	9.6(2)	TLS 客户端处理现在支持针对 RFC 6125 第 6 节中定义的服务器身份验证的规则。身份验证将在 PKI 验证期间仅针对与系统日志服务器和智能许可服务器的 TLS 连接执行。如果所显示的身份无法与配置的参考身份匹配，则不会建立连接。 添加或修改了以下命令：**crypto ca reference-identity**、**logging host** 和 **call home profile destination address**。
本地 CA 服务器	9.12(1)	要使注册 URL 的 FQDN 可配置，而不是使用 ASA 的已配置 FQDN，引入新的 CLI 选项。此新选项已添加到 crypto ca server 的 smpt 模式。 我们启用了本地 CA 服务器，并将在后续版本中删除 — 当 ASA 配置为本地 CA 服务器时，系统会启用该服务器以颁发数字证书、发布证书吊销列表 (CRL)，并安全地撤销已颁发的证书。此功能已过时，因此弃用加密 CA 服务器命令。
本地 CA 服务器	9.13(1)	删除了本地 CA 服务器支持。因此，将会删除 **crypto ca server** 命令及其子命令。 删除了以下命令：**crypto ca server** 及其所有子命令。
对 CRL 分发点命令的修改	9.13(1)	静态 CDP URL 配置命令将被删除并移至匹配证书命令。 新增/修改的命令：**crypto-ca-trustpoint crl**、**crl url** 与其他相关逻辑一起删除。**match-certificate override-cdp** 引入了。
增加了 CRL 缓存大小	9.13(1)	为防止大型 CRL 下载失败，增加了缓存大小，并且删除了单个 CRL 中的条目数限制。 • 在多情景模式下，将每个情景的 CRL 缓存总大小增加到 16 MB。 • 在单一情景模式下，将 CRL 缓存总大小增加到 128 MB。
恢复绕行证书有效性检查选项	9.15(1)	恢复了由于在 9.13(1) 中删除的 CRL 或 OCSP 服务器的连接问题而绕过吊销检查的选项已恢复。 新增/修改的命令：恢复了 **revocation-check crl none**、**revocation-check ocsp none**、**revocation-check crl ocsp none** 和 **revocation-check ocsp crl none** 。

功能名称	平台版本	说明
修改匹配证书命令以支持静态CRL分发点URL	9.15(1)	静态 CDP URL 配置命令允许将静态 CDP 唯一映射到正在验证的链中的每个证书。但是，每个证书仅支持一个此类映射。此次修改后，系统允许将静态配置的 CDP 映射到证书链以进行身份验证。 新增/修改的命令：**match certificate** *map* **override cdp** *seq* **url** *url* and **no match certificate** *map* **override cdp** *seq* **url** *url*
对信任点密钥对和加密密钥生成命令的修改	9.16（1）	不再支持密钥大小小于 2048 的证书。任何使用 512、768 或 1024 位选项的配置都将过渡到 2048，并发出通知。 不再支持使用 SHA1 散列算法进行认证。 **注释** 引入了 **crypto ca permit-weak-crypto** 命令以覆盖这些限制。 新的密钥选项 - EDDSA 已添加到现有 RSA 和 ECDSA 选项中。
支持 OCSP 和 CRL IPv6 URL	9.20(1)	添加了对使用 IPv6 OCSP 和 CRL URL 的支持。IPv6 地址必须用方括号括起来。



第 26 章

的 ARP 检测和 MAC 地址表

本章介绍如何自定义 MAC 地址表以及为网桥组配置 ARP 检测。

- 关于 ARP 检测和 MAC 地址表，第 905 页
- 默认设置，第 906 页
- ARP 检测和 MAC 地址表准则，第 906 页
- 配置 ARP 检测和其他 ARP 参数，第 907 页
- 自定义网桥组的 MAC 地址表，第 909 页
- 监控 ARP 检测和 MAC 地址表，第 910 页
- ARP 检测和 MAC 地址表的历史记录，第 911 页

关于 ARP 检测和 MAC 地址表

对于网桥组中的接口，ARP检测可防止“中间人”攻击。您还可以自定义其他ARP设置。您可以自定义网桥组的 MAC 地址表，包括添加静态 ARP 条目来防范 MAC 欺骗。

网桥组流量的 ARP 检测

默认情况下，桥接组成员之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量。

ARP检测可防止恶意用户模拟其他主机或路由器（称为ARP欺骗）。ARP欺骗能够启用“中间人”攻击。例如，主机向网关路由器发送 ARP 请求；网关路由器使用网关路由器 MAC 地址进行响应。但是，攻击者使用攻击者 MAC 地址（而不是路由器 MAC 地址）将其他 ARP 响应发送到主机。这样，攻击者即可在所有主机流量转发到路由器之前将其拦截。

ARP 检测确保只要静态 ARP 表中的 MAC 地址和相关 IP 地址正确，攻击者就无法利用攻击者 MAC 地址发送 ARP 响应。

当启用 ARP 检测查时，ASA 将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目进行比较，并执行下列操作：

- 如果 IP 地址、MAC 地址和源接口与 ARP 条目匹配，则数据包可以通过。
- 如果 MAC 地址、IP 地址或接口之间不匹配，则 ASA 会丢弃数据包。

- 如果 ARP 数据包与静态 ARP 表中的任何条目都不匹配，则可以将 ASA 设置为从所有接口向外转发数据包（泛洪），或者丢弃数据包。

注释 即使此参数设置为 flood，专用管理接口也绝不会以泛洪方式传输数据包。

MAC 地址表

当你使用网桥组时，ASA 以与一般网桥或交换机相似的方式获悉和构建 MAC 地址表：当某个设备通过网桥组发送数据包时，ASA 将在其表中添加 MAC 地址。此表将 MAC 地址与源接口相关联，以便ASA可了解如何将要发送到设备的任何数据包从正确的接口发出。由于网桥组成员之间的流量须遵守 ASA 安全策略，因此如果数据包的目标 MAC 地址不在此表中，则 ASA 不会像一般网桥那样以泛洪方式传输所有接口上的原始数据包。相反，它会为直连设备或远程设备生成以下数据包：

- 面向直连设备的数据包 - ASA 将生成针对目标 IP 地址的 ARP 请求，以使它能了解哪个接口接收 ARP 响应。
- 面向远程设备的数据包 - ASA将生成一个针对目标 IP 地址的 ping，以使它能了解哪个接口接收 ping 应答。

系统会丢弃原始数据包。

对于路由模式，可以选择在所有接口上启用非 IP 数据包泛洪。

默认设置

- 如果启用 ARP 检测，则默认情况下会以泛洪方式传输不匹配的数据包。
- 动态 MAC 地址表条目的默认超时值为 5 分钟。
- 默认情况下，每个接口会自动获悉进入流量的 MAC 地址，并且 ASA 会将对应的条目添加到 MAC 地址表中。

注释 Cisco Secure Firewall ASA 生成重置数据包以重置状态检测引擎拒绝的连接。在这里，数据包的目标MAC地址不是根据ARP表查找确定的，而是直接从被拒绝的数据包（连接）中获取的。

ARP 检测和 MAC 地址表准则

- ARP 检测仅支持网桥组。
- MAC 地址表配置仅支持网桥组。

配置 ARP 检测和其他 ARP 参数

对于网桥组，可以启用 ARP 检测。您还可以为网桥组和路由模式接口配置其他 ARP 参数。

过程

步骤 1 根据添加静态 ARP 条目并自定义其他 ARP 参数，第 907 页中所述添加静态 ARP 条目。ARP 检测会将 ARP 数据包与 ARP 表中的静态 ARP 条目作比较，因此该功能需要静态 ARP 条目。您还可以配置其他 ARP 参数。

步骤 2 根据启用 ARP 检测，第 908 页启用 ARP 检测。

添加静态 ARP 条目并自定义其他 ARP 参数

对于桥接组，默认情况下，桥接组成员接口之间允许所有 ARP 数据包。可以通过启用 ARP 检测来控制 ARP 数据包的流量。ARP 检测会对比 ARP 数据包与 ARP 表中的静态 ARP 条目。

对于路由接口，可以输入静态 ARP 条目，但通常动态条目就足够了。对于路由接口，使用 ARP 表向直连主机交付数据包。虽然发件人可根据 IP 地址识别数据包目标，但在以太网上实际交付数据包依赖于以太网 MAC 地址。当路由器或主机希望在直连网络上交付数据包时，它会发送 ARP 请求来寻求与该 IP 地址关联的 MAC 地址，然后根据 ARP 响应将数据包交付到 MAC 地址。主机或路由器可保留 ARP 表，所以不必对需要交付的每个数据包都发送 ARP 请求。只要在网络上发送 ARP 响应，便会动态更新 ARP 表，但如果一段时间未使用条目，则它会超时。如果某个条目错误（例如给定 IP 地址的 MAC 地址改变），该条目需要超时后，才能为其更新新信息。

对于透明模式，ASA 仅对进出 ASA 的流量（例如管理流量）使用 ARP 表中的动态 ARP 条目。

此外，还可以设置 ARP 超时和其他 ARP 行为。

过程

步骤 1 添加静态 ARP 条目：

arp *interface_name ip_address mac_address* [**alias**]

示例：

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

本示例在外部接口上允许来自地址 10.1.1.1、MAC 地址 0009.7cbe.2100 的路由器的 ARP 响应。

在路由模式下，指定 **alias** 可为此映射启用代理 ARP。如果 ASA 收到指定 IP 地址的 ARP 请求，则会使用 ASA MAC 地址做出响应。例如，此关键字在您有不执行 ARP 的设备时非常有用。在透明防火墙模式下，此关键字将被忽略；ASA 不执行代理 ARP。

步骤 2 设置动态 ARP 条目的 ARP 超时：

arp timeout 秒

示例：

```
ciscoasa(config)# arp timeout 5000
```

此字段设置 ASA 在重建 ARP 表前允许的时长，范围介于 60 到 4294967 秒之间。默认值为 14400 秒。重建 ARP 表会自动更新新的主机信息并删除旧的主机信息。由于主机信息频繁更改，因此可能要减少超时。

步骤 3 允许未连接的子网：

arp permit-nonconnected

ASA ARP 缓存默认仅包含来自直连子网的条目。可以启用 ARP 缓存，以将非直连子网也包含在内。除非您了解安全风险，否则不建议启用此功能。此功能可能有助于引发对 ASA 的拒绝服务 (DoS) 攻击；任意接口上的用户都可能发出许多 ARP 应答，并使 ASA ARP 表中的错误条目超载。

如果您使用以下对象，则可能要使用此功能：

- 辅助子网。
- 用于流量转发的相邻路由上的代理 ARP。

步骤 4 设置 ARP 速率限制以控制每秒的 ARP 数据包数：

arp rate-limit 秒

示例：

```
ciscoasa(config)# arp rate-limit 1000
```

输入 10 到 32768 之间的值。默认值取决于 ASA 型号。您可以自定义此值以防止 ARP 风暴攻击。

启用 ARP 检测

本节介绍如何为网桥组启用 ARP 检测。

过程

启用 ARP 检测：

arp-inspection *interface_name* **enable** [**flood** |**no-flood**]

示例：

```
ciscoasa(config)# arp-inspection outside enable no-flood
```

flood 关键字将不匹配的 ARP 数据包转发出所有接口，**no-flood** 则会丢弃不匹配的数据包。

默认设置是以泛洪方式传输不匹配的数据包。要通过 ASA 将 ARP 限制为仅静态条目，请将此命令设置为 **no-flood**。

自定义网桥组的 MAC 地址表

本部分介绍如何为网桥组自定义 MAC 地址表.

为网桥组添加静态 MAC 地址

通常，当来自特定 MAC 地址的流量进入某个接口时，MAC 地址会动态添加到 MAC 地址表中。可以向 MAC 地址表中添加静态 MAC 地址。添加静态条目的一个好处是，可以防止 MAC 欺骗。如果与静态条目具有相同 MAC 地址的客户端尝试向不匹配静态条目的接口发送流量，ASA 将会丢弃流量并生成系统消息。当添加静态 ARP 条目时（请参阅添加静态 ARP 条目并自定义其他 ARP 参数，第 907 页），静态 MAC 地址条目会自动添加到 MAC 地址表中。

要向 MAC 地址表中添加静态 MAC 地址，请执行以下步骤。

过程

添加静态 MAC 地址条目：

mac-address-table static *interface_name mac_address*

示例：

```
ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100
```

interface_name 是源接口。

设置 MAC 地址超时

动态MAC地址表条目的默认超时值为5分钟，但您可以更改超时。要更改超时，请执行以下步骤：

过程

设置 MAC 地址条目超时：

mac-address-table aging-time *timeout_value*

示例：

```
ciscoasa(config)# mac-address-table aging-time 10
```

timeout_value（以分钟为单位）介于 5 到 720（12 小时）之间。默认值为 5 分钟。

配置 MAC 地址学习

默认情况下，每个接口都会自动获悉进入流量的 MAC 地址，ASA 会将相应的条目添加至 MAC 地址表。如果需要，您可以禁用 MAC 地址获悉，不过除非您将 MAC 地址静态添加至此表中，否则没有流量可以通过 ASA。在路由模式下，可以在所有接口上启用非 IP 数据包泛洪。

要配置 MAC 地址学习，请执行以下步骤：

过程

步骤 1 禁用 MAC 地址获悉：

mac-learn *interface_name* **disable**

示例：

```
ciscoasa(config)# mac-learn inside disable
```

此命令的 **no** 形式会重新启用 MAC 地址获悉。

clear configure mac-learn 命令会在所有接口上重新启用 MAC 地址获悉。

步骤 2 （仅限路由模式）启用非 IP 数据包的泛洪。

mac-learn 泛洪

示例：

```
ciscoasa(config)# mac-learn flood
```

监控 ARP 检测和 MAC 地址表

- **show arp-inspection**

  监控 ARP 检测。显示所有接口上的 ARP 检测的当前设置。

- **show mac-address-table [*interface_name*]**

监控MAC地址表。可以查看整个MAC地址表（包括两个接口的静态和动态条目），也可以查看某个接口的 MAC 地址表。

以下是 **show mac-address-table** 命令（用于显示整个 MAC 地址表）的样本输出：

```
ciscoasa# show mac-address-table
interface        mac address           type         Time Left
------------------------------------------------------------------------
outside     0009.7cbe.2100       static    -
inside      0010.7cbe.6101       static    -
inside      0009.7cbe.5101       dynamic    10
```

以下是 **show mac-address-table** 命令（用于显示内部接口的 MAC 地址表）的样本输出：

```
ciscoasa# show mac-address-table inside
interface        mac address       type         Time Left
------------------------------------------------------------------------
inside      0010.7cbe.6101       static    -
inside      0009.7cbe.5101       dynamic    10
```

以下是 **show mac-address-table** 命令（用于静态和动态网桥组条目的总数）的样本输出：

```
ciscoasa# show mac-address-table count
Static     mac-address bridges (curr/max): 0/16384
Dynamic    mac-address bridges (curr/max): 0/16384
```

ARP 检测和 MAC 地址表的历史记录

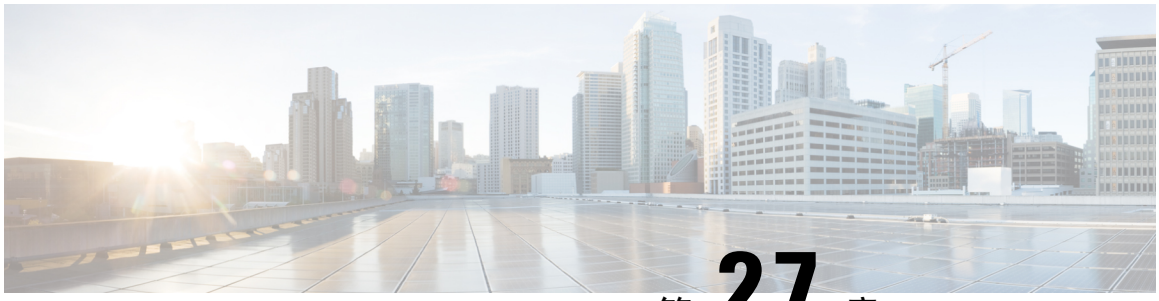
功能名称	平台版本	功能信息
ARP 检测	7.0(1)	ARP 检测会将所有 ARP 数据包中的 MAC 地址、IP 地址和源接口与 ARP 表中的静态条目作比较。此功能适用于透明防火墙模式，而且自 9.7(1) 起，还适用于透明模式和路由模式下桥接组中的接口。 引入了以下命令：**arp**、**arp-inspection** 和 **show arp-inspection**。
MAC 地址表	7.0(1)	您可能希望为透明防火墙模式自定义 MAC 地址表，而且自 9.7(1) 起，还为透明模式和路由模式下桥接组中的接口进行自定义。 引入了以下命令：**mac-address-table static**、**mac-address-table aging-time**、**mac-learn disable** 和 **show mac-address-table**。

功能名称	平台版本	功能信息
针对未连接的子网添加 ARP 缓存	8.4(5)/9.1(2)	在默认情况下，ASA ARP 缓存仅包含来自直连子网的条目。现在，可以启用 ARP 缓存，以将非直连子网也包含在内。除非您了解安全风险，否则不建议启用此功能。此功能可能有助于引发对 ASA 的拒绝服务 (DoS) 攻击；任意接口上的用户都可能发出许多 ARP 应答，并使 ASA ARP 表中的错误条目超载。 如果您使用以下对象，则可能要使用此功能： • 辅助子网。 • 用于流量转发的相邻路由上的代理 ARP。 引入了以下命令：**arp permit-nonconnected**。
可自定义的 ARP 速率限制	9.6(2)	您可以设置每秒允许的最大 ARP 数据包数。默认值取决于 ASA 型号。您可以自定义此值以防止 ARP 风暴攻击。 添加了以下命令：**arp rate-limit**、**show arp rate-limit**
集成的路由与桥接	9.7(1)	集成路由和桥接提供了在网桥组和路由接口之间路由的功能。网桥组指 ASA 桥接（而非路由）的接口组。ASA 并非真正的网桥，因为 ASA 仍继续充当防火墙：控制接口之间的访问控制，并执行所有常规防火墙检查。以前，您只能在透明防火墙模式下配置网桥组，而无法在网桥组之间路由。通过此功能，可以在路由防火墙模式下配置网桥组，并在网桥组之间以及网桥组与路由接口之间进行路由。网桥组使用网桥虚拟接口 (BVI) 作为网桥组的网关，由此参与路由。如果 ASA 上还有额外接口可分配给网桥组，集成路由和桥接可提供替代使用外部第 2 层交换机的其他方案。在路由模式下，BVI 可以是已命名接口，并可独立于成员接口参与某些功能，例如访问规则和DHCP服务器。 路由模式不支持透明模式下支持的以下功能：多情景模式、ASA 集群。以下功能在 BVI 上也不受支持：动态路由和组播路由。 修改了以下命令：**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn**

第 V 部分

IP 路由

- 路由概述， 第 915 页
- 静态和默认路由， 第 927 页
- 策略型路由， 第 937 页
- 路由映射， 第 957 页
- 双向转发检测路由， 第 963 页
- BGP， 第 973 页
- OSPF， 第 1015 页
- IS-IS， 第 1077 页
- EIGRP， 第 1125 页
- 组播路由， 第 1155 页



第 27 章

路由概述

本章介绍有关路由如何在 ASA 内部运行。

- 确定路径，第 915 页
- 支持的路由类型，第 916 页
- 支持的互联网路由协议，第 917 页
- 路由表，第 917 页
- 管理流量的路由表，第 923 页
- 等价多路径 (ECMP) 路由，第 924 页
- 禁用代理 ARP 请求，第 925 页
- 显示路由表，第 926 页
- 路由概述的历史记录，第 926 页

确定路径

路由协议使用指标来评估传播数据包的最佳路径。指标是一种测量标准，例如供路由算法用于确定目标的最佳路径的路径带宽。为帮助执行确定路径的过程，路由算法会初始化和维护其中包含路由信息的路由表。路由信息根据所使用的路由算法而异。

路由算法使用各种信息来填充路由表。目标或下一跳关联告知路由器，可以通过将数据包发送到特定路由器（表示通往最终目标的下一跳）来以最优路径到达特定目标。当路由器收到传入数据包时，会检查目标地址并尝试将此地址与下一跳关联。

路由表还包含其他信息，例如有关路径可取性的数据。路由器通过比较指标来确定最佳路由，而这些指标根据所使用的路由算法的设计而异。

路由器互相进行通信，并通过传输各种消息来维护其路由表。路由更新消息是通常由路由表的全部或部分内容组成的消息。通过分析来自所有其他路由器的路由更新，路由器可以构建详细的网络拓扑图。链路状态通告（路由器之间发送的另一种消息）用于告知其他路由器发送方链路的状态。链路信息还可用于构建完整网络拓扑图，以使路由器能够确定通向网络目标的最佳路径。

注释 在多情景模式下，仅主用/主用故障转移支持非对称路由。

支持的路由类型

路由器可以使用多种路由类型。ASA 使用以下路由类型：

- 静态与动态
- 单路径与多路径
- 平面与分层
- 链路状态与距离矢量

静态与动态

静态路由算法实际上是网络管理员建立的表映射。除非网络管理员修改这些映射，否则映射不会发生更改。使用静态路由的算法设计简单，并且在网络流量相对可预测且网络设计相对简单的环境下适用。

由于静态路由系统无法对网络更改作出反应，因此通常被认为不适合大型且不断变化的网络。大多数主要的路由算法为动态路由算法，这些算法通过分析传入路由更新消息来适应变化的网络环境。如果有消息表明网络发生更改，则路由软件会重新计算路由并发出新的路由更新消息。这些消息会渗入网络，促使路由器重新运行其算法并相应地更改其路由表。

可以酌情使用静态路由对动态路由算法进行补充。例如，可以将必备路由器（所有无法路由的数据包都发送到的路由器的默认路由）指定为所有无法路由的数据包的存储库，从而确保所有消息都至少以某种方式进行处理。

单路径与多路径

某些综合路由协议支持指向同一目标的多个路径。与单路径算法不同，这些多路径算法允许流量在多条线路上多路复用。多路径算法的优势在于显著提高吞吐量和可靠性，通常称为负载共享。

平面与分层

某些路由算法在平面空间中运行，而其他算法则使用路由层次结构。在平面路由系统中，路由器是所有其他路由器的对等体。在分层路由系统中，某些路由器形成实际上的路由主干。来自非主干路由器的数据包会传播到主干路由器，在此数据包通过主干进行发送，直至到达目标的大致区域。此时，数据包通过一个或者多个非主干路由器从最后一个主干路由器传播到最终目标。

路由系统通常会指定一些逻辑节点组，称为域、自治系统或区域。在分层系统中，一个域中的一些路由器可以与其他域中的路由器进行通信，而其他路由器只能与其本域中的路由器进行通信。在超大网络中，还可能存在其他分层级别，其中位于最高分层级别的路由器形成路由主干。

分层路由的主要优点在于，它会模仿大多数公司的组织，从而很好地支持这些公司的流量模式。大多数网络通信发生在小型公司组（域）中。由于域内路由器只需知道其域中的其他路由器即可，因此可以简化这些路由器的路由算法，并根据所使用的路由算法相应地减少路由更新流量。

链路状态与距离矢量

链路状态算法（也称最短路径优先算法）将路由信息以泛洪形式发送给互联网络中的所有节点。但是，每条路由器仅发送用于说明其自身链路状态的路由表部分。在链路状态算法中，每条路由器在其路由表中构建整个网络的情景。距离矢量算法（也称为 Bellman-Ford 算法）要求每条路由器仅向其邻居发送其路由表的全部或部分内容。实质上，链路状态算法会四处发送小的更新，而距离矢量算法只将较大的更新发送给相邻路由器。距离矢量算法仅知道其邻居。通常，链路状态算法与OSPF路由协议结合使用。

支持的互联网路由协议

ASA 支持多种互联网路由协议。本节对每种协议进行简单介绍。

- 增强型内部网关路由协议 (EIGRP)

  EIGRP 是思科专有协议，用于提供与 IGRP 路由器的兼容性和无缝互操作性。通过自动重分发机制，可将 IGRP 路由导入到增强型 IGRP（反之亦然），从而可以将增强型 IGRP 逐渐添加到现有 IGRP 网络。

- 开放最短路径优先 (OSPF)

  OSPF 是由互联网工程任务小组 (IETF) 的内部网关协议 (IGP) 工作小组开发的面向互联网协议 (IP) 网络的路由协议。OSPF 使用链路状态算法构建和计算所有到达已知目标的最短路径。OSPF 区域中的每条路由器包含相同的链路状态数据库，该数据库是由每条路由器可使用的接口和可访问邻居组成的列表。

- 路由信息协议 (RIP)

  RIP 是一种使用跳数作为指标的距离矢量协议。RIP 广泛用于路由全局互联网中的流量，并且是一种内部网关协议 (IGP)，意味着在单个自治系统内执行路由。

- 边界网关协议 (BGP)

  BGP 是一种自治系统间路由协议。BGP 用于交换互联网的路由信息，并且是互联网服务提供商 (ISP) 之间所使用的协议。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

- 中间系统到中间系统 (IS-IS)

  IS-IS 是链路状态内部网关协议 (IGP)。链路状态协议的主要特点是：传播所需的信息以在每个参与的路由器上建立完整网络连接映射。然后，该映射会用于计算到目标的最短路径。

路由表

ASA对数据流量（通过设备）和管理流量（来自设备）使用单独的路由表。本部分介绍路由表 的工作原理。有关管理路由表的信息，另请参阅 管理流量的路由表 ， 第 923 页。

路由表的填充方式

ASA 路由表可以通过静态定义的路由、直连路由以及动态路由协议发现的路由来填充。由于 ASA 设备除具有路由表中的静态路由和已连接路由外，还可以运行多条路由协议，因此可通过多种方式发现或输入同一路由。当在路由表中放入同一目标的两条路由时，将按如下确定保留在路由表中的路由：

- 如果两个路由具有不同的网络前缀长度（网络掩码），则会将两个路由都视为唯一并输入到路由表中。然后，由数据包转发逻辑确定使用哪一条路由。

  例如，如果 RIP 和 OSPF 进程发现以下路由：

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  即使 OSPF 路由具有更好的管理距离，但由于两条路由具有不同的前缀长度（子网掩码），因此均会安装在路由表中。这两条路由被视为不同目标，数据包转发逻辑会确定使用哪条路由。

- 如果 ASA 设备从单个路由协议（例如 RIP）获悉通向同一目标的多条路径，则会在路由表中输入具有更佳指标的路由（由路由协议确定）。

  度量是与特定路由关联的值，从最高优先到最低优先进行排序。用于确定度量的参数根据路由协议而异。具有最低指标的路径选择作为最佳路径并安装在路由表中。如果有多个度量相等的通向同一目的地的路径，则会在这些等价路径上进行负载均衡。

- 如果ASA设备从多个路由协议获悉目标，则会比较路由的管理距离，并在路由表中输入管理距离较短的路由。

路由的管理距离

您可以更改由路由协议发现或重分发到路由协议中的路由的管理距离。如果来自两个不同路由协议的两条路由具有相同的管理距离，则会将具有较短默认管理距离的路由输入到路由表中。对于EIGRP和 OSPF 路由，如果 EIGRP 路由和 OSPF 路由具有相同的管理距离，则默认选择 EIGRP 路由。

管理距离是 ASA在有两个或多个通向同一目标（来自两个不同路由协议）的路由时，用于选择最佳路径的路由参数。由于路由协议具有基于不同于其他协议的算法的度量，因此并非总能够确定通向由不同路由协议生成的同一目的地的两条路由的最佳路径。

每个路由协议使用管理距离值划分优先级。下表显示 ASA支持的路由协议的默认管理距离值。

表 *33:* 受支持的路由协议的默认管理距离

路由源	默认管理距离
已连接的接口	0
VPN 路由	1
静态路由	1

路由源	默认管理距离
EIGRP 汇总路由	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部路由	170
内部和本地 BGP	200
未知	255

管理距离值越小，协议的优先等级越高。例如，如果 ASA从 OSPF 路由进程（默认管理距离 - 110）和 RIP 路由进程（默认管理距离 - 120）均收到通向特定网络的路由，则 ASA 会选择 OSPF 路由，因为 OSPF 具有更高的优先级。在这种情况下，路由器会将 OSPF 版本的路由添加到路由表。

VPN 通告路由 (V-Route/RRI)）相当于默认管理距离为 1 的静态路由。但与网络掩码 255.255.255.255 一样，它具有更高的优先级。

在本示例中，如果 OSPF 派生路由的源丢失（例如，由于电源关闭），则 ASA会使用 RIP 派生路由，直至 OSPF 派生路由再次出现。

管理距离是一项本地设置。例如，如果您更改通过 OSPF 获取的路由的管理距离，那么这种更改只会影响在其上输入该命令的 ASA的路由表。在路由更新中不会通告管理距离。

管理距离不影响路由进程。路由进程仅通告路由进程已发现或重分发到路由进程中的路由。例如，即使在 路由表中使用 OSPF 路由进程发现的路由，RIP 路由进程也会通告 RIP 路由。

备份动态和浮动静态路由

当由于安装另一条路由而导致初始尝试将路由安装在路由表中失败时，系统会注册备用路由。如果安装在路由表中的路由失败，则路由表维护进程会呼叫已注册备用路由的每个路由协议进程，并请求它们重新在路由表中安装此路由。如果有多个协议为失败路由注册了备用路由，则根据管理距离选择优先路由。

鉴于以上过程，当动态路由协议发现的路由失败时，您可以创建安装在路由表中的浮动静态路由。浮动静态路仅仅是配置有比 ASA上运行的动态路由协议更大的管理距离的静态路由。当动态路由进程发现的对应路由失败时，会在路由表中安装静态路由。

如何制定转发决策

系统按如下制定转发决策：

- 如果目的不匹配路由表中的条目，则通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，则会丢弃数据包。
- 如果目的匹配路由表中的单个条目，则通过与该路由关联的接口转发数据包。
- 如果目的匹配路由表中的多个条目，则通过与具有较长网络前缀的路由相关联的接口转发数据包。

例如，发往 192.168.32.1 的数据包到达在路由表中拥有以下路由的接口：

- 192.168.32.0/24 网关 10.1.1.2
- 192.168.32.0/19 网关 10.1.1.3

在这种情况下，发往 192.168.32.1 的数据包直接发送到 10.1.1.2，因为 192.168.32.1 属于 192.168.32.0/24 网络。它也属于路由表中的其他路由，但 192.168.32.0/24 在路由表中的前缀最长（24 位对比 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。

注释 即便新的相似连接将因路由中的变化而导致不同行为，现有连接也将继续使用其已建立的接口。

动态路由和故障转移

当主用设备上的路由表发生更改时，在备用设备上同步动态路由。这意味着主用设备上的所有添加、删除或更改都将立即传播到备用设备。如果备用设备在主用/备用就绪 故障转移对中处于活动状态，则它会有与前一个主用设备相同的路由表，因为路由作为 故障转移批量同步和连续复制过程的一部分进行同步。

动态路由和集群

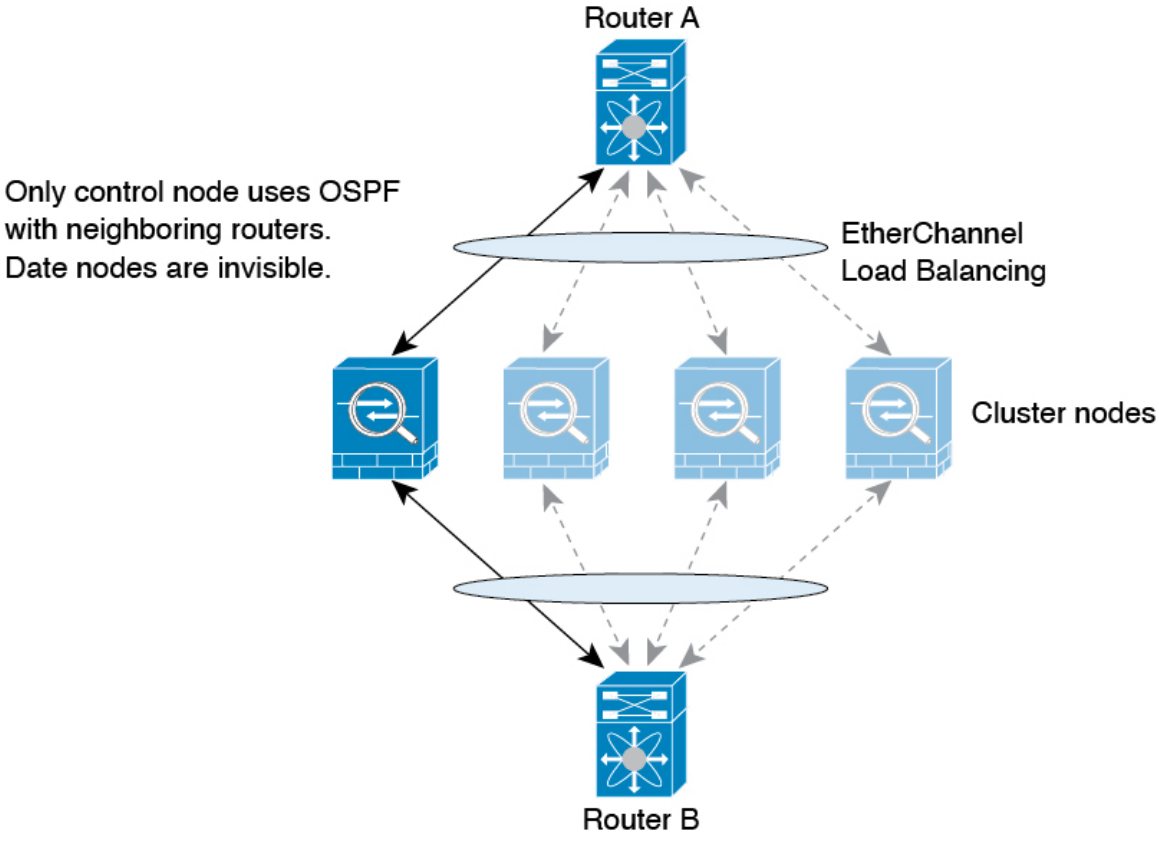
本部分介绍如何使用动态路由和集群。

跨区以太网通道模式下的动态路由

注释 跨区以太网通道模式不支持 IS-IS。

路由过程仅在控制节点上运行，并且通过控制节点学习路线后复制到数据节点。如果路由数据包到达数据节点，它将重定向到控制节点。

图 *73:* 跨区以太网通道模式下的动态路由



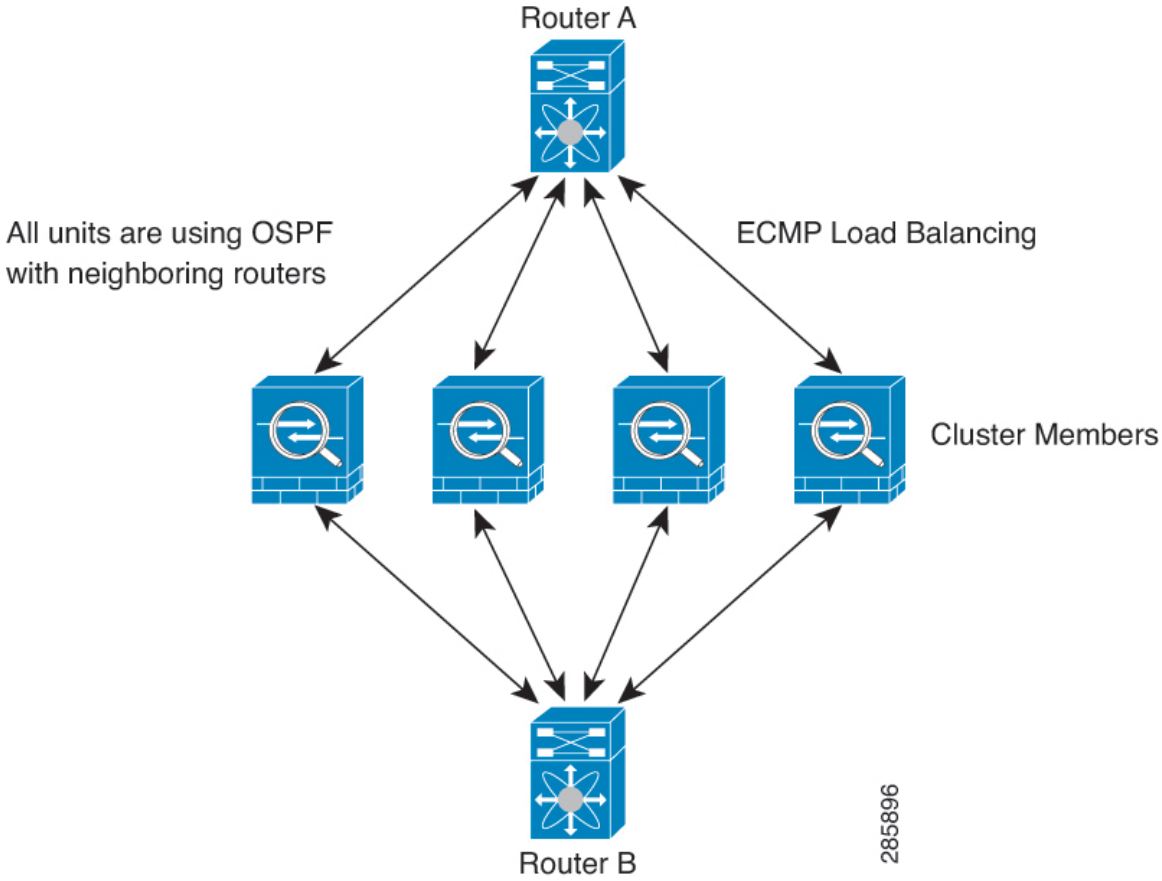
在数据节点向控制节点学习路线后，每个节点将单独做出转发决策。

OSPF LSA 数据库不会从控制节点同步到数据节点。如果切换了控制节点，邻近路由器将检测到重新启动；切换是不透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。请参阅 OSPF 无间断转发功能，解决中断问题。

独立接口模式下的动态路由

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *74:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一个节点。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每个节点在与外部路由器通信时，都会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

EIGRP 与单个接口模式下的集群对等体不构成邻居关系。

注释 如果该集群为实现冗余有多个设备与同一个路由器相邻，则非对称路由可能会造成不可接受的流量损失。要避免非对称路由，请将所有这些节点接口分组到同一流量区域中。请参阅配置流量区域，第 806 页。

多情景模式下的动态路由

在多情景模式下，每个情景维护单独的路由表和路由协议数据库。因而您可以在每个情景中独立配置 OSPFv2 和 EIGRP。您可以在某些情景中配置 EIGRP，并在相同或不同的情景中配置 OSPFv2。

在混合情景模式下，您可以在处于路由模式下的情景中启用任何动态路由协议。在多情景模式下，不支持 RIP 和 OSPFv3。

下表列出了 EIGRP 及 OSPFv2 的属性、用于将路由分发到 OSPFv2 和 EIGRP 进程中的路由映射、以及在 OSPFv2 中用于筛选路由更新（多情景模式下进入或离开某个区域）的前缀列表：

EIGRP	OSPFv2	路由映射和前缀列表
每个情景支持一个实例。	每个情景支持两个实例。	N/A
在系统情景中禁用。		N/A
两个情景可能使用相同或不同的自治系统编号。	两个情景可能使用相同或不同的区域 ID。	N/A
两个情景的共享接口可能会运行多个 EIGRP 实例。	两个情景的共享接口可能会运行多个 OSPP 实例。	N/A
支持跨共享接口的 EIGRP 实例交互。	支持跨共享接口的 OSPFv2 实例交互。	N/A
在单模式下可用的所有 CLI 在多情景模式下也可用。		
每个 CLI 仅在对其进行了使用的情景中起作用。		

路由资源管理

资源类（称为路由）指定可存在于情景中的路由表条目的最大数量。这可解决一个情景影响另一个情景中的可用路由表条目的问题，您也可以对每个情景的最大路由条目数进行更好的控制。

由于没有明确的系统限制，因此只能为此资源限制指定绝对值，不能使用百分比限制。此外，每个情景没有最小限制和最大限制，因此默认类不会进行更改。如果您在某个情景中为静态或动态路由协议（已连接、静态、OSPF、EIGRP 和 RIP）添加新的路由，但情景的资源限制已被耗尽，则路由添加失败，并会生成系统日志消息。

管理流量的路由表

作为一项标准安全实践，通常需要将管理（关联设备）流量与数据流量分开并隔离。要实现这种隔离， ASA 设备为管理专用流量和数据流量使用单独的路由表。单独的路由表意味着您也可以创建用于数据和管理的单独默认路由。

每个路由表的流量类型

关联设备流量始终使用数据路由表。

关联设备流量（根据类型）在默认情况下使用管理专用路由表或数据路由表。如果在默认路由表中找不到匹配项，则会检查其他路由表。

- 管理专用路由表关联设备流量包括使用 HTTP、SCP、TFTP、**copy** 命令、智能许可、Smart Call Home、**trustpoint**、**trustpool**等打开远程文件的功能。

- 数据路由表关联设备流量包括所有其他功能，如 ping、DNS、DHCP 等。

管理专用路由表中包含的接口

管理专用接口包括所有 管理 x/x 接口以及您配置为管理专用接口的所有接口。

回退到其他路由表

如果在默认路由表中找不到匹配项，则会检查其他路由表。

使用非默认路由表

如果您需要传出流量退出默认路由表中不存在的接口，则您可能需要在配置接口时指定接口，而不是依赖于回到另一个表。ASA 仅检查指定接口的路由。例如，如果需要 ping 命令来退出管理专用接口，请在 ping 函数中指定该接口。否则，如果数据路由表中具有默认路由，则将匹配默认路由且绝不回到管理路由表。

动态路由

管理专用路由表支持独立于数据接口路由表的动态路由。给定的动态路由进程必须在管理专用接口或数据接口上运行；不能将两种类型混用。 当不使用单独的管理路由表从早期版本升级时，如果混用使用同一动态路由进程的数据接口和管理接口，则管理接口将被丢弃。

面向 VPN 要求的管理访问功能

如果配置了管理访问功能，以允许对使用 VPN 时并非从其进入 ASA 的接口进行管理访问，那么由于使用单独的管理和数据路由表所带来的路由顾虑，VPN 终端接口和管理访问接口需要为同一类型：二者需要同为管理专用接口或普通数据接口。

管理接口识别

配置为仅管理的接口被视为管理接口。

在以下配置中，GigabitEthernet0/0 和 Management0/0 接口被视为管理接口。

```
a/admin(config-if)# show running-config int g0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.10.10.123 255.255.255.0
 ipv6 address 123::123/64
a/admin(config-if)# show running-config int m0/0
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 10.106.167.118 255.255.255.0
a/admin(config-if)#
```

等价多路径 (ECMP) 路由

ASA支持等价多路径 (ECMP) 路由。

每个接口最多支持 8 个等价静态或动态路由。例如，您可以在外部接口上配置多个默认路由，指定不同的网关：

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

在这种情况下，流量在外部接口上的 10.1.1.2、10.1.1.3 和 10.1.1.4 之间进行负载均衡。流量基于散列源和目标 IP 地址、传入接口、协议、源与目标端口的算法在 指定网关之间进行分发。

使用流量区域跨多个接口的 ECMP

如果将流量区域配置为包含一组接口，在每个区域中最多可以跨 8 个接口配置最多 8 个等价静态或动态路由。例如，您可以在区域中跨三个接口配置多个默认路由：

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同样，动态路由协议可以自动配置等价路由。ASA使用更稳健的负载均衡机制跨接口对流量进行负载均衡。

当某条路由丢失时，设备会将流量无缝移至其他路由。

禁用代理 ARP 请求

当主机将IP流量发送到同一以太网网络上的其他设备时，该主机需要知道该设备的MAC地址。ARP是一个第 2 层协议，用于将 IP 地址解析为 MAC 地址。主机发送 ARP 请求，询问“谁有此 IP 地址？”拥有该 IP 地址的设备回答“我有该 IP 地址；这是我的 MAC 地址。”

当设备使用自身的 MAC 地址响应 ARP 请求时，会使用代理 ARP，即使该设备不具有 IP 地址也如此。配置 NAT 并指定与 ASA 接口位于同一网络的映射地址时，ASA 使用代理 ARP。仅当 ASA 使用代理 ARP 宣布已为目标映射地址分配 MAC 地址时，流量才可以到达主机。

在极少数情况下，您可能要为 NAT 地址禁用代理 ARP。

如果您有一个与现有网络重叠的 VPN 客户端地址池，则 ASA 默认会在所有接口上发送代理 ARP 请求。如果有另一个接口位于同一个第2层域中，则该接口将会看到ARP请求，并以自身接口的MAC地址进行回应。结果将是面向内部主机的VPN客户端的返回流量转至错误的接口并被丢弃。在这种情况下，您应在不需要代理 ARP 请求的接口上禁用代理 ARP 请求。

过程

禁用代理 ARP 请求：

sysopt noproxyarp *interface*

示例：

```
ciscoasa(config)# sysopt noproxyarp exampleinterface
```

显示路由表

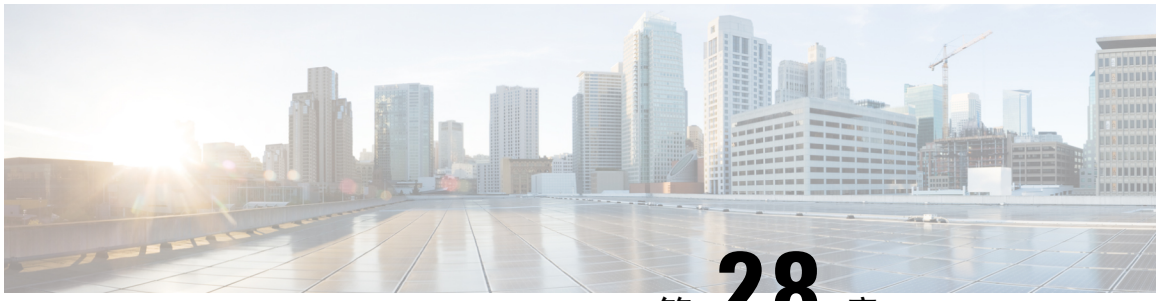
使用 **show route**命令来查看路由表。

```
ciscoasa# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

S    10.1.1.0 255.255.255.0 [3/0] via 10.86.194.1, outside
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

路由概述的历史记录

表 *34:* 路由的历史记录概述

功能名称	平台版本	功能信息
管理接口的路由表	9.5(1)	为了分隔和隔离管理流量与数据流量，对于管理流量添加了单独的 对于 ASA 每个情景的 IPv4 和 IPv6，分别为管理和数据创建了单独 表。而且，对于 ASA 的每个情景，在 RIB 和 FIB 中添加了两个额外 表。 引入了以下命令：show route management-only、show ipv6 route management-only、show asp table route-management- only、clear route management-only、clear ipv6 route management-only、copy interface < tftp/ftp



第 28 章

静态和默认路由

本章介绍如何在 ASA 上配置静态路由和默认路由。

- 关于静态路由和默认路由，第 927 页
- 静态和默认路由准则，第 929 页
- 配置默认路由和静态路由，第 930 页
- 监控静态路由或默认路由，第 934 页
- 静态路由或默认路由示例，第 934 页
- 静态和默认的历史记录，第 934 页

关于静态路由和默认路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。通常，您必须配置至少一个静态路由：所有流量的默认路由（不是通过其他方式路由到默认网络网关），通常是指下一跳路由器。

默认路由

最简单的方法是配置一个默认静态路由，将所有流量都发送到上游路由器，从而依靠该路由器来为您路由流量。默认路由对网关 IP 地址进行标识，ASA将所有不具有已获悉或静态路由的数据包发送到该网关地址。默认静态路由是以 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 作为目标 IP 地址的静态路由。

应始终定义一个默认路由。

由于ASA设备使用用于数据流量和管理流量的单独路由表，所以，您可以选择配置数据流量的默认路由和管理流量的另一默认路由。请注意，关联设备流量默认使用管理专用或数据路由表，具体取决于类型，但如果未找到路由，则会退回至其他路由表。默认路由将始终匹配流量，并将阻止退回至其他路由表。在这种情况下，如果接口不在默认路由表中，则必须指定要用于出口流量的接口。

静态路由

在以下情况下，您可能希望使用静态路由：

- 您的网络使用不受支持的路由器发现协议。

- 网络规模较小，并且可以轻松管理静态路由。
- 不希望流量或 CPU 开销与路由协议相关联。
- 在某些情况下，仅使用默认路由并不足够。默认网关可能无法到达目标网络，因此还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法将直接流量定向到未直接与ASA连接的任何内部网络。
- 您使用的是不支持动态路由协议的功能。

使用到 null0 接口的路由丢弃不必要的流量

通过访问规则，您可以根据其报头中包含的信息过滤数据包。到null0接口的静态路由是访问规则的补充性解决方案。您可以使用 null0 路由转发不必要或不需要的流量，从而丢弃该流量。

静态 null0 路由具有良好的性能配置文件。您还可以使用静态 null0 路由防止产生路由环路。BGP 可以利用静态 null0 路由进行远程触发黑洞路由。

路由优先级

- 标识具体目标的路由优先于默认路由。
- 当存在通向同一目标的多个路由（静态或动态）时，路由的管理距离即可确定优先级。静态路由设置为 1，因此其通常是优先级最高的路由。
- 当您具有多个管理距离相同的通向同一目标的静态路由时，请参阅 等价多路径 (ECMP) 路由，第 924 页。
- 对于来自具有 Tunneled 选项的隧道的新流量，此路由覆盖任何其他已配置或已知悉的默认路由。

透明防火墙模式和网桥组路由

对于源自 ASA并且通过网桥组成员接口为非直接连接网络定义的流量，需要配置默认路由或静态路由，以使 ASA了解通过哪个网桥组成员接口发出流量。源自 ASA 的流量可能包括与系统日志服务器或 SNMP 服务器的通信。如果存在无法通过单个默认路由进行访问的服务器，则必须配置静态路由。对于透明模式，不能将 BVI 指定为网关接口；只能使用成员接口。 对于路由模式下的网桥组，必须在静态路由中指定 BVI；不能指定成员接口。有关详细信息，请参阅#unique_1181。

静态路由跟踪

使用静态路由的一个问题是，缺乏用于确定路由处于开启还是关闭状态的内在机制。即使下一跳网关变得不可用，这些路由依然保留在路由表中。只有ASA上的关联接口发生故障时，才会从路由表中删除静态路由。

静态路由跟踪功能提供在主路由发生故障的情况下跟踪静态路由的可用性和安装备用路由的方法。例如，您可以定义一条到 ISP 网关的默认路由和一条到辅助 ISP的备用默认路由，以防主 ISP 不可用。

ASA 通过将静态路由与 ASA 使用 ICMP 回应请求监控的目标网络上的监控目标主机相关联来实施静态路由跟踪。如果在指定时间内没有收到回应回复，则主机将被视为关闭，并且会从路由表中删除关联路由。使用具有较高指标的未跟踪备用路由替代已删除的路由。

选择监控目标时，您需要确保它能够响应 ICMP 回应请求。该目标可以是您选择的任何网络对象，但是应考虑使用以下对象：

- ISP 网关（用于支持双 ISP）地址
- 下一跳网关地址（如果您关注网关的可用性）
- 目标网络上的服务器，例如 ASA 需要与之进行通信的系统日志服务器
- 目标网络上的持久网络对象

注释 可能会在夜间关闭的 PC 不是一个理想选择。

您可以为静态定义的路由或通过 DHCP 或 PPPoE 获取的默认路由配置静态路由跟踪。您只能在配置了路由跟踪的多个接口上启用 PPPoE 客户端。

静态和默认路由准则

防火墙模式和网桥组

- 在透明模式下，静态路由必须使用桥接组成员接口作为网关；不能指定 BVI。
- 在路由模式下，必须指定 BVI 作为网关；不能指定成员接口。
- 静态路由跟踪不支持网桥组成员接口或 BVI。

支持的网络地址

- IPv6 不支持静态路由跟踪。
- ASA 不支持 E 类路由，因此 E 类网络不能在静态路由中路由。

集群和多情景模式

- 在集群中，仅控制节点上支持静态路由跟踪。
- 多情景模式下不支持静态路由跟踪。

ASP 和 RIB 路由条目

在 ASP 路由表中捕获设备上安装的所有路由及其距离。这对于所有静态和动态路由协议都是通用的。在 RIB 表中仅捕获最佳距离路由。

配置默认路由和静态路由

您至少应配置一个默认路由。您可能还需要配置静态路由。在本节中，我们将配置默认路由，配置静态路由以及跟踪静态路由。

配置默认路由

默认路由是以 0.0.0.0/0 作为目标 IP 地址的静态路由。您应始终具有默认路由：通过此程序手动配置或者从 DHCP 服务器或其他路由协议派生。

开始之前

请参阅有关 Tunneled 选项的以下准则：

- 请勿在隧道路由的传出接口上启用单播 RPF （**ip verify reverse-path** 命令），因为此设置会导致会话失败。
- 请勿在隧道路由的传出接口上启用 TCP 拦截，因为此设置会导致会话失败。
- 请勿使用带有隧道路由的 VoIP 检测引擎（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY)、DNS 检测引擎或 DCE RPC 检测引擎，因为这些检测引擎会忽略隧道路由。
- 不能使用 tunneled 选项定义多个默认路由。
- 不支持隧道流量的 ECMP。
- 桥接组不支持隧道路由，因为不支持直通流量的 VPN 终止。

过程

添加一个默认路由。

IPv4：

route *if_name* **0.0.0.0 0.0.0.0** *gateway_ip* [**distance**] [**tunneled**]

IPv6：

ipv6 route *if_name* **::/0** *gateway_ip* [**distance**] [**tunneled**]

示例：

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.4
ciscoasa(config)# route inside 0.0.0.0 0.0.0.0 10.1.2.3 tunneled
```

```
ciscoasa(config)# ipv6 route inside ::/0 3FFE:1100:0:CC00::1
```

if_name 是要通过其发送特定流量的接口。请为透明模式指定网桥组成员接口名称。 对于具有网桥组的路由模式，请指定 BVI 名称。

distance 参数是路由的管理距离，该值介于 1 和 254 之间。如果未指定值，则默认值为 **1**。管理距离是用于比较不同路由协议之间路由的参数。静态路由的默认管理距离为 1，这使其优先于动态路由协议所发现的路由，但不优先于直连路由。OSPF 所发现路由的默认管理距离为 110。如果静态路由与动态路由的管理距离相同，则静态路由优先。已连接的路由始终优先于静态路由或动态发现的路由。

注释
对于通过设备的流量，如果您在具有不同指标的不同接口上同时配置两个默认路由，则从具有更高指标的接口到 ASA 的连接会失败，但是从具有较低指标的接口到 ASA 的连接则会如预期成功。对于设备外流量，如果在具有不同度量的不同接口上配置了两个默认路由，则两个接口可能会用于设备外流量，具体取决于用于传入连接的接口。

如果希望 VPN 流量使用与非 VPN 流量不同的默认路由，可以使用 **tunneled** 关键字定义单独的 VPN 流量。例如，从VPN连接传入的流量可以轻松定向到内部网络，而来自内部网络的流量可以定向到外部。使用 tunneled 选项创建默认路由时，来自终止于无法使用已获悉或静态路由进行路由的 ASA 的隧道的所有流量都会发送到该路由。桥接组不支持此选项。

提示
您可以为目标网络地址和掩码输入 **0 0** 而非 **0.0.0.0 0.0.0.0**，如下例所示：**route outside 0 0 192.168.2.4**

配置静态路由

静态路由用于定义为特定目标网络发送流量的位置。

过程

添加一个静态路由：

IPv4：

route *if_name dest_ip mask gateway_ip* [**distance**]

IPv6：

ipv6 route *if_name dest_ipv6_prefix/prefix_length gateway_ip* [**distance**]

示例：

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
ciscoasa(config)# ipv6 route outside 2001:DB8:1::0/32 2001:DB8:0:CC00::1
```

if_name 是要用于发送特定流量的接口。要丢弃不必要的流量，请输入 **null0** 接口。请为透明模式指定网桥组成员接口名称。 对于具有网桥组的路由模式，请指定 BVI 名称。

dest_ip 和 *mask* 或 *dest_ipv6_prefix/prefix_length* 参数指示目标网络的 IP 地址，*gateway_ip* 参数则是下一跳路由器的地址。为静态路由指定的地址是在进入 ASA 并执行 NAT 之前的数据包内的地址。

distance 参数是路由的管理距离。如果未指定值，则默认值为 **1**。管理距离是用于比较不同路由协议之间路由的参数。静态路由的默认管理距离为 1，这使其优先于动态路由协议所发现的路由，但不优先于直连路由。OSPF 所发现路由的默认管理距离为 110。如果静态路由与动态路由的管理距离相同，则静态路由优先。已连接的路由始终优先于静态路由或动态发现的路由。

示例

以下示例显示 3 个通向同一网关的网络和另一个通向不同网关的网络的静态路由。

```
route outside 10.10.10.0 255.255.255.0 192.168.1.1
route outside 10.10.20.0 255.255.255.0 192.168.1.1
route outside 10.10.30.0 255.255.255.0 192.168.1.1
route inside 10.10.40.0 255.255.255.0 10.1.1.1
```

配置静态路由跟踪

要配置静态路由跟踪，请完成以下步骤：

过程

步骤 1 为用于连接网络的接口 (outside 1) 配置静态路由：

```
ciscoasa(config)# route outside1 172.29.139.134 255.255.255.255 10.0.0.1
```

步骤 2 定义监控进程：

sla monitor sla_id

示例：

```
ciscoasa(config)# sla monitor 5
ciscoasa(config-sla-monitor)#
```

步骤 3 指定监控协议、被跟踪网络上的目标主机，以及访问网络所通过的接口。

type echo protocol ipicmpecho target_ip **interface** if_name

示例：

```
ciscoasa(config-sla-monitor)# type echo protocol ipicmpecho 172.29.139.134 interface outside1
ciscoasa(config-sla-monitor-echo)#
```

target_ip 参数是跟踪进程监控其可用性的网络对象的 IP 地址。当该对象可用时，跟踪进程路由会添加到路由表中。当该对象不可用时，跟踪进程删除该路由并改用备用路由进行替代。

步骤 4 （可选）配置监控选项。有关以下命令，请参阅命令参考：**frequency**、**num-packets**、**request-data-size**、**threshold**、**timeout** 和 **tos**。

步骤 5 安排监控进程：

sla monitor schedule sla_id [**life** {**forever** | seconds}] [**start-time** {hh:mm [:ss] [month day | day month] | **pending** | **now** | **after** hh:mm:ss}] [**ageout** seconds] [**recurring**]

示例：

```
ciscoasa(config)# sla monitor schedule 5 life forever start-time now
```

通常情况下，您将使用 **sla monitor schedule** *sla_id***life forever start-timenow** 命令监控计划，并让监控配置确定进行测试的频率。

不过，您可以将监控进程安排在未来开始并仅在指定时间发生。

步骤 6 将被跟踪的静态路由与 SLA 监控进程相关联：

track track_id **rtr** sla_id **reachability**

示例：

```
ciscoasa(config)# track 6 rtr 5 reachability
```

track_id 参数为您使用此命令分配的跟踪编号。*sla_id* 参数为 SLA 进程的 ID 编号。

步骤 7 跟踪以下路由类型之一：

- 静态路由：

  route if_name dest_ip mask gateway_ip [distance] **track** track_id

  示例：

  ```
  ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 track 6
  ```

  您不能使用 **tunneled** 选项。

- 通过 DHCP 获取的默认路由：

  ```
  interface interface_id
    dhcp client route track track_id
    ip address dhcp setroute
  ```

- 通过 PPPoE 获取的默认路由：

```
interface interface_id
  pppoe client route track track_id
  ip address pppoe setroute
```

步骤 8 创建一个未进行跟踪的备用路由。

备用路由是与被跟踪路由通向同一目标的静态路由，但是通过不同的接口或网关。您必须为此路由分配比被跟踪路由更大的管理距离（指标）。

监控静态路由或默认路由

- **show route**

  显示路由表。

静态路由或默认路由示例

以下示例显示如何创建静态路由，该路由将以 10.1.1.0/24 为目标的所有流量发送到与内部接口连接的路由器 10.1.2.45，定义三个用于将流量定向到 dmz 接口上的三个不同网关的等价静态路由，并为隧道流量和常规流量各添加一个默认路由。

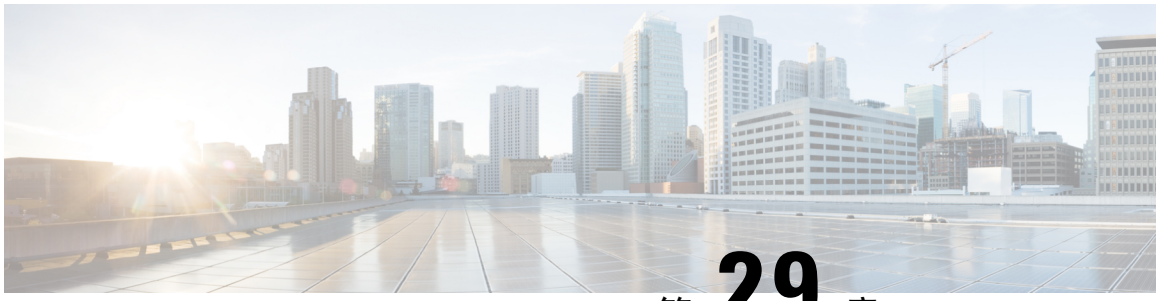
```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

静态和默认的历史记录

表 *35:* 静态和默认路由功能的历史记录

功能名称	平台版本	功能信息
静态路由跟踪	7.2(1)	静态路由跟踪功能提供在主路由发生故障的情况下跟踪静态路由的可用性和安装备用路由的方法。 引入了以下命令：**clear configure sla**、**frequency**、**num-packets**、**request-data-size**、**show sla monitor**、**show running-config sla**、**sla monitor**、**sla monitor schedule**、**threshold**、**timeout**、**tos**、**track rtr**

功能名称	平台版本	功能信息
丢弃流量的静态 null0 路由	9.2(1)	向 null0 接口发送流量会导致丢弃发往指定网络的数据包。此功能有助于为 BGP 配置远程触发黑洞 (RTBH)。 修改了以下命令：**route**。



第 29 章

策略型路由

本章介绍如何配置 ASA 以支持基于策略的路由 (PBR)。以下部分介绍基于策略的路由、PBR 准则和 PBR 配置。

- 关于策略型路由， 第 937 页
- 基于策略的路由准则， 第 939 页
- 路径监控， 第 941 页
- 配置基于策略的路由， 第 942 页
- 基于策略的路由示例， 第 946 页
- 基于策略的路由的历史记录， 第 955 页

关于策略型路由

传统路由是以目标为基础的，这意味着数据包基于目标 IP 地址进行路由。但是，在基于目标的路由系统中更改特定流量的路由是较为困难的。使用基于策略的路由 (PBR)，您可以基于非目标网络的条件定义路由 - 通过 PBR，可以基于源地址、源端口、目标地址、目标端口、协议或所有这些的组合来路由流量。

基于策略的路由：

- 用于为差分流量提供服务质量 (QoS)。
- 用于跨低带宽、低成本的永久路径以及高带宽、高成本的交换路径分发交互式和批处理流量。
- 允许互联网运营商及其他组织通过明确定义的网络连接来路由源自各组用户的流量。

基于策略的路由通过在网络边缘对流量进行分类和标记，然后在整个网络中使用 PBR 沿着特定路径路由标记的流量，来实施 QoS。这样，可以将源自不同源的数据包路由至不同网络，甚至在目标不同时亦可以；并且在将多个私有网络互连时，这一点可能很有用。

为什么使用基于策略的路由？

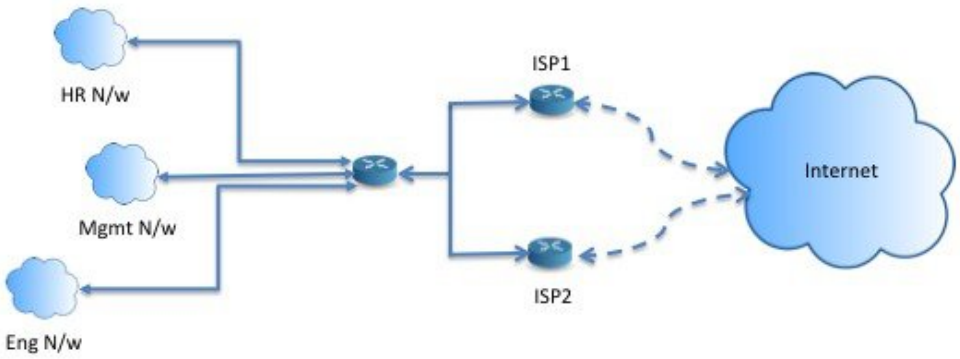
假设一家公司在不同位置之间有两条链路：一条是高带宽、低延迟、较为昂贵的链路，而另一条是低带宽、高延迟、不太昂贵的链路。使用传统路由协议时，高带宽链路将基于通过该链路的带宽和/或延迟（使用 EIGRP 或 OSPF）特性所实现的指标节约而获得大部分（如果不是全部）跨该链路发

送的流量。通过PBR，您可以通过高带宽/低延迟的链路来路由优先级较高的流量，而通过低带宽/高延迟链路发送其他所有流量。

基于策略的路由的部分应用为：

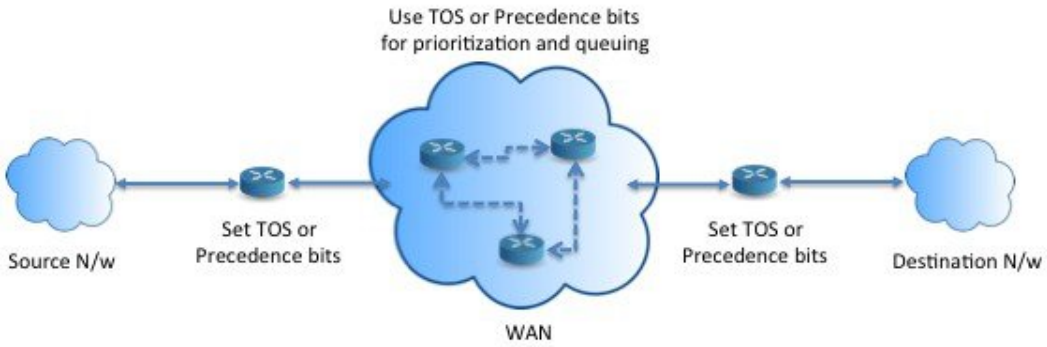
同等访问权限和源敏感路由

在此拓扑中，来自人力资源网络和管理网络的流量可配置为通过ISP-1，来自工程网络的流量可配置为通过ISP-2。因此，基于策略的路由支持网络管理员提供同等访问权限和源敏感路由，如下所示。



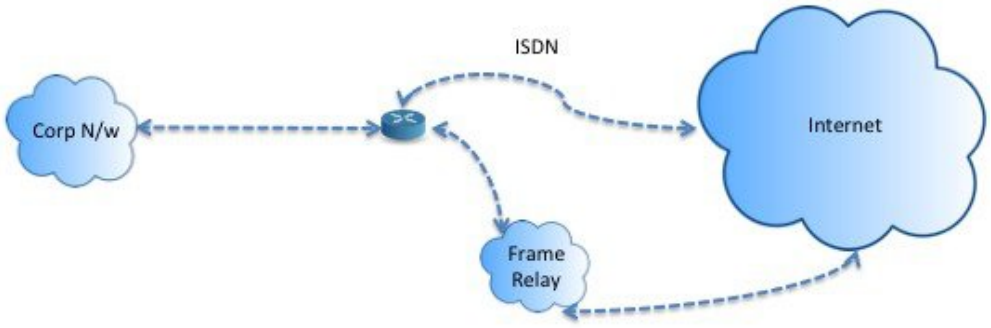
服务质量

通过标记使用基于策略的路由的数据包，网络管理员可以在网络边界对各种服务级别的网络流量进行分类，然后使用优先级、自定义或加权公平排队（如下图所示）在网络核心中实施这些服务级别。此设置无需在主干网络核心中的每个 WAN 接口对流量进行明确分类，从而能够提升网络性能。



成本节约

组织可以通过定义拓扑，将与特定活动关联的批处理流量定向为在短时间内使用较高带宽的高成本链路，并将较低带宽的低成本链路上的基本连接继续用于交互式流量，如下所示。



负载分担

除 ECMP 负载均衡提供的动态负载共享功能外，网络管理员现在还可以实施策略来根据流量特征在多个路径之间分发流量。

例如，在同等访问和基于源的路由场景所描绘的拓扑中，管理员可以配置基于策略的路由来对从人力资源网络至 ISP1 的流量和从工程网络至 ISP2 的流量进行负载共享。

实施 PBR

ASA 使用 ACL 来匹配流量，然后对流量执行路由操作。具体而言，配置指定用于进行匹配的 ACL 的路由映射，然后为该流量指定一个或多个操作。最后，将路由映射与接口相关联，在该接口上要对所有传入流量应用 PBR。

注释 在继续进行配置之前，请确保每个会话的入口和出口流量流经同一面向 ISP 的接口，以避免路由不对称导致的意外行为，尤其是在使用 NAT 和 VPN 时。

基于策略的路由准则

防火墙模式

仅在路由防火墙模式下受支持。不支持透明防火墙模式。

每数据流路由

由于ASA基于每个数据流执行路由，所以会在第一个数据包上应用策略路由，并将生成的路由决策存储在为该数据包创建的数据流中。属于同一连接的所有后续包将简单地与此数据流匹配并正确进行路由。

未对输出路由查询应用的 PBR 策略

基于策略的路由是一种仅入口功能；也就是说，它仅会应用于新传入连接的第一个数据包，并在此时选择连接转发支路的出口接口。请注意，如果传入数据包属于现有连接，则不会触发 PBR，或者已应用 NAT，则 NAT 选择出口接口。

PBR 策略不适用于初期流量

注释 初期连接是指源与目标之间尚未完成必要握手的连接。

在添加新的内部接口并使用唯一地址池来创建新的VPN策略时，PBR将应用于与新客户端池的源匹配的外部接口。因此，PBR 会将流量从客户端发送到新接口上的下一跳。但是，PBR 不会涉及从尚未与新内部接口建立连接的主机到客户端的返回流量。因此，从主机到VPN客户端的返回流量（具体而言，VPN 客户端响应）会由于缺少有效路由而被丢弃。必须在内部接口上配置具有更高指标的加权静态路由。

集群

- 支持集群。
- 在集群情景下，没有静态或动态路由，已启用ip-verify-reverse路径，非对称流量可能会被丢弃。因此，建议禁用 ip-verify-reverse 路径。

IPv6 支持

支持 IPv6

路径监控准则

以下是在接口上配置路径监控的准则：

- 接口必须具有名称。
- 管理专用接口不能配置路径监控。要配置路径监控，必须取消选中**将此接口用于管理**复选框。
- 在透明或多情景系统模式下的设备上不支持路径监控。
- 隧道接口不支持自动监控类型（auto、auto4 和 auto6）。
- 无法为以下接口配置路径监控：
  - BVI
  - 环回
  - DVTI

其他准则

- 所有现有路由映射相关的配置限制和局限性都将继续适用。
- 请勿将包含匹配策略列表的路由映射用于基于策略的路由。match policy-list 仅用于 BGP。
- 单播反向路径转发 (uRPF) 会根据路由表而不是 PBR 路由映射来验证接口上接收的数据包的源 IP 地址。启用 uRPF 时，通过 PBR 在接口上接收的数据包将被丢弃，因为它们没有特定路由条目。因此，使用 PBR 时，请确保禁用 uRPF。

路径监控

路径监控（在接口上配置）会派生指标，例如往返时间 (RTT)、抖动、平均意见得分 (MOS) 和每个接口的丢包。这些指标会被用于确定路由 PBR 流量的最佳路径。

接口上的指标会使用 ICMP 探测消息动态收集到接口的默认网关或指定的远程对等体。

默认监控计时器

对于指标收集和监控，使用以下计时器：

- 接口监控的平均间隔时间为 30 秒。此间隔时间表示探测平均值的频率。
- 接口监控器更新间隔时间为30秒。此时间间隔表示计算所收集的值的平均值并使其可用于PBR以确定最佳路由路径的频率。
- ICMP 的接口监控器探测间隔时间为一秒。此间隔时间表示发送 ICMP ping 的频率。
- HTTP 的应用监控探测间隔为 10 秒。此间隔时间表示发送 HTTP ping 的频率。路径监控使用 HTTP ping 的最后 30 个样本来计算平均指标。

注释 您不能配置或修改任何计时器的间隔时间。

在 PBR 中，流量通常会根据出口接口上配置的优先级值（接口成本）进行转发。从管理中心版本 7.2，PBR 使用基于 IP 的路径监控来收集出口接口的性能指标（RTT、抖动、丢包和 MOS）。PBR 会使用指标来确定转发流量的最佳路径（出口接口）。路径监控会定期向 PBR 通知其指标已更改的受监控接口。PBR 会从路径监控数据库中检索受监控接口的最新指标值，并更新数据路径。

只有在接口上设置了 RTT、抖动、丢包或 MOS 变量时，路径监控功能才会使用动态指标。路径监控对静态指标-接口成本（在接口中设置的成本）不起作用。

您必须为接口启用路径监控并配置监控类型。PBR 策略页面允许您为确定路径指定所需的指标。参阅配置基于策略的路由，第 942 页。

配置路径监控

您可以配置路径监控，以根据网络服务组执行基于策略的路由。要在没有NSG的情况下使用路径监控，可以导航至 **接口** > **编辑** 页面并指定路径监控类型。请参阅 配置基于策略的路由。

过程

步骤 1 在 ASDM 中，依次选择 **配置** > **设备设置** > **接口设置** > **接口**。

步骤 2 从 **接口** 下拉列表中选择接口。

步骤 3 在 **可用网络服务组** 复选框中选择网络服务组 (NSG)。要选择多个 NSG，请使用 Ctrl 键并点击所需的 NSG。

步骤 4 点击 **添加** 以添加网络服务组。

步骤 5 点击 **Apply**。

步骤 6 要删除配置，请从 **添加的网络服务组** 复选框中选择 NSG，然后点击 **删除**，然后点击 **应用**。

配置基于策略的路由

路由映射由一个或多个路由映射语句组成。每个语句都有序列号以及 permit 或 deny 子句。每个 route-map 语句都包含 match 和 set 命令。match 命令表示要对数据包应用的匹配条件。set 命令表示要对数据包采取的操作。

- 在路由映射同时配置有 IPv4 和 IPv6 match/set 子句时或在使用了与 IPv4 和 IPv6 流量匹配的统一 ACL 时，将根据目标 IP 版本应用 set 操作。
- 当多个下一跳或接口被配置为 set 操作时，系统将逐个评估所有选项，直到找到有效的可用选项。在已配置的多个选项之间将不进行负载均衡。
- Verify-availability 选项不支持多情景模式。

过程

步骤 1 定义标准或扩展访问列表：

access-list *name* **standard** {**permit** | **deny**} {**any4** | **host** *ip_address* | *ip_address mask*}

access-list *name* **extended** {**permit** | **deny**} *protocol source_and_destination_arguments*

示例：

```
ciscoasa(config)# access-list testacl extended permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
```

如果使用标准ACL，则仅基于目标地址进行匹配。如果使用扩展ACL，可基于源、目标或两者进行匹配。

对于扩展 ACL，可以指定 IPv4、IPv6、身份防火墙或思科 TrustSec 参数。您还可以包括网络服务对象。有关完整语法，请参阅 ASA 命令参考。

步骤 2 创建路由映射条目：

route-map *name* {**permit** | **deny**} [*sequence_number*]

示例：

```
ciscoasa(config)# route-map testmap permit 12
```

路由映射条目按顺序读取。可使用 *sequence_number* 参数标识顺序，否则 ASA 将使用添加路由映射条目的顺序。

此外，ACL 还包括自己的 permit 和 deny 语句。对于路由映射与 ACL 之间的 Permit/Permit 匹配，继续执行基于策略的路由处理。对于 Permit/Deny 匹配，对此路由映射的处理结束并检查其他路由映射。如果结果仍是 Permit/Deny，则使用普通路由表。对于 Deny/Deny 匹配，继续基于策略的路由处理。

注释
如果配置的路由映射不含 permit 或 deny 操作且不含序列号，则默认假定操作为 permit，序列号为 10。如果未指定操作和序列号，则会显示有关不完整 CLI 命令的警告消息，尽管使用默认值配置了路由映射。

步骤 3 使用访问列表定义要应用的匹配条件：

match ip address *access-list_name* [*access-list_name...*]

示例：

```
ciscoasa(config-route-map)# match ip address testacl
```

注释
确保访问列表不包含任何非活动规则。不能将具有非活动规则的匹配 ACL 设置为 PBR。

步骤 4 配置一个或多个 set 操作：

- 设置下一跳地址：

  set {ip | ipv6} next-hop *ipv4_or_ipv6_address*

  您可以配置多个下一跳 IP 地址，在这种情况下将按指定顺序对它们进行评估，直到找到有效的可路由下一跳 IP 地址。所配置的下一跳应为直连式，否则不会应用 set 操作。

- 设置默认下一跳地址：

  set {ip | ipv6} default next-hop *ipv4_or_ipv6_address*

  如果匹配流量的正常路由查询失败，则 ASA 会使用此指定的下一跳 IP 地址转发流量。

- 设置递归下一跳 IPv4 地址：

set ip next-hop recursive *ip_address*

set ip next-hop 和 **set ip default next-hop** 都要求可在直连式子网中找到下一跳。如果使用 **set ip next-hop recursive**，则下一跳地址不需要是直连式。匹配流量不会在下一跳地址上执行递归查询，而是根据路由器中使用的路由路径被转发到该路由条目使用的下一跳中。

- 验证路由映射的下一 IPv4 跳是否可用：

  set ip next-hop verify-availability *next-hop-address sequence_number* **track** *object*

  您可以配置 SLA 监控跟踪对象来验证下一跳的可访问性。要验证多个下一跳的可用性，可使用不同的序列号和不同的跟踪对象来配置多个 **set ip next-hop verify-availability** 命令。

- 设置数据包的输出接口：

  set interface *interface_name*

  或

  set interface null0

  此命令可配置通过其转发匹配流量的接口。您可以配置多个接口，在这种情况下将按指定顺序对它们进行评估，直到找到有效的接口。当指定 **null0** 时，匹配路由映射的所有流量将被丢弃。对于可通过指定接口（静态或动态）路由的目标，必须存在路由。

- 根据接口的成本设置输出接口：

  set adaptive-interface cost *interface_list*

  出口接口从以空格分隔的接口列表中选择。如果接口的成本相同，则这是主用-主用配置，数据包在出口接口上进行负载均衡（轮询）。如果成本不同，则选择成本最低的接口。仅当接口处于启用状态时，才会考虑这些接口。例如：

  ```
  set adaptive-interface cost output1 output2
  ```

- 将默认接口设置为 null0：

  set default interface null0

  如果正常路由查询失败，ASA 将转发流量 null0，并且该流量将被丢弃。

- 在 IP 报头中设置不分段 (DF) 位值：

  set ip df {0|1}

- 通过在数据包中设置差分服务代码点 (DSCP) 或 IP 优先值对 IP 流量进行分类：

  set {ip | ipv6} dscp *new_dscp*

注释
当配置了多个 set 操作时，ASA 将按以下顺序评估它们：**set ip next-hop verify-availability**；**set ip next-hop**；**set ip next-hop recursive**；**set interface**；**set adaptive-interface cost**；**set ip default next-hop**；**set default interface**。

步骤 5 配置接口并进入接口配置模式：

interface *interface_id*

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
```

步骤 6 如果在路由映射中将 **set adaptive-interface cost** 用作条件，请在接口上设置开销：

policy-route cost *value*

值可以是 1-65535。默认值为 0，您可以使用命令中的 **no** 版本进行重置。数值越低，优先级越高。例如，1 的优先级高于 2。

当您设置策略-路由成本，并在路由映射中使用 **set adaptive-interface cost** 命令时，出口流量将在具有相同接口成本的任何选定接口（假设它们处于启用状态）之间进行循环负载均衡。如果成本不同，则使用成本较高的接口作为成本最低的接口的备选。

例如，通过在 2 个 WAN 链路上设置相同的成本，您可以负载均衡这些链路上的流量以提高性能。但是，如果一条 WAN 链路的带宽高于另一条 WAN 链路，则可以将带宽较高的链路的成本设置为 1，将带宽较低的链路设置为 2，以便仅在带宽较高的链路关闭时使用带宽较低的链路。

步骤 7 您可以为接口的对等体设置监控类型以收集灵活指标：

policy-route path-monitoring{**IPv4** | **IPv6** | **auto** | **auto4** | **auto6**}

其中，

- **auto** - 将 ICMP 探测发送到接口的 IPv4 默认网关（如果存在 - 与自动 IPv4 相同）。否则，发送到接口的 IPv6 默认网关（与自动 IPv6 相同）。
- **ipv4** - 将 ICMP 探测发送到指定的对等 IPv4 地址（下一跳 IP）以进行监控。
- **ipv6** - 将 ICMP 探测发送到指定的对等 IPv4 地址（下一跳 IP）以进行监控。
- **自动4**-将 ICMP 探测发送到接口的 IPv4 默认网关。
- **自动6**-将 ICMP 探测发送到接口的默认 IPv6 网关。

示例：

```
ciscoasa(config-if)# policy-route ?

interface mode commands/options:
  cost              set interface cost
  path-monitoring   Keyword for path monitoring
  route-map         Keyword for route-map
ciscoasa(config-if)# policy-route path-monitoring ?
interface mode commands/options:
  A.B.C.D     peer-ipv4
  X:X:X:X::X  peer-ipv6
  auto        Use remote peer IPv4/6 based on config
  auto4       Use only IPv4 address based on config
  auto6       Use only IPv6 address based on config

ciscoasa(config-if)# policy-route path-monitoring auto
```

要清除接口上的路径监控设置，请使用 **clear path-monitoring** 命令：

示例：

```
clear path-montoring outside1
```

步骤 8 为通过设备的流量配置基于策略的路由：

`policy-route route-map` *route_map_name*

示例：

```
ciscoasa(config-if)# policy-route route-map testmap
```

要删除现有的基于策略的路由映射，只需输入此命令的 **no** 形式即可。

示例：

```
ciscoasa(config-if)# no policy-route route-map testmap
```

基于策略的路由示例

以下部分显示路由映射配置示例、基于策略的路由以及现行 PBR 的特定示例。

路由映射配置示例

在以下示例中，由于未指定操作和顺序，因此假设隐式操作为允许且序列号为 10：

```
ciscoasa(config)# route-map testmap
```

在以下示例中，由于未指定匹配条件，因此假设隐式匹配为“any”：

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10
```

在本示例中，与 <acl> 匹配的所有流量都将通过外部接口进行策略路由和转发。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
ciscoasa(config-route-map)# set interface outside
```

在本示例中，由于未配置接口或下一跳操作，因此与 <acl> 匹配的所有流量都将根据配置修改 df 位字段和 dscp 字段，并使用普通路由进行转发。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
set ip df 1
set ip precedence af11
```

在以下示例中，与 <acl_1> 匹配的所有流量都使用下一跳 1.1.1.10 进行转发，与 <acl_2> 匹配的所有流量都使用下一跳2.1.1.10进行转发，并会丢弃其余流量。“match”条件并不暗示隐式匹配“any”。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl_1>
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address <acl_2>

ciscoasa(config-route-map)# set ip next-hop 2.1.1.10
ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# set interface Null0
```

在以下示例中，路由映射评估结果将是 (i) 路由映射操作 permit 和 acl 操作 permit 将应用 set 操作 (ii) 路由映射操作 deny 和 acl 操作 permit 将跳至普通路由查找 (iii) 路由映射操作 permit/deny 和 acl 操作 deny 将继续处理下一个路由映射条目。当没有下一个路由映射条目可用时，将不会回退到普通路由查找。

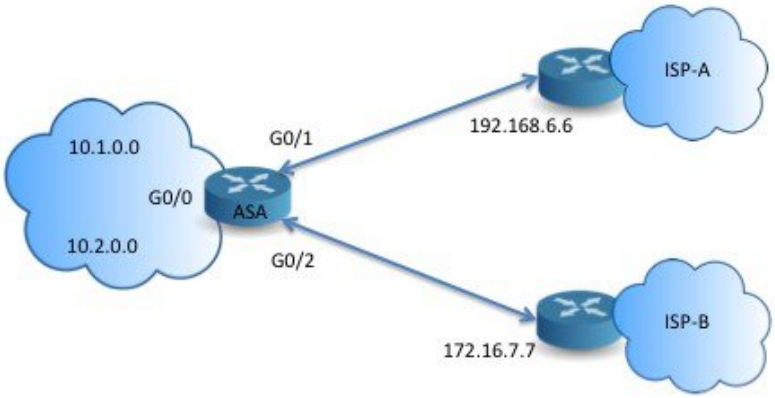
```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address permit_acl_1 deny_acl_2
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap deny 20
ciscoasa(config-route-map)# match ip address permit_acl_3 deny_acl_4
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10

ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# match ip address deny_acl_5
ciscoasa(config-route-map)# set interface outside
```

在以下示例中，当配置了多个 set 操作时，将按照上述顺序对其进行评估。仅当 set 操作的所有选项都已评估且无法应用时，才会考虑后续 set 操作。此排序将确保首先尝试可用性最高 且距离最近的下一跳，然后尝试下一个可用性最高且距离最近的 下一跳，依此类推。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address acl_1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.10 1 track 1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.11 2 track 2
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.12 3 track 3
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10 2.1.1.11 2.1.1.12
ciscoasa(config-route-map)# set ip next-hop recursive 3.1.1.10
ciscoasa(config-route-map)# set interface outside-1 outside-2
ciscoasa(config-route-map)# set ip default next-hop 4.1.1.10 4.1.1.11
ciscoasa(config-route-map)# set default interface Null0
```

PBR 配置示例

本节介绍为以下场景配置 PBR 所需的全套配置：



首先，需要配置接口。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-1
ciscoasa(config-if)# ip address 192.168.6.5 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-2
ciscoasa(config-if)# ip address 172.16.7.6 255.255.255.0
```

然后，我们需要配置一个访问列表来匹配流量。

```
ciscoasa(config)# access-list acl-1 permit ip 10.1.0.0 255.255.0.0
ciscoasa(config)# access-list acl-2 permit ip 10.2.0.0 255.255.0.0
```

我们需要将上述访问列表指定为匹配条件，并指定需要执行的一系列操作，以此来配置一个路由映射。

```
ciscoasa(config)# route-map equal-access permit 10
ciscoasa(config-route-map)# match ip address acl-1
ciscoasa(config-route-map)# set ip next-hop 192.168.6.6

ciscoasa(config)# route-map equal-access permit 20
ciscoasa(config-route-map)# match ip address acl-2
ciscoasa(config-route-map)# set ip next-hop 172.16.7.7

ciscoasa(config)# route-map equal-access permit 30
ciscoasa(config-route-map)# set ip interface Null0
```

现在，此路由映射必须连接至接口。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map equal-access
```

显示策略路由配置。

```
ciscoasa(config)# show policy-route
Interface                  Route map
GigabitEthernet0/0   equal-access
```

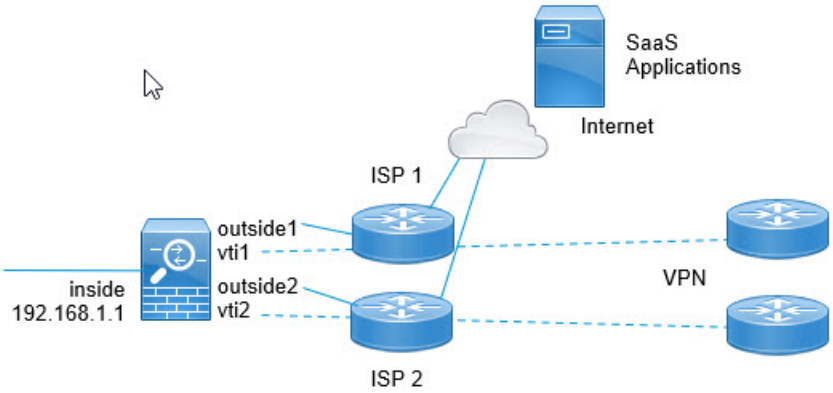
使用软件定义的 WAN 直接访问互联网

典型的分支机构网络使用站点间VPN将分支机构连接到企业中心。然后，所有非本地流量都将被定向到公司网络，在此将被定向到内部服务或互联网（视情况而定）。

此设置会在企业中心造成瓶颈。如果某些分支机构流量用于互联网服务（例如Google搜索或Gmail），则无需先访问公司网络再访问互联网。

使用基于策略的路由，您可以改为从分支机构为不需要公司网络服务的流量设置直接互联网访问。因此，发往互联网的流量不会发送到公司中心，中心只需要处理发往公司网络内部服务的流量。此配置应提高整体网络性能和吞吐量。

以下示例显示如何为以下设置设置直接互联网访问，其中两个外部接口连接到不同的互联网服务提供商，虚拟隧道接口 (VTI) 托管到企业网络的站点间 VPN连接。示例显示如何将发往特定 SaaS 应用的流量定向到互联网，从而绕过公司网络。



开始之前

此示例假设您已使用在外部（面向广域网）接口上定义的虚拟隧道接口 (VTI) 定义了站点间 VPN，以将分支机构连接到公司集线器，并且它运行正常。路由到VTI接口的流量因此被定向到公司网络，而直接路由到外部接口的流量则流向互联网。

它还假设您已在设备接口上配置DNS服务器并启用了 DNS 解析。使用 **show dns trusted-source detail** 命令查看将监听哪些服务器。如果要限制使用的服务器，请使用 **no dns trusted-source** 命令在所选服务器上关闭监听。

过程

步骤 1 配置网络服务对象和组以定义所需的流量。

以下示例创建对象以定义 Office365 和 WebEx，然后创建 SaaS_Applications 对象组以包含这些对象。您必须创建对象组，不能直接在访问控制条目中使用对象。

```
object network-service office365
    domain outlook.office365.com tcp eq 443
    domain onlineapps.live.com tcp eq 443
    domain skype.live.com tcp eq 443

object network-service webex
    domain webex.com tcp eq 443

object-group network-service SaaS_Applications
    network-service-member office365
    network-service-member webex
```

步骤 2 创建扩展 ACL 以匹配所需流量。

以下示例匹配从内部网络到 SaaS 应用对象组的流量。

```
access-list DIA_traffic extended permit ip 192.168.1.0 255.255.255.0
object-group-network-service SaaS_Applications
```

步骤 3 （可选。）配置出口接口的开销。

假设 output1 和 output2 接口已配置且正常运行，只需添加 policy-route cost 命令。如果要将系统配置为使用轮询处理来跨 2 个出口 WAN 链路进行负载均衡，则此步骤为可选步骤。但是，如果要创建主用/备份配置，则必须设置开销，其中使用一个链路，除非链路关闭。

以下是等价主用/主用设置示例。

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 1
```

以下是 output1 是首选链路，而 output2 仅在 output1 关闭时使用的示例。

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 2
```

步骤 4 创建路由映射以匹配扩展 ACL 并相应地引导流量。

以下示例使用 ACL 匹配流量，然后使用自适应接口开销将流量定向到出口接口。

```
route-map mymap 10
  match ip address DIA_traffic
  set adaptive-interface cost outside1 outside2
```

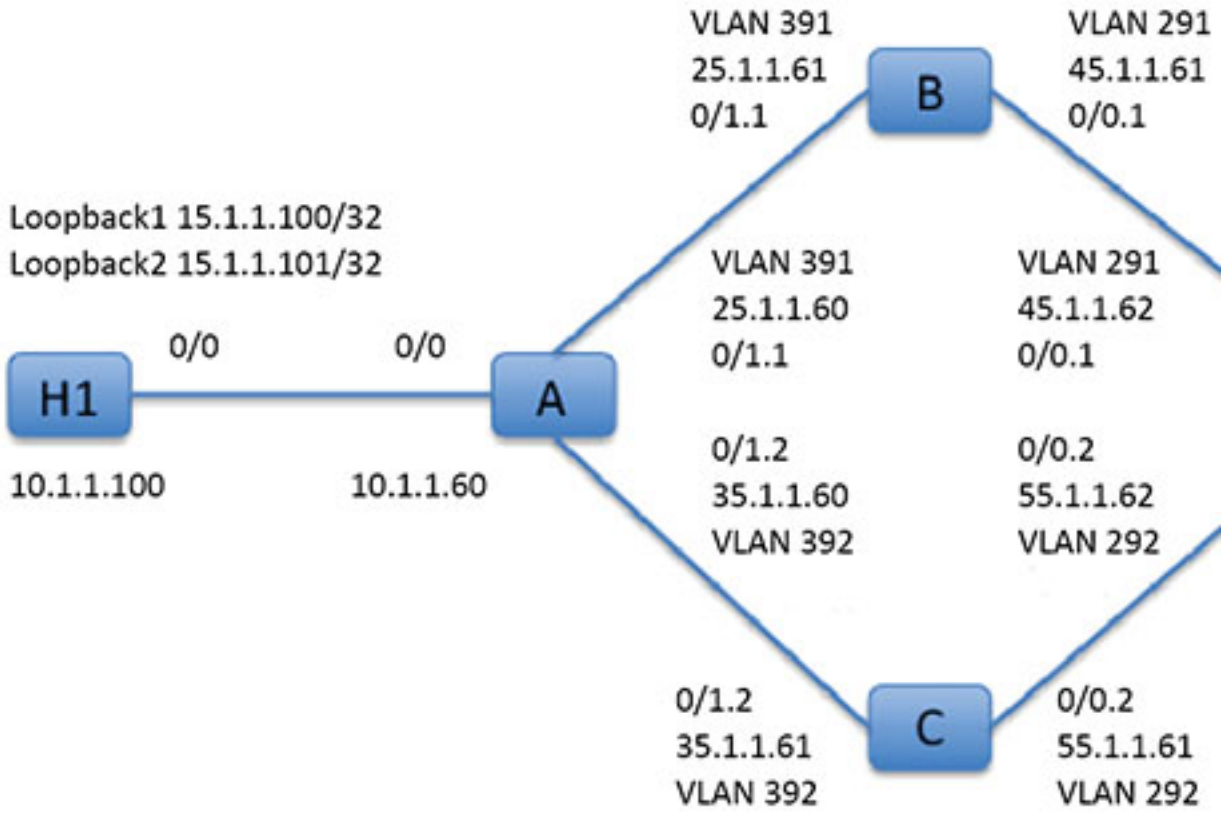
步骤 5 在入口接口上配置基于策略的路由，以将 SaaS 流量发送到外部接口。

以下示例将路由映射附加到内部接口，为直接互联网访问启用基于策略的路由。

```
interface G1/0
  nameif inside
  policy-route route-map mymap
```

正在使用的基于策略的路由

我们将使用此测试设置以不同的匹配条件配置基于策略的路由，并设置操作以了解如何评估和应用这些策略。



首先，我们了解一下设置中所涉及的所有设备的基本配置。这里，A、B、C 和 D 代表 ASA 设备，H1 和 H2 代表 IOS 路由器。

ASA-A：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.60 255.255.255.0
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 25.1.1.60 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 35.1.1.60 255.255.255.0
```

ASA-B：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 45.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 25.1.1.61 255.255.255.0
```

ASA-C：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 55.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.2
```

```
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 35.1.1.61 255.255.255.0
```

ASA-D：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config) #interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif inside-1
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 45.1.1.62 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif inside-2
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 55.1.1.62 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 65.1.1.60 255.255.255.0
```

H1：

```
ciscoasa(config)# interface Loopback1
ciscoasa(config-if)# ip address 15.1.1.100 255.255.255.255

ciscoasa(config-if)# interface Loopback2
ciscoasa(config-if)# ip address 15.1.1.101 255.255.255.255

ciscoasa(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.60
```

H2：

```
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# ip address 65.1.1.100 255.255.255.0

ciscoasa(config-if)# ip route 15.1.1.0 255.255.255.0 65.1.1.60
```

我们将在 ASA-A 上配置 PBR 以路由源自 H1 的流量。

ASA-A：

```
ciscoasa(config-if)# access-list pbracl_1 extended permit ip host 15.1.1.100 any

ciscoasa(config-if)# route-map testmap permit 10
ciscoasa(config-if)# match ip address pbracl_1
ciscoasa(config-if)# set ip next-hop 25.1.1.61

ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmap
```

```
ciscoasa(config-if)# debug policy-route
```

H1：ping 65.1.1.100 repeat 1 source loopback1

```
pbr: policy based route lookup called for 15.1.1.100/44397 to 65.1.1.100/0 proto 1 sub_proto
 8 received on interface inside
pbr: First matching rule from ACL(2)
pbr: route map testmap, sequence 10, permit; proceed with policy routing
pbr: evaluating next-hop 25.1.1.61
pbr: policy based routing applied; egress_ifc = outside : next_hop = 25.1.1.61
```

数据包使用路由映射中的下一跳地址按预期转发。

当配置了下一跳时，将在输入路由表中执行查找，以确定到所配置的下一跳的已连接路由，并使用对应的接口。此处显示了本例的输入路由表（匹配路由条目已亮显）。

```
in   255.255.255.255 255.255.255.255 identity
in   10.1.1.60       255.255.255.255 identity
in   25.1.1.60       255.255.255.255 identity
in   35.1.1.60       255.255.255.255 identity
in   10.127.46.17    255.255.255.255 identity
in   10.1.1.0        255.255.255.0   inside
in   25.1.1.0        255.255.255.0   outside
in   35.1.1.0        255.255.255.0   dmz
```

接下来，我们将 ASA-A 配置为将数据包从 H1 loopback2 路由到 ASA-A dmz 接口外。

```
ciscoasa(config)# access-list pbracl_2 extended permit ip host 15.1.1.101 any

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address pbracl
ciscoasa(config-route-map)# set ip next-hop 35.1.1.61

ciscoasa(config)# show run route-map
!
route-map testmap permit 10
  match ip address pbracl_1
  set ip next-hop 25.1.1.61
!
route-map testmap permit 20
  match ip address pbracl_2
  set ip next-hop 35.1.1.61
!
```

H1：ping 65.1.1.100 repeat 1 source loopback2

调试如下所示：

```
pbr: policy based route lookup called for 15.1.1.101/1234 to 65.1.1.100/1234 proto 6 sub_proto
 0 received on interface inside
pbr: First matching rule from ACL(3)
pbr: route map testmap, sequence 20, permit; proceed with policy routing
pbr: evaluating next-hop 35.1.1.61
pbr: policy based routing applied; egress_ifc = dmz : next_hop = 35.1.1.61
```

从输入路由表中所选的路由条目如下所示：

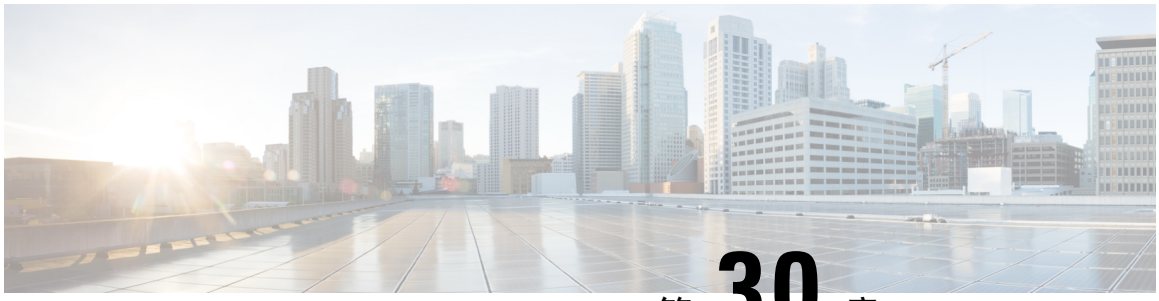
```
in   255.255.255.255 255.255.255.255 identity
 in    10.1.1.60       255.255.255.255 identity
 in    25.1.1.60       255.255.255.255 identity
 in    35.1.1.60       255.255.255.255 identity
 in    10.127.46.17    255.255.255.255 identity
 in    10.1.1.0        255.255.255.0   inside
 in    25.1.1.0        255.255.255.0   outside
 in    35.1.1.0        255.255.255.0   dmz
```

基于策略的路由的历史记录

表 *36:* 路由映射的历史记录

功能名称	平台版本	功能信息
通过 HTTP 客户端进行路径监控	9.20(1)	PBR 现在可以使用通过应用域上的 HTTP 客户端进行路径监控收集的性能指标（RTT、抖动、丢包和 MOS），而不是特定目标 IP 上的指标。基于 HTTP 的路径监控可以使用网络服务组对象在接口上进行配置。
PBR 中的路径监控指标。	9.18(1)	PBR 会使用指标来确定转发流量的最佳路径（出口接口）。路径监控会定期向 PBR 通知其指标已更改的受监控接口。PBR 会从路径监控数据库中检索受监控接口的最新指标值，并更新数据路径。 新增/修改的命令：**clear path-monitoring**、**policy-route**、**show path-monitoring**
基于策略的路由	9.4(1)	基于策略的路由 (PBR) 是一种机制，基于该机制，流量可以使用 ACL，通过带有指定 QoS 的特定路径进行路由。基于数据包的第 3 层和第 4 层报头的内容，ACL 可以对流量进行分类。管理员通过此解决方案可向不同的流量提供 QoS，在低带宽、低成本永久路径与高带宽、高成本交换式路径之间分发交互式和批处理流量，并允许互联网运营商和其他组织通过明确定义的互联网连接来路由源自各类用户的流量。 引入了以下命令：**set ip next-hop verify-availability**、**set ip next-hop**、**set ip next-hop recursive**、**set interface**、**set ip default next-hop**、**set default interface**、**set ip df**、**set ip dscp**、**policy-route route-map**、**show policy-route** 和 **debug policy-route**
为策略型路由提供 IPv6 支持	9.5(1)	策略型路由现在支持 IPv6 地址。 引入了以下命令：**set ipv6 next-hop**、**set default ipv6-next hop**、**set ipv6 dscp**

功能名称	平台版本	功能信息
为策略型路由提供 VXLAN 支持	9.5(1)	现在您可以在 VNI 接口中启用策略型路由。 未修改任何命令。
为身份防火墙和思科 TrustSec 提供策略型路由支持	9.5(1)	您可以先配置身份防火墙和思科 TrustSec，然后再在策略型路由的路由图中使用身份防火墙和思科 TrustSec ACL。 未修改任何命令。



第 30 章

路由映射

本章介绍如何为 ASA 配置和自定义路由映射。

- 关于路由映射， 第 957 页
- 路由映射准则， 第 959 页
- 定义路由映射， 第 959 页
- 自定义路由映射， 第 959 页
- 路由映射示例， 第 962 页
- 路由映射的历史记录， 第 962 页

关于路由映射

在将路由重新分发到 OSPF、RIP、EIGRP 或 BGP 路由进程时会使用路由映射。在为 OSPF 路由进程生成默认路由时也会使用路由映射。路由映射定义了允许将来自指定路由协议的哪些路由重新分发到目标路由进程。

路由映射与广为人知的 ACL 具有许多相同功能。以下是两者共有的一些特征：

- 它们都是单独语句的有序序列，各自具有允许或拒绝结果。ACL 或路由映射的评估包括采用预先确定顺序的列表扫描，以及每条语句匹配条件的评估。一旦找到第一个语句匹配即中止列表扫描，并且会执行与语句匹配相关联的操作。
- 它们是通用机制。条件匹配和匹配解释由它们的应用方式和使用它们的功能决定。应用于不同功能的相同路由映射可能以不同方式进行解释。

以下是路由映射与 ACL 之间的一些差异：

- 路由映射比 ACL 更加灵活，可以根据 ACL 无法验证的条件对路由进行验证。例如，路由映射可以验证路由的类型是否为内部路由。
- 每个 ACL 按照设计约定以隐式拒绝语句结尾。如果在匹配尝试期间到达路由映射的结尾，则结果取决于路由映射的特定应用。应用于重新分发的路由映射与 ACL 的行为方式相同：如果路由与路由映射中的任何子句不匹配，则会拒绝路由重新分发，就如同路由映射的结尾包含拒绝语句一样。

Permit 和 Deny 子句

路由映射可以具有 permit 和 deny 子句。deny 子句可拒绝来自重新分发的路由匹配。您可以使用 ACL 作为路由映射中的匹配标准。由于 ACL 还有 permit 和 deny 子句，因此数据包与 ACL 匹配时会应用以下规则：

- ACL permit + route map permit：重新分发路由。
- ACL permit + route map deny：重新分发路由。
- ACL deny + route map permit or deny：不匹配 route map 子句，并且对下一个 route-map 子句进行评估。

Match 和 Set 子句值

每个路由映射子句均具有两种类型的值：

- match 值用于选择应将此子句应用于的路由。
- set 值用于修改将重新分发到目标协议的信息。

对于要重新分发的每个路由，路由器首先评估路由映射中子句的匹配条件。如果匹配条件成功，则按照 permit 或 deny 子句的指示重新分发或拒绝路由，其某些属性可能会通过 set 命令设置的值修改。如果匹配条件失败，则此子句不适用于路由，软件会根据路由映射中下一个子句继续评估路由。路由映射扫描将继续，直到发现匹配路由的子句或达到路由映射的结尾。

如果存在下列条件中的一个，则每个子句中的 match 值或 set 值可能会缺失或多次重复：

- 如果一个子句中存在多个匹配条目，则对于给定路由而言，所有这些条目必须都符合，该路由才与该子句匹配（也即，为多个 match 命令应用逻辑 AND 算法）。
- 如果一个 match 条目引用了一个条目中的多个对象，那么其中任何一个对象都应匹配（应用逻辑 OR 算法）。
- 如果匹配条目不存在，则所有路由都匹配子句。
- 如果一个 set 条目在 route map permit 子句中不存在，则该路由将被重新分发，而不修改其当前属性。

注释 请勿在 route map deny 子句中配置 set 条目，因为 deny 子句会禁止路由重新分发 - 没有要修改的信息。

没有 match 或 set 条目的 route map 子句需要执行操作。空 permit 子句允许重新分发剩余路由而不进行修改。空 deny 子句不允许重新分发其他路由（如果路由映射在经过完整扫描后，未发现明确的匹配项，此为默认操作）。

路由映射准则

防火墙模式

仅在路由防火墙模式下受支持。不支持透明防火墙模式。

其他准则

路由映射不支持其中包含用户、用户组和完全限定域名对象的 ACL。

定义路由映射

当指定允许将来自指定路由协议的哪些路由重新分发到目标路由进程时，必须定义路由映射。

过程

创建路由映射条目：

route-map *name* {**permit** | **deny**} [*sequence_number*]

示例：

```
ciscoasa(config)# route-map name {permit} [12]
```

路由映射条目按顺序读取。可使用 *sequence_number* 参数标识顺序，否则 ASA 将使用添加路由映射条目的顺序。

自定义路由映射

本节介绍如何自定义路由映射。

定义路由以匹配特定的目标地址

过程

步骤 1 创建路由映射条目：

route-map *name* {**permit** | **deny**} [*sequence_number*]

示例：

```
ciscoasa(config)# route-map name {permit} [12]
```

路由映射条目按顺序读取。可使用 *sequence_number* 选项标识顺序，否则 ASA 会使用添加路由映射条目的顺序。

步骤 2 匹配包含目标网络并与标准 ACL 或前缀列表相匹配的所有路由：

match ip address {*acl_id* [*acl_id*] [...] | **prefix-list** *prefix_list_id* [*prefix_list_id*] [...]}

示例：

```
ciscoasa(config-route-map)# match ip address acl1 acl2 acl3
```

如果指定多个 ACL 或前缀列表，则路由可以匹配任何 ACL 或前缀列表。

注释
OSPF 不支持前缀列表。

步骤 3 匹配具有指定指标的任何路由：

match metric *metric_value*

示例：

```
ciscoasa(config-route-map)# match metric 200
```

metric_value 范围可在 0 到 4294967295 之间。

步骤 4 匹配包含下一跳路由器地址并与标准 ACL 相匹配的任何路由：

match ip next-hop *acl_id* [*acl_id*] [...]

示例：

```
ciscoasa(config-route-map)# match ip next-hop acl2
```

如果指定多个 ACL，则路由可以匹配任何 ACL。

步骤 5 匹配带有指定下一跳接口的任何路由：

match interface *if_name*

示例：

```
ciscoasa(config-route-map)# match interface if_name
```

如果指定多个接口，则路由可以匹配任一接口。

步骤 6 匹配已由与标准 ACL 相匹配的路由器通告的任何路由：

match ip route-source *acl_id* [*acl_id*] [...]

示例：

```
ciscoasa(config-route-map)# match ip route-source acl_id [acl_id] [...]
```

如果指定多个 ACL，则路由可以匹配任何 ACL。

步骤 7 匹配路由类型：

match route-type {**internal** | **external** [**type-1** | **type-2**]}

为路由操作配置度量值

如果路由与 **match** 命令匹配，则以下 **set** 命令会确定在重新分发路由之前要对路由执行的操作。

要为路由操作配置指标值，请执行以下步骤：

过程

步骤 1 创建路由映射条目：

route-map *name* {**permit** | **deny**} [*sequence_number*]

示例：

```
ciscoasa(config)# route-map name {permit} [12]
```

路由映射条目按顺序读取。可使用 *sequence_number* 参数标识顺序，否则 ASA 将使用添加路由映射条目的顺序。

步骤 2 为路由映射设置指标值：

set metric *metric_value*

示例：

```
ciscoasa(config-route-map)# set metric 200
```

metric_value 参数范围可在 0 到 294967295 之间。

步骤 3 为路由映射设置指标类型：

set metric-type {**type-1** | **type-2**}

示例：

```
ciscoasa(config-route-map)# set metric-type type-2
```

metric-type 参数可能是 type-1 或 type-2。

路由映射示例

以下示例显示如何将跳数等于 1 的路由重新分发到 OSPF。

ASA 将这些路由作为外部接口进行重新分发，其中指标为 5，指标类型为类型 1。

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

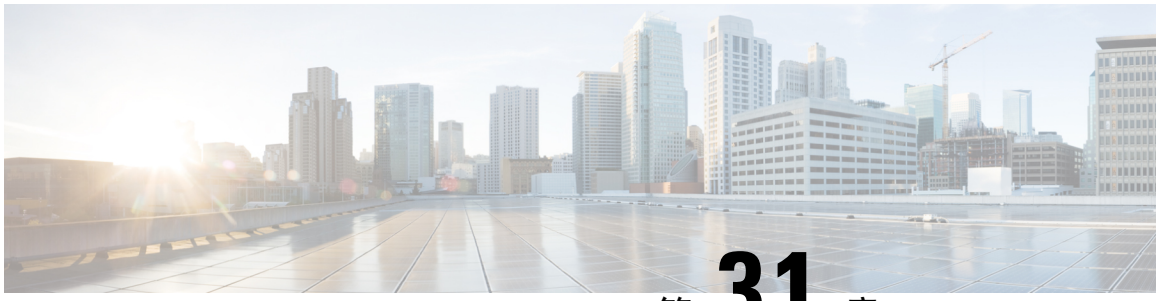
以下示例显示如何使用配置的指标值将 10.1.1.0 静态路由重新分发到 eigrp 进程 1：

```
ciscoasa(config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config-router)# redistribute static metric 250 250 1 1 1 route-map mymap2
```

路由映射的历史记录

表 *37:* 路由映射的功能历史记录

功能名称	平台版本	功能信息
路由映射	7.0(1)	引入了此功能。 引入了以下命令：**route-map**。
增强了对静态和动态路由映射的支持	8.0(2)	添加了对动态和静态路由映射的增强支持。
支持动态路由协议（EIGRP、OSPF 和 RIP）的状态故障转移以及常规路由相关操作的调试	8.4(1)	引入了以下命令：**debug route** 和 **show debug route**。 修改了以下命令：**show route**。
多情景模式下的动态路由	9.0(1)	在多情景模式下支持路由映射。
支持 BGP	9.2(1)	引入了此功能。 引入以下命令：**router bgp**
IPv6 支持前缀规则	9.3.2	引入了此功能。



第 31 章

双向转发检测路由

本章介绍如何配置 ASA 以使用双向转发检测 (BFD) 路由协议。

- 关于 BFD 路由，第 963 页
- BFD 路由准则，第 966 页
- 配置 BFD，第 967 页
- BFD 监控，第 971 页
- BFD 路由的历史记录，第 972 页

关于 BFD 路由

BFD 是一个检测协议，旨在为媒体类型、封装、拓扑和路由协议提供快速转发路径故障检测时间。BFD 可以在单播、点对点模式下对正在两系统之间转发的任何数据协议上运行。数据包在适用于媒体和网络的封装协议负载中携带。

除了快速转发路径故障检测外，BFD 还为网络管理员提供一致的故障检测方法。由于网络管理员可以使用 BFD 按照统一的速率检测转发路径故障，而不是为不同的路由协议呼叫机制采用不同的速率，因此网络分析和计划更简单，重新聚合时间一致且可预测。

BFD 异步模式和回应功能

不管是否启用回应功能，BFD 均可在异步模式下运行。

异步模式

在异步模式下，系统之间会定期发送BFD控制数据包，如果某一行中有大量此类数据包未被其他系统接收，则会话将宣布关闭。纯异步模式（无回应功能）很有用，因为它达到特定检测时间所需的数据包数量是回应功能所需数据包数量的一半。

BFD 回应功能

BFD回应功能将回应数据包从转发引擎发送至直连单跳BFD邻居。回应数据包由转发引擎负责发送，并沿同一条路径重新进行转发，以执行检测。另一端的BFD会话不参与回应包的实际转发。回应功能和转发引擎负责检测进程，BFD邻居之间发出的BFD控制数据包数量将减少。此

外，由于转发引擎在远程邻居系统上测试转发路径，并未涉及远程系统，因此数据包间的延迟差异增大了。这会导致故障检测时间缩短。

启用回应功能后，BFD可以使用较慢的计时器降低异步会话的速度并减少BFD邻居之间发送的BFD 控制数据包的数量，从而降低处理开销，同时提高故障检测速度。

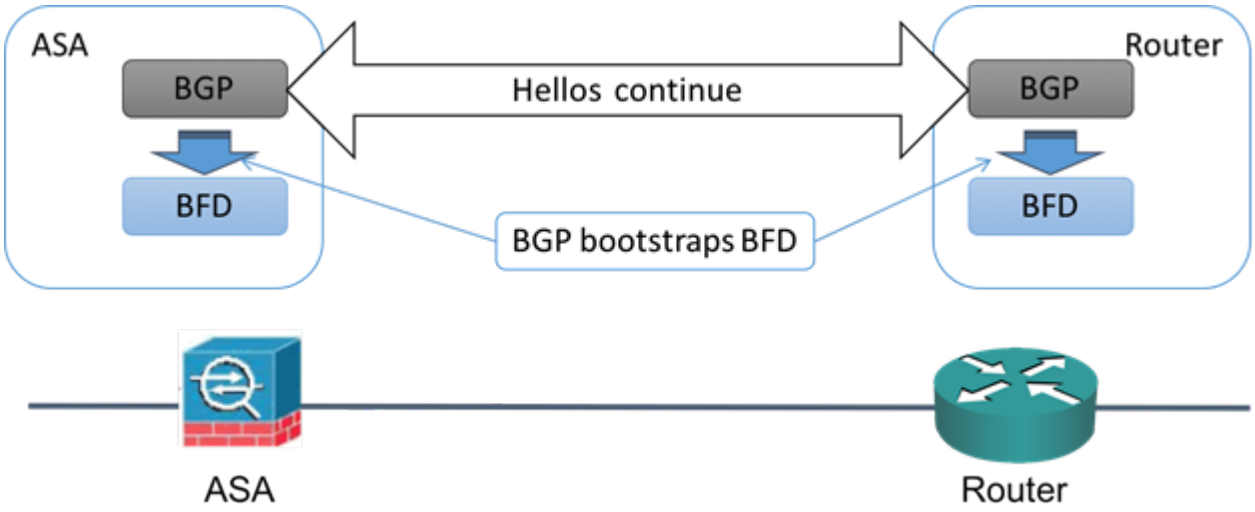
注释 IPv4 多跳或 IPv6 单跳 BFD 邻居不支持回应功能。

您可以在接口级别和路由协议级别启用BFD。您必须在两个系统（BFD对等体）上配置BFD。在接口上并且在相应路由协议的路由器级别启用 BFD 后，将会创建 BFD 会话，协商 BFD 计时器，并且 BFD 对等体在协商的级别互相发送 BFD 控制数据包。

BFD 会话建立

以下示例显示ASA和运行边界网关协议(BGP)的相邻路由器。当两台设备启动时，二者之间不会建立 BFD 会话。

图 *75:* 建立的 *BFD* 会话



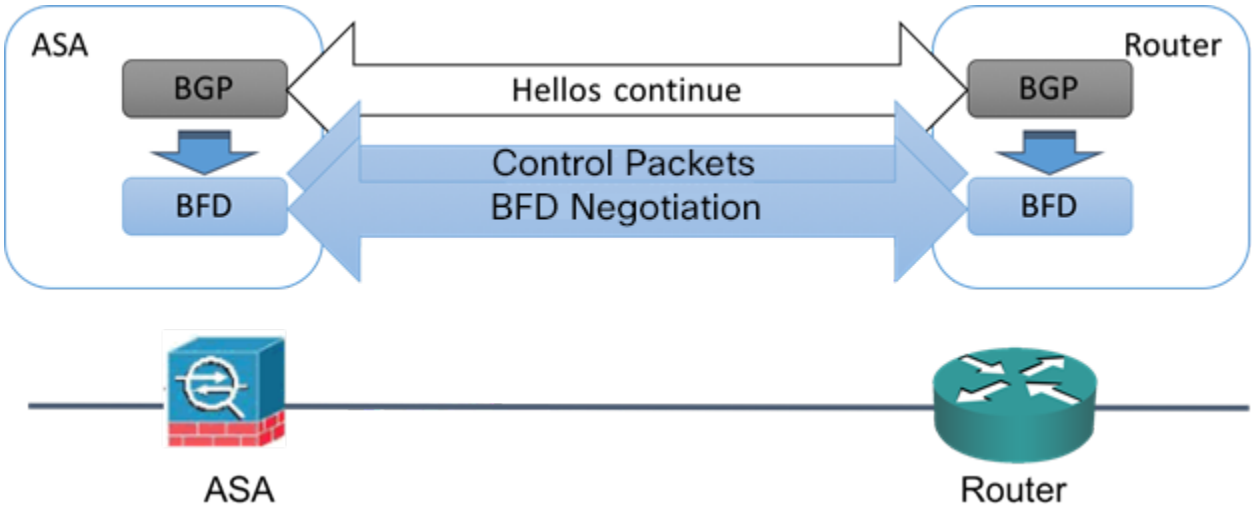
BGP 识别其 BGP 邻居后，会使用邻居的 IP 地址通过引导程序启动 BFD 进程。BFD 不是动态发现其对等体。它依靠配置的路由协议告知它要使用的 IP 地址以及要形成的对等体关系。

路由器上的 BFD 和 ASA 上的 BFD 共同形成 BFD 控制数据包，并开始以一秒的间隔向彼此发送数据包，直到 BFD 会话建立为止。来自任一系统的初始控制数据包都非常相似，例如 Vers、Diag，H、D、P 和 F 位都设置为零，State 设置为 Down。My Discriminator 字段设置为一个在传输设备上唯一的值。Your Discriminator 字段设置为零，因为 BFD 会话尚未建立。TX 和 RX 计时器设置为在设备配置中找到的值。

远程 BFD 设备在会话初始阶段收到 BFD 控制数据包后，会将 My Discriminator 字段中的值复制到其自己的 Your Discriminator 字段中，并从 Down 状态过度到 Init 状态，最终进入 Up 状态。一旦两个系统都在各自控制数据包中看到自己的 Discriminator，会话即正式建立。

下图显示了建立的 BFD 连接。

图 *76:* 未建立 ***BFD*** 会话的 ***BGP***



BFD 计时器协商

BFD 设备必须协商 BFD 计时器，以控制和同步 BFD 控制包的发送速率。设备需要确保以下条件，才能协商 BFD 计时器：

- 其对等设备看到包含本地设备的建议计时器的数据包
- 它发送 BFD 控制包的速度永远不会超过被配置为接收这些数据包的对等体
- 对等体发送 BFD 控制包的速度永远不会超过被配置为接收这些数据包的本地系统

Your Discriminator 字段和 H 位的设置足以使远程设备在首次计时器交换期间看到本地设备的数据包。在接收 BFD 控制包后，每个系统都将获得所需最小接收间隔，并将该间隔与其自己的所需最小发送间隔进行比较，然后取两个值中较大者（速度较慢者），并将该值用作其 BFD 数据包的传输速率。两个系统中速度较慢者将决定传输速率。

在协商这些计时器后，可在会话期间随时重新协商它们，而不会导致会话重置。更改其计时器的设备将在所有后续 BFD 控制包上设置 P 位，直到其收到通过远程系统设置了 F 位的 BFD 控制包为止。这种位的交换可以保护数据包，否则它们可能会在传输过程中丢失。

注释 远程系统设置 F 位，并不意味着它将接受新建议的计时器。它表示远程系统已经看到已经更改其中的计时器的数据包。

BFD 故障检测

如果 BFD 会话和计时器已经过协商，则 BFD 对等体按照协商的间隔互相发送 BFD 控制数据包。这些控制数据包作为检测信号，这非常类似于 IGP 呼叫协议，不同之处是速率得到了显著加速。

只要每个BFD对等体在配置的检测间隔（所需的最小RX间隔）内接收到BFD控制数据包，则BFD会话会保持，并且与 BFD 关联的任何路由协议均保持其邻接关系。如果 BFD 对等未在此间隔内收到控制数据包，则会向参与该BFD会话的所有客户端通知故障情况。路由协议可确定对该信息的适当响应。典型的响应是终止路由协议对等会话和重新收敛，从而绕过出现故障的对等体。

每次 BFD 对等体在 BFD 会话中成功接收到 BFD 控制数据包时，该会话的检测计时器都会重置为零。因此故障检测取决于接收的数据包，而不是接收方上次何时传输数据包。

BFD 部署场景

以下内容介绍了 BFD 在这些特定场景中如何运行。

故障转移

在故障转移场景中，将在主用设备与邻居设备之间建立和保留BFD会话。备用设备不会通过邻居保留任何BFD会话。当发生故障转移时，新主用设备必须通过邻居发起会话建立，因为主用设备与备用设备之间的会话信息没有同步。

对于无中断重新启动/NSF 场景，客户端 (BGP IPv4/IPv6) 负责通知其邻居关于事件的信息。当邻居收到该信息时，它将保留 RIB 表，直到故障转移完成为止。在故障转移期间，设备上的 BFD 和 BGP 会话将关闭。在故障转移完成后，当 BGP 会话启动时，将在邻居之间建立新的 BFD 会话。

跨网络 EtherChannel 和 L2 集群

在跨网络 EtherChannel 集群场景中，将在主设备与其邻居之间建立和保留 BFD 会话。从属设备不会通过邻居保留任何 BFD 会话。如果由于交换机上的负载均衡而将 BFD 数据包路由到从属设备，则该从属设备必须通过集群链路将此数据包转发到主设备。当发生集群故障恢复时，新主设备必须通过邻居发起会话建立，因为主设备与从属设备之间的会话信息没有同步。

单个接口模式和 L3 集群

在单个接口模式集群场景中，单个设备将通过其邻居保留其 BFD 会话。

BFD 路由准则

情景模式准则

支持单一和多情景模式。

防火墙模式准则

在路由防火墙模式下受支持；支持独立、故障转移和集群模式。在故障转移和集群接口上不支持 BFD。在集群中，仅在主设备上支持此功能。在透明模式下不支持 BFD。

IPv6 准则

IPv6 不支持回送模式。

其他准则

支持 OSPFv2、OSPFv3、BGP IPv4 和 BGP IPv6 协议。

不支持 IS-IS 和 EiGRP 协议。

不支持用于静态路由的 BFD。

不支持传输和隧道上的 BFD。

注释 为优化路由，在设备上为 NSF 配置 BGP 平稳重启时，请勿配置 BFD。

配置 BFD

本节介绍如何在系统中启用和配置 BFD 路由进程。

过程

步骤 1 创建 BFD 模板，第 967 页。
步骤 2 配置 BFD 接口，第 969 页。
步骤 3 配置 BFD 映射，第 970 页。

创建 BFD 模板

本节介绍创建 BFD 模板和进入 BFD 配置模式所需的步骤。

BFD 模板指定一组 BFD 间隔值。BFD 模板中配置的 BFD 间隔值并不是特定于单个接口。此外，还可以为单跳和多跳会话配置身份验证。可以仅在单跳上启用回应。

过程

步骤 1 通过创建单跳或多跳 BFD 模板在 ASA 上作为路由协议启用 BFD：

bfd-template [single-hop | multi-hop] *template_name*

示例：

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
```

```
ciscoasa(config-bfd)#
```

- **single-hop**- 指定单跳 BFD 模板。
- **multi-hop**- 指定多跳 BFD 模板。
- *template-name* - 指定模板名称。模板名称不能包含空格。

使用 **bfd-template** 命令可创建 BFD 模板并进入 BFD 配置模式。

步骤 2 （可选）在单跳 BFD 模板上配置回应：

bfd-template single-hop *template_name*

示例：

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa (config-bfd)# echo
```

只能在单跳模板上启用回应模式。BFD 回应不支持 IPv6 BFD 会话。

步骤 3 在 BFD 模板中配置间隔：

interval [**both** *milliseconds* | **microseconds {both | min-tx}** *microseconds* | **min-tx** *milliseconds*

示例：

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# interval both 50
```

- **both** - 最低传输和接收间隔功能。
- *milliseconds* - 间隔以毫秒为单位。范围为 50 到 999。
- **microseconds** - 为 **both** 和 **min-tx** 指定 BFD 间隔（以毫秒为单位）。
- *microseconds* - 范围介于 50,000 到 999,000 之间。
- **min-tx**- 最低传输间隔功能。

作为 BFD 模板的一部分指定的 BFD 间隔值并不是特定于单个接口。您可以对每个接口应用各自的 BFD 模板。请参阅配置 BFD 接口，第 969 页。

步骤 4 在 BFD 模板中配置身份验证：

authentication {md5 | meticulous-mds | meticulous-sha-1 | sha-1} [0|8] *word* **key-id** *id*

示例：

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# authentication sha-1 0 cisco key-id 10
```

- **authentication** - 指定身份验证类型。
- **md5**- 消息摘要 5 (MD5) 身份验证。

- **meticulous-md5** - Meticulous keyed MD5 身份验证。
- **meticulous-sha-1** - Meticulous keyed SHA-1 身份验证。
- **sha-1** - Keyed SHA-1 身份验证。
- **0|8**- 0 指定后面是未加密的密码。8 指定后面是已加密的密码。
- *word* - BFD 密码（密钥），单位数密码/密钥，最长 29 个字符。不支持以数字开头后跟空格的密码，例如“0 pass”和“1”均为无效密码。
- **key-id**- 身份验证密钥 ID。
- *id* - 匹配密钥字符串的共享密钥 ID。范围介于 0 到 255 个字符之间。

可以在单跳和多跳模板中配置身份验证。我们建议您配置身份验证，以增强安全性。在每个BFD源目标对上必须配置身份验证，而且两台设备上的身份验证参数必须匹配。

配置 BFD 接口

您可以将 BFD 模板绑定至接口，按接口配置基准 BFD 会话参数，然后按接口启用回应模式。

过程

步骤 1 进入接口配置模式：

interface *interface_id*

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#
```

步骤 2 将 BFD 模板应用到接口：

bfd template *template-name*

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# bfd template TEMPLATE1
```

即使未使用 **bfd-template** 命令创建模板，也可以在接口下配置模板的名称，但是，该模板会被视为无效，直到您定义该模板。您不必再重新配置模板名称。它会自动变为有效。

步骤 3 配置 BFD 会话参数：

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-router)# bfd interval 200 min_rx 200 multiplier 3
```

- **interval** *milliseconds* - 指定将 BFD 控制数据包发送到 BFD 对等体的速率。范围介于 50 到 999 毫秒之间。
- **min_rx** *milliseconds* - 指定预期从 BFD 对等体接收 BFD 控制数据包的速率。范围介于 50 到 999 毫秒之间。
- **multiplier** *multiplier-value* - 指定在 BFD 声明对等体不可用并通知第 3 层 BFD 对等体相关故障之前必须错过来自该 BFD 对等体的连续 BFD 控制数据包数。范围为 3 到 50。

步骤 4 在接口上启用 BFD 回应模式。

bfd echo

示例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(if)# bfd echo
```

默认情况下会启用回应模式，但该模式在 BFD IPv6 会话中不受支持。当启用回应模式后，将从 **bfd interval** *milliseconds* **min_rx** *milliseconds* 配置获取最小回应传输级别和所需的最小传输间隔值。

注释
在使用 BFD 回应模式之前，您必须使用 **no ip redirects** 命令禁用 ICMP 重定向消息。这样可以避免 CPU 使用率过高。

配置 BFD 映射

您可以创建包含可与多跳模板关联的目标的 BFD 映射。您必须已配置多跳 BFD 模板。

过程

步骤 1 创建一个多跳 BFD 模板。请参阅创建 BFD 模板，第 967 页了解相关程序。

步骤 2 将该 BFD 多跳模板与目标的映射相关联：

bfd map {ipv4 | ipv6} *destination/cdir source/cdire template-name*

示例：

```
ciscoasa(config)# bfd map ipv4 10.11.11.0/24 10.36.42.5/32 MULTI-TEMPLATE1
ciscoasa(config-bfd)#
```

- **ipv4** - 配置 IPv4 地址。

- **ipv6** - 配置 IPv6 地址。
- *destination/cdir* - 指定目标前缀/长度。格式为 A.B.C.D/<0-32>。
- *source/cdir* - 指定目标前缀/长度。格式为 X:X:X;X::X/<0-128>。
- *template-name* - 指定与此 BFD 映射关联的多跳模板的名称。

步骤 3 （可选）配置 BFD 慢计时器值：

bfd slow-timers [*milliseconds*]

示例：

```
ciscoasa(config)# bfd slow-timers 14000
ciscoasa(config-bfd)#
```

milliseconds -（可选）BFD 慢计时器值。范围为 1000 到 30000。默认值为 1000。

BFD 监控

可以使用以下命令监控 BFD 路由进程。有关命令输出的示例和说明，请参阅命令参考。

要监控或禁用各种 BFD 路由统计信息，请输入以下其中一个命令：

- **show bfd neighbors**

  显示现有 BFD 邻接关系逐行列表。

- **show bfd summary**

  显示 BFD、BFD 客户端或 BFD 会话的摘要信息。

- **show bfd drops**

  显示 BFD 中已丢弃的数据包数。

- **show bfd map**

  显示配置的 BFD 映射。

- **show running-config bfd**

  显示 BFD 映射和其他 BFD 相关配置。

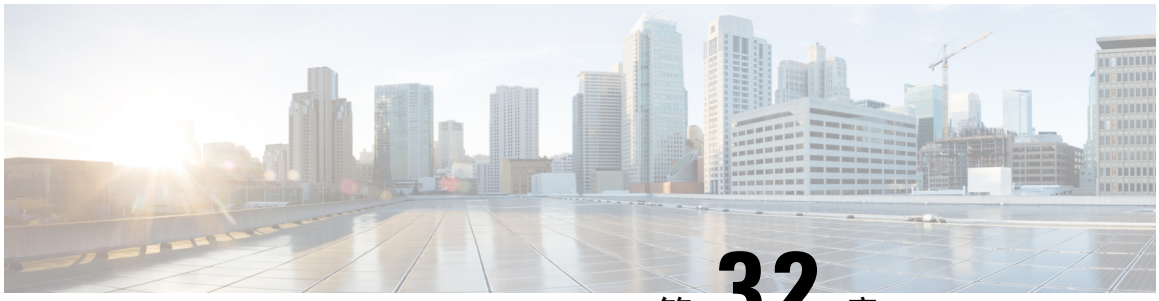
- **show running-config bfd-template**

  显示 BFD 模板相关配置。

BFD 路由的历史记录

表 *38: BFD* 路由的功能历史记录

功能名称	平台版本	功能信息
BFD 路由支持	9.6(2)	ASA 现在支持 BFD 路由协议。添加了对配置 BFD 模板、接口和映射的支持。还添加了对 BGP 路由协议使用 BFD 的支持。 添加了以下命令：**bfd echo**、**bfd interval**、**bfd map**、**bfd slow-timers**、**bfd-template**、**clear bfd counters**、**clear conf bfd**、**neighbor fall-over bfd**、**show bfd drops**、**show bfd map**、**show bfd neighbors**、**show bfd summary**、**show running-config bfd**



第 32 章

BGP

本章介绍如何配置 ASA，以使用边界网关协议 (BGP) 来路由数据、执行身份验证以及重新分发路由信息。

- 关于 BGP，第 973 页
- BGP 准则，第 976 页
- 配置 BGP，第 977 页
- 监控 BGP，第 1007 页
- BGP 示例，第 1009 页
- BGP 的历史记录，第 1012 页

关于 BGP

BGP 是一种外部和内部自主系统路由协议。自治系统是一个或一组接受共同管理并采用共同路由策略的网络。BGP 用于交换互联网的路由信息，并且是互联网运营商 (ISP) 之间所使用的协议。

何时使用 BGP

客户网络（例如，大学和公司）通常使用 OSPF 等内部网关协议 (IGP) 在其网络内交换路由信息。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

BGP 也可用于通过 IPv6 网络承载有关 IPv6 前缀的路由信息。

注释 如果一台 BGPv6 设备加入集群，那么当启用日志级别 7 时，该设备会生成软回溯。

路由表更改

在 BGP 邻居之间首次建立 TCP 连接时，BGP 邻居会交换完整路由信息。当检测到对路由表所做的更改时，BGP 路由器仅会向其邻居发送已更改的路由。BGP 路由器不会发送定期路由更新，并且 BGP 路由更新仅对到达目标网络的最佳路径进行通告。

注释 系统通过扫描完整的 AS 路径（在 AS_PATH 属性中指定）并检查本地系统的 AS 编号是否未出现在 AS 路径中来完成 AS 环路检测。默认情况下，EBGP 将获知的路由通告给同一对等体，以防止在执行环路检查时 ASA 上出现额外的 CPU 周期，并避免现有传出更新任务中出现延迟。

当存在多个到达某个特定目标的路由时，通过 BGP 获悉的路由的属性可用于确定到达该目标的最佳路径。这些属性称为 BGP 属性，可在路由选择过程中使用：

- 权重 - 这是思科定义的路由器本地属性。权重属性不会向相邻路由器进行通告。如果路由器获悉有多个到达同一目标的路由，则首选权重最高的路由。
- 本地首选项 - 本地首选项属性用于从本地 AS 中选择出口点。与权重属性不同，本地优先属性在整个本地 AS 中传播。如果有多个来自 AS 的出口点，则使用具有最高本地优先属性的出口点作为特定路由的出口点。
- 多出口鉴别器 - 多出口鉴别器 (MED) 或度量属性可用作对外部 AS 关于进入正在通告此度量的 AS 的首选路径的建议。因为正在接收 MED 的外部 AS 也可能正在使用其他 BGP 属性选择路由，所以它仅作为建议。首选 MED 指标较低的路由。
- 源 - 源属性指示 BGP 获悉某个特定路由的方式。源属性可能具有下面三个可能值中的一个，用于路由选择。
  - IGP - 此路由是源 AS 的内部路由。当使用网络路由器配置命令向 BGP 注入路由时，会设置该值。
  - EGP - 此路由通过外部边界网关协议 (EBGP) 获悉。
  - 不完整 - 路由源未知或通过其他方式获悉。当路由重新分发到 BGP 时，可能会出现源不完整的情况。
- AS_path - 当路由通告通过一个自治系统时，会在按顺序排列的 AS 编号列表中添加 AS 编号，标识路由通告已经穿越的 AS。仅将拥有最短 AS_path 列表的路由添加至 IP 路由表中。
- 下一跳 - EBGP 下一跳属性是用于到达通告路由器的 IP 地址。对于 EBGP 对等体，下一跳地址是对等体之间的连接 IP 地址。对于 IBGP，EBGP 下一跳地址会携带至本地 AS 中。但是，当下一个跃点与 eBGP 对等体的对等地址位于同一子网时，下一个跃点不会被修改。此行为称为第三方下一个跃点。

  在将 VPN 通告的路由重新分发到 iBGP 对等体时，请使用 **next-hop-self** 命令，以确保使用正确的下一跳 IP 重新分发路由。
- 社区 - 社区属性提供一种目标（称为社区）的分组方式，可对社区应用路由决策（例如，接受、首选项和重新分发）。路由映射用于设置社区属性。预定义的社区属性如下：

- no-export - 不向 EBGP 对等体通告相应路由。
- no-advertise - 不向任何对等体进行通告。
- internet - 此路由向互联网社区进行通告；网络中的所有路由器均属于此类型。

BGP 路径选择

BGP 可能会从不同来源接收同一路由的多个通告。BGP 仅选择一个路径作为最佳路径。选择此路径后，BGP 将选定的路径放在 IP 路由表中，并将此路径传播给其邻居。BGP 按显示的顺序使用以下条件为目标选择路径：

- 如果路径指定的下一跳不可访问，则放弃更新。
- 首选权重最高的路径。
- 如果权重相同，则首选具有最高本地优先值的路径。
- 如果本地优先值相同，则首选 BGP 在此路由器上运行所发起的路径。
- 如果未发起路由，则首选 AS_path 最短的路由。
- 如果所有路径的 AS_path 长度相同，则首选源类型最低的路径（其中，IGP 低于 EGP，EGP 低于不完整路径）。
- 如果源代码相同，则首选 MED 属性最低的路径。
- 如果路由的 MED 相同，则首选外部路径而非内部路径。
- 如果路径依然相同，则首选穿过最近的 IGP 邻居的路径。
- 在 BGP 多路径，第 975 页的路由表中确定是否需要安装多个路径。
- 如果两个路径都是外部路径，则首选第一个接收的路径（最早的路径）。
- 首选具有由 BGP 路由器 ID 指定的最低 IP 地址的路径。
- 如果多个路径的发起方或路由器 ID 相同，则首选集群列表长度最短的路径。
- 首选来自最低邻居地址的路径。

BGP 多路径

BGP 多路径允许将多个等成本 BGP 路径的 IP 路由表安装到相同的目标前缀。然后，跨安装的所有路径共享到目标前缀的流量。

这些路径连同最佳路径一起安装在表中，以实现负载共享。BGP 多路径不影响最佳路径选择。例如，路由器仍会根据算法将其中一个路径指定为最佳路径，并将此最佳路径通知其 BGP 对等体。

要想成为多路径的候选对象，指向同一目标的路径需要具有与最佳路径特性相同的以下特性：

- 重量

- 本地优先级
- AS-PATH 长度
- 源代码
- 多出口鉴别器 (MED)
- 以下选项之一：
  - 相邻的 AS 或子 AS（在添加 BGP 多路径之前）
  - AS 路径（在添加 BGP 多路径之后）

某些 BGP 多路径功能对多路径候选对象有一些额外要求：

- 此路径应从外部或联盟外部邻居 (eBGP) 获悉。
- BGP 下一跳的 IGP 指标应等于最佳路径 IGP 指标。

这些是内部 BGP (iBGP) 多路径候选对象的额外要求：

- 此路径应从内部邻居 (eBGP) 获悉。
- BGP 下一跳的 IGP 指标应等于最佳路径 IGP 指标，除非路由器是面向非等成本 iBGP 多路径配置的。

BGP 可将最多 *n* 个最近收到的路径从多路候选对象插入到 IP 路由表中，其中 *n* 是要安装到路由表的路由数，如配置 BGP 多路径时所指定的那样。禁用多路径时的默认值为 1。

对于非等成本的负载平衡，您还可以使用 BGP 链路带宽。

注释 等效的下一自跳将在从 eBGP 中选择的最佳路径上执行，并且是在最佳路径转发至内部对等体之前执行。

BGP 准则

情景模式准则

- 同时支持单情景和多情景模式。
- 所有情景仅支持一个自治系统 (AS) 编号。

防火墙模式准则

不支持透明防火墙模式。仅在路由模式下支持 BGP。

IPv6 准则

支持 IPv6。

其他准则

- 系统不会在 CP 路由表中为通过 PPPoE 接收的 IP 地址添加路由条目。BGP 始终查看用于发起 TCP 会话的 CP 路由表，因此 BGP 不会形成 TCP 会话。

  因此，不支持通过 PPPoE 发送 BGP。

- 仅管理或 BVI 接口不支持 BGP。
- 要避免在路由更新大于链路上的最小 MTU 时丢弃由于路由更新而导致的邻接摆动，请确保在链路两端的接口上配置相同的 MTU。
- 如果 MTU 发现失败，使用 PATH MTU (PMTU) 的 BGP 可能会导致邻接失效，特别是在 ECMP 路由情况下。因此，在使用 BGP、PMTU 和 ECMP 时一定要谨慎，因为如果 MTU 发现因任何原因失败，都可能导致数据包丢弃。
- 成员设备的 BGP 表未与控制设备表同步。仅其路由表与控制单元路由表同步。

配置 BGP

本节介绍如何在系统中启用和配置 BGP 进程。

过程

步骤 1 启用 BGP，第 977 页。
步骤 2 定义 BGP 路由进程的最佳路径，第 979 页。
步骤 3 配置策略列表，第 980 页。
步骤 4 配置 AS 路径过滤器，第 981 页。
步骤 5 配置社区规则，第 982 页。
步骤 6 配置 IPv4 地址系列设置，第 983 页。
步骤 7 配置 IPv6 地址系列设置，第 995 页。

启用 BGP

本节介绍启用 BGP 路由、建立 BGP 路由进程和配置常规 BGP 参数所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

autonomous-num 的有效值范围是 1-4294967295 和 1.0-XX.YY。

步骤 2 丢弃 as-path 分段超过指定值的路由。

bgp maxas-limit number

示例：

```
ciscoasa(config-router)# bgp maxas-limit 15
```

number 参数指定允许的自治系统网段的最大数。有效值范围为 1 至 254。

步骤 3 日志 BGP 邻居重置：

bgp log-neighbor-changes

步骤 4 使 BGP 能够自动发现每个 BGP 会话的最佳 TCP 路径 MTU：

bgp transport path-mtu-discovery

步骤 5 使 BGP 能够在用于到达对等体的链接中断时，终止任何直接相邻对等体的外部 BGP 会话；无需等待抑制计时器到期：

bgp fast-external-fallover

步骤 6 如果外部 BGP (eBGP) 对等体未在传入路由的 AS_PATH 属性中将其自治系统 (AS) 编号列为首个 AS 路径分段，则允许 BGP 路由进程放弃从这些外部 BGP 对等体接收的更新。

bgp enforce-first-as

步骤 7 将 BGP 4 字节自治系统编号的默认显示和正则表达式匹配格式从 asplain（十进制值）更改为点分表示法。

bgp asnotation dot

步骤 8 调整 BGP 网络计时器：

timers bgp keepalive holdtime [min-holdtime]

示例：

```
ciscoasa(config-router)# timers bgp 80 120
```

- keepalive - ASA 向其对等体发送 keepalive 消息的频率（以秒为单位）。默认值为 60 秒。
- holdtime - ASA 在未接收到 keepalive 消息后声明对等体处于失效状态的间隔（以秒为单位）。默认值为 180 秒。
- （可选）min-holdtime - ASA 在未从邻居接收到 keepalive 消息后声明邻居处于失效状态的间隔（以秒为单位）。

  注释
  保持时间小于 20 秒会增加对等体振荡的可能性。

步骤 9 启用 BGP 无中断重新启动功能：

bgp graceful-restart [restart-time seconds|stalepath-time seconds][all]

示例：

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- restart-time - 重新启动事件发生后，ASA 等待支持无中断重新启动的邻居恢复正常运行的最大时间间隔（以秒为单位）。默认值为 120 秒。有效值范围为 1 至 3600 秒。
- stalepath-time - ASA 为正在重新启动的对等体保留过期路径的最大时长（以秒为单位）。此计时器到期后，将删除所有过时路径。默认值为 360 秒。有效值范围为 1 至 3600 秒。

定义 BGP 路由进程的最佳路径

本节介绍配置 BGP 最佳路径所需的步骤。有关最佳路径的详细信息，请参阅BGP 路径选择，第 975 页。

过程

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 更改默认本地优先值：

bgp default local-preference number

示例：

```
ciscoasa(config-router)# bgp default local-preference 500
```

number 参数是介于 0 与 4294967295 之间的任意值。值越大，表示优先级越高。

默认值为 100。

步骤 3 启用从不同自治系统中的不同邻居获悉的路径之间的多出口鉴别器 (MED) 比较：

bgp always-compare-med

步骤 4 在最佳路径选择过程中，比较从外部 BGP (eBGP) 接收的类似路径，并将最佳路径切换到路由器 ID 最低的路由：

bgp bestpath compare-routerid

步骤 5 选择相邻 AS 通告的最佳 MED 路径：

bgp deterministic-med

步骤 6 将缺少 MED 属性的路径设置为最不优先考虑的路径：

bgp bestpath med missing-as-worst

配置策略列表

当在路径映射中引用策略列表时，将评估并处理此策略列表中的所有匹配语句。通过一个路由映射可以配置两个或更多策略列表。策略列表也可以与任何其他预先存在的匹配共存，并设置在同一路径映射内部、策略列表外部配置的语句。本节介绍配置策略列表所需的步骤。

过程

步骤 1 创建 BGP 策略列表。

policy-list *policy_list_name* {**permit** | **deny**}

permit 关键字允许访问匹配条件。

deny 关键字拒绝访问匹配条件。

示例：

```
ciscoasa(config)# policy-list Example-policy-list1 permit
```

步骤 2 分发使其下一跳脱离其中一个指定接口的路由：

match interface [*interface_name* [*interface_name*] [⋯]]

示例：

```
ciscoasa(config-policy-list)# match interface outside
```

步骤 3 通过匹配以下任一或所有项重新分发路由：目标地址、下一跳路由器地址和路由器/接入服务器源：

match ip {**address** | **next-hop** | **route-source**}

步骤 4 匹配 BGP 自治系统路径：

match as-path

步骤 5 匹配 BGP 社区：

match community {*community-list_name* | **exact-match**}

- *community-list_name* - 一个或多个社区列表。
- **exact-match** - 表示要求精确匹配。所有社区以及仅指定社区必须存在。

示例：

```
ciscoasa(config-policy-list)# match community ExampleCommunity1
```

步骤 6 重新分发带指定指标的路由：

match metric *metric* [*metric* […]]

步骤 7 重新分发路由表中匹配指定标记的路由：

match tag *tag* [*tag* […]]

配置 AS 路径过滤器

AS路径过滤器允许您使用访问列表来过滤路由更新消息，并且查看更新消息中的单个前缀。如果更新消息中的前缀与过滤条件相匹配，则会过滤掉或接受该单个前缀，具体视过滤器条目已配置为执行的操作内容而定。本节介绍配置 AS 路径过滤器所需的步骤。

注释 as-path 访问列表不同于常规防火墙 ACL。

过程

在全局配置模式下，使用正则表达式配置自治系统路径过滤器：

as-path access-list acl-number {permit|deny} regexp

示例：

```
ciscoasa(config)# as-path access-list 35 permit testaspath
```

- *acl-number* - AS 路径访问列表编号。有效值为从 1 到 500。
- regexp - 用于定义 AS 路径过滤器的正则表达式。自治系统编号的表示范围为 1 至 65535。

配置社区规则

社区是指一组共享某个通用属性的目标。您可以使用社区列表创建要在路由映射的匹配子句中使用的社区组。如同访问列表一样，可以创建一系列社区列表。系统会检查语句，直至找到匹配项为止。只要满足一个语句，便会结束测试。本节介绍配置社区规则所需的步骤。

过程

创建或配置 BGP 社区列表，并控制对它的访问：

community-list {standard| community list-name {deny|permit} [community-number] [AA:NN] [internet] [no-advertise][no-export]}| {expanded|expanded list-name {deny| permit}regexp}

示例：

```
ciscoasa(config)# community-list standard excomm1 permit 100 internet no-advertise no-export
```

- standard - 使用 1 至 99 的数字配置标准社区列表，以确定社区的一个或多个允许或拒绝组。
- （可选）community-number - 以 1 至 4294967200 的 32 位数字表示的社区。可以输入单个社区，也可以输入以空格分隔的多个社区。
- AA:NN - 以 4 字节新社区格式输入的自治系统号和网络号。该值使用两个以冒号分隔的 2 字节编号进行配置。可以为每个 2 字节编号输入 1 至 65535 的数字。可以输入单个社区，也可以输入以空格分隔的多个社区。
- （可选）internet - 指定互联网社区。系统向所有对等体（内部和外部）通告具有此社区的路由。
- （可选）no-advertise - 指定无通告社区。系统不向任何对等体（内部或外部）通告具有此社区的路由。
- （可选）no-export - 指定无导出社区。系统仅向同一自治系统中的对等体或仅向联盟内的其他子自治系统通告具有此社区的路由。不会向外部对等体通告这些路由。
- （可选）expanded - 配置一个从 100 至 500 的扩展社区列表号，以确定社区的一个或多个允许或拒绝组。
- regexp - 用于定义 AS 路径过滤器的正则表达式。自治系统编号的表示范围为 1 至 65535。

注释

正则表达式只能用于扩展社区列表。

配置 IPv4 地址系列设置

可以从 BGP 配置设置中的 IPv4 系列选项来设置 BGP 的 IPv4 设置。IPv4 系列部分包括以下子部分：常规设置、汇聚地址设置、过滤设置和邻居设置。其中每个子部分都支持您自定义特定于 IPv4 系列的参数。

配置 IPv4 系列常规设置

本节介绍配置常规 IPv4 设置所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使路由器进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 4 (IPv4) 地址前缀配置路由会话：

address-family ipv4 [unicast]

关键字 unicast 指定 IPv4 单播地址前缀。这是默认设置，即使未指定也如此。

步骤 3 （可选）为本地 BGP 路由进程配置固定路由器 ID：

bgp router-id A.B.C.D

示例：

```
ciscoasa(config-router-af)# bgp router-id 10.86.118.3
```

参数 A.B.C.D 以 IP 地址形式指定路由器标识符。如果不指定路由器 ID，则会自动分配路由器 ID。

步骤 4 （可选）在单个接口 (L3) 模式下配置 IP 地址集群池：

bgp router-id cluster-pool

示例：

```
ciscoasa(config-router-af)# bgp router-id cp
```

注释

在 L3 集群中，不能将 BGP 邻居定义为其中一个集群池 IP 地址。

步骤 5 配置 BGP 路由的管理距离：

distance bgp external-distance internal-distance local-distance

示例：

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance - 外部 BGP 路由的管理距离。从外部自治系统获悉的路由是外部路由。此参数值的范围为 1 至 255。
- internal-distance - 内部 BGP 路由的管理距离。从本地自治系统中的对等体获悉的路由是内部路由。此参数值的范围为 1 至 255。
- local-distance - 本地 BGP 路由的管理距离。本地路由是指通过网络路由器配置命令列出的网络，通常作为正在从其他进程重新分发的路由器或网络的后门。此参数值的范围为 1 至 255。

步骤 6 使用 BGP 获悉的路由更新 IP 路由表时，修改指标和标签值。

table-map {WORD|route-map_name}

示例：

```
ciscoasa(config-router-af)# table-map example1
```

参数 route-map_name 指定来自 route-map 命令的路由映射名称。

步骤 7 配置 BGP 路由进程，以分发默认路由（网络 0.0.0.0）：

default-information originate

步骤 8 将子网路由配置为自动汇总到网络级路由中

auto-summary

步骤 9 抑制未装载至路由信息库 (RIB) 中的路由的通告：

bgp suppress-inactive

步骤 10 在 BGP 与内部网关协议 (IGP) 系统之间同步：

synchronization

步骤 11 将 iBGP 配置为重新分发到 IGP 中，例如 OSPF：

bgp redistribute-internal

步骤 12 为下一跳验证配置 BGP 路由器扫描间隔：

bgp scan-time scanner-interval

示例：

```
ciscoasa(config-router-af)# bgp scan-time 15
```

参数 scanner-interval 指定 BGP 路由信息的扫描间隔。有效值范围为 5 至 60 秒。默认值为 60 秒。

步骤 13 配置 BGP 下一跳地址跟踪：

bgp nexthop trigger {delay seconds|enable}

示例：

```
ciscoasa(config-router-af)# bgp nexthop trigger delay 15
```

- trigger - 指定使用 BGP 下一跳地址跟踪。此关键字与关键字 delay 结合用于更改下一跳跟踪延迟。此关键字与关键字 enable 结合用于启用下一跳地址跟踪。
- delay - 更改前后两次对路由表中安置的已更新下一跳路由进行检查的延迟间隔。
- seconds - 指定以秒为单位的延迟。范围为 0 至 100。默认值为 5。
- enable - 立即启用 BGP 下一跳地址跟踪。

步骤 14 控制可以安置在路由表中的并行 iBGP 路由的最大数量：

maximum-paths {number_of_paths|ibgp number_of_paths}

示例：

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

注释
如果未使用关键字 ibgp，则参数 number_of_paths 会控制并行 EBGP 路由的最大数量。

参数 number_of_paths 指定安置到路由表中的路由的数量。有效值介于 1 与 8 之间。

配置 IPv4 系列汇聚地址设置

本节介绍将特定路由定义为聚合成一个路由所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 4 (IPv4) 地址前缀配置路由会话：

address-family ipv4 [unicast]

关键字 unicast 指定 IPv4 单播地址前缀。这是默认设置，即使未指定也如此。

步骤 3 在 BGP 数据库中创建聚合条目：

aggregate-address address mask [as-set][summary-only][suppress-map map-name][advertise-map map-name][attribute-map map-name]

示例：

```
ciscoasa(config-router-af) aggregate-address 10.86.118.0 255.255.255.0 as-set summary-only
 suppress-map example1 advertise-map example1 attribute-map example1
```

- address - 汇聚地址。
- mask- 聚合掩码。
- map-name - 路由映射。
- （可选）as-set - 生成自治系统集路径信息。
- （可选）summary-only - 过滤来自更新的所有更具体的路由。
- （可选）Suppress-map map-name - 指定用于选择要抑制的路由的路由映射的名称。
- （可选）Advertise-map map-name - 指定用于选择创建 AS_SET 源社区所用路由的路由映射的名称。
- （可选）Attribute-map map-name - 指定用于设置聚合路由属性的路由映射的名称。

配置 IPv4 系列过滤设置

本部分介绍过滤在传入 BGP 更新中接收的路由或网络所需的步骤。

过程

步骤 1 启用 BGP 路由进程并进入路由器配置模式。

router bgp *autonomous-num*

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 4 (IPv4) 地址前缀配置路由会话：

address-family ipv4 [**unicast**]

关键字 unicast 指定 IPv4 单播地址前缀。这是默认设置，即使未指定也如此。

步骤 3 过滤在传入 BGP 更新中接收或在传出 BGP 更新中通告的路由或网络：

distribute-list *acl-number* {**in** | **out**} [*protocol process-number* | **connected** | **static**]

参数 *acl-number* 指定 IP 访问列表号。此访问列表定义要在路由更新中接收的网络和要抑制的网络。

关键字 **in**指定过滤器必须应用于传入BGP更新，关键字 **out** 指定过滤器必须应用于传出BGP更新。

对于出站过滤器，您可以通过进程号（不包括 RIP）选择性地指定一个协议（**bgp**、**eigrp**、**ospf** 或 **rip**）以应用到分发列表。您还可以根据对等体和网络是通过 **connected** 还是 **static** 路由获知的进行过滤。

示例：

```
ciscoasa(config-router-af)# distribute-list ExampleAcl in bgp 2
```

配置 IPv4 系列 BGP 邻居设置

本节介绍定义 BGP 邻居和邻居设置所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使路由器进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 4 (IPv4) 地址前缀配置路由会话：

address-family ipv4 [unicast]

关键字 unicast 指定 IPv4 单播地址前缀。这是默认设置，即使未指定也如此。

步骤 3 向 BGP 邻居表添加条目：

neighbor ip-address remote-as autonomous-number

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remote-as 3
```

步骤 4 （可选）禁用邻居或对等组：

neighbor ip-address shutdown

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 shutdown 3
```

步骤 5 与 BGP 邻居交换信息：

neighbor ip-address activate

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 activate
```

步骤 6 为 BGP 邻居启用或禁用边界网关协议 (BGP) 平稳重启功能：

neighbor ip-address ha-mode graceful-restart [disable]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ha-mode graceful-restart
```

（可选）关键字 disable 为邻居禁用 BGP 平稳重启功能。

步骤 7 按访问列表中的指定分发 BGP 邻居信息：

neighbor {ip-address} distribute-list {access-list-name}{in|out}

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 distribute-list ExampleAcl in
```

- access-list-number - 标准或扩展访问列表的编号。标准访问列表号的范围为 1 至 99。扩展访问列表号的范围为 100 至 199。
- expanded-list-number - 扩展访问列表的编号。扩展访问列表号的范围为 1300 至 2699。
- access-list-number - 标准或扩展访问列表的名称。
- prefix-list-name - BGP 前缀列表的名称。
- in - 访问列表应用于传入到此邻居的通告。
- out - 访问列表应用于传出到此邻居的通告。

步骤 8 将路由映射应用于传入或传出路由：

neighbor {ip-address} route-map map-name {in|out}

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 route-map example1 in
```

关键字 in 将路由映射应用于传入路由。

关键字 out 将路由映射应用于传出路由。

步骤 9 按前缀列表中的指定分发 BGP 邻居信息：

neighbor {ip-address} prefix-list prefix-list-name {in|out}

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 prefix-list NewPrefixList in
```

关键字 in 意味着前缀列表应用于从此邻居传入的通告。

关键字 out 意味着前缀列表应用于传出到此邻居的通告。

步骤 10 设置过滤器列表：

neighbor {ip-address} filter-list access-list-number {in|out}

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 filter-list 5 in
```

- access-list-name - 指定自治系统路径访问列表的编号。您可以使用 ip as-path access-list 命令定义此访问列表。
- in - 访问列表应用于从此邻居传入的通告。
- out - 访问列表应用于传出到此邻居的通告。

步骤 11 控制可以从邻居接收的前缀的数量：

neighbor {ip-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 maximum-prefix 7 75 restart 12
```

- maximum - 从此邻居允许的前缀的最大数量。
- （可选）threshold - 整数，用于指定路由器开始生成警告消息时所达到的最大值的百分比。范围为 1 至 100，默认值为 75（百分比）。
- （可选）restart interval - 整数值（以秒为单位），用于指定 BGP 邻居重新启动前的时间间隔。
- （可选）warning-only - 允许路由器在超过最大前缀数量时生成日志消息，而不是终止对等。

步骤 12 允许 BGP 发言者（本地路由器）将默认路由 0.0.0.0 发送到邻居，以用作该邻居的默认路由：

neighbor {ip-address} default-originate [route-map map-name]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 default-originate route-map example1
```

参数 map-name 是路由映射的名称。路由映射允许有条件地注入路由 0.0.0.0。

步骤 13 设置前后两次发送 BGP 路由更新的最小间隔：

neighbor {ip-address} advertisement-interval seconds

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 advertisement-interval 15
```

参数 seconds 是时间（以秒为单位）。有效值范围为 0 至 600。

步骤 14 通告 BGP 表中与已配置的路由映射相匹配的路由：

neighbor {ip-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

示例：

```
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name - 将在达到存在映射或非存在映射的条件时通告的路由映射的名称。
- exist-map map name - 与 BGP 表中的路由进行比较以确定是否对通告映射路由进行通告的存在映射的名称。
- non-exist-map map name - 与 BGP 表中的路由进行比较以确定是否对通告映射路由进行通告的非存在映射的名称。
- （可选）check all paths - 使具有 BGP 表中的前缀的存在映射可检查所有路径。

步骤 15 从出站路由更新中删除专用自治系统号：

neighbor {ip-address} remove-private-as

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remove-private-as
```

步骤 16 为特定 BGP 对等体或对等组设置计时器。

neighbor {ip-address} timers keepalive holdtime min holdtime

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 timers 15 20 12
```

- keepalive - ASA 向其对等体发送 keepalive 消息的频率（以秒为单位）。默认值为 60 秒。有效值范围为 0 至 65535。
- holdtime - ASA 在未接收到 keepalive 消息后声明对等体处于失效状态的间隔（以秒为单位）。默认值为 180 秒。
- min holdtime - ASA 在未接收到 keepalive 消息后声明对等体处于失效状态的最小间隔（以秒为单位）。

注释
保持时间小于 20 秒会增加对等体振荡的可能性。

步骤 17 在两个 BGP 对等体之间的 TCP 连接上启用消息摘要 5 (MD5) 身份验证：

neighbor {ip-address} password string

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 password test
```

参数 string 是区分大小写的密码，启用 service password-encryption 命令时，其长度最大为 25 个字符；未启用 service password-encryption 命令时，其长度最大为 81 个字符。此字符串可以包含任意字母数字字符，包括空格。

注释
当您将密码的第一个字符设置为数字时，请勿在第二位使用空格。即，您不能指定 number-space-anything 格式的密码。数字后的空格会导致身份验证失败。

步骤 18 指定应将社区属性发送到 BGP 邻居：

neighbor {ip-address} send-community

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 send-community
```

步骤 19 将路由器配置为 BGP 发言邻居或对等组的下一跳：

neighbor {ip-address}next-hop-self

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 next-hop-self
```

步骤 20 接受并尝试建立与未直接连接的网络上的外部对等体的 BGP 连接：

neighbor {ip-address} ebgp-multihop [ttl]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ebgp-multihop 5
```

参数 ttl 指定生存时间，范围为 1 至 255 跳。

步骤 21 禁用连接验证可与使用环回接口的单跳对等体建立 eBGP 对等会话：

neighbor {ip-address} disable-connected-check

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 disable-connected-check
```

步骤 22 保护 BGP 对等会话，并且配置用于分隔两个外部 BGP (eBGP) 对等体的最大跳数。

neighbor {ip-address} ttl-security hops hop-count

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

参数 hop-count 是用于分隔 eBGP 对等体的跳数。TTL 值由路由器根据已配置的 hop-count 参数计算得出。有效值范围为 1 至 254。

步骤 23 向邻居连接分配权重：

neighbor {ip-address} weight number

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 weight 30
```

参数 number 是分配给邻居连接的权重。有效值范围为 0 至 65535。

步骤 24 将 ASA 配置为仅接受特定 BGP 版本：

neighbor {ip-address} version number

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 version 4
```

参数 number 指定 BGP 版本号。版本可以设置为 2，以强制软件仅对指定邻居使用版本 2。默认使用版本 4，如有要求，可以动态地协商降至版本 2。

步骤 25 为 BGP 会话启用 TCP 传输会话选项：

neighbor {ip-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 transport path-mtu-discovery
```

- connection-mode - 连接类型（active 或 passive）。
- path-mtu-discovery - 启用 TCP 传输路径最大传输单位 (MTU) 发现。默认情况下会启用 TCP 路径 MTU 发现。
- （可选）disable - 禁用 TCP 路径 MTU 发现。

步骤 26 为从外部边界网关协议 (eBGP) 邻居接收的路由自定义 AS_PATH 属性：

neighbor {ip-address} local-as [autonomous-system-number[no-prepend]]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- （可选）autonomous-system-number - 向 AS_PATH 属性预置的自治系统号。此参数值的范围是从 1 至 4294967295 或 1.0 至 XX.YY 的任意有效自治系统号。
- （可选）no-prepend - 不向从 eBGP 邻居接收的任何路由预置本地自治系统号。

步骤 27 要将接口更新为 BGP 邻居关系的源，请执行以下操作：

neighbor *ip_address* **update-source** *interface_name*

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 update-source loop1
```

参数 *interface_name* 是 BGP 邻居用作 BGP 路由源的接口的名称。

注释
如果将环回接口更新为 BGP 邻居关系的源，则会在网络中通告环回接口的 IP 地址。环回接口充当 eBGP 对等体并参与路由。由于环回接口在启用时稳定，并且在管理性关闭之前保持可用，因此始终可通过环回接口 IP 地址访问 ASA。

配置 IPv4 网络设置

本部分介绍定义要由 BGP 路由进程通告的网络所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 4 (IPv4) 地址前缀配置路由会话：

address-family ipv4 [unicast]

关键字 unicast 指定 IPv4 单播地址前缀。这是默认设置，即使未指定也如此。

步骤 3 指定将由 BGP 路由进程通告的网络：

network {network-number [mask network-mask]}[route-map map-tag]

示例：

```
ciscoasa(config-router-af)# network 10.86.118.13 mask 255.255.255.255 route-map example1
```

注释
要通告网络前缀，路由表中必须存在通往设备的路由。

- network-number - BGP 将通告的网络。
- （可选）network-mask - 带掩码地址的网络或子网掩码。
- （可选）map-tag - 已配置的路由映射的标识符。应检查路由映射，以过滤要通告的网络。如果未指定，则通告所有网络。

配置 IPv4 重新分发设置

本节介绍定义将其他路由域中的路由重新分发到 BGP 所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 4 (IPv4) 地址前缀配置路由会话：

address-family ipv4 [unicast]

示例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

关键字 unicast 指定 IPv4 单播地址前缀。这是默认设置，即使未指定也如此。

步骤 3 将路由从其他路由域重新分发到 BGP 自治系统：

redistribute protocol [process-id] [metric] [route-map [map-tag]]

示例：

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol - 从中重新分发路由的源协议。它可以是以下协议之一：Connected、EIGRP、OSPF、RIP 或 Static。
- （可选）process-id - 特定路由进程的名称。
- （可选）metric - 已重新分发的路由的指标。
- （可选）map-tag - 已配置路由映射的标识符。

注释

应检查路由映射，以过滤要重新分发的网络。如果未指定，则重新分发所有网络。

配置 IPv4 路由注入设置

本部分介绍定义有条件地注入 BGP 路由表中的路由所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 4 (IPv4) 地址前缀配置路由会话：

address-family ipv4 [unicast]

示例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

关键字 unicast 指定 IPv4 单播地址前缀。这是默认设置，即使未指定也如此。

步骤 3 配置有条件的路由注入，以将更具体的路由注入 BGP 路由表：

bgp inject-map inject-map exist-map exist-map [copy-attributes]

示例：

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map - 用于指定要注入本地 BGP 路由表的前缀的路由映射的名称。
- exist-map - 包含 BGP 发言者将跟踪的前缀的路由映射的名称。
- （可选）copy-attributes - 将已注入的路由配置为继承聚合路由的属性。

配置 IPv6 地址系列设置

可以从 BGP 配置设置中的 IPv6 系列选项来设置 BGP 的 IPv6 设置。IPv6 系列部分包括以下子部分：常规设置、汇聚地址设置和邻居设置。其中每个子部分都支持您自定义特定于 IPv6 系列的参数。

本节介绍如何自定义 BGP IPv6 系列设置。

配置 IPv6 系列常规设置

本节介绍配置常规 IPv6 设置所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使路由器进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 6 (IPv6) 地址前缀配置路由会话：

address-family ipv6 [unicast]

步骤 3 配置 BGP 路由的管理距离：

distance bgp external-distance internal-distance local-distance

示例：

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance - 外部 BGP 路由的管理距离。从外部自治系统获悉的路由是外部路由。此参数值的范围为 1 至 255。
- internal-distance - 内部 BGP 路由的管理距离。从本地自治系统中的对等体获悉的路由是内部路由。此参数值的范围为 1 至 255。
- local-distance - 本地 BGP 路由的管理距离。本地路由是指通过网络路由器配置命令列出的网络，通常作为正在从其他进程重新分发的路由器或网络的后门。此参数值的范围为 1 至 255。

步骤 4 （可选）配置 BGP 路由进程，以分发默认路由（网络 0.0.0.0）：

default-information originate

步骤 5 （可选）抑制未装载至路由信息库 (RIB) 中的路由的通告：

bgp suppress-inactive

步骤 6 在 BGP 与内部网关协议 (IGP) 系统之间同步：

synchronization

步骤 7 将 iBGP 配置为重新分发到 IGP 中，例如 OSPF：

bgp redistribute-internal

步骤 8 为下一跳验证配置 BGP 路由器扫描间隔：

bgp scan-time scanner-interval

示例：

```
ciscoasa(config-router-af)# bgp scan-time 15
```

参数 scanner-interval 的有效值范围为 5 至 60 秒。默认值为 60 秒。

步骤 9 控制可以安置在路由表中的并行 iBGP 路由的最大数量：

maximum-paths {number_of_paths|ibgp number_of_paths}

示例：

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

参数 number_of_paths 的有效值介于 1 与 8 之间。

如果未使用关键字 ibgp，则参数 number_of_paths 会控制并行 EBGP 路由的最大数量。

配置 IPv6 系列汇聚地址设置

本节介绍将特定路由定义为聚合成一个路由所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 6 (IPv6) 地址前缀配置路由会话：

address-family ipv6 unicast

步骤 3 在 BGP 数据库中创建聚合条目：

aggregate-address ipv6-address/cidr [as-set][summary-only][suppress-map map-name][advertise-map ipv6-map-name][attribute-map map-name]

示例：

```
ciscoasa(config-router-af) aggregate-address 2000::1/8 summary-only
```

- address - 聚合 IPv6 地址。

- （可选）as-set - 生成自治系统集路径信息。
- （可选）summary-only - 过滤来自更新的所有更具体的路由。
- （可选）suppress-map map-name - 指定用于选择要抑制的路由的路由映射的名称。
- （可选）advertise-map map-name - 指定用于选择创建 AS_SET 源社区所用路由的路由映射的名称。
- （可选）attribute-map map-name - 指定用于设置聚合路由属性的路由映射的名称。

步骤 4 设置 BGP 路由的聚合时间间隔：

bgp aggregate-timer seconds

示例：

```
ciscoasa(config-router-af)bgp aggregate-timer 20
```

配置 IPv6 系列 BGP 邻居设置

本节介绍定义 BGP 邻居和邻居设置所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使路由器进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 6 (IPv6) 地址前缀配置路由会话：

address-family ipv6 [unicast]

步骤 3 向 BGP 邻居表添加条目：

neighbor ipv6-address remote-as autonomous-number

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 remote-as 3
```

参数 ipv6-address 指定可用于到达指定网络的下一跳的 IPv6 地址。此下一跳的 IPv6 地址不需要直接连接；为查找直接连接的下一跳的 IPv6 地址，需要执行递归。当指定接口类型和接口号时，您可以根据需要指定数据包输出到的下一跳的 IPv6 地址。使用链路本地地址作为下一跳（链路本地下一跳也必须是相邻设备）时，必须指定接口类型和接口号。

注释
此参数必须采用 RFC 2373 中记录的形式，其中地址是用冒号分隔的十六进制 16 位值。

步骤 4 （可选）禁用邻居或对等组：

neighbor ipv6-address shutdown

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 shutdown 3
```

步骤 5 与 BGP 邻居交换信息：

neighbor ipv6-address activate

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 activate
```

步骤 6 为 BGP 邻居启用或禁用边界网关协议 (BGP) 平稳重启功能：

neighbor {ip-address} ha-mode graceful-restart [disable]

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 ha-mode graceful-restart
```

（可选）关键字 disable 为邻居禁用 BGP 平稳重启功能。

步骤 7 将路由映射应用于传入或传出路由：

neighbor {ipv6-address} route-map map-name {in|out}

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 route-map example1 in
```

关键字 in 将路由映射应用于传入路由。

关键字 out 将路由映射应用于传出路由。

步骤 8 按前缀列表中的指定分发 BGP 邻居信息：

neighbor {ipv6-address} prefix-list prefix-list-name {in|out}

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 prefix-list NewPrefixList in
```

关键字 in 意味着前缀列表应用于从此邻居传入的通告。

关键字 out 意味着前缀列表应用于传出到此邻居的通告。

步骤 9 设置过滤器列表：

neighbor {ipv6-address} filter-list access-list-name {in|out}

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 filter-list 5 in
```

- access-list-name - 指定自治系统路径访问列表的编号。您可以使用 ip as-path access-list 命令定义此访问列表。
- in - 访问列表应用于从此邻居传入的通告。
- out - 访问列表应用于传出到此邻居的通告。

步骤 10 控制可以从邻居接收的前缀的数量：

neighbor {ipv6-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 maximum-prefix 7 75 restart 12
```

- maximum - 从此邻居允许的前缀的最大数量。
- （可选）threshold - 整数，用于指定路由器开始生成警告消息时所达到的最大值的百分比。范围为 1 至 100，默认值为 75（百分比）。
- （可选）restart interval - 整数值（以秒为单位），用于指定 BGP 邻居重新启动前的时间间隔。
- （可选）warning-only - 允许路由器在超过最大前缀数量时生成日志消息，而不是终止对等。

步骤 11 允许 BGP 发言者（本地路由器）将默认路由 0.0.0.0 发送到邻居，以用作该邻居的默认路由：

neighbor {ipv6-address} default-originate [route-map map-name]

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 default-originate route-map example1
```

参数 map-name 是路由映射的名称。路由映射允许有条件地注入路由 0.0.0.0。

步骤 12 设置前后两次发送 BGP 路由更新的最小间隔：

neighbor {ipv6-address} advertisement-interval seconds

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 advertisement-interval 15
```

参数 seconds 是时间（以秒为单位）。有效值范围为 0 至 600。

步骤 13 从出站路由更新中删除专用自治系统号：

neighbor {ipv6-address} remove-private-as

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 remove-private-as
```

步骤 14 通告 BGP 表中与已配置的路由映射相匹配的路由：

neighbor {ipv6-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name - 将在达到存在映射或非存在映射的条件时通告的路由映射的名称。
- exist-map map name - 与 BGP 表中的路由进行比较以确定是否对通告映射路由进行通告的存在映射的名称。
- non-exist-map map name - 与 BGP 表中的路由进行比较以确定是否对通告映射路由进行通告的非存在映射的名称。
- （可选）check all paths - 使具有 BGP 表中的前缀的存在映射可检查所有路径。

步骤 15 为特定 BGP 对等体或对等组设置计时器。

neighbor {ipv6-address} timers keepalive holdtime min holdtime

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 timers 15 20 12
```

- keepalive - ASA 向其对等体发送 keepalive 消息的频率（以秒为单位）。默认值为 60 秒。有效值范围为 0 至 65535。
- holdtime - ASA 在未接收到 keepalive 消息后声明对等体处于失效状态的间隔（以秒为单位）。默认值为 180 秒。
- min holdtime - ASA 在未接收到 keepalive 消息后声明对等体处于失效状态的最小间隔（以秒为单位）。

  注释
  保持时间小于 20 秒会增加对等体振荡的可能性。

步骤 16 在两个 BGP 对等体之间的 TCP 连接上启用消息摘要 5 (MD5) 身份验证：

neighbor {ipv6-address} password string

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 password test
```

参数 string 是区分大小写的密码，启用 service password-encryption 命令时，其长度最大为 25 个字符；未启用 service password-encryption 命令时，其长度最大为 81 个字符。此字符串可以包含任意字母数字字符，包括空格。

注释
当您将密码的第一个字符设置为数字时，请勿在第二位使用空格。即，您不能指定 number-space-anything 格式的密码。数字后的空格会导致身份验证失败。

步骤 17 指定应将社区属性发送到 BGP 邻居：

neighbor {ipv6-address} send-community [standard]

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 send-community
```

（可选）关键字 standard - 仅发送标准社区。

步骤 18 将路由器配置为 BGP 发言邻居或对等组的下一跳：

neighbor {ipv6-address}next-hop-self

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 next-hop-self
```

步骤 19 接受并尝试建立与未直接连接的网络上的外部对等体的 BGP 连接：

neighbor {ipv6-address} ebgp-multihop [ttl]

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 ebgp-multihop 5
```

参数 ttl 指定生存时间，范围为 1 至 255 跳。

步骤 20 禁用连接验证可与使用环回接口的单跳对等体建立 eBGP 对等会话：

neighbor {ipv6-address} disable-connected-check

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 disable-connected-check
```

步骤 21 保护 BGP 对等会话，并且配置用于分隔两个外部 BGP (eBGP) 对等体的最大跳数。

neighbor {ipv6-address} ttl-security hops hop-count

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

参数 hop-count 是用于分隔 eBGP 对等体的跳数。TTL 值由路由器根据已配置的 hop-count 参数计算得出。有效值范围为 1 至 254。

步骤 22 向邻居连接分配权重：

neighbor {ipv6-address} weight number

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 weight 30
```

参数 number 是分配给邻居连接的权重。有效值范围为 0 至 65535。

步骤 23 将 ASA 配置为仅接受特定 BGP 版本：

neighbor {ipv6-address} version number

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 version 4
```

参数 number 指定 BGP 版本号。默认为版本 4。目前仅支持 BGP 版本 4。

步骤 24 为 BGP 会话启用 TCP 传输会话选项：

neighbor {ipv6-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 transport connection-mode active
```

- connection-mode - 连接类型（active 或 passive）。
- path-mtu-discovery - 启用 TCP 传输路径最大传输单位 (MTU) 发现。默认情况下会启用 TCP 路径 MTU 发现。
- （可选）disable - 禁用 TCP 路径 MTU 发现。

步骤 25 为从外部边界网关协议 (eBGP) 邻居接收的路由自定义 AS_PATH 属性：

neighbor {ipv6-address} local-as [autonomous-system-number[no-prepend]]

示例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- （可选）autonomous-system-number - 向 AS_PATH 属性预置的自治系统号。此参数值的范围是从 1 至 4294967295 或 1.0 至 XX.YY 的任意有效自治系统号。
- （可选）no-prepend - 不向从 eBGP 邻居接收的任何路由预置本地自治系统号。

注意

BGP预置路由穿越的每个BGP网络的自治系统号，以维护网络可达性信息和防止路由环路。此命令应配置为仅用于自治系统迁移，并且在完成迁移后应将其删除。此程序应仅由经验丰富的网络操作员尝试执行。配置不当可能会造成路由环路

步骤 26 要将接口更新为 BGP 邻居关系的源，请执行以下操作：

neighbor {ipv6-address} update-source {interface name}

示例：

```
ciscoasa(config-router-af)# neighbor 2000::1 update-source loop1
```

参数 interface name 指定 BGP 邻居用作 BGP 路由源的接口的名称。

注释
如果将环回接口更新为 BGP 邻居关系的源，则会在网络中通告环回接口的 IP 地址。环回接口充当eBGP对等体并参与路由。由于环回接口在启用时稳定，并且在管理性关闭之前保持可用，因此始终可通过环回接口 IP 地址访问 ASA。

配置 IPv6 网络设置

本部分介绍定义要由 BGP 路由进程通告的网络所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp *autonomous-num*

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 6 (IPv6) 地址前缀配置路由会话：

address-family ipv6 [unicast]

步骤 3 指定将由 BGP 路由进程通告的网络：

network {*prefix_delegation_name* [*subnet_prefix*/*prefix_length*] | *ipv6_prefix*/*prefix_length*} [**route-map** *route_map_name*]

示例：

```
ciscoasa(config-router-af)# network 2001:1/64 route-map test_route_map
ciscoasa(config-router-af)# network outside-prefix 1::/64
ciscoasa(config-router-af)# network outside-prefix 2::/64
```

- *prefix_delegation_name* - 如果您启用 DHCPv6 前缀授权客户端 (**ipv6 dhcp client pd**)，则您可通告前缀。要添加子网前缀，指定 *subnet_prefix*/*prefix_length*。

- *ipv6 network*/*prefix_length* - BGP 将通告的网络。
- （可选）**route-map** *name* - 已配置的路由映射的标识符。应检查路由映射，以过滤要通告的网络。如果未指定，则通告所有网络。

配置 IPv6 重新分发设置

本节介绍定义将其他路由域中的路由重新分发到 BGP 所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 6 (IPv6) 地址前缀配置路由会话：

address-family ipv6 [unicast]

示例：

```
ciscoasa(config-router)# address-family ipv6[unicast]
```

步骤 3 将其他路由域中的路由重新分发到 BGP 自主系统：

```
redistribute protocol [process-id][autonomous-num][metric metric value][match{internal|
external1|external2|NSSA external 1|NSSA external 2}][route-map [map-tag]][subnets]
```

示例：

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol - 从中重新分发路由的源协议。它可以是以下协议之一：Connected、EIGRP、OSPF、RIP 或 Static。
- （可选）process-id - 对于 ospf 协议，这是指从中重新分发路由的相应 OSPF 进程 ID。这可以标识路由进程。该值采用非零十进制数字的形式。

  注释
  系统会为其他协议自动填充该值。

- （可选）metric metric value - 当从一个 OSPF 进程重新分发到同一路由器的另一个 OSPF 进程中时，如果未指定度量值，则会将一个进程的度量传输到另一个进程。将其他进程重新分发到 OSPF 进程时，如果未指定指标值，则默认指标为 20。默认值为 0。
- （可选）match internal | external1 | external2 | NSSA external 1 | NSSA external 2 - 指将 OSPF 路由重新分发到其他路由域的条件。它可以是下列类型之一：
  - internal - 特定自主系统的内部路由。
  - external 1 - 自主系统的外部路由，但会被作为 OSPF 类型 1 外部路由导入到 BGP。
  - external 2 - 自主系统的外部路由，但会被作为 OSPF 类型 2 外部路由导入到 BGP。
  - NSSA external 1 - 自主系统的外部路由，但会被作为 OSPF NSSA 类型 1 外部路由导入到 BGP。
  - NSSA external 2 - 自主系统的外部路由，但会被作为 OSPF NSSA 类型 2 外部路由导入到 BGP。
- （可选）map-tag - 已配置路由映射的标识符。

注释
应检查路由映射，以过滤要重新分发的网络。如果未指定，则重新分发所有网络

配置 Ipv6 路由注入设置

本部分介绍定义有条件地注入 BGP 路由表中的路由所需的步骤。

过程

步骤 1 启用 BGP 路由进程，从而使 ASA 进入路由器配置模式：

router bgp autonomous-num

示例：

```
ciscoasa(config)# router bgp 2
```

步骤 2 进入地址系列配置模式，以使用标准 IP 版本 6 (IPv6) 地址前缀配置路由会话：

address-family ipv6 [unicast]

示例：

```
ciscoasa(config-router)# address-family ipv6 [unicast]
```

步骤 3 配置有条件的路由注入，以将更具体的路由注入 BGP 路由表：

bgp inject-map inject-map exist-map exist-map [copy-attributes]

示例：

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map - 用于指定要注入本地 BGP 路由表的前缀的路由映射的名称。
- exist-map - 包含 BGP 发言者将跟踪的前缀的路由映射的名称。
- （可选）copy-attributes - 将已注入的路由配置为继承聚合路由的属性。

监控 BGP

您可以使用以下命令监控BGP路由进程。有关命令输出的示例和说明，请参阅命令参考。此外，您可以禁用邻居变更消息和邻居警告消息的日志记录。

要监控各种 BGP 路由统计信息，请输入以下其中一个命令：

- **show bgp** [ip-address [mask [longer-prefixes [injected] | shorter-prefixes [length]]]| prefix-list name | route-map name]

  显示 BGP 路由表中的条目。

- **show bgp** cidr-only

  显示带有非自然网络掩码的路由（即，无类别域间路由，或 CIDR）。

- **show bgp community community-number [exact-match][no-advertise][no-export]**

  显示属于指定 BGP 社区的路由。

- **show bgp community-list community-list-name [exact-match]**

  显示 BGP 社区列表允许的路由。

- **show bgp filter-list** *access-list-number*

  显示与指定的过滤器列表相符的路由。

- **show bgp injected-paths**

  显示 BGP 路由表中所有注入的路径。

- **show bgp ipv4 unicast**

  显示 IP 版本 4 (IPv4) BGP 路由表中的单播会话条目。

- show bgp ipv6 unicast

  显示 IPv6 边界网关协议 (BGP) 路由表中的条目。

- show bgp ipv6 community

显示属于指定 IPv6 边界网关协议 (BGP) 社区的路由。

- show bgp ipv6 community-list

  显示 IPv6 边界网关协议 (BGP) 社区列表允许的路由。

- show bgp ipv6 filter-list

  显示与指定的 IPv6 过滤器列表相符的路由。

- show bgp ipv6 inconsistent-as

  显示源自治系统不一致的 IPv6 边界网关协议 (BGP) 路由。

- show bgp ipv6 neighbors

  显示到邻居的 IPv6 边界网关协议 (BGP) 连接的相关信息。

- show bgp ipv6 paths

  显示数据库中的所有 IPv6 边界网关协议 (BGP) 路径。

- show bgp ipv6 prefix-list

  显示与前缀列表相匹配的路由。

- show bgp ipv6 quote-regexp

  显示与作为引用字符串的自治系统路径正则表达式相匹配的 IPv6 边界网关协议 (BGP) 路由。

- show bgp ipv6 regexp

  显示与自治系统路径正则表达式相匹配的 IPv6 边界网关协议 (BGP) 路由。

- show bgp ipv6 route-map

  显示无法安置在路由表中的 IPv6 边界网关协议 (BGP) 路由。

- show bgp ipv6 summary

  显示所有 IPv6 边界网关协议 (BGP) 连接的状态。

- show bgp neighbors ip_address

  显示到邻居的 BGP 和 TCP 连接的相关信息

- show bgp paths [LINE]

  显示数据库中的所有 BGP 路径。

- show bgp pending-prefixes

  显示有待删除的前缀。

- show bgp prefix-list prefix_list_name [WORD]

  显示与指定的前缀列表相匹配的路由。

- show bgp regexp regexp

显示与自治系统路径正则表达式相匹配的路由。

- show bgp replication [index-group | ip-address]

  显示 BGP 更新组的更新复制统计信息。

- show bgp rib-failure

  显示无法安置在路由信息库 (RIB) 表中的 BGP 路由。

- show bgp route-map map-name

  根据已指定的路由映射显示 BGP 路由表中的条目。

- show bgp summary

  显示所有 BGP 连接的状态。

- show bgp system-config

  显示多情景模式下的系统情景特定 BGP 配置。

  此命令可用于多情景模式下的所有用户情景。

- show bgp update-group

  显示有关 BGP 更新组的信息。

注释 要禁用 BGP Log 消息，请在路由器配置模式下输入 **no bgp log-neighbor-changes** 命令。这会禁用邻居变更消息的日志记录。请在BGP路由进程的路由器配置模式下输入此命令。默认情况下，系统会记录领导变更。

BGP 示例

此示例显示如何通过各种可选进程启用和配置 BGPv4。

1. 定义要路由从一个路由协议重新分发到另一个路由协议的条件，或者启用策略路由：

```
ciscoasa(config)# route-map mymap2 permit 10
```

2. 重新分发具有路由地址或与已指定的某个访问列表传递的数据包相匹配的任何路由：

```
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

3. 指示用于输出为策略路由传递路由映射匹配子句的数据包的目标位置：

```
ciscoasa(config-route-map)# set ip next-hop peer address
```

4. 从全局配置模式启用 BGP 路由进程：

```
ciscoasa(config)# router bgp 2
```

5. 在地址系列配置模式下为本地边界网关协议 (BGP) 路由进程配置固定路由器 ID：

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. 向 BGP 邻居表添加条目：

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 remote-as 65
```

7. 将路由映射应用于传入或传出路由：

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 route-map mymap2 in
```

8. 将接口更新为 BGP 邻居的源：

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 update-source loop1
```

本例显示如何使用各种可选进程启用和配置 BGPv6。

1. 定义要路由从一个路由协议重新分发到另一个路由协议的条件，或者启用策略路由：

```
ciscoasa(config)# route-map mymap1 permit 10
```

2. 重新分发具有路由地址或与已指定的某个访问列表传递的数据包相匹配的任何路由：

```
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

3. 指示用于输出为策略路由传递路由映射匹配子句的数据包的目标位置：

```
ciscoasa(config-route-map)# set ipv6 next-hop peer address
```

4. 从全局配置模式启用 BGP 路由进程：

```
ciscoasa(config)# router bgp 2
```

5. 在地址系列配置模式下为本地边界网关协议 (BGP) 路由进程配置固定路由器 ID：

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. 进入地址系列配置模式，以使用标准 IP 版本 6 (IPv6) 地址前缀配置路由会话：

```
address-family ipv6 [unicast]
```

7. 向 BGP 邻居表添加条目：

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 remote-as 64600
```

8. 将路由映射应用于传入或传出路由：

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 route-map mymap1 in
```

9. 将接口更新为 BGP 邻居的源：

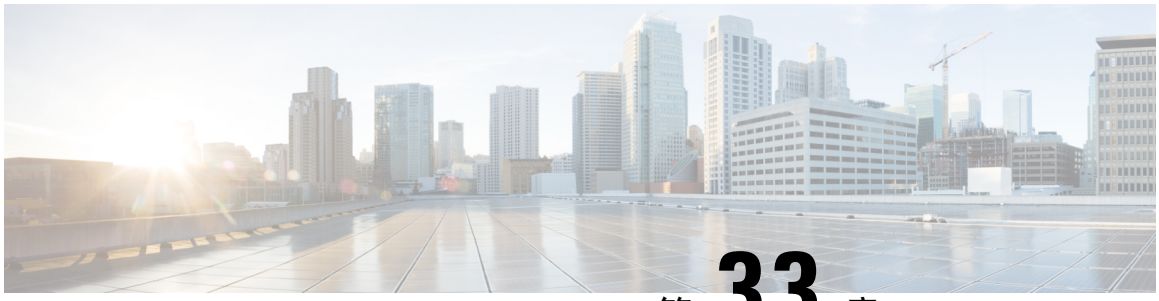
```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 update-source loop1
```

BGP 的历史记录

表 *39: BGP* 的功能历史记录

功能名称	平台版本	功能信息
BGP 支持	9.2(1)	系统添加了以下支持：可以使用边界网关协议路由数据、执行身份验证以及重新分发和监控路由信息。 引入了以下命令：**router bgp**、**bgp maxas-limit**、**bgp log-neighbor-changes**、**bgp transport path-mtu-discovery**、**bgp fast-external-fallover**、**bgp enforce-first-as**、**bgp asnotation dot**、**timers bgp**、**bgp default local-preference**、**bgp always-compare-med**、**bgp bestpath compare-routerid**、**bgp deterministic-med**、**bgp bestpath med missing-as-worst**、**policy-list**、**match as-path**、**match community**、**match metric**、**match tag**、**as-path access-list**、**community-list**、**address-family ipv4**、**bgp router-id**、**distance bgp**、**table-map**、**bgp suppress-inactive**、**bgp redistribute-internal**、**bgp scan-time**、**bgp nexthop**、**aggregate-address**、**neighbor**、**bgp inject-map**、**show bgp**、**show bgp cidr-only**、**show bgp all community**、**show bgp all neighbors**、**show bgp community**、**show bgp community-list**、**show bgp filter-list**、**show bgp injected-paths**、**show bgp ipv4 unicast**、**show bgp neighbors**、**show bgp paths**、**show bgp pending-prefixes**、**show bgp prefix-list**、**show bgp regexp**、**show bgp replication**、**show bgp rib-failure**、**show bgp route-map**、**show bgp summary**、**show bgp system-config**、**show bgp update-group**、**clear route network**、**maximum-path**、**network**。 修改了以下命令：**show route**、**show route summary**、**show running-config router**、**clear config router**、**clear route all**、**timers lsa arrival**、**timers pacing**、**timers throttle**、**redistribute bgp**。
BGP 对 ASA 集群的支持	9.3(1)	我们添加了对 L2 和 L3 集群的支持。 引入了以下命令：bgp router-id clusterpool
不间断转发的 BGP 支持	9.3(1)	我们添加了对不间断转发的支持。 引入了以下命令：bgp graceful-restart、neighbor ha-mode graceful-restart

功能名称	平台版本	功能信息
通告映射的 BGP 支持	9.3(1)	我们添加了对 BGPv4 通告映射的支持。 引入了以下命令：neighbor advertise-map
IPv6 的 BGP 支持	9.3(2)	我们添加了对 IPv6 的支持。 引入了以下命令：address-family ipv6、ipv6 prefix-list、ipv6 prefix-list description、ipv6 prefix-list sequence-number、match ipv6 next-hop、match ipv6 route-source、match ipv6-address prefix-list、set ipv6-address prefix -list、set ipv6 next-hop、set ipv6 next-hop peer-address 修改了以下命令：bgp router-id
授权前缀的 IPv6 网络通告	9.6(2)	ASA 现在支持 DHCPv6 Prefix Delegation 客户端。ASA 获取来自 DHCPv6 服务器的授权前缀。然后，ASA 可以使用这些前缀来配置其他 ASA 接口地址，以便无状态地址自动配置 (SLAAC) 客户端可以自动配置同一网络上的 IPv6 地址。您可以配置 BGP 路由器来通告这些前缀。 修改了以下命令：**network**
环回接口支持 BGP 流量	9.18(2)	现在，您可以添加环回接口并将其用于 BGP 流量。 新增/修改的命令： **interface loopback**、**neighbor update-source**
IPv6 支持平稳重启	9.19(1)	已添加 IPv6 地址系列的平稳重启支持。



第 33 章

OSPF

本章介绍如何将 ASA 配置为使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发路由信息。

- 关于 OSPF，第 1015 页
- OSPF 准则，第 1018 页
- 配置 OSPFv2，第 1020 页
- 配置 OSPFv2 路由器 ID，第 1024 页
- 配置 OSPF 快速呼叫数据包，第 1025 页
- 自定义 OSPFv2，第 1026 页
- 配置 OSPFv3，第 1041 页
- 配置无中断重启，第 1062 页
- OSPFv2 示例，第 1067 页
- OSPFv3 示例，第 1069 页
- 监控 OSPF，第 1070 页
- OSPF 的历史记录，第 1073 页

关于 OSPF

OSPF 是一种使用链路状态而非距离矢量进行路径选择的内部网关路由协议。OSPF 传播链路状态通告而非路由表更新。由于仅交换 LSA 而不是整个路由表，因此 OSPF 网络比 RIP 网络更快收敛。

OSPF 使用链路状态算法构建和计算所有到达已知目标的最短路径。OSPF 区域中的每台路由器包含相同的链路状态数据库，该数据库是由每台路由器可使用的接口和可到达的邻居组成的列表。

相比 RIP，OSPF 具有以下优点：

- OSPF 链路状态数据库更新的发送频率低于 RIP 更新，并且随着过时信息的超时，链路状态数据库即时而非逐步更新。
- 路由决策基于开销，它表明通过特定接口发送数据包所需的开销。ASA 根据链路带宽而非到目标的跃点数计算接口的开销。可以配置开销来指定首选路径。

最短路径优先算法的缺点是需要大量 CPU 周期和内存。

ASA 可以在不同接口集上同时运行 OSPF 协议的两个进程。如果您具有使用相同 IP 地址的接口（NAT 允许这些接口共存，但是 OSPF 不允许重叠地址），则可能要运行两个进程。或者，可能要在内部运行一个进程，在外部运行另一个进程，并且在两个进程之间重新分发路由的子集。同样，可能需要将专用地址与公用地址分离。

您可以将路由从一个 OSPF 路由进程、RIP 路由进程或从在启用了 OSPF 的接口上配置的静态路由和已连接路由重新分发到另一个 OSPF 路由进程中。

ASA 支持以下 OSPF 功能：

- 区域内、区域间和外部（I 类和 II 类）路由。
- 虚拟链路。
- LSA 泛洪。
- OSPF 数据包身份验证（密码和 MD5 身份验证）。
- 将 ASA 配置为指定路由器或指定备用路由器。ASA 也可以设置为 ABR。
- 末节区域和次末节区域。
- 区域边界路由器 3 类 LSA 筛选。

OSPF 支持 MD5 和明文邻居身份验证。如有可能，应将身份验证与所有路由协议配合使用，因为在 OSPF 和其他协议（如 RIP）之间的路由重新分发可能会被攻击者用于破坏路由信息。

如果使用 NAT，如果 OSPF 是在公共和专用区域上运行，并且如果要求地址过滤，则需要运行两个 OSPF 进程，一个进程对应于公共区域，一个进程对应于专用区域。

在多个区域中具有接口的路由器称为区域边界路由器 (ABR)。充当网关以在使用 OSPF 的路由器与使用其他路由协议的路由器之间重新分发流量的路由器称为自治系统边界路由器 (ASBR)。

ABR 使用 LSA 将有关可用路由的信息发送到其他 OSPF 路由器。使用 ABR 3 类 LSA 筛选，您可以具有单独的以 ASA 作为 ABR 的专用和公共区域。3 类 LSA（区域间路由）可以从一个区域筛选到另一个区域，从而允许您在不通告专用网络即的情况下配合使用 NAT 和 OSPF。

注释 只能筛选 3 类 LSA。如果在专用网络中将 ASA 配置为 ASBR，它将发送描述专用网络的 5 类 LSA，后者会泛洪至整个 AS，包括公共区域。

如果采用 NAT 但 OSPF 仅在公共区域中运行，则可以在专用网络内将到公共网络的路由作为默认或 5 类 AS 外部 LSA 重新分发。但是，需要为受 ASA 保护的专用网络配置静态路由。此外，不应在同一 ASA 接口上混用公用和专用网络。

您可以同时在 ASA 上运行两个 OSPF 路由进程、一个 RIP 路由进程和一个 EIGRP 路由进程。

快速呼叫数据包 OSPF 支持

OSPF 快速呼叫数据包支持功能提供了一种以短于一秒的间隔发送呼叫数据包的配置方式。此类配置在开放式最短路径优先 (OSPF) 网络中会导致更快的收敛。

OSPF 支持快速呼叫数据包的前提条件

OSPF 必须已在网络中进行配置或与快速呼叫数据包 OSPF 支持功能同时配置。

关于快速呼叫数据包的 OSPF 支持

与快速呼叫数据包的 OSPF 支持相关的主要概念，以及 OSPF 快速呼叫数据包的优势如下所述：

OSPF 呼叫间隔和停顿间隔

OSPF 呼叫数据包是 OSPF 进程向其 OSPF 邻居发送以保持与这些邻居的连接的数据包。呼叫数据包按照可配置间隔（以秒为单位）进行发送。对于以太网链路，默认值为10秒；对于非广播链路，默认值为30秒。呼叫数据包包含在停顿间隔内为其接收到呼叫数据包的所有邻居的列表。停顿间隔也是可配置间隔（以秒为单位），并且默认为呼叫间隔值的四倍。所有呼叫间隔的值在网络中都必须相同。同样，所有停顿间隔的值在网络中也必须都相同。

这两种间隔通过表明链路可运行来结合用于保持连接。如果路由器在停顿间隔内没有从邻居接收到呼叫数据包，则将声明该邻居关闭。

OSPF 快速呼叫数据包

OSPF 快速呼叫数据包是指按照小于1秒的间隔发送的呼叫数据包。要了解快速呼叫数据包，您应已了解 OSPF 呼叫数据包与停顿间隔之间的关系。请参阅 OSPF 呼叫间隔和停顿间隔，第 1017 页。

通过使用 ospf dead-interval 命令来获取 OSPF 快速呼叫数据包。停顿间隔设置为 1 秒，并且 hello-multiplier 值设置为在该1秒期间要发送的呼叫数据包的数量，从而提供亚秒或“快速”呼叫数据包。

当在接口上配置了快速呼叫数据包时，此接口发出的呼叫数据包中通告的呼叫间隔设置为 0。系统将忽略通过此接口接收到的呼叫数据包中的呼叫间隔。

无论停顿间隔设置为1秒（对于快速呼叫数据包）还是设置为任何其他值，它在分片上都必须一致。只要在停顿间隔内发送了至少一个呼叫数据包，呼叫乘数对于整个分片便无需相同。

OSPF 快速呼叫数据包的优势

OSPF 快速呼叫数据包功能的优势是OSPF 网络将比没有快速呼叫数据包的情况更快收敛。通过此功能，您可以在 1 秒内检测丢失的邻居。它在开放式系统互连 (OSI) 物理层和数据链路层可能未检测到邻居丢失的 LAN 分片中尤其有用。

OSPFv2 与 OSPFv3 之间的实施差异

OSPFv3 不向后兼容 OSPFv2。要使用 OSPF 路由 IPv4 和 IPv6 流量，必须同时运行 OSPFv2 和 OSPFv3。它们会共存但不相互交互。

OSPFv3 提供的其他功能包括：

- 按链路进行协议处理。
- 删除寻址语义。
- 添加泛洪范围。

- 支持每条链路多个实例。
- 使用 IPv6 链路本地地址执行网络发现和其他功能。
- 以前缀和前缀长度表示 LSA。
- 添加两种 LSA 类型。
- 处理未知 LSA 类型。
- 使用 OSPFv3 路由协议流量的 IPsec ESP 标准支持身份验证，如 RFC-4552 所指定。

OSPF 准则

情景模式准则

OSPFv2 支持单情景模式和多情景模式。

- 由于默认情况下不支持跨共享接口的情景间组播流量交换，因此 OSPFv2 实例不能跨共享接口相互建立邻接关系。但是，您可以使用 OSPFv2 进程下 OSPFv2 进程配置中的静态邻居配置，在共享接口上建立 OSPFv2 邻居关系。
- 支持单独的接口上的情景间 OSPFv2。

OSPFv3 仅支持单情景模式。

密钥链身份验证准则

OSPFv2 同时在物理和虚拟模式下支持单一和多模式下的密钥链身份验证。但是，在多模式下，仅可在情景模式下配置密钥链。

- 轮换密钥仅适用于 OSPFv2 协议。不支持密钥链的 OSPF 区域身份验证。
- 但仍支持 OSPFv2 中无时间范围的现有 MD5 身份验证以及新的轮换密钥。
- 尽管平台支持 SHA1 和 MD5 加密算法，但只有 MD5 加密算法会用于身份验证。

防火墙模式准则

OSPF 仅支持路由防火墙模式。OSPF 不支持透明防火墙模式。

故障转移 准则

OSPFv2 和 OSPFv3 支持状态 故障转移。

IPv6 准则

- OSPFv2 不支持 IPv6。
- OSPFv3 支持 IPv6。

- OSPFv3 使用 IPv6 进行身份验证。
- ASA 将 OSPFv3 路由安装到 IPv6 RIB 中，前提是它是最佳路由。
- 可以在 **capture** 命令中使用 IPv6 ACL 滤除 OSPFv3 数据包。

OSPFv3 Hello 数据包和 GRE

通常，OSPF流量不会通过 GRE 隧道。当 IPv6 上的 OSPFv3 封装在 GRE 内时，安全检查（例如组播目标）的IPv6报头验证失败。由于隐式安全检查验证，数据包被丢弃，因为此数据包具有目标IPv6组播。

您可以定义预过滤器规则来绕过GRE流量。但是，使用预过滤器规则，检测引擎不会询问内部数据包。

集群准则

- 不支持 OSPFv3 加密。如果尝试在集群环境中配置 OSPFv3 加密，系统将显示错误消息。
- 在跨接口模式下，仅管理接口上不支持动态路由。
- 在单个接口模式下，确保已作为 OSPFv2 或 OSPFv3 邻居建立控制和数据单元。
- 在单个接口模式下，只能在控制单元共享接口上的两个情景之间建立 OSPFv2 邻接。仅在点对点链路上支持配置静态邻居；因此，在接口上仅允许一个邻居声明。
- 当集群中的控制角色发生变化时，会发生以下行为：
  - 在跨接口模式中，路由器进程仅在控制单元上处于活动状态，在数据单元上处于暂停状态。各集群设备具有同一路由器 ID，因为已从控制单元对配置进行同步。因此，在角色更改过程中，相邻路由器不会注意到集群的路由器 ID 发生的任何更改。
  - 在单个接口模式中，路由器进程在所有单个集群设备上都处于活动状态。各集群设备从已配置的集群池中选择其自己独特的路由器ID。集群中的控制角色更改不会以任何方式更改路由拓扑。

多协议标签交换 (MPLS) 和 OSPF 准则

如果MPLS配置的路由器发送的链路状态(LS)更新数据包包含不透明Type-10链路状态通告(LSA)，而且其中包括 MPLS 报头，则身份验证会失败且设备会自动丢弃更新数据包，而不是确认它们。最终，对等路由器将终止邻居关系，因为它没有收到任何确认。

禁用 ASA 上的不透明功能，以确保邻居关系保持稳定：

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```

注释 Firepower 4100/9300 型号在使用 MPLS 时可能具有高延迟，因为它们缺乏跨多个接收队列的负载均衡。

双向和转发检测 (BFD)及 OSPF 准则

- 您可以在 OSPFv2 和 OSPFv3 接口（物理接口、子接口和端口通道）上启用 BFD。
- VTI 隧道、DVTI 隧道、环回接口、交换机端口、VNI、VTEP 和 IRB 接口不支持 BFD。

路由重分布准则

- 支持在 OSPFv2 上重新分配带有 IPv4 前缀列表的路由映射。但是，不支持在 OSPFv3 上重新分配带有 IPv6 前缀列表的路由映射。 使用 OSPF 上的路由映射中的访问列表进行重新分发。
- 在属于 EIGRP 网络的设备上配置 OSPF 时，请确保将 OSPF 路由器配置为标记路由（EIGRP 尚不支持路由标记）。

  将 OSPF 重新分发到 EIGRP 并将 EIGRP 重新分发到 OSPF 时，如果其中一个链路、接口中断，甚至当路由发起方关闭时，就会发生路由环路。为了防止将路由从一个域重新分发回同一域，路由器可以在重新分发时标记属于某个域的路由，并且可以根据相同的标记在远程路由器上过滤这些路由。由于这些路由不会安装到路由表中，因此它们不会重新分发到同一域中。

其他准则

- OSPFv2 和 OSPFv3 在接口上支持多个实例。
- OSPFv3 在非集群环境中通过 ESP 报头支持加密。
- OSPFv3 支持非负载加密。
- OSPFv2 根据 RFC 4811、4812 和 3623 定义分别支持思科 NSF 平稳重启和 IETF NSF 平稳重启机制。
- OSPFv3 根据 RFC 5187 定义支持平稳重启机制。
- 可分发的区域内（类型 1）路由数具有限制。对于这些路由，单一 1 类 LSA 包含所有前缀。由于系统的数据包大小限制为 35 KB，所以 3000 个路由会导致数据包超出该限制。考虑设置 2900 个 1 类路由作为支持的最大数量。
- 要避免在路由更新大于链路上的最小 MTU 时丢弃由于路由更新而导致的邻接摆动，请确保在链路两端的接口上配置相同的 MTU。
- 由于 Azure 云路由的性质，ASA Virtual 无法使用 EIGRP、OSPF 等动态内部路由协议。无论虚拟客户端是否配置了任何静态/动态路由，有效路由表都会确定下一跳。

  目前，您无法查看有效路由表或系统路由表。
- 如果数据包大小超过 8190，OSPFv3 会放弃 LS 更新。因此，邻接关系将终止。因此，使用“ospfv3 mtu-ignore”命令来配置交换机，以避免邻接关系终止。

配置 OSPFv2

此部分介绍如何在 ASA 上启用 OSPFv2 进程。

启用 OSPFv2 后，您需要定义路由映射。有关详细信息，请参阅定义路由映射，第 959 页。然后，生成默认路由。有关详细信息，请参阅配置静态路由，第 931 页。

为 OSPFv2 进程定义路由映射后，您可以根据特定需要对其进行自定义。要了解任何在 ASA 上自定义 OSPFv2 进程，请参阅自定义 OSPFv2，第 1026 页.

要启用 OSPFv2，您需要创建 OSPFv2 路由进程，指定与该路由进程关联的 IP 地址的范围，然后指定与 IP 地址范围关联的区域 ID。

您最多可以启用两个 OSPFv2 进程实例。每个 OSPFv2 进程具有其自己的关联区域和网络。

要启用 OSPFv2，请执行以下步骤：

过程

步骤 1 创建 OSPF 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。您最多可以使用两个进程。

如果仅在 ASA 上启用了一个 OSPF 进程，则默认情况下会选择该进程。编辑现有区域时，无法更改 OSPF 进程 ID。

步骤 2 定义 OSPF 运行所在的 IP 地址和该接口的区域 ID：

network *ip_address mask* **area** *area_id*

示例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

添加新区域时，输入区域 ID。您可以将区域 ID 指定为十进制数字或 IP 地址。有效十进制值范围为 0 到 4294967295。编辑现有区域时，无法更改区域 ID。

步骤 3 要在所有 OSPFv2 接口上启用 BFD，请执行以下操作：

bfd all-interfaces

示例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# bfd all-interfaces
```

步骤 4 要在支持 OSPFv2 的特定接口上启用 BFD，请执行以下操作：

bfd interface *interface*

示例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# bfd interface inside
```

配置身份验证所用的密钥链

为了增强设备的数据安全和防护，你可以启用 IGP 对等体进行身份验证的轮换密钥。轮换密钥可阻止任何恶意用户猜测用于路由协议身份验证的密钥，从而保护网络，避免通告错误的路由和重定向流量。频繁更改密钥可降低密钥最终被猜到的风险。在配置提供密钥链的路由协议的身份验证时，请为密钥链中的密钥配置重叠的生存期。这有助于防止由于缺少活动密钥而丢失受密钥保护的通信。如果密钥生存期到期且未找到活动密钥，则 OSPF 会使用最后一个有效密钥来维持对等体之间的邻接关系。

本节介绍如何为 OSPF 对等体身份验证创建密钥链。配置密钥链对象后，您可以将其用于定义接口和虚拟链路的 OSPFv2 身份验证。为对等体使用相同的身份验证类型（MD5 或密钥链）和密钥 ID，以建立成功的邻接关系。要了解如何为接口定义身份验证，请参阅配置 OSPFv2 接口参数，第 1030 页。

要配置密钥链，请执行以下步骤：

过程

步骤 1 使用名称配置密钥链：

key chain*key-chain-name*

示例：

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)#
```

您现在可以继续定义密钥链的关联参数。

步骤 2 配置密钥链的标识符：

key*key-id*

密钥 ID 值可介于 0 到 255 之间。仅在表明无效密钥时使用值 0。

示例：

```
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)#
```

步骤 3 配置密钥链的密钥或密码：

key-string [**0** | **8**] *key-string-text*

- 如示例所示，使用 **0** 表示未加密的密码。
- 使用 **8** 表示要遵循的加密密码。
- 密码的最大长度可为 80 个字符。
- 密码不能为单个数字或以数字加空格开头。例如，“0 pass”或“1”为无效密码。

示例：

```
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)#
```

步骤 4 配置密钥链的加密算法：

cryptographic-algorithm*md5*

您需要提供加密身份验证算法。虽然平台支持 SHA1 和 MD5，但只有 MD5 支持密钥链管理。

示例：

```
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)#
```

步骤 5 （可选）配置密钥链的生命周期设置：

accept-lifetime [**local** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

send-lifetime [**ocal** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

您可以指定设备在与其他设备交换密钥期间接受/发送密钥的时间间隔。结束时间可为持续时间或绝对时间，即接受/发送生命周期结束时的绝对时间，也可以是永不到期。

以下为开始值和结束值的验证规则：

- 在指定了结束生存期时，开始生存期不可为空值。
- 接受或发送生存期的开始生存期必须早于结束生存期。

示例：

```
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite
ciscoasa(config-keychain-key)#
```

您可以使用 **show key chain** 命令查看设备上的启动密钥链配置；**show run key chain** 命令用于查看当前在设备上运行的密钥链配置。

```
ciscoasa# show key chain
Key-chain CHAIN2:
    key 1 -- text "KEY1CHAIN2"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
  * key 2 -- text "(unset)"
        accept lifetime (11:00:12 UTC Sep 1 2018) - (11:12:12 UTC Sep 1 2018)
```

```
        send lifetime (always valid) - (always valid) [valid now]
Key-chain CHAIN1:
    key 1 -- text "CHAIN1KEY1STRING"
        accept lifetime (11:22:33 UTC Sep 1 2018) - (-1 seconds)
        send lifetime (always valid) - (always valid) [valid now]
ciscoasa#


ciscoasa# sh run key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa# sh run key chain CHAIN1
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

下一步做什么

现在，您可以应用配置的密钥链来定义接口的 OSPFv2 身份验证。

- 配置 OSPFv2 接口参数 ，第 1030 页

配置 OSPFv2 路由器 ID

OSPF Router-ID 用于标识 OSPF 数据库中的特定设备。在 OSPF 系统中，任何两个路由器都不能具有相同的 router-id。

如果未在 OSPF 路由进程中手动配置 router-id，路由器将自动配置从主用接口中的最高 IP 地址确定的 router-id。在配置 router-id 时，将不会自动更新邻居，直至路由器出现故障或 OSPF 进程已被清除并且已重新建立邻居关系。

手动配置 OSPF 路由器 ID

本节介绍如何在 ASA 上手动配置 OSPFv2 进程中的 router-id。

过程

步骤 1 要使用固定路由器 ID，请使用 **router-id** 命令。

router-id *ip-address*

示例：

```
ciscoasa(config-router)# router-id 193.168.3.3
```

步骤 2 要恢复到以前的 OSPF 路由器 ID 行为，请使用 **no router-id** 命令。

no router-id *ip-address*

示例：

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

迁移时的路由器 ID 行为

在从一个 ASA（譬如 ASA 1）向另一个 ASA（譬如 ASA 2）迁移开放式最短路径优先配置（OSPF 配置）时，可以观察到以下路由器 id 选择行为：

1. 当所有接口都处于关闭模式时，ASA 2 不将任何 IP 地址用于 OSPF router-id。当所有接口都处于“管理关闭”状态或关闭模式时，配置 router-id 可能出现的情况如下：
   - 如果 ASA 2 之前没有配置任何 router-id，您将看到以下消息：

     ```
     %OSPF：路由器进程 1 未在运行，请配置一个 router-id
     ```

     在第一个接口启用后，ASA 2 会将此接口的 IP 地址作为路由器 id。
   - 如果 ASA 2 之前已配置 router-id，并且所有接口在发出“no router-id”命令时都处于“管理关闭”状态，那么 ASA 2 将使用旧的路由器 id。即使启用的接口上的 IP 地址发生了更改，ASA 2 仍会使用旧的路由器 id，直至发出“clear ospf process”命令为止。
2. 如果 ASA 2 之前已配置 router-id，并且在发出“no router-id”命令时至少有一个接口未处于“管理关闭”状态或关闭模式，则 ASA 2 将使用新的路由器 id。即使接口处于“关闭/关闭”状态，ASA 2 也会使用这些接口的 IP 地址作为新的路由器 id。

配置 OSPF 快速呼叫数据包

本节介绍如何配置 OSPF 快速呼叫数据包。

过程

步骤 1 配置接口：

interface *port-channel number*

示例：

```
ciscoasa(config)# interface port-channel 10
```

number 参数表示端口通道接口号。

步骤 2 设置在其期间必须接收至少一个呼叫数据包，否则会将邻居视为关闭的间隔：

ospf dead-interval minimal hello-multiplier *no.of times*

示例：

```
ciscoasa(config-if)# ospf dead-interval minimal hell0-multiplier 5
ciscoasa
```

no. of times 参数表示每秒要发送的呼叫数据包的数量。有效值介于 3 和 20 之间。

在本示例中，通过指定 minimal 关键字以及 hello-multiplier 关键字和值启用了 OSPF 支持快速呼叫数据包功能。由于乘数设置为 5，因此每秒将发送五个呼叫数据包。

自定义 OSPFv2

本节介绍如何自定义 OSPFv2 进程。

将路由重新分发到 OSPFv2 中

ASA 可以控制路由在 OSPFv2 路由进程之间的重新分发。

注释 如果要通过定义允许将来自指定路由协议的哪些路由重新分发到目标路由进程中来重新分发路由，必须先生成默认路由。请参阅配置静态路由，第 931 页，然后根据定义路由映射，第 959 页定义路由映射。

要将静态路由、已连接路由、RIP 路由或 OSPFv2 路由重新分发到 OSPFv2 进程中，请执行以下步骤：

过程

步骤 1 创建 OSPF 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 将已连接路由重新分发到 OSPF 路由进程中：

redistribute connected [[**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

示例：

```
ciscoasa(config)# redistribute connected 5 type-1 route-map-practice
```

步骤 3 将静态路由重新分发到 OSPF 路由进程中：

redistribute static [**subnets**] [**route-map** *map_name*]

示例：

```
ciscoasa(config)# redistribute static subnets
```

此命令会将所有静态路由传递到OSPF。要重新分配选择性静态路由，请确保使用静态路由创建访问列表，然后将其包含在路由映射表中：

示例：

```
ciscoasa(config)# ip access-list extended R1_Loopback
ciscoasa(config-ext-nacl)#permit ip host 1.1.1.1 any
ciscoasa(config-ext-nacl)#exit

ciscoasa(config)#route-map Permit_to_Distribute
ciscoasa(config-route-map)#match ip address R1_Loopback
ciscoasa(config-route-map)#exit
```

在创建路由映射后，将其包含在 redistribute 命令中，如下所示：

示例：

```
ciscoasa(config)#router ospf 2
ciscoasa(config-router)#redistribute static subnets route-map Permit_to_Distribute
```

步骤 4 将路由从一个 OSPF 路由进程重新分发到另一个 OSPF 路由进程中：

redistribute ospf pid [**match {internal** | **external** [**1** | **2]** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

示例：

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

您可以在此命令中使用 **match** 选项来匹配和设置路由属性，也可以使用路由映射。**subnets** 选项在 **route-map** 命令中没有等效项。如果在 **redistribute** 命令中同时使用路由映射和 **match** 选项，则其必须匹配。

示例通过将路由与等于 1 的指标相匹配来显示从 OSPF 进程 1 到 OSPF 进程 2 中的路由重新分发。ASA 将这些路由作为外部接口重新进行分发，其中指标为 5，指标类型为类型 1。

步骤 5 将路由从一个 RIP 路由进程重新分发到另一个 OSPF 路由进程中：

redistribute rip [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

示例：

```
ciscoasa(config)# redistribute rip 5
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

步骤 6 将路由从一个 EIGRP 路由进程重新分发到另一个 OSPF 路由进程中：

redistribute eigrp as-num [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

示例：

```
ciscoasa(config)# redistribute eigrp 2
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

配置将路由重新分发到 OSPFv2 时的路由汇总

将来自其他协议的路由重新分发到 OSPF 中时，将在外部 LSA 中单独通告每个路由。不过，可以将 ASA 配置为对于指定网络地址和掩码包含的所有重新分发路由通告单一路由。此配置可减小 OSPF 链路状态数据库的大小。

可以抑制与指定 IP 地址/掩码对相匹配的路由。标签值可用作用于通过路由映射控制重新分发的值。

添加路由汇总地址

要在一个汇总路由上配置适用于为网络地址和掩码包含的所有重新分发的路由的软件通告，请执行以下步骤：

过程

步骤 1 创建 OSPF 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 设置汇总地址：

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

示例：

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

在本示例中，汇总地址 10.1.0.0 包含地址 10.1.1.0、10.1.2.0、10.1.3.0，依此类推。在外部链路状态通告中仅通告地址 10.1.0.0。

配置 OSPFv2 区域之间的路由汇总

路由汇总是通告地址的整合。此功能导致通过区域边界路由器向其他区域通告单个汇总路由。在 OSPF 中，区域边界路由器将一个区域中的网络通告到另一个区域中。如果以某种方式分配区域中的网络号来使其连续，则可以将区域边界配置为通告汇总路由，包括该区域内属于指定范围的所有单独网络。

要定义汇总路由的地址范围，请执行以下步骤：

过程

步骤 1 创建 OSPF 路由进程并进入此 OSPF 进程的路由器配置模式：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符。它可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 设置地址范围：

area *area-id* range *ip-address mask* [**advertise** | **not-advertise**]

示例：

```
ciscoasa(config-rtr)# area 17 range 12.1.0.0 255.255.0.0
```

在本示例中，地址范围设置在 OSPF 区域之间。

配置 OSPFv2 接口参数

如有必要，您可以更改某些特定于接口的 OSPFv2 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：**ospf hello-interval**、**ospf dead-interval** 和 **ospf authentication-key**。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

要配置 OSPFv2 接口参数，请执行以下步骤：

过程

步骤 1 创建 OSPF 路由进程：

router ospf*process-id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是内部针对此路由进程使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 定义 OSPF 运行所在的 IP 地址和该接口的区域 ID：

network*ip-address mask***area***area-id*

示例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

步骤 3 进入接口配置模式：

interface*interface-name*

示例：

```
ciscoasa(config)# interface my_interface
```

步骤 4 要在此接口上启用 bfd，请执行以下操作：

ospf bfd

示例：

```
ciscoasa(config-interface)# ospf bfd
```

步骤 5 指定接口的身份验证类型：

ospf authentication [**key-chain** *key-chain-name* | **message-digest** | **null**]

提供配置的密钥链名称。有关配置密钥链的信息，请参阅 配置身份验证所用的密钥链，第 1022 页

示例：

```
ciscoasa(config-interface)# ospf authentication message-digest
```

步骤 6 分配要供相邻 OSPF 路由器在使用 OSPF 简单密码身份验证的网段上使用的密码：

ospf authentication-key密钥

示例：

```
ciscoasa(config-interface)# ospf authentication-key cisco
```

key 参数可以是长度最多为 8 字节的任何连续字符串。

当 ASA 软件发出路由协议数据包时，此命令创建的密码用作直接插入到 OSPF 标头中的密钥。可以为每个接口的每个网络指定单独的密码。同一网络上的所有相邻路由器都必须具有同一密码才能交换 OSPF 信息。

步骤 7 明确指定在 OSPF 接口上发送数据包的开销：

ospf cost成本

示例：

```
ciscoasa(config-interface)# ospf cost 20
```

cost 是从 1 至 65535 的整数。

在本示例中，cost 设置为 20。

步骤 8 设置设备在因未接收到呼叫数据包而声明邻居 OSPF 路由器关闭之前必须等待的秒数：

ospf dead-interval秒

示例：

```
ciscoasa(config-interface)# ospf dead-interval 40
```

该值必须对于网络上的所有节点都相同。

步骤 9 指定 ASA 在 OSPF 接口上发送呼叫数据包间隔的时间长度：

ospf hello-interval秒

示例：

```
ciscoasa(config-interface)# ospf hello-interval 10
```

该值必须对于网络上的所有节点都相同。

步骤 10 启用 OSPF MD5 身份验证：

ospf message-digest-key*key-id***md5***key*

示例：

```
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
```

可以设置以下参数值：

key_id - 范围在 1 至 255 内的标识符。

key - 最多为 16 字节的字母数字密码。

通常，每个接口使用一个密钥在发送数据包时生成身份验证信息并对传入数据包进行身份验证。邻居路由器上的同一密钥标识符必须具有相同密钥值。

建议不要每个接口保留多个密钥。每次添加新密钥时，应删除旧密钥以防止本地系统继续与知道旧密钥的恶意系统进行通信。删除旧密钥还会减少滚动更新期间的开销。

步骤 11 设置优先级以帮助确定网络的 OSPF 指定的路由器：

ospf priority *number-value*

示例：

```
ciscoasa(config-interface)# ospf priority 20
```

number_value 参数范围为 0 至 255。

在多情景模式下，对于共享接口，请指定 0 以确保设备不会成为指定路由器。OSPFv2 实例无法跨共享接口相互建立邻接关系。

步骤 12 指定属于 OSPF 接口的邻接的 LSA 重新传输间隔秒数：

ospf retransmit-interval*number-value*

示例：

```
ciscoasa(config-interface)# ospf retransmit-interval seconds
```

seconds 的值必须大于连接的网络上任意两个路由器之间的预期往返延迟。范围是从 1 到 8192 秒。默认值为 5 秒。

步骤 13 设置在 OSPF 接口上发送链路状态更新数据包所需的估计秒数。

ospf transmit-delay*秒*

示例：

```
ciscoasa(config-interface)# ospf transmit-delay 5
```

seconds 值的范围为 1 至 8192 秒。默认值为 1 秒。

步骤 14 设置在 1 秒内发送的呼叫数据包的数量。

ospf dead-interval minimal hello-interval multiplier*整数*

示例：

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 6
```

有效值是介于 3 和 20 之间的整数。

步骤 15 将接口指定为点对点非广播网络：

ospf network point-to-point non-broadcast

示例：

```
ciscoasa(config-interface)# ospf network point-to-point non-broadcast
```

将接口指定为点对点和非广播时，您必须手动定义OSPF 邻居；无法实现动态邻居发现。有关详情，请参见定义静态 OSPFv2 邻居 ， 第 1037 页。此外，您只能在该接口上定义一个 OSPF 邻居。

配置 OSPFv2 区域参数

您可以配置多个 OSPF 区域参数。这些区域参数（显示在以下任务列表中）包括设置身份验证、定义末节区域以及向默认汇总路由分配特定开销。身份验证提供基于密码的区域非授权访问防御。

末节区域是有关外部路由的信息未发送到的区域。相反，ABR 生成了到自治系统外部目标的末节区域中的默认外部路由。要利用 OSPF 末节区域支持，必须在末节区域中使用默认路由。要进一步减少发送到末节区域中的 LSA 数量，您可以在 ABR 上使用 **area stub** 命令的 **no-summary** 关键字，以防止其将汇总链路通告（3 类 LSA）发送到该末节区域中。

过程

步骤 1 创建 OSPF 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 为 OSPF 区域启用身份验证：

area *area-id* authentication

示例：

```
ciscoasa(config-rtr)# area 0 authentication
```

步骤 3 为 OSPF 区域启用 MD5 身份验证：

area *area-id* authentication message-digest

示例：

```
ciscoasa(config-rtr)# area 0 authentication message-digest
```

配置 OSPFv2 过滤器规则

使用以下程序可过滤 OSPF 更新中接收或传输的路由或网络。

过程

步骤 1 启用 OSPF 路由进程并进入路由器配置模式：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

步骤 2 过滤传入 OSPF 更新中收到或传出 OSPF 更新中通告的路由或网络：

distribute-list *acl-number* **in** [**interface** *ifname*]

distribute-list *acl-number* **out** [*protocol process-number* | **connected** | **static**]

参数 *acl-number* 指定 IP 访问列表号。此访问列表定义要在路由更新中接收的网络和要抑制的网络。

要将过滤器应用于传入更新，请指定 **in**。您可以选择性地指定某个接口来限制用于该接口上收到的更新的过滤器。

To apply the filter to outbound updates, specify **out**。您可以通过进程号（不包括 RIP）选择性地指定一个协议（**bgp**、**eigrp**、**ospf** 或 **rip**）以应用到分发列表。您还可以根据对等体和网络是通过 **connected** 还是 **static** 路由获知的进行过滤。

示例：

```
ciscoasa(config-rtr)# distribute-list ExampleAcl in interface inside
```

配置 OSPFv2 NSSA

NSSA 的 OSPFv2 实施类似于 OSPFv2 末节区域。NSSA 不会将 5 类外部 LSA 从核心泛洪至该区域中，但是可在区域内以有限的方法导入自治系统外部路由。

NSSA 通过重新分发在 NSSA 区域内导入 7 类自治系统外部路由。这些 7 类 LSA 由 NSSA ABR 转换为在整个路由域中泛洪的 5 类 LSA。在转换过程中支持汇总和筛选。

如果您是必须将使用 OSPFv2 的中心站点连接到对 NSSA 使用其他路由协议的远程站点的 ISP 或网络管理员，则可以简化管理。

在 NSSA 实施前，企业站点边界路由器和远程路由器之间的连接不能作为 OSPFv2 末节区域运行，因为远程站点的路由无法重新分发到末节区域中，并且需要保持两种路由协议。通常会运行简单协议（例如 RIP）并使用其处理重新分发。在使用 NSSA 的情况下，您可以通过将企业路由器和远程路由器之间的区域定义为 NSSA 来将 OSPFv2 扩展至覆盖远程连接。

使用此功能之前，请遵循以下准则：

- 您可以设置用于到达外部目标的 7 类默认路由。配置时，路由器会生成到 NSSA 或 NSSA 区域边界路由器中的 7 类默认路由。
- 同一区域内的每个路由器都必须同意区域为 NSSA；否则，路由器无法相互通信。

过程

步骤 1 创建 OSPF 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符。它可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 定义 NSSA 区域：

area *area-id* nssa [**no-redistribution**] [**default-information-originate**]

示例：

```
ciscoasa(config-rtr)# area 0 nssa
```

步骤 3 设置汇总地址并帮助减小路由表的大小：

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

示例：

```
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

对 OSPF 使用此命令会导致 OSPF ASBR 将一个外部路由通告为该地址覆盖的所有重新分发的路由的聚合。

在本示例中，汇总地址 10.1.0.0 包含地址 10.1.1.0、10.1.2.0、10.1.3.0，依此类推。在外部链路状态通告中仅通告地址 10.1.0.0。

注释
OSPF 不支持汇总地址 0.0.0.0 0.0.0.0。

为集群配置 IP 地址池（OSPFv2 和 OSPFv3）

如果使用的是单个接口集群，则可以为路由器 ID 集群池分配 IPv4 地址范围。

要为 OSPFv2 和 OSPFv3 的单个接口集群中的路由器 ID 集群池分配 IPv4 地址范围，请输入以下命令：

过程

指定单个接口集群的路由器 ID 集群池：

router-id cluster-pool hostname | A.B.C.D ip_pool

示例：

```
hostname(config)# ip local pool rpool 1.1.1.1-1.1.1.4
hostname(config)# router ospf 1
hostname(config-rtr)# router-id cluster-pool rpool
hostname(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
hostname(config-rtr)# log-adj-changes
```

在配置了单个接口集群时，**cluster-pool** 关键字会启用 IP 地址池的配置。**hostname | A.B.C.D.** 关键字指定此 OSPF 进程的 OSPF 路由器 ID。*ip_pool* 参数指定 IP 地址池的名称。

注释

如果使用的是集群，则无需指定路由器 ID 的 IP 地址池。如果不配置 IP 地址池，则 ASA 使用自动生成的路由器 ID。

定义静态 OSPFv2 邻居

您需要定义静态 OSPFv2 邻居来通过点对点非广播网络通告 OSPFv2 路由。通过此功能，您可以跨现有 VPN 连接广播 OSPFv2 通告，而不必将通告封装在 GRE 隧道中。

开始之前，必须创建到 OSPFv2 邻居的静态路由。有关创建静态路由的详细信息，请参阅配置静态路由，第 931 页。

过程

步骤 1 创建 OSPFv2 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 定义 OSPFv2 邻近区域：

neighbor *addr* [**interface** if_name]

示例：

```
ciscoasa(config-rtr)# neighbor 255.255.0.0 [interface my_interface]
```

addr 参数是 OSPFv2 邻居的 IP 地址。*if_name* 参数是用于与邻居进行通信的接口。如果 OSPFv2 邻居与任何直接连接的接口不在同一网络上，则必须指定接口。

配置路由计算计时器

您可以配置 OSPFv2 接收拓扑更改时与其启动 SPF 计算时之间的延迟时间。您还可以配置两次连续 SPF 计算之间的保持时间。

过程

步骤 1 创建 OSPFv2 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 配置路由计算时间：

timers throttle spf *spf-start spf-hold spf-maximum*

示例：

```
ciscoasa(config-router)# timers throttle spf 500 500 600
```

spf-start 参数是 OSPF 接收拓扑更改时和其启动 SPF 计算时之间的延迟时间（以毫秒为单位）。它可以是介于 0 和 600000 之间的整数。

spf-hold 参数是两次连续 SPF 计算间隔的最短时间（以毫秒为单位）。它可以是介于 0 和 600000 之间的整数。

spf-maximum 参数是两次连续 SPF 计算间隔的最长时间（以毫秒为单位）。它可以是 0 到 600000 之间的整数。

记录邻居启动或关闭

默认情况下，在 OSPFv2 邻居启动或关闭时会生成系统日志消息。

如果要在不开启 **debug ospf adjacency** 命令的情况下了解 OSPFv2 邻居是启动还是关闭，请配置 **log-adj-changes** 命令。**log-adj-changes** 命令使用更少的输出提供对等关系的高级视图。如果要查看各状态更改的消息，请配置 **log-adj-changes detail** 命令。

过程

步骤 1 创建 OSPFv2 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是此路由进程的内部使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 为启动或关闭的邻居配置日志记录：

log-adj-changes [**detail**]

配置身份验证所用的密钥链

为了增强设备的数据安全和防护，你可以启用 IGP 对等体进行身份验证的轮换密钥。轮换密钥可阻止任何恶意用户猜测用于路由协议身份验证的密钥，从而保护网络，避免通告错误的路由和重定向流量。频繁更改密钥可降低密钥最终被猜到的风险。在配置提供密钥链的路由协议的身份验证时，请为密钥链中的密钥配置重叠的生存期。这有助于防止由于缺少活动密钥而丢失受密钥保护的通信。如果密钥生存期到期且未找到活动密钥，则 OSPF 会使用最后一个有效密钥来维持对等体之间的邻接关系。

本节介绍如何为 OSPF 对等体身份验证创建密钥链。配置密钥链对象后，您可以将其用于定义接口和虚拟链路的 OSPFv2 身份验证。为对等体使用相同的身份验证类型（MD5 或密钥链）和密钥 ID，以建立成功的邻接关系。要了解如何为接口定义身份验证，请参阅 配置 OSPFv2 接口参数，第 1030 页。

要配置密钥链，请执行以下步骤：

过程

步骤 1 使用名称配置密钥链：

key chain*key-chain-name*

示例：

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)#
```

您现在可以继续定义密钥链的关联参数。

步骤 2 配置密钥链的标识符：

key*key-id*

密钥 ID 值可介于 0 到 255 之间。仅在表明无效密钥时使用值 0。

示例：

```
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)#
```

步骤 3 配置密钥链的密钥或密码：

key-string [**0** | **8**] *key-string-text*

- 如示例所示，使用 **0** 表示未加密的密码。
- 使用 **8** 表示要遵循的加密密码。
- 密码的最大长度可为 80 个字符。
- 密码不能为单个数字或以数字加空格开头。例如，“0 pass”或“1”为无效密码。

示例：

```
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)#
```

步骤 4 配置密钥链的加密算法：

cryptographic-algorithm*md5*

您需要提供加密身份验证算法。虽然平台支持 SHA1 和 MD5，但只有 MD5 支持密钥链管理。

示例：

```
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)#
```

步骤 5 （可选）配置密钥链的生命周期设置：

accept-lifetime [**local** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

send-lifetime [**ocal** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

您可以指定设备在与其他设备交换密钥期间接受/发送密钥的时间间隔。结束时间可为持续时间或绝对时间，即接受/发送生命周期结束时的绝对时间，也可以是永不到期。

以下为开始值和结束值的验证规则：

- 在指定了结束生存期时，开始生存期不可为空值。
- 接受或发送生存期的开始生存期必须早于结束生存期。

示例：

```
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite
ciscoasa(config-keychain-key)#
```

您可以使用 **show key chain** 命令查看设备上的启动密钥链配置；**show run key chain** 命令用于查看当前在设备上运行的密钥链配置。

```
ciscoasa# show key chain
Key-chain CHAIN2:
    key 1 -- text "KEY1CHAIN2"
```

```
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
  * key 2 -- text "(unset)"
        accept lifetime (11:00:12 UTC Sep 1 2018) - (11:12:12 UTC Sep 1 2018)
        send lifetime (always valid) - (always valid) [valid now]
Key-chain CHAIN1:
    key 1 -- text "CHAIN1KEY1STRING"
        accept lifetime (11:22:33 UTC Sep 1 2018) - (-1 seconds)
        send lifetime (always valid) - (always valid) [valid now]
ciscoasa#


ciscoasa# sh run key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa# sh run key chain CHAIN1
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

下一步做什么

现在，您可以应用配置的密钥链来定义接口的 OSPFv2 身份验证。

- 配置 OSPFv2 接口参数，第 1030 页

配置 OSPFv3

本节介绍配置 OSPFv3 路由进程所涉及的任务。

启用 OSPFv3

要启用 OSPFv3，您需要创建 OSPFv3 路由进程，创建 OSPFv3 的区域，启用 OSPFv3 的接口，然后将路由重新分发到目标 OSPFv3 路由进程中。

过程

步骤 1 创建 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config)# ipv6 router ospf 10
```

process_id 参数是此路由进程的内部使用的标签，可以是任何正整数。此标签不必与任何其他设备上的标签匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 启用接口：

interface *interface_name*

示例：

```
ciscoasa(config)# interface Gigabitethernet0/0
```

步骤 3 创建具有指定进程 ID 的 OSPFv3 路由进程和具有指定区域 ID 的 OSPFv3 区域。

ipv6 ospf *process-id* **area** *area_id*

示例：

```
ciscoasa(config)# ipv6 ospf 200 area 100
```

配置 OSPFv3 接口参数

如有必要，您可以更改某些特定于接口的 OSPFv3 参数。无需更改其中任何参数，但是以下接口参数在连接的网络中的所有路由器之间必须一致：hello-interval 和 dead-interval。如果配置其中任何参数，请确保网络上所有路由器的配置都具有兼容值。

过程

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 10
```

process_id 参数是此路由进程的内部使用的标签，可以是任何正整数。此标签不必与任何其他设备上的标签匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 要在此接口上启用 bfd，请执行以下操作：

ipv6 ospf bfd

示例：

```
ciscoasa(config-if)# ipv6 ospf bfd
```

步骤 3 创建 OSPFv3 区域：

ipv6 ospf **area** [*area-num*] [**instance**]

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

area-num 参数是要为其启用身份验证的区域，可以是十进制值或 IP 地址。**instance** 关键字指定要分配给接口的区域实例 ID。接口只能有一个 OSPFv3 区域。您可以在多个接口上使用同一区域，并且每个接口可以使用不同的区域实例 ID。

步骤 4 指定在 OSPF 接口上发送数据包的开销：

ipv6 ospf cost *interface-cost*

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

interface-cost 参数指定表示为链路状态指标的无符号整数值，其值的范围可以为 1 至 65535。默认开销基于带宽。

步骤 5 筛选到 OSPFv3 接口的传出 LSA：

ipv6 ospf database-filter all out

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
```

```
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf database-filter all out
```

默认情况下，所有传出 LSA 都泛洪至该接口。

步骤 6 设置在邻居表明路由器关闭之前不得查看呼叫数据包的时间段（以秒为单位）：

ipv6 ospf dead-interval *seconds*

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf dead-interval 60
```

该值必须对于同一网络上的所有节点都相同，并且范围可以是 1 至 65535。默认值是 **ipv6 ospf hello-interval** 命令设置的间隔的四倍。

步骤 7 指定接口的加密类型：

ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [[*key-encryption-type*] *key* | **null**}

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D
```

ipsec 关键字指定 IP 安全协议。**spi** *spi* 关键字参数对指定安全策略索引，它必须在范围 256 至 42949667295 内并以十进制形式输入。

esp 关键字指定封装安全负载。*encryption-algorithm* 算法参数指定要与 ESP 配合使用的加密算法。有效值包括：

- aes-cdc - 启用 AES-CDC 加密。
- 3des - 启用 3DES 加密。
- des - 启用 DES 加密。
- null - 指定不带加密的 ESP。

key-encryption-type 参数可以是以下两个值之一：

- 0 - 密钥未加密。
- 7 - 密钥已加密。

key 参数指定消息摘要计算中使用的数字。该数字长度为 32 个十六进制数字（16 字节）。密钥的大小取决于使用的加密算法。通过某些协议（例如 AES-CDC）可以选择密钥的大小。
authentication-algorithm 参数指定要使用的加密身份验证算法，可以是以下之一：

- md5 - 启用消息摘要 5 (MD5)。
- sha1 - 启用 SHA-1。

null 关键字覆盖区域加密。

如果在接口上启用了 OSPFv3 加密且邻居位于其他区域（例如，区域 0）上，并且您希望 ASA 与该区域形成邻接，则必须更改 ASA 上的区域。将 ASA 上的区域更改为 0 之后，在 OSPFv3 邻接形成之前有一个两分钟的延迟。

步骤 8 指定减少到接口的 LSA 泛洪：

ipv6 ospf flood-reduction

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

步骤 9 指定接口上发送的呼叫数据包之间的间隔（以秒为单位）：

ipv6 ospf hello-interval *seconds*

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf hello-interval 15
```

该值必须对于特定网络上的所有节点都相同，并且范围可以是 1 至 65535。默认间隔对于以太网接口为 10 秒，对于非广播接口为 30 秒。

步骤 10 接收到 DBD 数据包后，禁用 OSPF MTU 不匹配检测：

ipv6 ospf mtu-ignore

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf mtu-ignore
```

默认情况下，OSPF MTU 不匹配检测已启用。

步骤 11 将 OSPF 网络类型设置为除默认以外的其他类型，具体取决于网络类型：

ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf network point-to-point non-broadcast
```

point-to-point non-broadcast 关键字可将网络类型设置为点对点非广播。**broadcast** 关键字可将网络类型设置为广播。

步骤 12 设置路由器优先级，这有助于为网络确定指定的路由器：

ipv6 ospf priority *number-value*

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf priority 4
```

有效值范围为 0 到 255。

步骤 13 配置与非广播网络的 OSPFv3 路由器互连：

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

步骤 14 指定属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）：

ipv6 ospf retransmit-interval *seconds*

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-interval 8
```

该时间必须大于连接的网络上任意两个路由器之间的预期往返延迟。有效值的范围为 1 到 65535 秒。默认值为 5 秒。

步骤 15 设置在接口上发送链路状态更新数据包所需的估计时间（以秒为单位）：

ipv6 ospf transmit-delay *seconds*

示例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-delay 3
```

有效值的范围为 1 到 65535 秒。默认值为 1 秒。

配置 OSPFv3 路由器参数

过程

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config)# ipv6 router ospf 10
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 配置 OSPFv3 区域参数：

中转区

示例：

```
ciscoasa(config-rtr)# area 10
```

支持的参数包括从 0 至 4294967295 的十进制值形式的区域 ID 和 IP 地址格式 **A.B.C.D** 的区域 ID。

步骤 3 将命令设置为其默认值：

default

示例：

```
ciscoasa(config-rtr)# default originate
```

originate 参数分发默认路由。

步骤 4 控制默认信息的分发：

default-information

步骤 5 根据路由类型定义 OSPFv3 路由管理距离：

distance

示例：

```
ciscoasa(config-rtr)# distance 200
```

支持的参数包括值为 1 至 254 的管理距离和 OSPFv3 距离的 **ospf**。

步骤 6 当路由器接收 6 类多播 OSPF (MOSPF) 数据包的链路状态通告 (LSA) 时，抑制使用 **lsa** 参数发送系统日志消息：

ignore

示例：

```
ciscoasa(config-rtr)# ignore lsa
```

步骤 7 将路由器配置为在 OSPFv3 邻居启动或关闭时发送系统日志消息：

log-adjacency-changes

示例：

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

通过 **detail** 参数，将会记录所有状态更改。

步骤 8 抑制在接口上发送和接收路由更新：

passive-interface [*interface_name*]

示例：

```
ciscoasa(config-rtr)# passive-interface inside
```

interface_name 参数指定 OSPFv3 进程运行所在的接口的名称。

步骤 9 配置将路由从一个路由域重新分发到另一个路由域：

redistribute {**connected** | **ospf** | **static**}

其中：

- **connected** - 指定已连接路由。
- **ospf** - 指定 OSPFv3 路由。
- **static** - 指定静态路由。

示例：

```
ciscoasa(config-rtr)# redistribute ospf
```

步骤 10 为指定进程创建固定路由器 ID：

router-id {*A.B.C.D* | **cluster-pool** | **static**}

其中：

A.B.C.D - 以 IP 地址格式指定 OSPF 路由器 ID。

cluster-pool - 在配置了单个接口集群时配置 IP 地址池。有关集群中使用的 IP 地址池的详细信息，请参阅为集群配置 IP 地址池（OSPFv2 和 OSPFv3），第 1036 页。

示例：

```
ciscoasa(config-rtr)# router-id 10.1.1.1
```

步骤 11 配置有效值为 0 至 128 的 IPv6 地址汇总：

summary-prefix *X:X:X:X::X/*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# router-id 192.168.3.3
ciscoasa(config-router)# summary-prefix FECO::/24
ciscoasa(config-router)# redistribute static
```

X:X:X:X::X/ 参数指定 IPv6 前缀。

步骤 12 调整路由计时器：

timers

路由计时器参数如下：

- **lsa** - 指定 OSPFv3 LSA 计时器。
- **nsf** - 指定 OSPFv3 NSF 等待计时器。
- **pacing** - 指定 OSPFv3 步调设置计时器。
- **throttle** - 指定 OSPFv3 调速计时器。

示例：

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

配置 OSPFv3 区域参数

过程

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。

此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 设置 NSSA 区域或末节区域的汇总默认开销：

area *area-id* **default-cost** *cost*

示例：

```
ciscoasa(config-rtr)# area 1 default-cost nssa
```

步骤 3 仅汇总与边界路由器的地址和掩码匹配的路由：

area *area-id* **range** *ipv6-prefix*/ *prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]

示例：

```
ciscoasa(config-rtr)# area 1 range FE01:1::1/64
```

- *area-id* 参数标识要为其汇总路由的区域。值可以指定为十进制或 IPv6 前缀。
- *ipv6-prefix* 参数指定 IPv6 前缀。*prefix-length* 参数指定前缀长度。
- **advertise** 关键字将地址范围状态设置为已通告并生成 3 类汇总 LSA。
- **not-advertise** 关键字将地址范围状态设置为 DoNotAdvertise。
- 抑制 3 类汇总 LSA，并保持向其他网络隐藏组件网络。

- **cost** *cost* 关键字/参数对指定汇总路由的指标或开销，它在 OSPF SPF 计算过程中用于确定到达目标的最短路径。
- 有效值范围为 0 到 16777215。

步骤 4 指定 NSSA 区域：

area *area-id* **nssa**

示例：

```
ciscoasa(config-rtr)# area 1 nssa
```

步骤 5 指定末节区域：

area *area-id* **stub**

示例：

```
ciscoasa(config-rtr)# area 1 stub
```

步骤 6 定义虚拟链路及其参数：

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

示例：

```
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello-interval 5
```

- *area-id* 参数标识要为其汇总路由的区域。**virtual link** 关键字指定创建虚拟链路邻居。
- *router-id* 参数指定与虚拟链路邻居关联的路由器 ID。
- 输入 **show ospf** 或 **show ipv6 ospf** 命令以显示路由器 ID。没有默认值。
- **hello-interval** 关键字指定在接口上发送的呼叫数据包的间隔时间（以秒为单位）。呼叫数据包间隔是将在呼叫数据包中通告的无符号整数。对于连接到公用网络的所有路由器和接入服务器，值必须相同。有效值范围为 1 到 8192。默认值为 10。
- **retransmit-interval** *seconds* 关键字/参数对指定属于接口的邻接的 LSA 重新传输的间隔时间（以秒为单位）。重新传输间隔是连接的网络上任意两个路由器之间的预期往返延迟。该值必须大于预期往返延迟，并且范围可以为 1 至 8192。默认值为 5。
- **transmit-delay** *seconds* 关键字/参数对指定在接口上发送链路状态更新数据包所需的估计时间（以秒为单位）。整数值必须大于零。更新数据包中的 LSA 在传输之前会按此数量递增其自己的年龄。值的范围可以是从 1 至 8192。默认值为 1。
- **dead-interval** *seconds* 关键字/参数对指定在邻居表明路由器关闭之前不得查看呼叫数据包的时间（以秒为单位）。停顿间隔是无符号整数。默认值是呼叫间隔的四倍（或 40 秒）。对于连接到公用网络的所有路由器和接入服务器，值必须相同。有效值范围为 1 到 8192。

- **ttl-security hops** 关键字在虚拟链路上配置生存时间 (TTL) 安全。*hop-count* 参数值范围可以为 1 至 254。

配置 OSPFv3 被动接口

过程

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process_id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 抑制在接口上发送和接收路由更新：

passive-interface [*interface_name*]

示例：

```
ciscoasa(config-rtr)# passive-interface inside
```

interface_name 参数指定 OSPFv3 进程运行所在的接口的名称。如果指定了 *no interface_name* 参数，则 OSPFv3 进程 *process_id* 的所有接口都变为被动接口。

配置 OSPFv3 管理距离

过程

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process_id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 设置 OSPFv3 路由的管理距离：

distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

示例：

```
ciscoasa(config-rtr)# distance ospf external 200
```

ospf 关键字指定 OSPFv3 路由。**external** 关键字指定 OSPFv3 的外部 5 类和 7 类路由。**inter-area** 关键字指定 OSPVv3 的区域间路由。**intra-area** 关键字指定 OSPFv3 的区域内路由。*distance* 参数指定管理距离，它是从 10 至 254 的整数。

配置 OSPFv3 计时器

您可以为 OSPFv3 设置 LSA 到达计时器、LSA 步调设置计时器和调速计时器。

过程

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 设置 ASA 接受来自 OSPF 邻居的同一 LSA 的最低间隔：

timers lsa arrival *milliseconds*

示例：

```
ciscoasa(config-rtr)# timers lsa arrival 2000
```

milliseconds 参数指定前后两次接受从邻居到达的同一 LSA 之间必须经过的最小延迟（以毫秒为单位）。范围是从 0 到 6,000,000 毫秒。默认值为 1000 毫秒。

步骤 3 配置 LSA 泛洪数据包步调设置：

timers pacing flood *milliseconds*

示例：

```
ciscoasa(config-rtr)# timers lsa flood 20
```

milliseconds 参数指定在前后两次更新之间泛洪队列中的 LSA 设置步调的间隔时间（以毫秒为单位）。可配置范围是从 5 到 100 毫秒。默认值为 33 毫秒。

步骤 4 更改将 OSPFv3 LSA 收集到组中并刷新、校验和或老化的间隔：

timers pacing lsa-group *seconds*

示例：

```
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

seconds 参数指定将 LSA 分组、刷新、校验和或老化的间隔秒数。范围是从 10 到 1800 秒。默认值为 240 秒。

步骤 5 配置 LSA 重新传输数据包步调：

timers pacing retransmission *milliseconds*

示例：

```
ciscoasa(config-rtr)# timers pacing retransmission 100
```

milliseconds 参数指定重新传输队列中的 LSA 设置步调的间隔时间（以毫秒为单位）。可配置范围是从 5 到 200 毫秒。默认值为 66 毫秒。

步骤 6 配置 OSPFv3 LSA 调速：

timers throttle lsa *milliseconds1 milliseconds2 milliseconds3*

示例：

```
ciscoasa(config-rtr)# timers throttle lsa 500 6000 8000
```

- *milliseconds1* 参数指定生成 LSA 的第一次出现所需的延迟（以毫秒为单位）。*milliseconds2* 参数指定发起同一 LSA 所需的最大延迟（以毫秒为单位）。*milliseconds3* 参数指定发起同一 LSA 所需的最小延迟（以毫秒为单位）。
- 对于 LSA 调速，如果最短或最长时间小于第一次出现的值，则 OSPFv3 会自动更正为第一次出现的值。同样，如果指定的最大延迟小于最小延迟，则 OSPFv3 会自动更正为最小延迟值。
- 对于 *milliseconds1*，默认值为 0 毫秒。
- 对于 *milliseconds2* 和 *milliseconds3*，默认值为 5000 毫秒。

步骤 7 配置 OSPFv3 SPF 调速：

timers throttle spf *milliseconds1 milliseconds2 milliseconds3*

示例：

```
ciscoasa(config-rtr)# timers throttle spf 5000 12000 16000
```

- *milliseconds1* 参数指定接收对 SPF 计算的更改所需的延迟（以毫秒为单位）。*milliseconds2* 参数指定第一次和第二次 SPF 计算之间的延迟（以毫秒为单位）。*milliseconds3* 参数指定 SPF 计算的最长等待时间（以毫秒为单位）。
- 对于 SPF 调速，如果 *milliseconds2* 或 *milliseconds3* 小于 *milliseconds1*，则 OSPFv3 会自动更正为 *milliseconds1* 值。同样，如果 *milliseconds3* 小于 *milliseconds2*，则 OSPFv3 会自动更正为 *milliseconds2* 值。
- 对于 *milliseconds1*，SPF 调速的默认值为 5000 毫秒。
- 对于 *milliseconds2* 和 *milliseconds3*，SPF 调速的默认值为 10000 毫秒。

定义静态 OSPFv3 邻居

您需要定义静态 OSPFv3 邻居来通过点对点非广播网络通告 OSPF 路由。通过此功能，您可以跨现有 VPN 连接广播 OSPFv3 通告，而不必将通告封装在 GRE 隧道中。

开始之前，必须创建到 OSPFv3 邻居的静态路由。有关创建静态路由的详细信息，请参阅配置静态路由，第 931 页。

过程

步骤 1 启用 OSPFv3 路由进程并进入 IPv6 路由器配置模式。

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 配置与非广播网络的 OSPFv3 路由器互连。

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

示例：

```
ciscoasa(config-if)# interface ethernet0/0 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

重置 OSPFv3 默认参数

要将 OSPFv3 参数还原为其默认值，请执行以下步骤：

过程

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 将可选参数还原为其默认值：

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **discard-route | distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

示例：

```
ciscoasa(config-rtr)# default metric 5
```

- **area** 关键字指定 OSPFv3 区域参数。**auto-cost** 关键字根据带宽指定 OSPFv3 接口开销。
- **default-information** 关键字分发默认信息。**default-metric** 关键字指定重新分发的路由的指标。
- **discard-route** 关键字可启用或禁用丢弃安装路由。**distance** 关键字指定管理距离。
- **distribute-list** 关键字可筛选路由更新中的网络。
- **ignore** 关键字可忽略特定事件。**log-adjacency-changes** 关键字可记录邻接状态中的记录。
- **maximum-paths** 关键字可通过多个路径转发数据包。
- **passive-interface** 关键字可在接口上抑制路由更新。
- **redistribute** 关键字可重新分发来自其他路由协议的 IPv6 前缀。
- **router-id** 关键字指定所指定路由进程的路由器 ID。
- **summary-prefix** 关键字指定 IPv6 汇总前缀。
- **timers** 关键字指定 OSPFv3 计时器。

发送系统日志消息

将路由器配置为在 OSPFv3 邻居启动或关闭时发送系统日志消息。

过程

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 将路由器配置为在 OSPFv3 邻居启动或关闭时发送系统日志消息：

log-adjacency-changes [**detail**]

示例：

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

detail 关键字为每个状态发送系统日志消息，而不只是在 OSPFv3 启动或关闭时才发送系统日志消息。

抑制系统日志消息

要在路由器接收不受支持的 LSA 6 类多播 OSPF (MOSPF) 数据包时抑制发送系统日志消息，请执行以下步骤：

过程

步骤 1 启用 OSPFv2 路由进程：

router ospf *process_id*

示例：

```
ciscoasa(config-if)# router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 当路由器接收不受支持的 LSA 6 类 MOSPF 数据包时，抑制发送系统日志消息：

ignore lsa mospf

示例：

```
ciscoasa(config-rtr)# ignore lsa mospf
```

计算汇总路由成本

过程

恢复用于根据 RFC 1583 计算汇总路由开销的方法：

compatible rfc1583

示例：

```
ciscoasa (config-rtr)# compatible rfc1583
```

生成到 OSPFv3 路由域中的默认外部路由

过程

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 生成到 OSPFv3 路由域中的默认外部路由：

default-information originate [**always**]**metric** *metric-value* [**metric-type** *type-value*] [**route-map** *map-name*]

示例：

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
```

- **always** 关键字通告默认路由（无论默认路由是否存在）。
- **metric** *metric-value* 关键字/参数对指定用于生成默认路由的指标。
- 如果不使用 **default - metric** 命令指定值，则默认值为 10。有效十进制值范围为 0 到 16777214。
- **metric-type** *type-value* 关键字/参数对指定与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值可以是以下其中一项：
  - 1 - 1 类外部路由
  - 2 - 2 类外部路由

  默认为 2 类外部路由。
- **route-map** *map-name* 关键字/参数对指定在满足路由映射的情况下生成默认路由的路由进程。

配置 IPv6 汇总前缀

过程

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 配置 IPv6 汇总前缀：

summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# router-id 192.168.3.3
ciscoasa(config-rtr)# summary-prefix FECO::/24
ciscoasa(config-rtr)# redistribute static
```

prefix 参数是目标的 IPv6 路由前缀。**not-advertise** 关键字抑制与指定前缀/掩码对匹配的路由。此关键字仅适用于OSPFv3。**tag** *tag-value* 关键字/参数对指定可用作通过路由映射控制重新分发的匹配值的标签值。此关键字仅适用于 OSPFv3。

重新分发 IPv6 路由

过程

步骤 1 启用 OSPFv3 路由进程：

ipv6 router ospf *process-id*

示例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 参数是此路由进程的内部使用的标识符，在本地进行分配，可以是从 1 至 65535 的任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部管理使用。您最多可以使用两个进程。

步骤 2 将 IPv6 路由从一个 OSPFv3 进程重新分发到另一个 OSPFv3 进程中：

redistribute *source-protocol* [*process-id*] [**include-connected** {[**level-1** | **level-2**}] [*as-number*] [**metric** [*metric-value* | **transparent**}] **[metric-type** *type-value*] [**match** {**external** [**1**|**2**] | **internal** | **nssa-external** [**1**|**2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

示例：

```
ciscoasa(config-rtr)# redistribute connected 5 type-1
```

- *source-protocol* 参数指定从其重新分发路由的源协议，可以为 static、connected 或 OSPFv3。
- *process-id* 参数是在启用了 OSPFv3 路由进程时以管理方式分配的数字。
- **include-connected** 关键字允许目标协议重新分发源协议获知的路由以及源协议运行所在的接口上的已连接前缀。
- **level-1** 关键字指定对于中间系统对中间系统 (IS-IS)，1 级路由独立重新分发到其他 IP 路由协议中。
- **level-1-2** 关键字指定对于 IS-IS，1 级和 2 级路由均重新分发到其他 IP 路由协议中。
- **level-2** 关键字指定对于 (IS-IS)，2 级路由独立重新分发到其他 IP 路由协议中。
- 对于 **metric** *metric-value* 关键字参数对，当在同一路由器上将路由从一个 OSPFv3 进程重新分发到另一个 OSPFv3 进程时，如果未指定指标值，则会将指标从一个进程携带至另一个进程。将其他进程重新分发到 OSPFv3 进程时，如果未指定指标值，则默认指标为 20。
- **metric transparent** 关键字导致 RIP 使用重新分发的路由的路由表指标为 RIP 指标。

- **metric-type** *type-value* 关键字/参数对指定与通告到 OSPFv3 路由域中的默认路由关联的外部链路类型。有效值可以是以下其中一项：1（表示 1 类外部路由）或 2（表示 2 类外部路由）。如果没有为 **metric-type** 关键字指定任何值，则 ASA 采用 2 类外部路由。对于 IS-IS，链路类型可以是以下其中一项：内部（适用于小于 63 的 IS-IS 指标）或外部（适用于大于 64 且小于 128 的 IS-IS 指标）。默认为内部。
- **match** 关键字将路由重新分发到其他路由域中并与以下其中一个选项配合使用：**external** [**1**|**2**]，表示自治系统的外部路由，但会作为 1 类或 2 类外部路由导入到 OSPFv3 中；**internal**，表示特定自治系统的内部路由；**nssa-external** [**1**|**2**]，表示自治系统的外部路由，但会在 IPv6 的 NSSA 中作为 1 类或 2 类外部路由导入到 OSPFv3 中。
- **tag** *tag-value* 关键字/参数对指定连接到每个外部路由的 32 位十进制值，它可用于在 ASBR 之间传达信息。如果未指定任何内容，则对来自 BGP 和 EGP 的路由使用远程自治系统编号。对于其他协议，将会使用零。有效值范围为 0 到 4294967295。
- **route-map** 关键字指定路由映射来检查对从源路由协议到当前路由协议的路由的导入的筛选。如果未指定此关键字，则会重新分发所有路由。如果已指定此关键字，但未列出路由映射标签，则不会导入任何路由。*map-tag* 参数标识已配置的路由映射。

配置无中断重启

ASA 可能会遇到一些已知的故障情况，这些故障情况不应影响跨交换平台转发的数据包。不间断转发 (NSF) 功能允许在恢复路由协议信息的同时沿已知路由继续转发数据。

在高可用性模式下，当主用设备变为非主用设备且备用设备成为新的主用设备时，OSPF 进程会重新启动。同样，在集群模式下，当控制设备变为非活动状态且数据设备被选为新的控制设备时，OSPF 进程会重新启动。此类 OSPF 转换过程涉及相当长的延迟。您可以配置 NSF 以避免在 OSPF 进程状态更改期间丢失流量。当有计划的无中断软件升级时，NSF 功能也非常有用。

在 OSPFv2 和 OSPFv3 上均支持平稳重启。通过使用 NSF Cisco（RFC 4811 和 RFC 4812）或 NSF IETF (RFC 3623)，您可以在 OSPFv2 上配置平稳重启。您可以使用 graceful-restart (RFC 5187) 在 OSPFv3 上配置平稳重启。

配置 NSF 平稳重启功能涉及两个步骤；配置功能和将设备配置为支持 NSF 功能或 NSF 感知。支持 NSF 功能的设备可以向邻居表明其自己的重启活动，而支持 NSF 感知的设备可以帮助重新启动邻居。

根据某些条件，可以将设备配置为支持 NSF 功能的设备或 NSF 感知的设备：

- 设备可以配置为 NSF 感知的设备，而与其所处的模式无关。
- 设备必须处于 Failover 或 Spanned Etherchannel (L2) 集群模式下才能配置为支持 NSF 功能的设备。
- 为使设备支持 NSF 功能或 NSF 感知，应将其配置为能够根据需要处理不透明链路状态通告 (LSA)/本地链路信令 (LLS) 块。

注释 如果为 OSPFv2 配置了快速呼叫，则在主用设备重新加载且备用设备激活时不会发生平稳重启。这是因为角色更改所需的时间超过配置的停顿间隔。

配置功能

思科 NSF 平稳重启机制取决于 LLS 功能，因为它会发送含有呼叫数据包中设置的 RS 位的 LLS 块来表示重启活动。IETF NSF 机制取决于不透明 LSA 功能，因为它会发送不透明 9 类 LSA 来表示重启活动。要配置功能，请输入以下命令：

过程

步骤 1 创建 OSPF 路由进程并针对要重新分发的 OSPF 进程进入路由器配置模式。

router ospf *process_id*

示例：

```
ciscoasa(config)# router ospf 2
```

process_id 参数是内部针对此路由进程使用的标识符，可以是任何正整数。此 ID 不必与任何其他设备上的 ID 匹配；它仅供内部使用。您最多可以使用两个进程。

步骤 2 支持使用 LLS 数据块或不透明 LSA 来启用 NSF：

capability {lls|opaque}

lls 关键字用于为思科 NSF 平稳重启机制启用 LLS 功能。

opaque 关键字用于为 IETF NSF 平稳重启机制启用不透明 LSA 功能。

为 OSPFv2 配置无中断重启

对于 OSPFv2、思科 NSF 和 IETF NSF，存在两种平稳重启机制。一次只能为 ospf 实例配置其中一种平稳重启机制。支持 NSF 感知的设备既可以配置为思科 NSF 助手，也可以配置为 IETF NSF 助手，但是一次只能在思科 NSF 或 IETF NSF 模式中为 ospf 实例配置支持 NSF 功能的设备。

为 OSPFv2 配置思科 NSF 无中断重启

为 OSPFv2 配置思科 NFS 平稳重启（适用于支持 NSF 功能的设备或 NSF 感知的设备）。

过程

步骤 1 在支持 NSF 功能的设备上启用思科 NSF：

nsf cisco [enforce global]

示例：

```
ciscoasa(config-router)# nsf cisco
```

当检测到无法识别 NSF 的邻居设备时，enforce global 关键字将会取消 NSF 重启。

步骤 2 （可选）在支持 NSF 感知的设备上启用思科 NSF 助手模式。

capability {lls|opaque}

示例：

```
ciscoasa(config-router)# capability lls
```

默认情况下会启用此命令。使用命令的 no 形式可禁用该命令。

为 OSPFv2 配置 IETF NSF 无中断重启

为 OSPFv2 配置思科 IETF NSF 平稳重启（支持 NSF 功能的设备或 NSF 感知的设备）。

过程

步骤 1 在支持 NSF 功能的设备上启用 IETF NSF：

nsf ietf [restart-interval *seconds***]**

示例：

```
ciscoasa(config-router)# nsf ietf restart-interval 80
```

可以指定平稳重启间隔的长度（以秒为单位）。有效值为 1 到 1800 秒。默认值为 120 秒。

为重启间隔配置的值小于显示邻接关系所需的时间时，平稳重启可能会终止。例如，低于30秒的重启间隔不受支持。

步骤 2 在支持 NSF 感知设备上启用 IETF NSF 助手模式：

nsf ietf helper [strict-lsa-checking]

示例：

```
ciscoasa(config-router)# nsf ietf helper
```

strict-LSA-checking 关键字指示如果助手路由器在以下情况下将终止重新启动路由器的过程：它检测到会泛洪至正在重新启动的路由器的 LSA 发生更改，或者如果在启动平稳重启过程后正在重新启动的路由器的重新传输列表中有已更改的 LSA。

默认情况下会启用此命令。使用命令的 no 形式可禁用该命令。

为 OSPFv3 配置无中断重启

为 OSPFv3 配置 NSF 平稳重启功能涉及两个步骤：将一个设备配置为支持 NSF 功能，然后将另一个设备配置为支持 NSF 感知。

过程

步骤 1 在未配置有显式 IPv6 地址的接口上启用 IPv6 处理：

interface physical_interface ipv6 enable

示例：

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

physical_interface 参数标识参与 OSPFv3 NSF 的接口。

步骤 2 在支持 NSF 功能的设备上为 OSPFv3 启用 graceful-restart：

graceful-restart [restart interval seconds]

示例：

```
ciscoasa(config-router)# graceful-restart restart interval 80
```

restart interval seconds 指定平稳重启间隔的长度（以秒为单位）。有效值为 1 到 1800 秒。默认值为 120 秒。

使用小于邻接启动所需的时间的值来配置重启间隔时，可能会终止平稳重启。例如，不支持低于 30 秒的重启间隔。

步骤 3 在支持 NSF 感知的设备上为 OSPFv3 启用 graceful-restart：

graceful-restart helper [strict-lsa-checking]

示例：

```
ciscoasa(config-router)# graceful-restart helper strict-lsa-checking
```

strict-LSA-checking 关键字指示如果助手路由器在以下情况下将终止重新启动路由器的过程：它检测到会泛洪至正在重新启动的路由器的 LSA 发生更改，或者如果在启动平稳重启过程后正在重新启动的路由器的重新传输列表中有已更改的 LSA。

默认情况下会启用平稳重启助手模式。

为 OSPF 配置无中断重新启动等待计时器

如果 OSPF 路由器不知道所有邻居是否在数据包中列出，并且重新启动路由器需要保留邻接关系，但它们会在连接到 Hello 数据包的 EO 中设置 RS 位。但是，RS 位值不能超过 RouterDeadInterval 秒。因此，引入 **timers nsf wait** 命令，以将呼叫数据包中的 RS 位设置为小于 RouterDeadInterval 秒。NSF 等待计时器默认值为 20 秒。

开始之前

- 要为 OSPF 配置思科 NSF 等待时间，设备必须支持 NSF 或 NSF 功能。

过程

步骤 1 进入 OSPF 路由器配置模式。

示例：

```
ciscoasa(config)# router ospf
```

步骤 2 输入计时器并指定 nsf。

示例：

```
ciscoasa(config-router)# timers?
router mode commands/options:
  lsa       OSPF LSA timers
  nsf       OSPF NSF timer
  pacing    OSPF pacing timers
  throttle  OSPF throttle timers
ciscoasa(config-router)# timers nsf ?
```

步骤 3 输入平稳重启等待间隔。此值的范围为 1 到 65535。

示例：

```
ciscoasa(config-router)# timers nsf wait 200
```

通过使用平稳重启等待间隔，可以确保等待间隔不超过路由器失效间隔。

删除 OSPFv2 配置

删除 OSPFv2 配置。

过程

删除已启用的整个 OSPFv2 配置。

clear configure router ospf *pid*

示例：

```
ciscoasa(config)# clear configure router ospf 1000
```

清除配置后，您必须使用 **router ospf** 命令重新配置 OSPF。

删除 OSPFv3 配置

删除 OSPFv3 配置。

过程

删除已启用的整个 OSPFv3 配置。

clear configure ipv6 router ospf *process-id*

示例：

```
ciscoasa(config)# clear configure ipv6 router ospf 1000
```

清除配置后，您必须使用 **ipv6 router ospf** 命令重新配置 OSPFv3。

OSPFv2 示例

以下示例显示如何使用各种可选进程启用和配置 OSPFv2：

1. 要启用 OSPFv2，请输入以下命令：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

2. （可选）要将路由从一个 OSPFv2 进程重新分发到另一个 OSPFv2 进程，请输入以下命令：

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
```

```
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

3. （可选）要配置 OSPFv2 接口参数，请输入以下命令：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
ciscoasa(config-rtr)# interface inside
ciscoasa(config-interface)# ospf cost 20
ciscoasa(config-interface)# ospf retransmit-interval 15
ciscoasa(config-interface)# ospf transmit-delay 10
ciscoasa(config-interface)# ospf priority 20
ciscoasa(config-interface)# ospf hello-interval 10
ciscoasa(config-interface)# ospf dead-interval 40
ciscoasa(config-interface)# ospf authentication-key cisco
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
ciscoasa(config-interface)# ospf authentication message-digest
```

4. （可选）要配置 OSPFv2 区域参数，请输入以下命令：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# area 0 authentication
ciscoasa(config-rtr)# area 0 authentication message-digest
ciscoasa(config-rtr)# area 17 stub
ciscoasa(config-rtr)# area 17 default-cost 20
```

5. （可选）要配置路由计算计时器并显示邻居启动和关闭日志消息，请输入以下命令：

```
ciscoasa(config-rtr)# timers spf 10 120
ciscoasa(config-rtr)# log-adj-changes [detail]
```

6. （可选）要显示当前 OSPFv2 配置设置，请输入 **show ospf** 命令。

以下是 **show ospf** 命令的输出示例：

```
ciscoasa(config)# show ospf

Routing Process “ospf 2” with ID 10.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 5. Checksum Sum 0x 26da6
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x 209a3
```

```
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

7. 要清除 OSPFv2 配置，请输入以下命令：

```
ciscoasa(config)# clear configure router ospf pid
```

OSPFv3 示例

以下示例显示如何在接口级别启用和配置 OSPFv3：

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf 1 area 1
```

以下是来自 **show running-config ipv6** 命令的样本输出：

```
ciscoasa (config)# show running-config ipv6
ipv6 router ospf 1
 log-adjacency-changes
```

以下是来自 **show running-config interface** 命令的样本输出：

```
ciscoasa (config-if)# show running-config interface GigabitEthernet3/1
interface GigabitEthernet3/1
 nameif fda
 security-level 100
 ip address 1.1.11.1 255.255.255.0 standby 1.1.11.2
 ipv6 address 9098::10/64 standby 9098::11
 ipv6 enable
 ipv6 ospf 1 area 1
```

以下示例显示如何配置特定于 OSPFv3 的接口：

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# nameif fda
ciscoasa (config-if)# security-level 100
ciscoasa (config-if)# ip address 10.1.11.1 255.255.255.0 standby 10.1.11.2
ciscoasa (config-if)# ipv6 address 9098::10/64 standby 9098::11
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf cost 900
ciscoasa (config-if)# ipv6 ospf hello-interval 20
ciscoasa (config-if)# ipv6 ospf network broadcast
ciscoasa (config-if)# ipv6 ospf database-filter all out
ciscoasa (config-if)# ipv6 ospf flood-reduction
ciscoasa (config-if)# ipv6 ospf mtu-ignore
ciscoasa (config-if)# ipv6 ospf 1 area 1 instance 100
ciscoasa (config-if)# ipv6 ospf encryption ipsec spi 890 esp null md5
12345678901234567890123456789012
```

```
ciscoasa (config)# ipv6 router ospf 1
ciscoasa (config)# area 1 nssa
ciscoasa (config)# distance ospf intra-area 190 inter-area 100 external 100
ciscoasa (config)# timers lsa arrival 900
ciscoasa (config)# timers pacing flood 100
ciscoasa (config)# timers throttle lsa 900 900 900
ciscoasa (config)# passive-interface fda
ciscoasa (config)# log-adjacency-changes
ciscoasa (config)# redistribute connected metric 100 metric-type 1 tag 700
```

有关如何配置 OSPFv3 虚拟链路的示例，请参阅以下 URL：

http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080b8fd06.shtml

监控 OSPF

您可以显示特定统计信息，例如 IP 路由表、缓存和数据库的内容。您还可以使用所提供的信息确定资源利用率和解决网络问题。您也可以显示有关节点可达性的信息并发现设备数据包通过网络所采用的路由路径。

要监控或显示各种 OSPFv2 路由统计信息，请输入以下其中一个命令：

命令	目的
show ospf [*process-id* [*area-id*]]	显示有关 OSPFv2 路由进程的一般信息。
show ospf border-routers	向 ABR 和 ASBR 显示内部 OSPFv2 路由表条目。
show ospf [*process-id* [*area-id*]] database	显示与特定路由器 OSPFv2 数据库相关的信息列表。

命令	目的
show ospf flood-list *if-name*	显示等待通过接口泛洪的 LSA 的列表（以观察 OSPFv2 数据包步调设置）。 OSPFv2 更新数据包自动设置步调，因此其不会以小于 33 毫秒的间隔进行发送。如果没有步调设置，则在链路速度缓慢，邻居无法足够快速地接收更新或者路由器可能会用尽缓冲区空间的情况下，某些更新数据包可能会丢失。例如，如果没有步调设置，则在存在以下任一拓扑的情况下，可能会丢弃数据包： • 快速路由器通过点对点链路连接到速度较慢的路由器。 • 在泛洪期间，多个邻居同时向单个路由器发送更新。 在重新发送的间隔内也会使用步调设置，以提高效率并尽量减少重新传输丢失。您还可以显示等待从接口发出的 LSA。通过步调设置，可以更高效地发送OSPFv2更新数据包和重新传输数据包。 此功能没有配置任务；它自动进行配置。
show ospf interface [*if_name*]	显示与 OSPFv2 相关的接口信息。
show ospf neighbor [*interface-name*] [*neighbor-id*] [**detail**]	逐个接口显示 OSPFv2 邻居信息。
show ospf request-list *neighbor if_name*	显示路由器请求的所有 LSA 的列表。
show ospf retransmission-list *neighbor if_name*	显示等待重新发送的所有 LSA 的列表。
show ospf [*process-id*] summary-address	显示在 OSPFv2 进程下配置的所有汇总地址重新分发信息的列表。
show ospf [*process-id*] **traffic**	显示由特定 OSPFv2 实例发送或接收的不同类型的数据包的列表。
show ospf [*process-id*] virtual-links	显示与 OSPFv2 相关的虚拟链路信息。
show route cluster	显示集群中的其他 OSPFv2 路由同步信息。

要监控或显示各种 OSPFv3 路由统计信息，请输入以下其中一个命令：

命令	目的
show ipv6 ospf [*process-id* [*area-id*]]	显示有关 OSPFv3 路由进程的一般信息。

命令	目的
show ipv6 ospf [*process-id*] **border-routers**	向 ABR 和 ASBR 显示内部 OSPFv3 路由表条目。
show ipv6 ospf [*process-id* [*area-id*]] database [**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] | **self-originate**] [**internal**] [**database-summary**]	显示与特定路由器 OSPFv3 数据库相关的信息列表。
show ipv6 ospf [*process-id* [*area-id*]] **events**	显示 OSPFv3 事件信息。
ospf [*process-id*] [*area-id*] flood-list *interface-type interface-number*	显示等待通过接口泛洪的 LSA 的列表（以观察 OSPFv3 数据包步调设置）。 OSPFv3 更新数据包自动设置步调，因此其不会以小于 33 毫秒的间隔进行发送。如果没有步调设置，则在链路速度缓慢，邻居无法足够快速地接收更新或者路由器可能会用尽缓冲区空间的情况下，某些更新数据包可能会丢失。例如，如果没有步调设置，则在存在以下任一拓扑的情况下，可能会丢弃数据包： • 快速路由器通过点对点链路连接到速度较慢的路由器。 • 在泛洪期间，多个邻居同时向单个路由器发送更新。 在重新传输的间隔内也会使用步调设置，以提高效率并尽量减少重新传输丢失。您还可以显示等待从接口发出的 LSA。通过步调设置，可以更高效地发送OSPFv3更新数据包和重新传输数据包。 此功能没有配置任务；它自动进行配置。
show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]	显示与 OSPFv3 相关的接口信息。
show ipv6 ospf neighbor [*process-id*] [*area-id*] [*interface-type interface-number*] [*neighbor-id*] [**detail**]	逐个接口显示 OSPFv3 邻居信息。
show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]	显示路由器请求的所有 LSA 的列表。
show ipv6 ospf [*process-id*] [*area-id*] retransmission-list [*neighbor*] [*interface*] [*interface-neighbor*]	显示等待重新发送的所有 LSA 的列表。

命令	目的
show ipv6 ospf statistic [*process-id*] [**detail**]	显示各种 OSPFv3 统计信息。
show ipv6 ospf [*process-id*] summary-prefix	显示在 OSPFv3 进程下配置的所有汇总地址重新分发信息的列表。
show ipv6 ospf [*process-id*] **timers** [**lsa-group** | **rate-limit**]	显示 OSPFv3 计时器信息。
show ipv6 ospf [*process-id*] **traffic** [*interface_name*]	显示与 OSPFv3 流量相关的统计信息。
show ipv6 ospf virtual-links	显示与 OSPFv3 相关的虚拟链路信息。
show ipv6 route cluster [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]	显示集群中的 IPv6 路由表序号、IPv6 重新收敛计时器状态和 IPv6 路由条目序号。

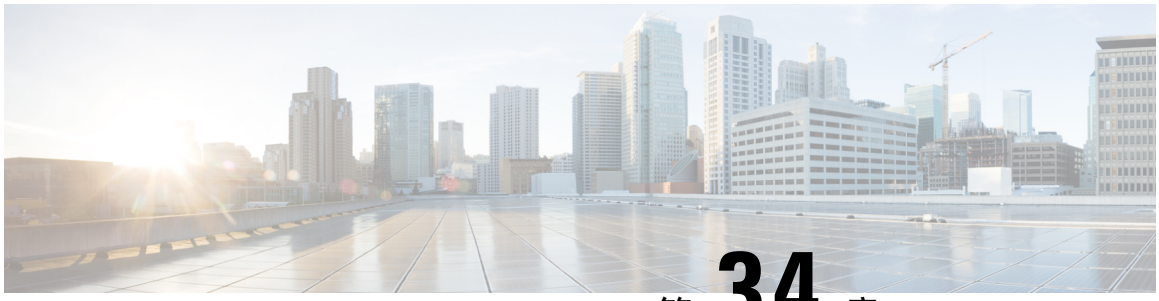
OSPF 的历史记录

表 *40: OSPF* 的功能历史记录

功能名称	平台版本	功能信息
OSPF 支持	7.0(1)	添加了对使用开放式最短路径优先 (OSPF) 路由协议来路由数据、执行身份验证以及重新分发和监控路由信息的支持。 引入了以下命令：**route ospf**
多情景模式下的动态路由	9.0(1)	在多情景模式中支持 OSPFv2 路由。
集群	9.0(1)	对于 OSPFv2 和 OSPFv3，在集群环境中支持批量同步、路由同步和跨网络 EtherChannel 负载均衡。 引入或修改了以下命令：**show route cluster**、**show ipv6 route cluster**、**debug route cluster**、**router-id cluster-pool**。

功能名称	平台版本	功能信息
OSPFv3 支持 IPv6	9.0(1)	IPv6 支持 OSPFv3 路由。 引入或修改了以下命令：**ipv6 ospf**、**ipv6 ospf area**、**ipv6 ospf cost**、**ipv6 ospf database-filter all out**、**ipv6 ospf dead-interval**、**ipv6 ospf encryption**、**ipv6 ospf hello-interval**、**ipv6 ospf mtu-ignore**、**ipv6 ospf neighbor**、**ipv6 ospf network**、**ipv6 ospf flood-reduction**、**ipv6 ospf priority**、**ipv6 ospf retransmit-interval**、**ipv6 ospf transmit-delay**、**ipv6 router ospf**、**ipv6 router ospf area**、**ipv6 router ospf default**、**ipv6 router ospf default-information**、**ipv6 router ospf distance**、**ipv6 router ospf exit**、**ipv6 router ospf ignore**、**ipv6 router ospf log-adjacency-changes**、**ipv6 router ospf no**、**ipv6 router ospf passive-interface**、**ipv6 router ospf redistribute**、**ipv6 router ospf router-id**、**ipv6 router ospf summary-prefix**、**ipv6 router ospf timers**、**area encryption**、**area range**、**area stub**、**area nssa**、**area virtual-link**、**default**、**default-information originate**、**distance**、**ignore lsa mospf**、**log-adjacency-changes**、**redistribute**、**router-id, summary-prefix**、**timers lsa arrival**、**timers pacing flood**、**timers pacing lsa-group**、**timers pacing retransmission**、**timers throttle**、**show ipv6 ospf**、**show ipv6 ospf border-routers**、**show ipv6 ospf database**、**show ipv6 ospf events**、**show ipv6 ospf flood-list**、**show ipv6 ospf graceful-restart**、**show ipv6 ospf interface**、**show ipv6 ospf neighbor**、**show ipv6 ospf request-list**、**show ipv6 ospf retransmission-list**、**show ipv6 ospf statistic**、**show ipv6 ospf summary-prefix**、**show ipv6 ospf timers**、**show ipv6 ospf traffic**、**show ipv6 ospf virtual-links**、**show ospf**、**show running-config ipv6 router**、**clear ipv6 ospf**、**clear configure ipv6 router**、**debug ospfv3**、**ipv6 ospf neighbor**。
OSPF 支持快速呼叫	9.2(1)	OSPF 支持快速呼叫数据包功能，从而产生在 OSPF 网络中导致更快收敛的配置。 修改了以下命令：**ospf dead-interval**
计时器	9.2(1)	添加了新 OSPF 计时器；弃用了旧 OSPF 计时器。 引入了以下命令：timers lsa arrival、timers pacing、timers throttle 删除了以下命令：Timers spf、timers lsa-grouping-pacing
使用访问列表筛选路由	9.2(1)	现在支持使用 ACL 筛选路由。 引入了以下命令：distribute-list
OSPF 监控增强功能	9.2(1)	添加了其他 OSPF 监控信息。 修改了以下命令：show ospf events, show ospf rib, show ospf statistics, show ospf border-routers [detail], show ospf interface brief
OSPF 重新分发 BGP	9.2(1)	添加了 OSPF 重新分发功能。 添加了以下命令：redistribute bgp

功能名称	平台版本	功能信息
OSPF 支持不间断转发 (NSF)	9.3(1)	添加了对 NSF 的 OSPFv2 和 OSPFv3 支持。 添加了以下命令：capability、nsf cisco、nsf cisco helper、nsf ietf、nsf ietf helper、nsf ietf helper strict-lsa-checking、graceful-restart、graceful-restart helper、graceful-restart helper strict-lsa-checking
OSPF 支持不间断转发 (NSF)	9.13(1)	添加了 NSF 等待计时器。 添加了一个新命令，用于为NSF重新启动间隔设置计时器。引入此命令是为了确保等待间隔不会长于路由器失效间隔。 我们引入了以下命令： **timers nsf wait<seconds>**



第 34 章

IS-IS

本章介绍中间系统到中间系统 (IS-IS) 路由协议。

- 关于 IS-IS，第 1077 页
- IS-IS 前提条件，第 1083 页
- IS-IS 准则，第 1083 页
- 配置 IS-IS，第 1083 页
- 监控 IS-IS，第 1113 页
- IS-IS 的历史记录，第 1115 页
- IS-IS 示例，第 1115 页

关于 IS-IS

IS-IS 路由协议是一种链路状态内部网关协议 (IGP)。链路状态协议的主要特征是传播在每个参与设备上建立完整网络连接图所需的信息。然后，该连接图会用于计算到达目的地的最短路径。IS-IS 实施支持 IPv4 和 IPv6。

您可以将路由域划分为一个或多个子域。每个子域称为一个区域，并会分配一个区域地址。同一个区域内的路由称为 1 级路由。在 1 级区域之间的路由称为 2 级路由。路由器称为中间系统 (IS)。IS 可以运行在 1 级、2 级或两者。运行在 1 级的 IS 与同一区域中的其他 1 级 IS 交换路由信息。运行在 2 级的 IS 与其他 2 级路由器交换路由信息，而不管它们是否处于相同的 1 级区域内。2 级路由器集合以及将它们互连的链路形成 2 级子域，子域不能再分区，否则路由无法正常工作。

关于 NET

IS 通过称为网络实体名称 (NET) 的地址来标识。NET 是网络服务接入点 (NSAP) 的地址，标识 IS 上运行的 IS-IS 路由协议实例。NET 的长度为网络是 8 到 20 个八位组，它具有以下三个部分：

- 区域地址 - 此字段长度为 1 到 13 个八位组，由地址的高位八位组组成。

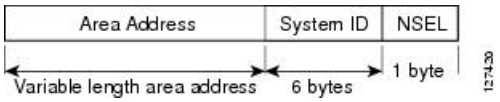
注释 您可以为一个 IS-IS 实例分配多个区域地址；在这种情况下，所有区域地址视为相同。当合并或拆分域中的区域时，多个相同的区域地址非常有用。合并或拆分完成后，您不需要为一个 IS-IS 实例分配超过一个区域地址。

- 系统 ID - 此字段的长度为 6 个八位组，它紧随区域地址之后。当 IS 在 Level 1 运行时，系统 ID 在相同区域中的所有 Level-1 设备中必须是唯一的。当 IS 在 Level 2 运行时，系统 ID 在域中的所有设备中必须是唯一的。

注释 您可以为一个 IS 实例分配一个系统 ID。

- NSEL - N-selector 字段的长度是 1 个八位组，它紧随系统 ID 之后。其必须设置为 00。

图 *77: NET* 格式



IS-IS 动态主机名

在 IS-IS 路由域中，使用系统 ID 代表每个 ASA。系统 ID 是为每个 IS-IS ASA 配置的 NET 的一部分。例如，NET 配置为 49.0001.0023.0003.000a.00 的 ASA 的系统 ID 为 0023.0003.000a。对于网络管理员而言，在 ASA 上进行维护以及故障排除期间，很难记住 ASA 名称与系统 ID 的映射。

输入 **show isis hostname** 命令可显示系统 ID 与 ASA 名称映射表中的条目。

动态主机名机制使用链路状态协议 (LSP) 泛洪来跨整个网络分发 ASA 名称与系统 ID 的映射信息。网络中的每个 ASA 都会尝试安装其路由表中的系统 ID 与 ASA 名称的映射信息。

如果一台一直在网络中通告动态名称类型、长度、值 (TLV) 的 ASA 突然停止通告，则最后收到的映射信息将在动态主机映射表中保留最多一个小时，以便网络遇到问题时网络管理员可以显示映射表中的条目。

IS-IS PDU 类型

ISes 使用协议数据单元 (PDU) 与其对等体交换路由信息。使用中间系统到中间系统 Hello PDU (IIH)、链路状态 PDU (LSP) 和序列号 PDU (SNP) 类型的 PDU。

IIH

IIH 将在已启用 IS-IS 协议的回路上的 IS 邻居之间交换。IIH 包括发送方的系统 ID、分配的区域地质，以及称为发送 IS 的回路上邻居的标识。还可包括其他可选信息。

有两种类型的 IIH：

- 1 级 LAN IIH - 当发送 IS 在该回路上作为 1 级设备运行时，将在多接入回路上发送这些信息。
- 2 级 LAN IIH - 当发送 IS 在该回路上作为 2 级设备运行时，将在多接入回路上发送这些信息。

LSP

IS 将生成 LSP，以通告其直接连接到 IS 的邻居和目标。LSP 通过以下方式进行唯一标识：

- 生成 LSP 的 IS 的系统 ID
- 伪节点 ID - 除非当 LSP 是伪节点 LSP 时，否则此值始终为 0。
- LSP 号（0 到 255）
- 32 位序列号

每当生成新版本的 LSP 时，序列号都会递增。

1 级 LSP 由支持 1 级的 IS 生成。1 级 LSP 将在整个 1 级区域泛洪。由某一区域内所有 1 级 IS 生成的 1 级 LSP 组是 1 级 LSP 数据库 (LSPDB)。某一区域内的所有 1 级 IS 都具有相同的 1 级 LSPDB，因此该区域具有相同的网络连接映射。

2 级 LSP 由支持 2 级的 IS 生成。2 级 LSP 将在整个 2 级子域泛洪。由相应域内所有 2 级 IS 生成的 2 级 LSP 组是 2 级 LSP 数据库 (LSPDB)。相应 2 级子域内的所有 2 级 IS 都具有相同的 2 级 LSPDB，因此该 2 级子域具有相同的连接映射。

SNP

SNP 包含一个或多个 LSP 的摘要说明。对于 1 级和 2 级，都有两种类型的 SNP：

- 完整序列号 PDU (CSNP) 用于针对指定级别发送 IS 具有的 LSPDB 的摘要。
- 部分序列号 PDU (PSNP) 用于针对指定级别发送 IS 在其数据库中具有或者需要获取的 LSP 的子网的摘要。

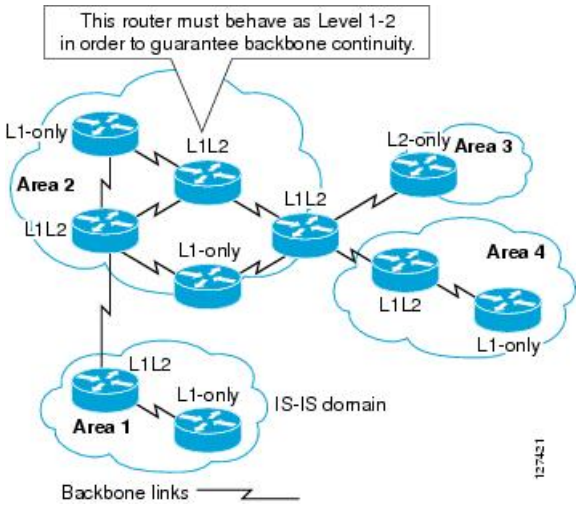
IS-IS 在多接入回路上的操作

多接入回路支持多个 ISes（即两个或更多）在回路上操作。对于多接入回路，必要的先决条件是能够使用组播或广播地址处理多个系统。在多接入回路上支持级别 1 的 IS 在回路上发送级别 1 LAN IIH。在多接入回路上支持级别 2 的 IS 在回路上发送级别 2 LAN IIH。ISes 针对每个级别与回路上的邻居 ISes 形成单独的邻接。

IS 与回路上支持级别 1 的其他 ISes 形成级别 1 邻接，并且具有匹配的区域地址。不支持两个支持级别 1 且具有一组断开连接的区域地址和的 ISes 位于同一多接入回路上。IS 与回路上支持级别 2 的其他 ISes 形成级别 2 邻接。

下图中 IS-IS 网络拓扑中的设备沿网络主干执行级别 1、级别 2 或者级别 1 和级别 2 路由。

图 *78: IS-IS* 网络拓扑中的级别 *1*、级别 *2*、级别 *1-2* 设备



指定 IS 的 IS-IS 选择

如果每个 IS 通告其 LSP 中的多路访问电路上的所有邻接关系，则所需的通告总数将为 N 2（其中 N 是在电路上给定级别运行的 IS 的数量）。为了解决这种可扩展性问题，IS-IS 定义了一个伪节点来表示该多路访问电路。在给定级别的电路上运行的所有 IS 选择其中一个 IS 充当该电路上的指定中间系统 (DIS)。对于电路上活动的每个级别，选择一个 DIS。

该 DIS 负责颁发伪节点 LSP。伪节点 LSP 包括在该电路上运行的所有 IS 的邻居通告。在电路（包括 DIS）上运行的所有 IS 在其非伪节点 LSP 中向伪节点提供邻居通告，而不会在多路访问电路上通告任何邻居。这样，所需的通告总数将作为 N-电路上运行的 IS 数的函数变化。

伪节点 LSP 由以下标识符唯一分类：

- 生成 LSP 的 DIS 的系统 ID
- 伪节点 ID（始终非零）
- LSP 号（0 到 255）
- 32 位序列号

非零伪节点 ID 是伪节点 LSP 与非伪节点 LSP 之间的区别，它由 DIS 选择，在 DIS 所处级别的所有 LAN 电路中是唯一的。

DIS 还负责在电路上发送定期 CSNP。其提供对 DIS 上 LSPDB 的当前内容的全面概述。然后，电路上的其他 IS 可执行以下活动，从而高效且可靠地同步多路访问电路上所有 IS 的 LSPDB：

- 泛洪 DIS 发送的 CSNP 中缺少的或比 CSNP 中所述的更新的 LSP。
- 对于 DIS 发送的 CSNP 中所述的本地数据库中缺少的 LSP 或比 CSNP 集中所述的 LSP 旧的 LSP，通过发送 PSNP 请求 LSP。

IS-IS LSPDB 同步

IS-IS 正常运行需要可靠和高效的进程，来同步每个 IS 上的 LSPDB。在 IS-IS 中，此进程称为更新进程。更新进程在每个受支持的级别独立运行。在本地生成的 LSP 始终是新 LSP。从回路上的邻居收到的 LSP 可能是由某个其他 IS 生成的，也可能是由本地 IS 生成的 LSP 的副本。与本地 LSPDB 的当前内容相比，收到的 LSP 可能较旧、龄期相同或较新。

处理较新的 LSP

在将较新的 LSP 添加到本地 LSPDB 时，它将替代 LSPDB 中相同 LSP 的较旧副本。较新的 LSP 将被标记为在所有回路上发送，在这些回路上，IS 当前在与较新的 LSP 相关联的级别包含一个处于运行状态的邻接 - 不包括在其上接收较新 LSP 的回路。

对于多接入回路，IS 会泛洪较新的 LSP 一次。IS 将检查 DIS 为多接入回路定期发送的 CNSP 组。如果本地 LSPDB 包含一个或多个比 CSNP 组中所述 LSP 更新的 LSP（这包括 CSNP 组中没有的 LSP），则将通过多接入回路重新泛洪这些 LSP。如果本地 LSPDB 包含一个或多个比 CSNP 组中所述内容更旧的 LSP（这包括 CSNP 组中所述但本地 LSPDB 中没有的 LSP），将在多接入回路上发送一个 PSNP，其中包含对需要更新的 LSP 的说明。用于多接入回路的 DIS 将通过发送请求的 LSP 作出响应。

处理较旧的 LSP

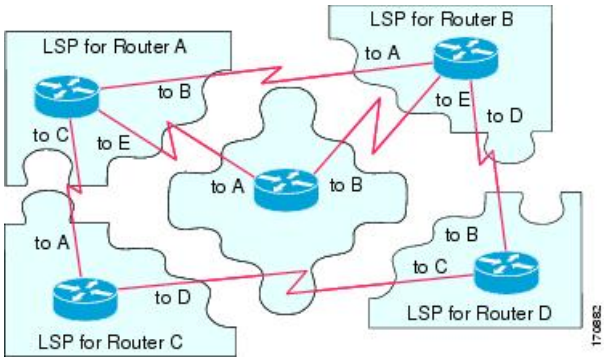
IS 可能会收到比本地 LSPDB 中的副本更旧的 LSP。IS 可能会收到 SNP（完整或部分），说明 LSP 比本地 LSPDB 中的副本更旧。在这两种情况下，IS 都会将本地数据库中的 LSP 标记为在收到较旧的 LSP 或包含该较旧 LSP 的 SNP 回路上泛洪。在向本地数据库添加新的 LSP 后，所采取的操作与上述操作相同。

处理龄期相同的 LSP

由于更新进程的分布式特性，IS 可能会收到与本地 LSPDB 的当前内容相同的 LSP 副本。在多接入回路中，收到龄期相同的 LSP 将被忽略。DIS 为该回路定期传输 CSNP 组，可以作为向发送方隐式确认已经收到 LSP。

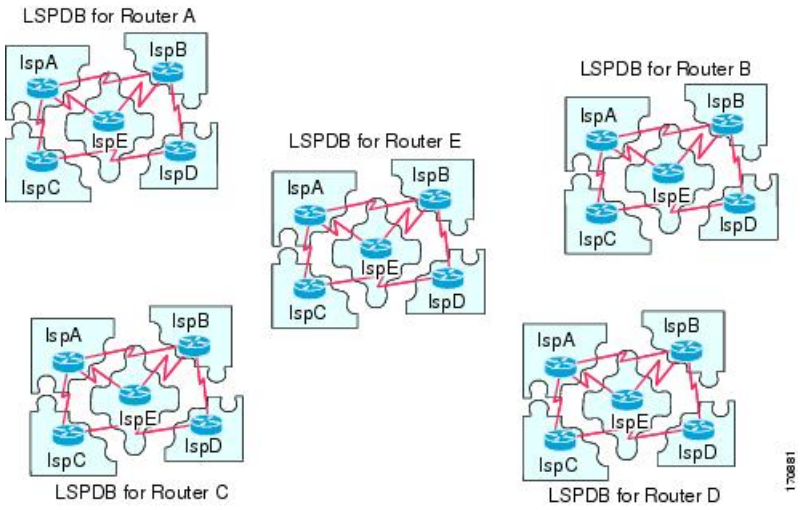
下图显示了如何使用 LSP 创建网络映射。请将网络拓扑视为拼图游戏。每个 LSP（代表一个 IS）都是一块拼图。这对某一区域中的所有 1 级设备或者 2 级子域中的所有 2 级设备都适用。

图 *79: IS-IS* 网络映射



下图显示了 IS-IS 网络中的每个设备，及其在邻居设备之间形成邻接之后已完全更新的链路状态数据库。这对某一区域中的所有 1 级设备或者 2 级子域中的所有 2 级设备都适用。

图 *80:* 包含已同步的 ***LSPDB*** 的 ***IS-IS*** 设备



IS-IS 最短路径计算

LSPDB 的内容发生变化时，每个 IS 都会独立重新运行最短路径计算。该算法基于著名的 Dijkstra 算法来延导向图查找最短路径，在导向图中，ISes 是图形的顶点，ISes 之间的链路是带有非负权重的边缘。将两个 ISes 之间的链路视为图形的一部分之前，将执行双向连接性检查。这样，可以防止在 LSPDB 中使用过时信息，例如，当一个 IS 不再在网络中运行，但又没有清除它在停止运行之前生成的一组 LSP 时。

SPF 的输出是一组元组（目标，下一跳）。目标是特定于协议的。支持多个成本相同的路径，不管是哪种情况，多个下一跳都会与同一目标关联。

对于 IS 支持的每个级别执行单独的 SPF。当级别 1 和级别 2 路径都到达同一目标时，优先选择级别 1 路径。

指示在其他区域有一个或多个级别 2 邻居的级别 2 IS 可能被与必备路径（也称为默认路由）处于同一区域的级别 1 设备所用。级别 2 IS 通过在其级别 1 LSP 0 设置连接位 (ATT) 来指示其与其他区域的连接。

注释 ID 可在每个级别生成多达 256 个 LSP。LSP 通过 0 至 255 之间的数字来标识。LSP 0 具有特定属性，包括设置 ATT 位以指示与其他区域的连接的重要性。当编号 1 至 255 的 LSP 设置了 ATT 位时，都没有意义。

IS-IS 关机协议

您可以关闭 IS-IS（将其置于管理停机状态）以对 IS-IS 协议配置进行更改，而不会丢失您的配置参数。您可以在全局 IS-IS 进程层面或接口层面关闭 IS-IS。如果在关闭该协议后重新启动该设备，则该协议预计会在禁用状态下恢复开机。如果将该协议设置为管理停机状态，将允许网络管理员以管

理方式关闭IS-IS协议的运行，而不会丢失协议配置；对协议配置进行一系列更改，而不必让协议转换的运行通过中间（也许不理想）状态；以及在以后适当时间重新启用该协议。

IS-IS 前提条件

在配置 IS-IS 之前，需要满足以下前提条件：

- 了解 IPv4 和 IPv6。
- 在配置 IS-IS 之前，了解您的网络设计以及您希望流量如何流过。
- 定义区域，准备设备的寻址计划（包括定义 NET）并确定将运行 IS-IS 的接口。
- 在配置设备之前，请准备一个邻接矩阵，显示邻接表中所期待的邻居。这样有助于进行验证。

IS-IS 准则

防火墙模式准则

仅在路由防火墙模式下受支持。不支持透明防火墙模式。

集群准则

仅在在单个接口模式下受支持；不支持跨网络 EtherChannel 模式。

其他准则

IS-IS 不支持双向转发。

配置 IS-IS

本节介绍如何在系统中启用和配置 IS-IS 进程。

过程

步骤 1 全局启用 IS-IS 路由，第 1084 页。
步骤 2 启用 IS-IS 身份验证，第 1087 页。
步骤 3 配置 IS-IS LSP，第 1091 页
步骤 4 配置 IS-IS 汇总地址，第 1095 页。
步骤 5 配置 IS-IS 被动接口，第 1096 页。
步骤 6 配置 IS-IS 接口，第 1097 页。

步骤 7 配置 IS-IS 接口呼叫传送，第 1101 页

步骤 8 配置 IS-IS IPv4 地址系列，第 1103 页。

步骤 9 配置 IS-IS IPv6 地址系列，第 1108 页。

全局启用 IS-IS 路由

IS-IS 配置在两部分中完成。首先，在全局配置模式下配置 IS-IS 进程，然后在路由器配置模式下为 IS-IS 指定 NET 和路由级别。您可在路由器配置模式下为您的网络配置比按接口配置更加有意义的其他常规参数。本节包含这些命令。

接下来，在接口配置模式下对各个接口启用 IS-IS 协议，以便接口参与动态路由并与相邻设备形成邻接关系。您必须先在一个或多个接口上启用路由，然后才可建立邻接关系和实现动态路由。请参阅配置 IS-IS 接口，第 1097 页，了解在接口上配置 IS-IS 的过程。

此过程介绍如何在 ASA 上启用 IS-IS 作为 IP 路由协议，以及在路由器配置模式下启用其他常规选项。

开始之前

在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入 **changeto context** *name* 命令。

过程

步骤 1 在 ASA 上启用 IS-IS 作为路由协议：

router isis

示例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

步骤 2 为路由进程指定 NET：

net *network-entity-title*

示例：

```
ciscoasa(config-router)# net 49.1234.aaaa.bbbb.cccc.00
```

NET 会识别用于 IS-IS 的设备。有关 NET 的详细信息，请参阅关于 NET，第 1077 页。

步骤 3 （可选）为 IS-IS 路由进程指定路由级别。

is-type [level-1 | level-2-only | level-1-2]

示例：

```
ciscoasa(config-router)# is-type level-1
```

- （可选）**level-1** - 表示区域内路由。ASA 只能理解在其区域内的目标。
- （可选）**level-2-only** - 表示区域内路由。ASA 是主干的一部分，它无法与自己区域内的第 1 级路由器通信。
- （可选）**level-1-2** - ASA 执行第 1 级和第 2 级路由。此路由器运行路由进程的两个实例。它具有一个 LSDB 用于区域中的目标（第 1 级路由），并且运行 SPF 计算来发现区域拓扑。它还具有包含其他所有主干（第 2 级）路由器的 LSP 的另一个 LSDB，并且运行其他 SPF 计算来发现主干的拓扑以及其他所有区域是否存在。

在常规 IS-IS 配置中，ASA 作为第 1 级（区域内部）和第 2 级（区域间）路由器。在多区域 IS-IS 配置中，配置 IS-IS 路由进程的第一个实例默认情况下是第 1-2 级（区域内部和区域间）路由器。配置的 IS-IS 进程的其余实例默认情况下是第 1 级路由器。

注释
我们强烈建议您配置 IS-IS 路由进程的类型。

步骤 4 在 ASA 上启用 IS-IS 动态主机名功能：

hostname dynamic

默认情况下会启用此命令。有关 IS-IS 中动态主机名的详细信息，请参阅IS-IS 动态主机名，第 1078 页。

步骤 5 在 ASA 上为所有接口配置呼叫填充：

hello padding multi-point

默认情况下会启用此命令。它将 IS-IS 呼叫配置为完整 MTU 大小。这允许及早检测因大型帧的传输问题导致的错误，或因相邻接口上的不匹配 MTU 导致的错误。

您可以禁用呼叫填充（**no hello padding multi-point** 用于 IS-IS 路由进程的某个路由器上的所有接口），以避免在两个接口的 MTU 相同或进行平移桥接时浪费网络带宽。当禁用呼叫填充时，ASA 仍然将填充的前五个 IS-IS 呼叫发送到完整的 MTU 大小，以保持发现 MTU 不匹配的优势。

在特权 EXEC 模式下输入 **show clns interface** 命令，以显示已在路由器级别关闭呼叫填充。有关详细信息，请参阅监控 IS-IS，第 1113 页。

步骤 6 （可选）使 ASA 可以在 NLSP IS-IS 邻接关系更改状态（运行或关闭）时生成日志消息：

log-adjacency-changes [all]

此命令默认禁用。当监控大型网络时，记录邻接关系更改非常有用。消息采用以下格式：

示例：

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

all-（可选）包括非 IIH 事件生成的更改。

步骤 7 （可选）禁用 IS-IS 协议，以便其无法在任何接口上形成任何邻接关系，并清除 LSP 数据库：

protocol shutdown

此命令使您可以禁用特定路由实例的 IS-IS 协议，而不删除任何现有 IS-IS 配置参数。当您输入此命令时，IS-IS 协议会继续在路由器上运行，并且您可以使用当前 IS-IS 配置，但是 IS-IS 不会在任何接口上形成任何邻接关系，而且它还会清除 IS-IS LSP 数据库。要为特定接口禁用 IS-IS，请使用 **isis protocol shutdown** 命令。请参阅配置 IS-IS 接口，第 1097 页了解相关程序。

步骤 8 （可选）为 IS-IS IP 前缀分配高优先级：

route priority high tag *tag-value*

示例：

```
ciscoasa(config-router)# route priority high tag 100
```

tag*tag-value* - 为以特定路由标记为前缀的 IS-IS IP 分配高优先级。范围为 1 到 4294967295。

使用此命令可标记优先级较高的 IS-IS IP 前缀，从而在全局路由表中更快地进行处理和安装，实现更快的汇聚。例如，您可以帮助 VoIP 网关地址首先得到处理，从而帮助 VoIP 流量比其他类型的数据包更加快速地进行更新。

步骤 9 （可选）全局更改所有 IS-IS 接口的指标值：

metric *default-value* **[level-1 | level-2]**

示例：

```
ciscoasa(config-router)# metric 55 level-1
```

- 默认值 - 要分配给链路的指标值，并且该指标值还用于计算到达目标的链路产生的路径开销。范围为 1 到 63。默认值为 10。
- （可选）**level-1** - 设置第 1 层 IPv4 或 Ipv6 指标。
- （可选）**level-2** - 设置第 2 层 IPv4 或 Ipv6 指标。

当您需要更改所有 IS-IS 接口的默认指标时，我们建议使用 **metric** 命令。这可以避免用户错误，例如意外地从接口中删除设置的指标而不配置新值，以及意外允许该接口恢复为默认指标 10，从而成为网络中的最佳首选接口。

步骤 10 （可选）配置 ASA 以仅生成和接受新式长度值对象 (TLV)：

metric-style narrow | transition | wide [level-1 | level-2 | level-1-2]

示例：

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**- 使用具有窄指标的旧样式 TLV。
- **transition**- 指示 ASA 同时接受旧样式和新样式 TLV。

- **wide**- 使用新样式 TLV 以承载更宽的指标。
- （可选）**level-1** - 在路由第 1 级上启用此命令。
- （可选）**level-2** - 在路由第 2 级上启用此命令。
- （可选）**level-1-2** - 在路由第 1 级和第 2 级上启用此命令。

此命令会导致 ASA 仅生成和接受新式 TLV，从而导致 ASA 使用比生成旧式和新式 TLV 时更少的内存和其他资源。

步骤 11 （可选）在所有接口上配置指定 ASA 的优先级：

priority *number-value*

示例：

```
ciscoasa(config-router)# priority 80
```

number-value - ASA 的优先级。范围为 0 到 127。默认值为 64。

步骤 12 （可选）配置 IS-IS 区域的其他手动地址：

max-area-addresses 编号

示例：

```
ciscoasa(config-router)# max-area-addresses 3
```

number - 要添加的手动地址数量。范围为 3 到 254。没有默认值。

此命令使您可以通过配置其他手动地址来最大化 IS-IS 区域的大小。您指定要添加的地址数，并分配一个 NET 地址来创建每个手动地址。有关 NET 的信息，请参阅关于 NET，第 1077 页。

步骤 13 为 IS-IS 配置多路径负载共享：

maximum-paths *number-of-paths*

示例：

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths - 要在路由表中安装的路由数。范围为 1 到 8。默认值为 1。

maximum-path 命令用于在 ASA 中配置 ECMP 时，配置 IS-IS 多负载共享。

启用 IS-IS 身份验证

IS-IS 路由身份验证可避免从来源引入未经授权或错误的路由消息。您可以为每个 IS-IS 区域或域设置密码，以防止未授权的路由器将错误的路由信息注入到链路状态数据库中，也可以配置 IS-IS 身份验证的类型：即 IS-IS MD5 身份验证或增强的明文身份验证。您还可以按接口设置身份验证。必须

使用相同的身份验证模式和密钥来配置接口上为 IS-IS 消息身份验证配置的所有 IS-IS 邻居，才能建立邻接关系。

有关区域和域的详细信息，请参阅关于 IS-IS，第 1077 页。

开始之前

必须先启用 IS-IS 并设置一个区域，然后才能启用 IS-IS 路由身份验证。请参阅全局启用 IS-IS 路由，第 1084 页了解相关程序。

过程

步骤 1 输入 IS-IS 路由器配置模式并配置 IS-IS 区域身份验证密码：

area-password 密码 [**authenticate snp {validate | send-only}**]

示例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

- *password* - 您分配的密码。
- （可选）**authenticate snp** - 导致系统将密码插入 SNP 中。
- **validate** - 导致系统将密码插入 SNP 中并将密码检入其收到的 SNP 中。
- **send-only**- 导致系统仅将密码插入 SNP 中，但不会将密码检入其收到的 SNP 中。请在软件升级期间使用此关键字，以简化传输。

在区域中的所有 ASA 上执行此命令可防止未授权的路由器在链路状态数据库中注入错误的路由信息。但是，此密码以纯文本形式进行交换，从而仅提供有限的安全性。

该密码会插入第 1 级（站路由器级别）PDU LSP、CSNP 和 PSNP 中。如果您不指定 **authenticate snp** 关键字与 **validate** 或 **send-only** 关键字，则 IS-IS 协议不会将密码插入 SNP 中。

步骤 2 输入 IS-IS 路由器配置模式并配置 IS-IS 域身份验证密码：

domain-password 密码 [**authenticate snp {validate | send-only}**]

示例：

```
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

- *password* - 您分配的密码。
- （可选）**authenticate snp** - 导致系统将密码插入序列号 PDU (SNP) 中。
- **validate** - 导致系统将密码插入 SNP 中并将密码检入其收到的 SNP 中。

- **send-only**- 导致系统仅将密码插入 SNP 中，但不会将密码检入其收到的 SNP 中。请在软件升级期间使用此关键字，以简化传输。

此密码以纯文本形式进行交换，从而仅提供有限的安全性。

该密码会插入第 2 级（区域路由器级别）PDU LSP、CSNP 和 PSNP 中。如果您不指定 **authenticate snp** 关键字与 **validate** 或 **send-only** 关键字，则 IS-IS 协议不会将密码插入 SNP 中。

步骤 3 全局配置 IS-IS 实例，或按接口配置以仅对正在发送（未接收）的 IS-IS 数据包执行身份验证：

路由器模式：**authentication send-only [level-1 | level-2]**

示例：

```
ciscoasa(config-router)# authentication send-only level-1
```

接口模式：**isis authentication send-only [level-1 | level-2]**

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis authentication send-only level-1
```

- （可选）**level-1** - 仅对正在发送（未接收）的第 1 级数据包执行身份验证。
- （可选）**level-2** - 仅对正在发送（未接收）的第 2 级数据包执行身份验证。

在配置身份验证模式和身份验证密钥链之前使用此命令，以便顺利地实施身份验证。如果您不指定第 1 级或第 2 级，则 send only 会同时应用于两个级别。

注释
如果身份验证仅插入正在发送的数据包，而未在正接收的数据包上检入，则对于要在每个 ASA 上配置的密钥，ASA 将有更多时间。使用此命令配置必须通信的所有 ASA 后，请在每个 ASA 上启用身份验证模式和密钥链。

步骤 4 全局或按接口为 IS-IS 实例指定 IS-IS 数据包中使用的身份验证模式类型：

路由器模式：**authentication mode {md5 | text} [level-1 | level-2]**

示例：

```
ciscoasa(config-router)# authentication mode md5 level-1
```

接口模式：**isis authentication mode {md5 | text} [level-1 | level-2]**

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#  isis authentication mode md5 level-1
```

- **md5** - 启用消息摘要 5 身份验证。

- **text** - 使用明文身份验证。
- （可选）**level-1** - 仅为第 1 级数据包启用指定的身份验证。
- （可选）**level-2** - 仅为第 2 级数据包启用指定的身份验证。

如果您使用 **area-password** 或 **domain-password** 配置了明文身份验证，则 isis authentication mode 会替代这两个命令。如果配置 **isis authentication mode**，然后尝试配置 **area-password** 或 **domain-password**，则不允许这样做。如果您不指定第 1 级或第 2 级，则该模式会同时应用于两个级别。

步骤 5 全局或按接口为 IS-IS 启用身份验证：

路由器模式：**authentication key [0 | 8]**密码**[level-1 | level-2]**

示例：

```
ciscoasa(config-router)# authentication key 0 site1 level-1
```

接口模式：**isis authentication key [0 | 8]**密码**[level-1 | level-2]**

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# router isis
ciscoasa(config-if)# isis authentication key 0 second level-1
```

- **0** - 指定将采用未加密的密码。
- **8** - 指定将采用加密的密码。
- *password* - 启用身份验证并指定密钥。
- （可选）**level-1** - 仅为第 1 级数据包启用指定的身份验证。
- （可选）**level-2** - 仅为第 2 级数据包启用指定的身份验证。

如果未通过 **key** 命令配置密码，则不执行密钥身份验证。密钥身份验证可以应用于明文或 MD5 身份验证。如要设置模式，请参阅第 4 步。一次仅将一个身份验证密钥应用于 IS-IS。如果您配置第二个密钥，则第一个密钥将被覆盖。如果您不指定第 1 级或第 2 级，则密码会同时应用于两个级别。

步骤 6 为接口配置身份验证密码：

isis password *password* **[level-1 | level-2]**

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis password analyst level-1
```

- *password* - 您分配至接口的身份验证密码。
- （可选）**level-1** - 单独为第 1 级配置身份验证密码。对于第 1 级路由，ASA 仅用作站路由器。

- （可选）**level-2** - 单独为第 2 级配置身份验证密码。对于第 2 级路由，ASA 仅用作区域路由器。

此命令使您可以防止未授权的路由器与此ASA形成邻接关系，从而保护网络免遭入侵者的侵害。该密码以纯文本形式进行交换，从而提供有限的安全性。您可以使用 **level-1** 和 **level-2** 关键字为不同的路由级别分配不同的密码。

示例

以下示例显示了对第 1 级数据包执行 MD5 身份验证的 IS-IS 实例，以及如何发送属于名为 site1 的密钥链的任何密钥：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

配置 IS-IS LSP

IS 生成 LSP 来通告其邻居和直接连接到 IS-IS 的目标。有关 LSP 的更多详细信息，请参阅IS-IS PDU 类型，第 1078 页。

使用以下命令配置 LSP，可以实现更快的收敛配置。

开始之前

在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入 **changeto context** *name* 命令。

过程

步骤 1 进入路由器配置模式：

router isis

示例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

步骤 2 配置 ASA 以忽略接收时发生内部校验和错误的 IS-IS LSP，而不是清除 LSP：

ignore-lsp-errors

示例：

```
ciscoas(config-router)# ignore-lsp-errors
```

IS-IS 要求接收方清除具有不正确数据链路校验和的 LSP，从而使数据包的发起程序重新生成该 LSP。如果网络具有导致数据损坏的链路，同时仍然传送具有正确数据链路校验和的 LSP，则可能会发生清除和重新生成大量数据包的连续循环，这可能导致网络无法正常工作。使用此命令可忽略 LSP 而不是将其清除。默认设置为启用。

步骤 3 配置 IS-IS 以仅通告属于被动接口的前缀：

advertise passive-only

此命令将已连接网络的 IP 前缀排除在 LSP 通告之外，从而减少收敛时间，因为在路由器非伪节点 LSP 中通告的前缀较少。

步骤 4 将 IS-IS LSP 配置为已满：

fast-flood *lsp-number*

示例：

```
ciscoasa(config-router)# fast-flood 7
```

（可选）*lsp-number* - 要在开始 SPF 前泛洪的 LSP 数目

此命令从 ASA 发送指定数目的 LSP。这些 LSP 在运行 SPF 之前调用 SPF。加速 LSP 泛洪过程可提高整体收敛时间。范围为 1 到 15。默认值为 5。

注释
我们建议您在路由器运行 SPF 计算之前启用 LSP 快速泛洪。

步骤 5 配置 IS-IS LSP 的 MTU 大小：

lsp-mtu *bytes*

示例：

```
ciscoasa(config-router)# lsp-mtu 1300
```

bytes - 以字节为单位的最大数据包大小。字节数必须小于或等于网络中任意链路的最小 MTU。范围为 128 到 4352。

步骤 6 设置 LSP 在 ASA 的数据库中不刷新存在的最长时间：

max-lsp-lifetime 秒

示例：

```
ciscoasa(config-router)# max-lsp-lifetime 2400
```

seconds - LSP 的有效期（以秒数为单位）。范围为 1 到 65,535。默认值为 1200。

如果在新 LSP 到达前超出有效期，该 LSP 将从数据库中删除。

步骤 7 自定义 SPF 计算的 IS-IS 限制：

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

示例：

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- （可选） **level-1** - 仅将间隔应用于第 1 层区域。
- （可选）**level-2** - 仅将间隔应用于第 2 层区域。
- *spf-max-wait* - 表示两次连续的 SPF 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 10 秒。
- （可选）*spf-initial-wait* - 表示在首次 SPF 计算前、拓扑更改后的初始等待时间。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 SPF 最大等待间隔为止。
- （可选）*spf-second-wait* - 表示首次 SPF 计算与第二次 SPF 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

仅当拓扑更改后，才会执行 SPF 计算。此命令将控制软件执行 SPF 计算的频率。

注释
SPF 计算是处理器密集型的作业。因此，限制完成此计算的频率可能非常有用，尤其是在区域较大并且拓扑经常更改时。增大 SPF 间隔将减轻 ASA 的处理器负载，但有可能降低收敛速率。

步骤 8 自定义 IS-IS 的 SPF 生成限制：

lsp-gen-interval [level-1 | level-2] *lsp-max-wait [lsp-intial-wait lsp-second wait]*

示例：

```
ciscoasa(config-router)#  lsp-gen-interval level-1 2 50 100
```

- （可选） **level-1** - 仅将间隔应用于第 1 层区域。
- （可选）**level-2** - 仅将间隔应用于第 2 层区域。
- *lsp-max-wait* - 表示两次连续的 LSP 生成之间的最大间隔。范围为 1 到 120 秒。默认值为 5 秒。
- （可选）*lsp-initial-wait* - 表示生成第一个 LSP 前的初始等待时间。范围是 1 到 120000 毫秒。默认值为 50 毫秒。

  每个后续的等待间隔均是前一个的两倍，直到等待间隔达到指定的 LSP 最大等待间隔。
- （可选）*lsp-second-wait* - 表示生成第一个和第二个 LSP 之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5000 毫秒（5 秒）。

  此命令控制生成 LSP 之间的延迟。

步骤 9 设置 LSP 刷新间隔：

lsp-refresh-interval 秒

示例：

```
ciscoasa(config-router)# lsp-refresh-interval 1080
```

（可选）*seconds* - LSP 的刷新间隔。范围为 1 到 65535 秒。默认值为 900 秒（15 分钟）。

刷新间隔确定该软件在 LSP 中定期发送其始发的路由拓扑信息的速率。这样做是为了防止数据库信息过时。

注释
在 LSP 的有效期到期前，必须定期刷新 LSP。为 **lsp-refresh-interval** 命令设置的值应小于为 **max-lsp-lifetime** 命令设置的值；否则 LSP 将在刷新前超时。如果设置的 LSP 有效期比 LSP 刷新间隔低很多，该软件将缩短 LSP 刷新间隔以防止 LSP 超时。

步骤 10 自定义 PRC 的 IS-IS 限制：

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

示例：

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait* - 表示两次连续的 PRC 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 5 秒。
- （可选）*prc-initial-wait* - 表示拓扑更改后的初始 PRC 等待时间。范围为 1 到 120,000 毫秒。默认值为 2000 毫秒。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 PRC 最大等待间隔为止。
- （可选）*prc-second-wait* - 指示第一次和第二次 PRC 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5000 毫秒（5 秒）。

  PRC 是计算路由而不执行 SPF 计算的软件进程。当路由系统自身的拓扑没有发生更改，但在特定 IS 发布的信息中检测到更改时，或当必须尝试在 RIB 中重新安装此类路由时，可能会执行此进程。

步骤 11 配置在 PDU 已满时抑制的路由：

lsp-full suppress {external [interlevel] | interlevel [external] | none}

示例：

```
ciscoasa(config-router)# lsp-full suppress interlevel external
```

- **external**- 抑制此 ASA 上的所有重新分发路由。
- **interlevel**- 抑制来自其他级别的所有路由。例如，如果 Level 2 LSP 已满，则将抑制来自 Level 1 的路由。

- **none**- 不抑制任何路由。

在对重新分发到 IS-IS 中的路由数目没有限制的网络（即未配置 **redistribute maximum-prefix** 命令）中，LSP 可能将填满，并且路由会被丢弃。使用 **lsp-full suppress** 命令可提前定义当 LSP 变满时要抑制的路由。

配置 IS-IS 汇总地址

给定级别下可以汇总多个地址组。从其他路由协议获知的路由也可以汇总。用于通告汇总的指标是所有较为具体路由的最小指标。这有助于减小路由表的大小。

如果要创建不发生在网络编号编辑的汇总地址，或者要在禁用了自动路由汇总的ASA上使用汇总地址，则需要手动定义汇总地址。

过程

步骤 1 进入路由器配置模式：

router isis

示例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

步骤 2 创建 IS-IS 的汇聚地址。

address mask tag-number metric-value **summary-address [level-1 | level-1-2 | level-2] tag metric**

示例：

```
ciscoasa(config-router)# summary-address 10.1.0.0 255.255.0.0 tag 100 metric 110
```

- *address* - 为一系列 IP 地址指定的汇总地址。
- *mask* - 用于汇总路由的 IP 子网掩码。
- （可选）**level-1** - 仅重新分发到第 1 级的路由通过配置的地址和掩码值汇总。
- （可选）**level-1-2** - 当重新分发路由到第 1 级和第 2 级时，以及当第 2 级 IS-IS 将第 1 级路由通告为在其区域中可访问时，汇总路由适用。
- （可选）**level-2** - 第 1 级路由了解的路由通过配置的地址和掩码值汇总到第 2 级主干。重新分发到第 2 级 IS-IS 中的路由也会汇总。
- （可选）**tag***tag-number* - 指定用于标记汇总路由的编号。范围为 1 到 4294967295。

- （可选）**metric***metric-value* - 指定应用到汇总路由的指标值。**metric** 关键字分配给链路，并且用于计算到达目标的链路产生的路径开销。您仅可为第 1 级或第 2 级路由配置此指标。范围为 1 到 4294967295。默认值为 10。

输入 **show clns interface** 命令以验证接口的指标值，请参阅 监控 IS-IS，第 1113 页 了解更多信息。

配置 IS-IS 被动接口

您可以禁用接口上的 IS-IS hello 数据包和路由更新，同时仍在拓扑数据库中包含接口地址。这些接口不会形成 IS-IS 邻居关系

如果有不希望参加 IS-IS 路由但已连接到要通告网络的接口，请配置被动接口（使用 **passive-interface** 命令），以防止该接口使用 IS-IS。此外，您还可以指定 ASA 用于更新的 IS-IS 版本。备用路由帮助控制 IS-IS 路由信息的通告并禁用在接口上发送和接收 IS-IS 路由更新。

过程

步骤 1 进入路由器配置模式：

router isis

示例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

步骤 2 在 ASA 上配置被动接口：

passive-interface *interface-name*

示例：

```
ciscoasa(config-router)# passive-interface inside
```

- **default** - 抑制所有接口上的路由更新。
- **management**- 抑制 Management 0/1 接口上的更新。
- **management2** - 抑制 Management 0/2 接口上的更新。
- **inside**- 抑制内部接口上的更新。

此命令配置接口 NOT 以形成 IS-IS 邻居邻接关系，并将接口地址包含在 IS-IS 数据库中。

步骤 3 配置 ASA 以通告被动接口：

advertise passive-only

示例：

```
ciscoasa(config-router)# advertise passive-only
```

此命令配置 IS-IS 以仅通过属于被动接口的前缀。它从 LSP 通告中排除连接的网络的 IP 前缀，从而缩短 IS-IS 汇聚时间。

配置 IS-IS 接口

此程序介绍如何为 IS-IS 路由修改各个 ASA 接口。您可以修改以下内容：

- 常规设置，如启用 IS-IS、启用 IS-IS 关机协议、优先级、标签和接口上的邻接筛选器。
- 身份验证密钥和模式 - 有关配置接口上的身份验证的程序，请参阅启用 IS-IS 身份验证，第 1087 页。
- 呼叫填充值 - 有关配置接口上的呼叫填充的程序，请参阅配置 IS-IS 接口呼叫传送，第 1101 页。
- LSP 设置
- IS-IS 指标计算中使用的接口延迟指标。

开始之前

必须分配一个 NET，并且一些接口必须启用 IS-IS，然后才能使用 IS-IS 路由进程。您只能配置一个进程来执行 2 级（区域间）路由。如果在任何进程上配置了 2 级路由，则所有其他进程都将被自动配置为 1 级。同时，您还可以将此进程配置为执行区域内（1 级）路由。除非是在相关联的路由进程既执行 1 级路由又执行 2 级路由的情况下，否则一个接口不能成为多个区域的组成部分。请参阅全局启用 IS-IS 路由，第 1084 页了解相关程序。

过程

步骤 1 进入接口配置模式：

interface *interface_id*

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

步骤 2 对 IS-IS 邻接的建立进行筛选：

isis adjacency-filter 名称 **[match-all]**

示例：

```
ciscoasa(config-if)# isis adjacency-filter ourfriends match-all
```

- 名称 - 要应用的筛选器集合或表达式的名称。
- （可选）**match-all** - 所有 NSAP 地址都必须与筛选器匹配，才能接受邻接。如果未指定（默认设置），则只需一个地址与筛选器匹配，即可接受邻接。

通过将呼叫中的每个区域地址与系统 ID 结合起来，在传入 IS-IS 呼叫数据包之外建立 NSAP 地址，进而执行筛选。随后，这些NSAP地址中的每个地址都将通过该筛选器。如果任何一个NSAP匹配，则该筛选器将被视为符合条件；除非指定**match-all**关键字，在这种情况下，所有地址都必须符合条件。**match-all** 关键字的功能在执行负面测试时非常有效，如仅在特定地址不存在时接受邻接。

步骤 3 在 IS-IS 接口上的 LSP 通告中通告已连接网络的 IS-IS 前缀：

isis advertise prefix

示例：

```
ciscoasa(config-if)# isis advertise prefix
```

默认情况下会启用此命令。因此，即使不打算分发已连接的路由，它们也会被分发。要停止不必要的已连接路由重新分发并缩短 IS-IS 融合时间，请使用 **no isis advertise prefix** 命令。这将从 LSP 通告中排除已连接网络的 IP 前缀，进而缩短 IS-IS 收敛时间。

注释
逐个 IS-IS 接口配置此命令的 **no** 形式是缩短 IS-IS 收敛时间的小规模解决方案，因为在路由器非伪节点 LSP 中通告的前缀较少。**isis advertise prefix** 命令的替代方法之一是 **advertise passive-only** 命令，这是一个可扩展的解决方案，因为可以逐个 IS-IS 实例配置此命令。

步骤 4 在 IS-IS 接口上启用 IPv6

ipv6 router isis

示例：

```
ciscoasa(config-if)# ipv6 router isis
```

步骤 5 逐个接口配置两次连续 IS-IS LSP 传输之间的时间延迟：

isis lsp-interval *milliseconds*

示例：

```
ciscoasa(config-if)# isis lsp-interval 100
```

milliseconds - 两次连续 LSP 之间的时间延迟。范围为 1 到 4294967298。默认值为 33 毫秒。

在包含大量 IS-IS 邻居和接口的拓扑中，ASA 可能难以处理 LSP 传输和接收造成的 CPU 负载。此命令可以降低 LSP 传输速率（言外之意，也会降低其他系统的接收速率）。

步骤 6 配置 IS-IS 指标的值：

isis metric {*metric-value* | **maximum**} [**level-1 | level-2**]

示例：

```
ciscoasa(config-if)# isis metric 15 level-1
```

- *metric-value* - 分配给链路并且用于计算从每个其他路由器通过网络中的链路到达其他目标的开销的指标。不能为 1 级和 2 级路由配置此指标。范围是从 1 到 63。默认值为 10。
- **maximum**- 从 SPF 计算中排除某一链路或邻接。
- （可选）**level-1** - 指定仅应将此指标用于 1 级（区域内）路由的 SPF 计算。如果未指定可选关键字，则将在 1 级和 2 级路由上启用该指标。
- （可选）**level-2** - 指定仅应将此指标用于 2 级（区域间）路由的 SPF 计算。如果未指定可选关键字，则将在 1 级和 2 级路由上启用该指标。

步骤 7 配置接口上指定 ASA 的优先级：
isis priority *number-value* **[level-1 | level-2]**

示例：

```
ciscoasa(config-if)# isis priority 80 level-1
```

- *number-value* - 设置 ASA 的优先级。范围为 0 到 127。默认值为 64。
- （可选）**level-1** - 独立设置 1 级的优先级。
- （可选）**level-2** - 独立设置 2 级的优先级。

该优先级用于确定 LAN 上的哪一个 ASA 将成为指定路由器或 DIS。优先级将在呼叫数据包中通告。优先级最高的 ASA 将成为 DIS。

注释
在 IS-IS 中，没有指定备份的路由器。将优先级设置为 0 将降低此系统成为 DIS 的几率，但不会阻止其成为 DIS。如果优先级更高的路由器上线，则它将接管当前 DIS 的角色。在优先级相等的情况下，最高 MAC 地址将打破平衡。

步骤 8 禁用 IS-IS 协议，这样它将无法在指定接口上形成邻接，并且会将该接口的 IP 地址置于 ASA 生成的 LSP 中：

isis protocol shutdown

示例：

```
ciscoasa(config-if)# isis protocol shutdown
```

此命令将使您能为指定接口禁用 IS-IS 协议，而不会删除配置参数。IS-IS 协议不会为已配置此命令的接口形成任何邻接，并且会将该接口的 IP 地址置于路由器生成的 LSP 中。如果您不希望 IS-IS 在任何接口上形成任何邻接，并且希望清除 IS-IS LSP 数据库，则请使用 **protocol shutdown** 命令。请参阅全局启用 IS-IS 路由，第 1084 页了解相关程序。

步骤 9 配置每个 IS-IS LSP 的两次重新传输之间的时间量：

isis retransmit-interval 秒

示例：

```
ciscoasa(config-if)#  isis retransmit-interval 60
```

（可选）*seconds* - 每个 LSP 的两次重新传输之间的时间。数字应该大于已连接网络上任意两个路由器之间的预计往返延迟。范围为 0 到 65535。默认值为 5 秒。

请确保保守地设置 *seconds* 参数，否则可能会导致不必要的重新传输。此命令对 LAN（多点）接口没有影响。

步骤 10 配置每个 IS-IS LSP 的两次重新传输之间的时间量：

isis retransmit-throttle-interval *milliseconds*

示例：

```
ciscoasa(config-if)#  isis retransmit-throttle-interval 300
```

（可选）*milliseconds* - 相应接口上两次 LSP 重新传输之间的最小延迟。范围为 0 到 65535。

在包含很多 LSP 和很多接口的大型网络中，作为控制 LSP 重新传输流量的一种方式，此命令可能非常有效。此命令可以控制可在接口上重新发送 LSP 的速率。

此命令与控制可在接口上发送 LSP 的速率（由 **isis lsp-interval** 命令控制）的命令不同，也与控制某一 LSP 的两次重新传输之间的时间段（由 **isis retransmit-interval** 命令控制）的命令不同。您可以组合使用这些命令，以控制从一个 ASA 到其邻居的路由流量的提供负载。

步骤 11 在将 IP 前缀置于 IS-IS LSP 中时，在为接口配置的 IP 地址上设置标签。

isis tag *tag-number*

示例：

```
ciscoasa(config-if)# isis tag 100
```

tag-number - 用作 IS-IS 路由上的标签的数字。范围为 1 到 4294967295。

直到使用标签时，才会对设置该标签的路由进行操作，例如，重新分发路由或汇总路由。配置此命令将触发 ASA 生成新的 LSP，因为标签是数据包中新的信息片段。

示例

在此示例中，使用不同的标签值为两个接口设置了标签。默认情况下，已将这两个 IP 地址置于 IS-IS 1 级和 2 级数据库中。不过，如果您使用包含路由映射的 **redistribute** 命令以匹配标签 110，则只会将 IP 地址 172.16. 0.0 置于 2 级数据库中。

```
ciscoasa (config)# interface GigabitEthernet1/0
ciscoasa (config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 120
ciscoasa (config)# interface GigabitEthernet1/1
ciscoasa (config-if)# ip address 172.16.0.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 110
ciscoasa (config-router)# route-map match-tag permit 10
ciscoasa (config-router)# match tag 110
ciscoasa (config)# router isis
ciscoasa (config-router)# net 49.0001.0001.0001.0001.00
ciscoasa (config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
```

配置 IS-IS 接口呼叫传送

呼叫数据包负责发现邻居，并维护邻接关系。您可以在接口级别配置以下呼叫传送参数。请参阅全局启用 IS-IS 路由，第 1084 页以启用/禁用整个 IS-IS 的呼叫传送。

过程

步骤 1 进入接口配置模式：

interface *interface_id*

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

步骤 2 进入接口配置模式可在 ASA 上所有接口的 IS-IS 呼叫协议数据单元 (IIH PDU) 上配置填充：

isis hello padding

示例：

```
ciscoasa(config-if)# isis hello padding
```

呼叫报文会填满MTU，这允许早期检测由于大帧的传输问题导致的错误或由于相邻接口上不匹配的MTU 导致的错误。IS-IS 呼叫传送默认启用。

注释
如果两个接口的 MTU 相同，或者在转换桥接的情况下，可以禁用呼叫传送以避免浪费网络带宽。当呼叫传送被禁用时，ASA 仍然会发送前五个IS-IS呼叫报文以填满MTU大小，从而维持发现MTU不匹配的优势。

步骤 3 指定 IS-IS 发送的连续呼叫数据包之间的时间长度：

isis hello-interval {*seconds* | **minimal**} **[level-1 | level-2]**

示例：

```
ciscoasa(config-if)# isis hello-interval 5 level-1
```

- *seconds* - 呼叫数据包之间的时间长度。默认情况下，将通告一个三倍于呼叫间隔（以秒为单位）的值，作为已发送的呼叫数据包中的保持时间。您可以通过配置 **isis hello-multiplier** 命令更改乘数 3。对于较小的呼叫间隔，检测到的拓扑变化更快，但路由流量更多。范围为 0 到 65535。默认值为 10。
- **minimal** - 使系统基于呼叫乘数（通过 **isis hello-multiplier** 命令指定）计算呼叫间隔，以使结果保持时间为 1 秒。
- （可选）**level-1** - 单独配置级别 1 的呼叫间隔。请在 X.25、交换式多兆位数据服务 (SMDS) 和帧中继多路访问网络上使用此配置。
- （可选）**level-2** - 单独配置级别 2 的呼叫间隔。请在 X.25、SMDS 和帧中继多路访问网络上使用此配置。

注释
虽然较慢的呼叫间隔可以节省带宽和CPU使用率，但在有些情况下，要优先使用更快的呼叫间隔，例如使用流量工程 (TE) 隧道的大型配置。如果 TE 隧道使用 IS-IS 作为内部网关协议 (IGP)，并且 IP 路由进程在网络入口处的路由器（头端）上重新启动，则所有 TE 隧道会以此默认呼叫间隔收到重复信号。更快的呼叫间隔可防止此重复信号。要配置更快的呼叫间隔，您需要使用**isis hello-multiplier** 命令手动增加 IS-IS 呼叫间隔。

步骤 4 指定 ASA 宣布邻接关系断开前该邻居必须错失的 IS-IS 呼叫数据包数目：

isis hello-multiplier *multiplier* **[level-1 | level-2]**

示例：

```
ciscoasa(config-if)# isis hello-multiplier 10 level-1
```

- *multipler* - IS-IS 呼叫数据包中通告的保持时间设置为呼叫间隔的呼叫乘数倍数。在通告的保持时间期间未收到任何 IS-IS 呼叫数据包后，邻居宣布与此 ASA 的邻接关系断开。您可以在每个接口的基础上设置保持时间（从而设置呼叫乘数和呼叫间隔），并且一个区域中的不同路由器之间的保持时间可以不同。范围为 3 到 1000。默认值为 3。
- （可选）**level-1** - 单独配置级别 1 邻接关系的呼叫乘数。
- （可选）**level-2** - 单独配置级别 2 邻接关系的呼叫乘数。

在呼叫数据包频繁丢失并且 IS-IS 邻接关系不必要地失败的情况下，使用此命令。

注释
使用较小的呼叫乘数将使收敛更快，但是会导致更加路由不稳定。在需要时将呼叫乘数更改为较大的值有助于网络稳定切勿配置小于默认值 3 的 呼叫乘数。

步骤 5 配置用于 IS-IS 的邻接关系类型：

isis circuit-type [level-1 | level-1-2 | level-2-only]

示例：

```
ciscoasa(config-if)# isis circuit-type level-2-only
```

- （可选） **level-1** - 仅为级别 1 邻接关系配置 ASA。
- （可选）**level-1-2** - 为级别 1 和级别 2 邻接关系配置 ASA。
- （可选） **level-2** - 仅为级别 2 邻接关系配置 ASA。

您通常不需要配置此命令。正确的方式是在 ASA 上配置级别。请参阅全局启用 IS-IS 路由，第 1084 页了解相关程序。您应在区域之间（级别 1-2 路由器）的 ASA 上将某些接口配置为仅级别 2。这会通过发出未使用的级别 1 呼叫数据包节省带宽。

步骤 6 配置定期 CSNP 数据包在广播接口上发送的间隔：

isis csnp-interval 秒 **[level-1 | level-1-2 | level-2]**

示例：

```
ciscoasa(config-if)#  isis csnp-interval 30 level-1
```

- *seconds* - 多路访问网络上 CSNP 传输之间的时间间隔。此间隔仅适用于指定 ASA。范围为 0 到 65,535。默认值为 10 秒。
- （可选）**level-1** - 单独配置 级别 1 的 CSNP 传输之间的时间间隔。
- （可选）**level-2** - 单独配置 级别 2 的 CSNP 传输之间的时间间隔。

您不太可能需要更改此命令的默认值。

此命令仅适用于指定接口的 DR。仅 DR 会发送 CSNP 数据包以维持数据库同步。您可以单独为级别 1 和级别 2 配置 CSNP 间隔。

配置 IS-IS IPv4 地址系列

允许路由器重新分发从任何其他路由协议、静态配置或已连接的接口获悉的外部前缀或路由。允许重新分发的路由处于第 1 层路由器或第 2 层路由器。

您可以设置邻接、最短路径优先 (SPF)，还可以定义针对 IPv4 地址将路由从另一个路由域重新分发到 ISIS（重新分发）的条件。

开始之前

必须先启用 IS-IS 并设置一个区域，然后才能启用 IS-IS 路由身份验证。请参阅全局启用 IS-IS 路由，第 1084 页了解相关程序。

过程

步骤 1 进入路由器配置模式，配置 IPv4 地址系列：

router isis

示例：

```
ciscoasa(config)# router isis
cisco(config-router)#
```

步骤 2 执行邻接检查，以检查 IS-IS 协议支持：

adjacency-check

示例：

```
cisco(config-router)# adjacency-check
```

步骤 3 定义分配给通过 IS-IS 协议发现的路由的管理距离：

distance *weight*

权重 - 分配给 IS-IS 路由的管理距离。范围为 1 到 255。默认值为 115。

示例：

```
ciscoasa(config-router)# distance 20
```

在 RIB 中插入 IS-IS 路由，并且这些路由影响它们优先于其他协议发现的、到相同目的地址的路由的可能性时，此命令会配置应用于这些 IS-IS 路由的距离。

注释
一般来说，管理距离的值越大，信任评分就越低。管理距离为255意味着根本无法信任路由信息源，应将其忽略。权重值是主观的；目前尚没有量化方法来选择权重值。

步骤 4 为 IS-IS 配置多路径负载共享：

maximum-paths *number-of-paths*

示例：

```
ciscoasa(config-router)# maximum-paths 8
```

路径数 - 要安装到路由表中的路由的数量。范围为 1 到 8。默认值为 1。

maximum-path 命令用于在 ASA 中配置 ECMP 时，配置 IS-IS 多负载共享。

步骤 5 生成到 IS-IS 路由域中的默认路由：

default-information originate [**route-map** *map-name*]

示例：

```
ciscoasa(config-router)# default-information originate route-map RMAP
```

（可选）**route-map** *map-name* - 如果满足路由映射，则路由进程将生成默认路由。

如果使用此命令配置的 ASA 的路由表中包含到 0.0.0.0 的路由，则 IS-IS 将在其 LSP 中为 0.0.0.0 发出一条通告。如果没有路由映射，则将仅在第 2 层 LSP 中通告默认值。对于第 1 层路由，还有另一种查找默认路由的机制，即查找最近的第 1 层或第 2 层路由器。可以通过查看第 1 层 LSP 中的 ATT 查找最近的第 1 层或第 2 层路由器。通过 **match ip address** *standard-access-list* 命令，您可以指定一个或多个必须存在的 IP 路由，然后 ASA 才能通告 0/0。

步骤 6 以全局方式为第 1 层和第 2 层设置 IS-IS 指标：

metric *default-value* **[level-1 | level-2]**

示例：

```
ciscoasa(config-router)# metric 55 level-1
ciscoasa(config-router)# metric 45 level-2
```

- 默认值 - 要分配给链路的指标值，并且该指标值还用于计算到达目标的链路产生的路径开销。范围为 1 到 63。默认值为 10。
- （可选）**level-1** - 设置第 1 层 IPv4 或 Ipv6 指标。
- （可选）**level-2** - 设置第 2 层 IPv4 或 Ipv6 指标。

步骤 7 指定指标样式以及将其应用于哪些层：

metric-style [narrow | transition | wide] [level-1 | level-2 | level-1-2]

示例：

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**- 指示 ASA 使用窄指标的旧样式 TLV。
- **transition**- 指示 ASA 在过渡期间接受旧样式和新样式的 TLV。
- **wide**- 指示 ASA 使用新样式的 TLV，以承载更广泛的指标。
- （可选）**level-1** - 设置第 1 层 IPv4 或 Ipv6 指标。
- （可选）**level-2** - 设置第 2 层 IPv4 或 Ipv6 指标。
- （可选）**level-1-2** - 设置第 1 层和第·2 层 IPv4 或 IPv6 指标。

步骤 8 为第 1 层 - 第 2 层路由器何时应该设置其附加位指定约束：

set-attached-bit route-map *map-tag*

示例：

```
ciscoasa(config-router)# set-attached-bit route-map check-for-L2_backbone_connectivity
```

route-map *map-tag* - 配置的路由映射的标识符。如果指定的路由映射匹配，则路由器将继续设置其附加位。此命令默认禁用。

在当前的 IS-IS 实施中，正如 ISO 10589 中指定的那样，第 1 层-第 2 层路由器将在其在自己的域中看到其他区域或者看到其他域时设置其第 1 层 LSP 附加位。不过，在某些网络拓扑中，不同区域内相邻的第 1 层-第 2 层路由器可能会失去到第 2 层主干的连接。第 1 层路由器随后可将发往区域或域以外的流量发送到可能没有此类连接的第 1 层-第 2 层路由器。

此命令允许对第 1 层-第 2 层路由器的附加位设置进行更好的控制。路由映射可以指定一条或多条 CLNS 路由。如果至少一个匹配地址路由映射子句与第 2 层 CLNS 路由表中的路由相匹配，并且如果已满足设置附加位的所有其他要求，则第 1 层-第 2 层路由器将继续在其第 1 层 LSP 中设置附加位。如果不满足要求，或者没有匹配地址路由映射子句与第 2 层 CLNS 路由表中的路由相匹配，则不会设置附加位。

步骤 9 将 ASA 配置为向其他路由器发送信号，告知它们不要在其 SPF 计算中将该 ASA 用作中间跳：

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

示例：

```
ciscoasa(config-router)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- （可选）**on-startup** - 设置系统启动时的过载位。根据指定的后续参数或关键字，过载位将在已配置的秒数内或在 BGP 收敛之前保持设置。
- （可选）秒数 - 在系统启动时设置过载位并且保持设置的秒数。范围为 5 到 86400。
- （可选）**wait-for-bgp** - 在配置 **on-startup** 关键字后，将导致在系统启动时设置过载位，并在 BGP 收敛之前保持设置。
- （可选）**suppress** - 导致通过一个或多个后续关键字标识的前缀类型被抑制。
- （可选）**interlevel** - 在配置 **suppress** 关键字后，将阻止通告从其他 IS-IS 层获悉的 IP 前缀。
- （可选）**external** - 在配置 **suppress** 关键字后，将阻止通告从其他协议获悉的 IP 前缀。

此命令将强制 ASA 在其非伪节点 LSP 中设置过载位（也称为跳跃位）。通常，仅当 ASA 遇到问题时，才允许设置过载位。例如，当 ASA 遇到内存不足的问题时，可能是因为链路状态数据库不完整，这将导致路由表不完整或不准确。通过在其 LSP 中设置过载位，其他路由器可以在其 SPF 计算中忽略不可靠的路由器，直到该路由器从其问题中恢复过来。结果是该 IS-IS 区域中的其他路由器不会看到任何通过此路由器的路径。不过，IP 和 CLNS 前缀将直接连接到此路由器。

步骤 10 自定义 PRC 的 IS-IS 限制：

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

示例：

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait* - 表示两次连续的 PRC 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 5 秒。
- （可选）*prc-initial-wait* - 表示拓扑更改后的初始 PRC 等待时间。范围为 1 到 120,000 毫秒。默认值为 2000 毫秒。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 PRC 最大等待间隔为止。
- （可选）*prc-second-wait* - 指示第一次和第二次 PRC 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5000 毫秒（5 秒）。

  PRC 是计算路由而不执行 SPF 计算的软件进程。当路由系统自身的拓扑没有发生更改，但在特定 IS 发布的信息中检测到更改时，或当必须尝试在 RIB 中重新安装此类路由时，可能会执行此进程。

步骤 11 自定义 SPF 计算的 IS-IS 限制：

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

示例：

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- （可选） **level-1** - 仅将间隔应用于第 1 层区域。
- （可选）**level-2** - 仅将间隔应用于第 2 层区域。
- *spf-max-wait* - 表示两次连续的 SPF 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 10 秒。
- （可选）*spf-initial-wait* - 表示在首次 SPF 计算前、拓扑更改后的初始等待时间。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 SPF 最大等待间隔为止。
- （可选）*spf-second-wait* - 表示首次 SPF 计算与第二次 SPF 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

仅当拓扑更改后，才会执行 SPF 计算。此命令将控制软件执行 SPF 计算的频率。

注释
SPF 计算是处理器密集型的作业。因此，限制完成此计算的频率可能非常有用，尤其是在区域较大并且拓扑经常更改时。增大 SPF 间隔将减轻 ASA 的处理器负载，但有可能降低收敛速率。

步骤 12 配置 IS-IS 在 SFP 计算期间履行外部指标：

use external-metrics

步骤 13 配置 BGP、Connected、IS-IS、OSPF 或 Static 路由重新分发：

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric 编号

示例：

```
ciscoasa(config-router)# redistribute bgp level-1 metric-type internal metric 6
```

注释
不支持使用与指标匹配的路由映射重新分配静态路由。

metric *number* - 指标的值。范围为 1 到 4294967295。

附加位配置

在下面的示例中，当路由器与 L2 CLNS 路由表中的 49.00aa 相匹配时，附加位将保持已设置状态：

```
ciscoasa(config)# router isis
 ciscoasa(config-router)# clns filter-set L2_backbone_connectivity permit 49.00aa
 ciscoasa(config-router)# route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# match clns address L2_backbone_connectivity
ciscoasa(config)# router isis
 ciscoasa(config-router)#set-attached-bit route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# end
 ciscoasa# show clns route 49.00aa

Known via "isis", distance 110, metric 30, Dynamic Entry
Routing Descriptor Blocks:
 via tr2, Serial0
   isis, route metric is 30, route version is 58
```

配置 IS-IS IPv6 地址系列

您可以设置邻接关系、SPF，并且可以针对 IPv6 地址定义条件以便将其他路由域中的路由重新分发到 IS-IS 中（重新分发）。

开始之前

必须先启用 IS-IS 并设置一个区域，然后才能启用 IS-IS 路由身份验证。请参阅全局启用 IS-IS 路由，第 1084 页了解相关程序。

过程

步骤 1 进入路由器配置模式：

router isis

示例：

```
cisco(config-router)#
```

步骤 2 将指标样式指定为宽：

metric-style wide [transition] [level-1 | level-2 | level-1-2]

示例：

```
ciscoas(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

- (Optional) **transition**— Instructs the router to accept both old- and new-style TLVs.
- （可选）**level-1** - 设置第 1 层 IPv4 或 Ipv6 指标。
- （可选）**level-2** - 设置第 2 层 IPv4 或 Ipv6 指标。
- （可选）**level-1-2** - 设置第 1 层和第·2 层 IPv4 或 IPv6 指标。

当您需要更改所有 IS-IS 接口的默认指标时，我们建议使用 **metric** 命令。这可以避免用户错误，例如意外地从接口中删除设置的指标而不配置新值，以及意外允许该接口恢复为默认指标 10，从而成为网络中的最佳首选接口。

步骤 3 进入地址系列配置模式，以配置使用标准 IPv4 或 IPv6 地址前缀的 IS-IS 路由会话：

address-family ipv6 [unicast]

示例：

```
ciscoasa(config-router)# address-family ipv6 unicast
cisco(config-router-af)#
```

步骤 4 执行邻接检查，以检查 IS-IS 协议支持：

adjacency-check

示例：

```
cisco(config-router-af)# adjacency-check
```

步骤 5 为 IS-IS 配置多路径负载共享：

maximum-paths *number-of-paths*

示例：

```
ciscoasa(config-router-af)# maximum-paths 8
```

number-of-paths - 要在路由表中安装的路由数。范围为 1 到 8。默认值为 1。

maximum-path 命令用于在 ASA 中配置 ECMP 时，配置 IS-IS 多负载共享。

步骤 6 定义分配给通过 IS-IS 协议发现的路由的管理距离：

distance *weight*

weight - 分配给 IS-IS 路由的管理距离。范围为 1 到 255。默认值为 115。

示例：

```
ciscoasa(config-router-af)# distance 20
```

在 RIB 中插入 IS-IS 路由，并且这些路由影响它们优先于其他协议发现的、到相同目的地址的路由的可能性时，此命令会配置应用于这些 IS-IS 路由的距离。

注释
一般来说，管理距离的值越大，信任评分就越低。管理距离为255意味着根本无法信任路由信息源，应将其忽略。权重值是主观的；目前尚没有量化方法来选择权重值。

步骤 7 生成到 IS-IS 路由域中的默认路由：

default-information originate [**route-map** *map-name*]

示例：

```
ciscoasa(config-router-af)# default-information originate route-map TEST7
```

（可选）**route-map** *map-name* - 如果满足路由映射，则路由进程将生成默认路由。

如果使用此命令配置的 ASA 的路由表中包含到 0.0.0.0 的路由，则 IS-IS 将在其 LSP 中为 0.0.0.0 发出一条通告。如果没有路由映射，则将仅在第 2 层 LSP 中通告默认值。对于第 1 层路由，还有另一种查找默认路由的机制，即查找最近的第 1 层或第 2 层路由器。可以通过查看第 1 层 LSP 中的 ATT 查找最近的第 1 层或第 2 层路由器。通过 **match ip address** *standard-access-list* 命令，您可以指定一个或多个必须存在的 IP 路由，然后 ASA 才能通告 0/0。

步骤 8 将 ASA 配置为向其他路由器发送信号，告知它们不要在其 SPF 计算中将该 ASA 用作中间跳：

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

示例：

```
ciscoasa(config-router-af)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- （可选）**on-startup** - 设置系统启动时的过载位。根据指定的后续参数或关键字，过载位将在已配置的秒数内或在 BGP 收敛之前保持设置。
- （可选）秒数 - 在系统启动时设置过载位并且保持设置的秒数。范围为 5 到 86400。
- （可选）**wait-for-bgp** - 在配置 **on-startup** 关键字后，将导致在系统启动时设置过载位，并在 BGP 收敛之前保持设置。
- （可选）**suppress** - 导致通过一个或多个后续关键字标识的前缀类型被抑制。
- （可选）**interlevel** - 在配置 **suppress** 关键字后，将阻止通告从其他 IS-IS 层获悉的 IP 前缀。
- （可选）**external** - 在配置 **suppress** 关键字后，将阻止通告从其他协议获悉的 IP 前缀。

此命令将强制 ASA 在其非伪节点 LSP 中设置过载位（也称为跳跃位）。通常，仅当 ASA 遇到问题时，才允许设置过载位。例如，当 ASA 遇到内存不足的问题时，可能是因为链路状态数据库不完整，这将导致路由表不完整或不准确。通过在其 LSP 中设置过载位，其他路由器可以在其 SPF 计算中忽略不可靠的路由器，直到该路由器从其问题中恢复过来。结果是该 IS-IS 区域中的其他路由器不会看到任何通过此路由器的路径。不过，IP 和 CLNS 前缀将直接连接到此路由器。

步骤 9 自定义 PRC 的 IS-IS 限制：

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

示例：

```
ciscoasa(config-router-af)#  prc-interval 5 10 20
```

- *prc-max-wait* - 表示两次连续的 PRC 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 5 秒。
- （可选）*prc-initial-wait* - 表示拓扑更改后的初始 PRC 等待时间。范围为 1 到 120,000 毫秒。默认值为 2000 毫秒。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 PRC 最大等待间隔为止。
- （可选）*prc-second-wait* - 指示第一次和第二次 PRC 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5000 毫秒（5 秒）。

  PRC 是计算路由而不执行 SPF 计算的软件进程。当路由系统自身的拓扑没有发生更改，但在特定 IS 发布的信息中检测到更改时，或当必须尝试在 RIB 中重新安装此类路由时，可能会执行此进程。

步骤 10 自定义 SPF 计算的 IS-IS 限制：

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

示例：

```
ciscoasa(config-router-af)#  spf-interval level-1 5 10 20
```

- （可选） **level-1** - 仅将间隔应用于第 1 层区域。
- （可选）**level-2** - 仅将间隔应用于第 2 层区域。
- *spf-max-wait* - 表示两次连续的 SPF 计算之间的最大间隔。范围为 1 到 120 秒。默认值为 10 秒。
- （可选）*spf-initial-wait* - 表示在首次 SPF 计算前、拓扑更改后的初始等待时间。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

  每个后续等待间隔都是上一个等待间隔的两倍，直到等待间隔达到指定的 SPF 最大等待间隔为止。
- （可选）*spf-second-wait* - 表示首次 SPF 计算与第二次 SPF 计算之间的间隔。范围为 1 到 120,000 毫秒。默认值为 5500 毫秒（5.5 秒）。

仅当拓扑更改后，才会执行 SPF 计算。此命令将控制软件执行 SPF 计算的频率。

注释
SPF 计算是处理器密集型的作业。因此，限制完成此计算的频率可能非常有用，尤其是在区域较大并且拓扑经常更改时。增大 SPF 间隔将减轻 ASA 的处理器负载，但有可能降低收敛速率。

步骤 11 配置 BGP、Connected、IS-IS、OSPF 或 Static 路由重新分发：
redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric 编号

示例：

```
ciscoasa(config-router-af)# redistribute static level-1 metric-type internal metric 6
```

metric *number* - 指标的值。范围为 1 到 4294967295。

步骤 12 具体而言，将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级：
redistribute isis {level-1 | level-2} into {level-2 | level-1} [[distribute-list *list-number* | **[route-map** *map-tag*]]

示例：

```
ciscoasa(config-router-af)# redistribute isis level-1 into level-2
distribute-list 100
```

- **level-1 | level-2** - 重新分配 IS-IS 路由的来源和目标级别。
- **into** - 将正在重新分发的路由级别与将路由重新分发到的级别分隔开的关键字。
- （可选）**distribute-list** *list-number* - 控制 IS-IS 重新分发的分发列表数。您可以指定分发列表或路由映射，而不是同时指定两者。
- （可选）**route-map** *map-tag* - 控制 IS-IS 重新分发的路由映射的名称。您可以指定分发列表或路由映射，而不是同时指定两者。

注释
您必须指定 **metric-style wide** 命令才能使 **redistribute isis** 命令正常工作。请参阅此程序的第 1 步。

在 IS-IS 中，所有区域都是末节区域，这意味着不会将主干（第 2 级）中的任何路由信息泄漏到末节区域（第 1 级）。仅第 1 级路由器使用到其区域内最近的 Level 1-Level 2 路由器的默认路由。此命令使您可以将第 2 级 IP 路由重新分发到第 1 级区域。此重新分发使仅第 1 级路由器可以选择 IP 前缀的最佳路径来离开区域。这是一个仅 IP 功能，CLNS 路由仍为末节路由。

注释
要提高控制力和稳定性，您可以配置分发列表或路由映射，以控制可以重新分发到第 1 级的第 2 级 IP 路由。这使大型 IS-IS-IP 网络可以使用区域获得更好的可扩展性。

步骤 13 为 IS-IS IPv6 路由创建汇聚前缀：

summary-prefix *ipv6-prefix* **[level-1 | level-1-2 | level-2]**

示例：

```
cisco(config-router-af)# summary-prefix 2001::/96 level-1
```

- *ipv6 address* - X.X.X.X.::X/0-128 形式的 IPv6 前缀。
- （可选）**level-1** - 仅重新分发到第 1 级的路由通过配置的地址和掩码值汇总。
- （可选）**level-1-2** - 将路由重新分发到第 1 级和第 2 级 IS-IS，以及第 2 级 IS-IS 将第 1 级路由通告为在其区域内可访问时，会应用汇总路由。
- （可选）**level-2** - 第 1 级路由了解的路由通过配置的地址和掩码值汇总到第 2 级主干。重新分发到第 2 级 IS-IS 中的路由也会汇总。

监控 IS-IS

可以使用以下命令监控 IS-IS 路由进程。有关命令输出的示例和说明，请参阅命令参考。

监控 IS-IS 数据库

使用以下命令监控 IS-IS 数据库：

- **show isis database [level-1 | l1] [level-2 | l2] [detail]** - 显示第 1 级、第 2 级 IS-IS 链路状态数据库，以及每个 LSP 的详细内容。
- **show isis database verbose** - 显示有关 IS-IS 数据库的详细信息，例如 LSP 的序列号、校验和以及保持时间。

监控 IS-IS 映射表条目

使用以下命令监控 IS-IS 主机名：

show isis hostname- 显示 IS-IS 路由器的路由器名称到系统 ID 映射表条目。

监控 IS-IS IPv4

使用以下命令监控 IS-IS IPv4：

- **show isis ip rib**- 显示 IS-IS 路由进程的 IPv4 地址系列特定的 RIB。
- **show isis ip spf-log**- 显示 IS-IS 路由进程的 IPv4 地址系列特定的 SPF 日志。
- **show isis ip topology**- 显示 IS-IS 路由进程的 IPv4 地址系列特定的拓扑。
- **show isis ip redistribution** [**level-1** | **level-2**] [*network-prefix*] - 显示获知的 IS-IS 和安装的 IPv6 路由。
- **show isis ip unicast**- 显示 IPv4 地址系列特定的 RIB、SPF 日志以及 ISes 路径。

监控 IS-IS IPv6

使用以下命令监控 IS-IS IPv6：

- **show isis ipv6 rib**- 显示 IS-IS 路由进程的 IPv6 地址系列特定的 RIB。
- **show isis ipv6 spf-log**- 显示 IS-IS 路由进程的 IPv6 地址系列特定的 SPF 日志。

- **show isis ipv6 topology**- 显示 IS-IS 路由进程的 IPv6 地址系列特定的拓扑。
- **show isis ipv6 redistribution** [**level-1** | **level-2**] [*network-prefix*] - 显示获知的 IS-IS 和安装的 IPv6 路由。
- **show isis ipv6 unicast**- 显示 IPv6 地址系列特定的 RIB、SPF 日志以及 ISes 路径。

监控 IS-IS 日志

使用以下命令监控 IS-IS 日志：

- **show isis lsp-log**- 显示触发新 LSP 的接口的第 1 级和第 2 级 IS-IS LSP 日志。
- **show isis spf-log**- 显示 ASA 运行 SPF 计算的频率

监控 IS-IS 协议

使用以下命令监控 IS-IS 协议：

show clns protocol - 显示 ASA 上每个 IS-IS 路由进程的协议信息。

监控 IS-IS 邻居和路由

使用以下命令监控 IS-IS 邻居：

- **show isis topology** - 显示所有区域中所有连接的路由器的列表。此命令可验证所有区域中所有路由器的存在性及其连接性。
- **show isis neighbors [detail]** - 显示 IS-IS 邻接关系信息。
- **show clns neighbors** [*process-tag*] [*interface-name*] [**detail**] - 显示终端系统 (ES)、中间系统 (IS) 和多拓扑 IS-IS (M-ISIS) 邻居。此命令显示通过 IPv6 的多拓扑 IS-IS 了解的邻接关系。
- **show clns is-neighbors** *[interface-name]* **[detail]** - 显示 IS-IS 设备邻接关系的 IS-IS 信息。

监控 IS-IS RIB

使用以下命令监控 IS-IS RIB：

- **show isis rib** [*ip-address* | *ip-address-mask*] - 显示特定路由或 RIB 中存储的主要网络下所有路由的路径。
- **show isis rib redistribution** [**level-1** | **level-2**] [*network-prefix*] - 显示本地重新分发缓存中的前缀。
- **show route isis** 显示路由表的当前状态。

监控 IS-IS 流量

使用以下命令监控 IS-IS 流量：

show clns traffic [since {bootup | show}] - 显示 ASA 已了解的 CLNS 流量统计信息。

调试 IS-IS

使用以下命令调试 IS-IS：

debug isis [adj-packets | authentication | checksum-errors | ip | ipv6 | local-updates | [rptpcp;-errors | rob | snp-packets | spf-events | spf-statistics | spf-triggers | update-packets]- 调试 IS-IS 路由协议的各个方面。

IS-IS 的历史记录

表 *41: IS-IS* 的功能历史记录

功能名称	平台版本	功能信息
IS-IS 路由	9.6(1)	ASA 现在支持中间系统到中间系统 (IS-IS) 路由协议。添加了对使用 IS-IS 路由协议进行路由数据、执行身份验证和重新分发及监控路由信息的支持。 引入了以下命令： **advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, router isis, set-attached-bit, set-overload-bit, show clns, show isis, show route isis, spf-interval, summary-address**.

IS-IS 示例

本部分针对 IS-IS 的不同方面及介绍拓扑配置示例。

IS-IS 路由配置

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   isis
```

IS-IS IPv6 路由配置

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   ipv6 address 2001:192:16:32::1/64
   ipv6 router isis
```

同一区域内的动态路由

```
iRouter --------(inside G0/1) ASA (G0/0 outside)------------ oRouter

ASA Configuration
  interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   ipv6 address 2001:192:16:32::1/64
   isis
   ipv6 router isis

  interface GigabitEthernet0/1
   nameif inside
   security-level 100
   ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
   ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
   isis
   ipv6 router isis

  router isis
   net 49.1234.2005.2005.2005.00
   is-type level-1
   metric-style wide

  interface GigabitEthernet0/0
   ip address 172.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:16:32::3/64
   ipv6 router isis
   isis priority 120

  interface GigabitEthernet0/1
   ip address 172.26.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:26:32::3/64
   ipv6 router isis

IOS Configuration
  iRouter
  router isis
   net 49.1234.2035.2035.2035.00
   is-type level-1
   metric-style wide

  oRouter
  interface GigabitEthernet0/0
   ip address 192.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:192:16:32::3/64
   ipv6 router isis

  oRouter
```

```
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis

 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

多个区域内的动态路由

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis

 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis

 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 5
  exit-address-family
 !

IOS Configuration
 iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120


 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis


 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
```

```
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide
```

重叠区域内的动态路由

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis

interface GigabitEthernet0/0.301
 nameif outside
```

```
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis

router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family

IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis priority 120
 isis ipv6 metric 600


interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
 metric-style wide
 maximum-paths 6
!
 address-family ipv6
 summary-prefix 2001::/8 tag 301
 summary-prefix 6001::/16 level-1-2 tag 800
 redistribute static metric 800 level-1-2
exit-address-family


oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip pim sparse-dense-mode
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis
 isis tag 301
```

```
oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

ASA Configuration
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family
!
```

路由重分布

```
iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis


 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 6
 exit-address-family
!

IOS Configuration
iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
```

```
 isis priority 120


iRouter
interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide
```

汇总地址

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis
```

```
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 redistribute static
 maximum-paths 5
address-family ipv6 unicast
 maximum-paths 6
exit-address-family
```

被动接口

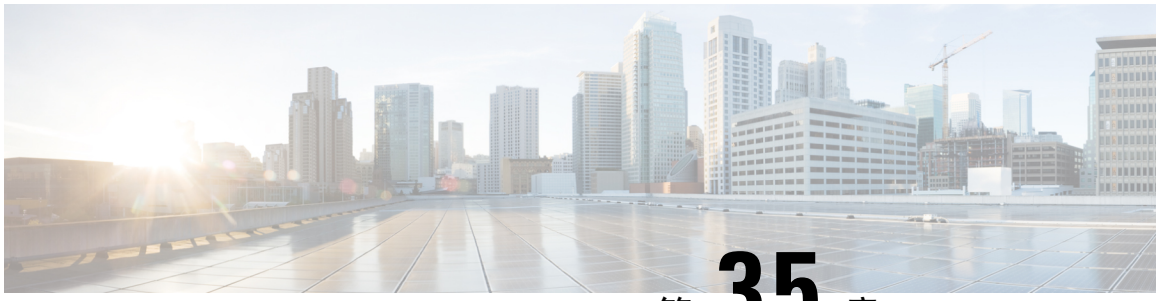
```
 iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0
  ipv6 address 2001:192:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0
  ipv6 address 2001:172:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/2
  nameif dmz
  security-level 0
  ip address 40.40.50.1 255.255.255.0
  ipv6 address 2040:95::1/64


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  passive-interface default

IOS Configuration
 iRouter
  interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120

 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
```

```
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis

iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis

oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis

oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide
```

身份验证

```
ASA ------------ Router

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
 ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
 ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
 isis
 ipv6 router isis


router isis
 net 49.1234.2005.2005.2005.00
 metric-style wide
 authentication mode md5
 authentication key cisco#123 level-2
```

```
IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis authentication mode md5
 isis authentication key-chain KeyChain level-2
 isis priority 120
 isis ipv6 metric 600


iRouter
key chain KeyChain
 key 1
  key-string cisco#123


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
```



第 35 章

EIGRP

本章介绍如何使用增强型内部网关路由协议 (EIGRP) 配置 ASA，以路由数据、执行身份验证以及重新分发路由信息。

- 关于 EIGRP，第 1125 页
- EIGRP 准则，第 1127 页
- 配置 EIGRP，第 1128 页
- 自定义 EIGRP，第 1130 页
- 配置 EIGRPv6 进程，第 1145 页
- EIGRP 监控，第 1150 页
- EIGRP 示例，第 1152 页
- EIGRP 的历史记录，第 1153 页

关于 EIGRP

EIGRP 是思科开发的增强版的 IGRP。与 IGRP 和 RIP 不同，EIGRP 不发送定期路由更新。仅在网络拓扑发生更改时才会发送 EIGRP 更新。将 EIGRP 与其他路由协议区分开来的主要功能包括快速收敛、支持可变长度子网掩码、支持部分更新以及支持多个网络层协议。

运行 EIGRP 的路由器会存储所有邻居路由表，以便可以迅速适应备用路由。如果不存在合适的路由，则 EIGRP 会查询其邻居以发现备用路由。这些查询会传播直至找到备用路由为止。对可变长度子网掩码功能的支持允许在网络号边界自动汇总路由。此外，还可以将 EIGRP 配置为在任何接口的任何位边界汇总。EIGRP 不会定期更新。相反，它仅在路由指标发生更改时才发送部分更新。部分更新的传播是自动绑定的，以便仅对需要该信息的路由器进行更新。得益于这两项功能，EIGRP 与 IGRP 相比可显著减少占用的带宽。

邻居发现是 ASA 用于动态获悉直连网络中其他路由器的过程。EIGRP 路由器发出组播 Hello 数据包，通告其在网络中的存在状态。当 ASA 收到来自新邻居的问候数据包时，会将其包含初始化位集的拓扑表发送至邻居。当邻居收到包含初始化位集的拓扑更新时，邻居将其拓扑表发回到 ASA。

Hello 数据包作为组播消息发出。预期不对 Hello 消息作出响应。但对静态定义的邻居除外。如果您使用 **neighbor** 命令或在 ASDM 中配置呼叫间隔以配置一个邻居，则发送到该邻居的 Hello 消息将作为单播消息发送。路由更新和确认消息作为单播消息发出。

一旦邻居关系建立后，除非网络拓扑发生更改，否则便不会交换路由更新。邻居关系通过 Hello 数据包来维护。从邻居收到的每个 Hello 数据包均包括保持时间。这是 ASA 预期可收到来自该邻居的 Hello 数据包的时间。如果 ASA 在保持时间内未收到由该邻居通告的 Hello 数据包，则 ASA 会将该邻居视为不可用。

EIGRP 协议使用四种关键算法技术，包括邻居发现/恢复、可靠的传输协议 (RTP) 和对于路由计算非常重要的 DUAL。DUAL 将目标的所有路由都保存在拓扑表中，而不只是保存最低成本路由。最低成本路由会插入到路由表中。其他路由则保留在拓扑表中。如果主路由发生故障，可以从可行后继路由中选择另一个路由。后继路由是指用于进行数据包转发的具有到达目标的最低成本路径的邻居路由器。可行性计算可确保路径不是路由环路的一部分。

如果在拓扑表中找不到可行后继路由，则必须重新计算路由。在路由重新计算期间，DUAL 会查询 EIGRP 邻居获取路由，该邻居反过来又会查询其邻居。当路由器没有可用于路由的可行后继路由时，会返回一个无法访问消息。

在路由重新计算期间，DUAL 会将路由标记为活动状态。默认情况下，ASA 等待三分钟接收来自其邻居的响应。如果 ASA 未收到来自邻居的响应，则会将路由标记为陷入主动状态。系统会删除拓扑表中作为可行性后继路由指向无响应邻居的所有路由。

注释 如果没有 GRE 隧道，则 EIGRP 邻居关系就不会通过 IPSec 隧道受到支持。

EIGRPv6

可以像 EIGRP IPv4 一样配置 EIGRP for IPv6。EIGRPv6 仅与 IPv6 对等体通信，并且仅通告 IPv6 路由。EIGRPv6 在许多方面与 EIGRPv4 类似：

- DUAL 用于具有相同度量的路由计算和选择。
- 它可扩展到大型网络实施。
- 维护邻居表、路由表和拓扑表。
- 提供等价负载均衡和非等价负载均衡。

但是，EIGRPv6 在许多方面与 EIGRPv4 不同，例如：

- IPv6 中不使用 network 命令； EIGRP 使用链路进行配置。
- 在配置期间，必须在每个接口上显式启用 EIGRPv6。

Null0 和 EIGRP

默认情况下，EIGRP 会将 Null0 路由作为汇总路由通告给对等体，以防止通告该汇总路由的路由器转发它没有路由的任何数据包。

例如，考虑两个路由器 R1 和 R2。R1 上的三个接口具有以下网络：192.168.0.0/24、192.168.1.0/24 和 192.168.3.0/24。使用汇总路由 192.168.0.0/22 配置 R1 并将其通告给 R2。当 R2 有一个发往 192.168.2.x 的 IP 数据包时，它会将其转发给 R1。R1 会丢弃该数据包，因为它的路由表中没有 192.168.2.x。但是，如果 R1 也连接到 ISP，并且它有一个指向 ISP 的默认路由，则 192.168.2.x 数据

包会转发到 ISP。为了防止此转发操作，EIGRP 会生成一个与汇总路由匹配的条目，指向 Null0。因此，当收到发往 192.168.2.x 的数据包时，R1 将丢弃该数据包，而不是使用默认路由。

EIGRP 准则

防火墙模式准则

仅在路由防火墙模式下受支持。不支持透明防火墙模式。

集群准则

对于单个接口模式下的集群，EIGRP 可以使用集群池作为路由器 ID 与集群对等体形成邻居关系。

IPv6 准则

支持 IPv6 路由。

情景准则

- 由于默认情况下不支持跨共享接口的情景间组播流量交换，因此 EIGRP 实例不能跨共享接口相互建立邻接关系。但是，您可以使用 EIGRP 进程下 EIGRP 进程配置中的静态邻居配置，在共享接口上建立 EIGRP 邻居关系。
- 在单独的接口上支持情景间 EIGRP。

重新分配准则

在属于 OSPF 网络的设备上配置 EIGRP 时，请确保将 OSPF 路由器配置为标记路由（EIGRP 不支持路由标记）。

将 EIGRP 重新分发到 OSPF 并将 OSPF 重新分发到 EIGRP 时，如果其中一个链路、接口中断，甚至当路由发起方关闭时，就会发生路由环路。为了防止将路由从一个域重新分发回同一域，路由器可以在重新分发时标记属于某个域的路由，并且可以根据相同的标记在远程路由器上过滤这些路由。由于这些路由不会安装到路由表中，因此它们不会重新分发到同一域中。

其他准则

- 最多支持一个 EIGRP 进程。
- 每当应用配置更改时，都会发生 EIGRP 邻接摆动，这会导致修改邻居发送或接收的路由信息（尤其是在分发列表、偏移列表中）和更改汇总。路由器同步后，EIGRP 会在邻居之间重新建立邻接关系。断开并重新建立邻接关系后，系统将清除邻居之间的所有已获知路由，并使用新的分发列表重新执行邻居之间的完整同步。
- 对 EIGRP 邻居的最大数量没有限制。但是，为了防止不必要的 EIGRP 摆动，建议您将数量限制为每设备 500 个。

配置 EIGRP

本节介绍如何在系统中启用 EIGRP 进程。启用 EIGRP 后，请参阅以下各节了解如何在系统中自定义 EIGRP 进程。

启用 EIGRP

只能在 ASA 中启用一个 EIGRP 路由进程。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp as-num

示例：

```
ciscoasa(config)# router eigrp 2
```

要启用 EIGRP IPv6 路由进程，请输入以下命令：

as-num 参数为 EIGRP 路由进程的自主系统编号。

步骤 2 配置参与 EIGRP 路由的接口和网络：

network ip-addr [mask]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

可以使用此命令配置一个或多个 **network** 语句。

ASA 将通告位于已定义网络范围内的直连和静态网络。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅为 EIGRP 配置接口，第 1131 页。

启用 EIGRP 末节路由

您可以启用并将 ASA 配置为 EIGRP 末节路由器。末节路由可减小 ASA 上的内存和处理要求。作为末节路由器，ASA 不需要维护完整的 EIGRP 路由表，因为它会将所有非本地流量转发到分发路由器。通常情况下，除了发送末节路由器的默认路由以外，分布路由器不需要发送任何其他信息。

只有指定的路由会从末节路由器传播到分布路由器。作为末节路由器，ASA 可使用消息“inaccessible”响应对汇总、连接的路由、重新分发的静态路由、外部路由和内部路由的所有查询。将ASA配置为末节时，它会向所有邻接路由器发送一个特殊的对等信息数据包以作为末节路由器报告其状态。收到通知其末节状态数据包的任何邻居都不会查询末节路由器是否存在任何路由，且具有末节对等体的路由器也不会查询该对等体。末节路由器依赖于分布路由器将正确的更新发送到所有对等体。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp as-num

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数为 EIGRP 路由进程的自主系统编号。

步骤 2 配置参与 EIGRP 路由的接口和网络：

network ip-addr [mask]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

可以使用此命令配置一个或多个 **network** 语句。

ASA 将通告位于已定义网络范围内的直连和静态网络。此外，只有IP地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与EIGRP路由，但是该接口已连接到希望通告的网络，请参阅配置被动接口，第 1133 页一节。

步骤 3 配置末节路由进程：

eigrp stub {**receive-only** | [**connected**] [**redistributed**] [**static**] [**summary**]}

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# eigrp stub {receive-only | [connected] [redistributed] [static]
[summary]}
```

必须指定哪些网络由末节路由进程向分布路由器通告。静态网络和已连接网络不会自动重新分发到末节路由进程。

注释

末节路由进程不维护完整的拓扑表。末节路由至少需要分布路由器的一个默认路由，以做出路由决策。

自定义 EIGRP

本节介绍如何自定义 EIGRP 路由。

为 EIGRP 路由进程定义网络

通过网络表，可指定 EIGRP 路由进程所使用的网络。对于参与 EIGRP 路由的接口，它必须位于网络条目定义的地址范围内。对于要通告的直连网络和静态网络，它们也必须位于网络条目的范围内。

网络表显示为 EIGRP 路由进程配置的网络。表的每一行显示为指定的 EIGRP 路由进程配置的网络地址和关联掩码。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp as-num

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数为 EIGRP 路由进程的自主系统编号。

步骤 2 配置参与 EIGRP 路由的接口和网络：

network ip-addr [mask]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

可以使用此命令配置一个或多个 **network** 语句。

ASA 将通告位于已定义网络范围内的直连和静态网络。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅配置被动接口，第 1133 页。

为 EIGRP 配置接口

如果不希望一个接口参与EIGRP路由，但是该接口已连接到您希望通告的网络，您可以配置**network**中包含该接口所连接网络的命令，并使用**passive-interface**命令阻止该接口发送或接收EIGRP更新。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp as-num

示例：

```
ciscoasa(config)# router eigrp 2
```

要启用 EIGRP IPv6 路由进程，请输入以下命令：

ipv6 router eigrp as-num

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 参数为 EIGRP 路由进程的自主系统编号。

步骤 2 配置参与 EIGRP 路由的接口和网络：

network ip-addr [mask]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

可以使用此命令配置一个或多个 network 语句。但是，在 EIGRP IPv6 中不使用 **network** 命令。

ASA将通告位于已定义网络范围内的直连和静态网络。此外，只有IP地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅为 EIGRP 路由进程定义网络，第 1130 页。

步骤 3 控制默认候选路由信息的发送或接收：

no default-information {**in** | **out** | **WORD**}

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

输入 **no default-information in** 命令会导致在收到的路由中阻止候选默认路由位。

输入 **no default-information out** 命令会禁用已通告路由中默认路由位的设置。

有关详细信息，请参阅配置 EIGRP 中的默认信息，第 1143 页。

步骤 4 启用 EIGRP 数据包的 MD5 身份认证：

authentication mode eigrp as-num **md5**

示例：

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

as-num 参数是在 ASA 中配置的 EIGRP 路由进程的自治系统编号。如果 EIGRP 未启用或者如果输入错误编号，则 ASA 会返回以下错误消息：

```
% Asystem(100) specified does not exist
```

有关详细信息，请参阅在接口上启用 EIGRP 身份验证，第 1135 页。

步骤 5 设置延迟值：

delay 值

示例：

```
ciscoasa(config-if)# delay 200
```

输入的 *value* 参数以每 10 毫秒为单位。要设置延迟 2000 微秒，请输入 200 作为 *value* 的值。

要查看分配至接口的延迟值，请使用 **show interface** 命令。

有关详细信息，请参阅更改接口延迟值，第 1134 页。

步骤 6 更改呼叫间隔：

hello-interval eigrp as-num seconds

示例：

```
ciscoasa(config)# hello-interval eigrp 2 60
```

有关详细信息，请参阅自定义 EIGRP 呼叫间隔和保持时间，第 1141 页。

步骤 7 更改保持时间：

hold-time eigrp as-num seconds

示例：

```
ciscoasa(config)# hold-time eigrp 2 60
```

有关详细信息，请参阅自定义 EIGRP 呼叫间隔和保持时间，第 1141 页。

配置被动接口

可以将一个或多个接口配置为被动接口。在 EIGRP 中，被动接口既不发送也不接收路由更新。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp as-num

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数为 EIGRP 路由进程的自主系统编号。

步骤 2 配置参与 EIGRP 路由的接口和网络。可以使用此命令配置一个或多个 **network** 语句。

network ip-addr [mask]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

ASA 将通告位于已定义网络范围内的直连和静态网络。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅为 EIGRP 路由进程定义网络，第 1130 页。

步骤 3 阻止接口发送或接收 EIGRP 路由消息。

passive-interface {**default** | if-name}

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# passive-interface {default}
```

使用 **default** 关键字将会在所有接口上禁用 EIGRP 路由更新。按照 **nameif** 命令的定义指定接口名称将会在指定接口上禁用 EIGRP 路由更新。可以在 EIGRP 路由器配置中使用多个 **passive-interface** 命令。

在接口上配置汇总汇聚地址

可以逐个接口配置汇总地址。如果要创建不发生在网络编号编辑的汇总地址，或者要在禁用了自动路由汇总的 ASA 上使用汇总地址，则需要手动定义汇总地址。如果路由表中存在任何更具体的路由，则 EIGRP 将使用与所有更具体路由的最小值相等的指标从接口通告汇总地址。

过程

步骤 1 针对正在更改 EIGRP 所使用的延迟值的接口，进入接口配置模式：

interface phy_if

示例：

```
ciscoasa(config)# interface inside
```

步骤 2 创建汇总地址：

summary-address eigrp *as-num address mask* [*distance*]

示例：

```
ciscoasa(config-if)# summary-address eigrp 2 address mask [20]
```

要为 EIGRP IPv6 创建汇总地址，请执行以下操作：

ipv6 summary-address eigrp *as-num address mask* [*distance*]

示例：

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 summary-address eigrp 1 4001::1/64 ?
interface mode commands/options:
  <1-255>  Administrative distance
```

默认情况下，所定义的 EIGRP 汇总地址的管理距离为 5。可以通过在 **summary-address** 命令中指定可选的 *distance* 参数来更改此值。

更改接口延迟值

接口延迟值用于 EIGRP 距离计算。可以逐个接口修改该值。

过程

步骤 1 针对正在更改 EIGRP 所使用的延迟值的接口，进入接口配置模式：

interface phy_if

示例：

```
ciscoasa(config)# interface inside
```

步骤 2 设置延迟值：

delay 值

示例：

```
ciscoasa(config-if)# delay 200
```

输入的 *value* 参数以每 10 毫秒为单位。要设置 2000 微秒的延迟，可对 *value* 输入 200。

注释
要查看分配至接口的延迟值，请使用 **show interface** 命令。

在接口上启用 EIGRP 身份验证

EIGRP 路由身份验证提供对来自 EIGRP 路由协议的路由更新的 MD5 身份验证。每个 EIGRP 数据包中的 MD5 密钥摘要可防止从未批准的来源引入未经授权或虚假的路由消息。

系统会逐个接口配置 EIGRP 路由身份验证。必须使用相同的身份验证模式和密钥来配置接口上为 EIGRP 消息身份验证配置的所有 EIGRP 邻居，才能建立邻接关系。

注释 必须先启用 EIGRP，然后才能启用 EIGRP 路由身份验证。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp *as-num*

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2 配置参与 EIGRP 路由的接口和网络：

network *ip-addr* [*mask*]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

- 可以使用此命令配置一个或多个 network 语句。
- ASA 将通告位于已定义网络范围内的直连和静态网络。此外，只有 IP 地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。
- 如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅配置 EIGRP，第 1128 页。

步骤 3 针对正在配置 EIGRP 消息身份验证的接口，进入接口配置模式：

interface *phy_if*

示例：

```
ciscoasa(config)# interface inside
```

步骤 4 启用 EIGRP 数据包的 MD5 身份认证：

authentication mode eigrp *as-num* md5

示例：

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

as-num 参数是在 ASA 中配置的 EIGRP 路由进程的自治系统编号。如果 EIGRP 未启用或者如果输入错误编号，则 ASA 会返回以下错误消息：

```
% Asystem(100) specified does not exist
```

步骤 5 配置 MD5 算法所使用的密钥：

authentication key eigrp *as-num key* key-id *key-id*

示例：

```
ciscoasa(config)# authentication key eigrp 2 cisco key-id 200
```

- as-num 参数是在 ASA 中配置的 EIGRP 路由进程的自治系统编号。如果 EIGRP 未启用或者如果输入错误编号，则 ASA 会返回以下错误消息：

  ```
  % Asystem(100) specified does not exist%
  ```

- key 参数最多可包含 16 个字符，包括字母、数字和特殊字符。在 key 参数中不允许使用空格。
- key-id 参数是范围可从 0 到 255 的数字。

定义 EIGRP 邻居

EIGRP Hello 数据包以组播数据包的形式发送。如果 EIGRP 邻居位于整个非广播网络（例如隧道）内，则必须手动定义该邻居。当手动定义EIGRP邻居时，Hello数据包作为单播消息发送至该邻居。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp as-num

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数为 EIGRP 路由进程的自主系统编号。

步骤 2 配置参与 EIGRP 路由的接口和网络：

network ip-addr [mask]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

步骤 3 定义静态邻居：

neighbor *ip-addr* **interface** *if_name*

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

示例：

对于 EIGRP IPv6

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# neighbor 2001:DB8:0:ABCD::1 interface interface1
```

ip-addr 参数是邻居的 IP 地址。

if-name 参数是按照 **nameif** 命令指定的接口名称，邻居通过该名称可用。可以为 EIGRP 路由进程定义多个邻居。

注释
您必须配置参与 EIGRP 路由的接口网络，才能使邻居关系配置生效。

将路由重新分发到 EIGRP 中

您可以将 RIP 和 OSPF 发现的路由重新分布到 EIGRP 路由过程中。您还可以将静态路由和已连接路由重新分布到 EIGRP 路由过程中。如果已连接路由位于 EIGRP 配置中的 **network** 语句范围内，则无需将其重新分布。

注释　仅适用于 RIP：开始此程序之前，必须创建路由映射，以进一步定义将指定路由协议中的哪些路由重新分发到 RIP 路由进程。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp as-num

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数为 EIGRP 路由进程的自主系统编号。

步骤 2 （可选）指定应该应用于已重新分发到 EIGRP 路由进程的路由的默认指标：

default-metric bandwidth delay reliability loading mtu

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# default-metric bandwidth delay reliability loading mtu
```

如果未在 EIGRP 路由器配置中指定默认指标，则必须在每个 **redistribute** 命令中指定指标值。如果在 **redistribute** 命令中指定 EIGRP 指标且在 EIGRP 路由器配置中有 **default-metric** 命令，则使用 **redistribute** 命令中的指标。

步骤 3 将已连接路由重新分发到 EIGRP 路由进程。

redistribute connected [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

示例：

```
ciscoasa(config-router)# redistribute connected [metric bandwidth delay reliability loading
 mtu] [route-map map_name]
```

如果在 EIGRP 路由器配置中没有 **default-metric** 命令，则必须在 **redistribute** 命令中指定 EIGRP 指标值。

步骤 4 将静态路由重新分发到 EIGRP 路由进程：

redistribute static [**route-map** map_name]

示例：

```
ciscoasa(config-router)# redistribute static [route-map map_name]
```

此命令将把所有静态路由传递给 EIGRP。要重新分配选择性静态路由，请确保使用静态路由创建访问列表，然后将其包含在路由映射表中：

示例：

```
ciscoasa(config)# ip access-list extended R1_Loopback
ciscoasa(config-ext-nacl)#permit ip host 1.1.1.1 any
ciscoasa(config-ext-nacl)#exit

ciscoasa(config)#route-map Permit_to_Distribute
ciscoasa(config-route-map)#match ip address R1_Loopback
ciscoasa(config-route-map)#exit
```

在创建路由映射后，将其包含在 redistribute 命令中，如下所示：

示例：

```
ciscoasa(config)#router eigrp 2
ciscoasa(config-router)#redistribute static subnets route-map Permit_to_Distribute
```

步骤 5 将路由从 OSPF 路由进程重新分发到 EIGRP 路由进程：

redistribute ospf pid [**match** {**internal | external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** 带宽延迟可靠性负载 mtu] [**route-map** map_name]

示例：

```
ciscoasa(config-router): redistribute ospf pid [match {internal | external [1 | 2] |
nssa-external [1 | 2]}] [metric bandwidth delay reliability loading mtu] [route-map map_name]
```

步骤 6 将路由从 RIP 路由进程重新分发到 EIGRP 路由进程：

redistribute rip [**metric** 带宽延迟可靠性负载 mtu] [**route-map map_name**]

示例：

```
ciscoasa(config-router): redistribute rip [metric bandwidth delay
reliability load mtu] [route-map map_name]
```

在 EIGRP 中过滤网络

注释 开始此过程之前，必须创建标准ACL，以定义要通告的路由。也就是说，创建一个标准ACL，以定义要从发送或接收更新中过滤的路由。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp as-num

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数为 EIGRP 路由进程的自主系统编号。

步骤 2 配置参与 EIGRP 路由的接口和网络：

ciscoasa(config-router)# **network** ip-addr [mask]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

可以使用此命令配置一个或多个 network 语句。

ASA将通告位于已定义网络范围内的直连和静态网络。此外，只有IP地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅为 EIGRP 配置接口，第 1131 页。

步骤 3 过滤 EIGRP 路由更新中发送的网络：

distribute-list acl **out** [**connected** | **ospf** | **rip** | **static** | **interface** if_name]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router): distribute-list acl out [connected]
```

可以指定接口，以将过滤器仅应用于由该特定接口发送的更新。

可以在 EIGRP 路由器配置中输入多个 **distribute-list** 命令。

步骤 4 过滤 EIGRP 路由更新中接收的网络：

distribute-list acl **in** [**interface** if_name]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router): distribute-list acl in [interface interface1]
```

可以指定接口，以将过滤器仅应用于由该特定接口接收的更新。

自定义 EIGRP 呼叫间隔和保持时间

ASA 定期发送 Hello 数据包，以发现邻居以及获悉邻居何时变得无法访问或失效。默认情况下，每 5 秒发送一次 Hello 数据包。

问候数据包通告 ASA 保持时间。保持时间向 EIGRP 邻居指示邻居将路由器视为 ASA 可访问的时间长度。如果邻居在通告的保持时间内未收到 Hello 数据包，则将 ASA 视为无法访问。默认情况下，通告的保持时间是 15 秒（呼叫间隔的三倍）。

Hello 时间间隔和通告的保持时间均逐个接口进行配置。我们建议将保持时间至少设置为呼叫间隔的三倍。

过程

步骤 1 进入输入接口配置模式（针对正在配置呼叫间隔或通告保持时间的接口）：

interface phy_if

示例：

```
ciscoasa(config)# interface inside
```

步骤 2 更改呼叫间隔：

hello-interval eigrp as-num seconds

示例：

```
ciscoasa(config)# hello-interval eigrp 2 60
```

要更改 EIGRP IPv6 的 Hello 间隔，请执行以下操作：

ipv6 hello-interval eigrp as-num seconds

示例：

```
ciscoasa(config)# ipv6 hello-interval eigrp 2 60
```

步骤 3 更改保持时间：

hold-time eigrp as-num seconds

示例：

```
ciscoasa(config)# hold-time eigrp 2 60
```

要更改 EIGRP IPv6 的保持时间，请执行以下操作：

ipv6 hold-time eigrp as-num seconds

示例：

```
ciscoasa(config)# ipv6 hold-time eigrp 2 60
```

禁用自动路由汇总

默认情况下已启用自动路由汇总。EIGRP 路由进程在网络号边界上汇总。如果存在非连续网络，这可能会引起路由问题。

例如，如果路由器同时连接到 192.168.1.0、192.168.2.0 和 192.168.3.0 网络，且这些网络全部参与 EIGRP，则 EIGRP 路由进程会为这些路由创建汇总地址 192.168.0.0。如果另一个路由器添加到网络 192.168.10.0 和 192.168.11.0，且这些网络均参与 EIGRP，则它们也会汇总为 192.168.0.0。为防止可能出现的将流量路由到错误位置，应在创建冲突性汇总地址的路由器上禁用自动路由汇总。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp as-num

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数为 EIGRP 路由进程的自主系统编号。

步骤 2 禁用自动路由汇总：

no auto-summary

示例：

```
ciscoasa(config-router)# no auto-summary
```

自动汇总地址的默认管理距离为 5。

配置 EIGRP 中的默认信息

可以控制EIGRP更新中默认路由信息的发送和接收。默认情况下，将发送并接受默认路由。将ASA配置为禁止接收默认信息会导致已接收路由中的备选默认路由位被阻止。将ASA配置为禁止发送默认信息会禁用已通告路由中的默认路由位设置。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

router eigrp as-num

示例：

```
ciscoasa(config)# router eigrp 2
```

as-num 参数为 EIGRP 路由进程的自主系统编号。

步骤 2 配置参与 EIGRP 路由的接口和网络：

network ip-addr [mask]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

可以使用此命令配置一个或多个 network 语句。

ASA将通告位于已定义网络范围内的直连和静态网络。此外，只有IP地址在已定义网络范围内的接口才可参与 EIGRP 路由进程。

如果不希望一个接口参与 EIGRP 路由，但是该接口已连接到希望通告的网络，请参阅为 EIGRP 配置接口，第 1131 页。

步骤 3 控制默认候选路由信息的发送或接收：

no default-information {**in** | **out** | **WORD**}

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

注释

输入 **no default-information in** 命令会导致在收到的路由中阻止候选默认路由位。输入 **no default-information out** 命令会禁用已通告路由中默认路由位的设置。

禁用 EIGRP 水平分割

水平分割用于控制EIGRP更新和查询数据包的发送。在接口上启用水平分割时，不会为以此接口为下一跳的目标发送更新和查询数据包。以这种方式控制更新和查询数据包可降低路由环路的可能性。

默认情况下，所有接口上均启用水平分割。

水平分割可阻止路由器通告的路由信息从产生该信息的所有接口传出。此行为通常可优化多个路由设备之间的通信，尤其是在链路中断时。但是，使用非广播网络时，可能出现此行为不如人意的情况。对于这些情况，包括配置了 EIGRP 的网络，可能要禁用水平分割。

如果在某个接口上禁用水平分割，则必须同时在该接口上的所有路由器和接入服务器禁用水平分割。

要禁用 EIGRP 水平分割，请执行以下步骤：

过程

步骤 1 针对正在更改 EIGRP 所使用的延迟值的接口，进入接口配置模式：

interface phy_if

示例：

```
ciscoasa(config)# interface phy_if
```

步骤 2 禁用水平分割：

no split-horizon eigrp *as-number*

示例：

```
ciscoasa(config-if)# no split-horizon eigrp 2
```

要为 EIGRP IPv6 禁用水平分割，请执行以下操作：

no ipv6 split-horizon eigrp *as-number*

示例：

```
ciscoasa(config-if)# no ipv6 split-horizon eigrp 2
```

重新启动 EIGRP 进程

您可以重新启动 EIGRP 进程，也可以清除重分发计数器或清除计数器。

过程

重新启动 EIGRP 进程，或者清除重分发计数器或清除计数器：

clear eigrp pid {**1-65535** | **neighbors** | **topology** | **events)**}

示例：

```
ciscoasa(config)# clear eigrp pid 10 neighbors
```

配置 EIGRPv6 进程

本节介绍如何在系统中启用和配置 EIGRP IPv6 进程。

启用 EIGRPv6

只能在 ASA 中启用一个 EIGRPv6 路由进程。

过程

创建 EIGRP 路由进程，并进入此 EIGRP IPv6 进程的路由器配置模式：

ipv6 router eigrp *as-num*

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

EIGRPv6 中的过滤器规则

注释 开始此过程之前，必须创建标准ACL，以定义要通告的路由。也就是说，创建一个标准ACL，以定义要从发送或接收更新中过滤的路由。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

ipv6 router eigrp as-num

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2 将前缀列表应用于从接口通告的 IPv6 路由更新的 EIGRP：

distribute-list prefix-list name **out interface** if_name

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# distribute-list acl out interface interface2
```

可以在 EIGRPv6 路由器配置中输入多个 **distribute-list** 命令。

步骤 3 将前缀列表应用于 EIGRP 以获取在接口上接收的 IPv6 路由更新：

distribute-list prefix-list name **in** [**interface** if_name]

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# distribute-list acl in interface interface1
```

为 EIGRPv6 配置接口

如果不希望一个接口参与EIGRP路由，但是该接口已连接到您希望通告的网络，您可以配置其中包含该接口所连接网络的 **passive-interface** 命令， 阻止该接口发送或接收 EIGRP 更新。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP IPv6 进程的路由器配置模式：

ipv6 router eigrp as-num

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2 控制默认候选路由信息的发送或接收：

no default-information {**in** | **out** | **WORD**}

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

输入 **no default-information in** 命令会导致在收到的路由中阻止候选默认路由位。

输入 **no default-information out** 命令会禁用已通告路由中默认路由位的设置。

有关详细信息，请参阅配置 EIGRP 中的默认信息，第 1143 页。

步骤 3 更改呼叫间隔：

ipv6 hello-interval eigrp as-num seconds

示例：

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 hello-interval eigrp 2 60
```

有关详细信息，请参阅自定义 EIGRP 呼叫间隔和保持时间，第 1141 页。

步骤 4 更改保持时间：

ipv6 hold-time eigrp as-num seconds

示例：

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 hold-time eigrp 2 60
```

有关详细信息，请参阅自定义 EIGRP 呼叫间隔和保持时间，第 1141 页。

为 EIGRPv6 配置被动接口

可以将一个或多个接口配置为被动接口。在 EIGRPv6 中，被动接口既不发送也不接收路由更新。

过程

步骤 1 创建 EIGRPv6 路由进程，并进入此 EIGRP IPv6 进程的路由器配置模式：

ipv6 router eigrp as-num

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2 阻止接口发送或接收 EIGRP 路由消息。

passive-interface {**default** | if-name}

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# passive-interface {default}
```

使用 **default** 关键字将会在所有接口上禁用 EIGRPv6 路由更新。按照 **nameif** 命令的定义指定接口名称将会在指定接口上禁用 EIGRP 路由更新。可以在 EIGRPv6 路由器配置中使用多个 **passive-interface** 命令。

将路由重新分发到 EIGRPv6

您可以将发现的 OSPF、BGP、ISIS 路由重新分配到 EIGRP IPv6 路由进程中。您还可以将静态路由和已连接路由重新分布到 EIGRP 路由过程中。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

ipv6 router eigrp as-num

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2 （可选）指定应该应用于已重新分发到 EIGRP 路由进程的路由的默认指标：

default-metric[bandwidth | delay | reliability | loading | mtu]

示例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# default-metric bandwidth 10 delay 20
```

如果未在 EIGRP 路由器配置中指定默认指标，则必须在每个 **redistribute** 命令中指定指标值。如果在 **redistribute** 命令中指定 EIGRP 指标且在 EIGRP 路由器配置中有 **default-metric** 命令，则使用 **redistribute** 命令中的指标。

注释
指定 default-metric 时，ASA 中的 show run-config 命令不会显示 default-metric 配置。

步骤 3 将已连接路由重新分发到 EIGRP 路由进程。

redistribute connected [**metric** bandwidth | delay | reliability | loading | mtu] [**route-map** map_name]

示例：

```
ciscoasa(config-router)# redistribute connected [metric bandwidth 100] [route-map map_name]
```

如果在 EIGRP 路由器配置中没有 **default-metric** 命令，则必须在 **redistribute** 命令中指定 EIGRP 指标值。

步骤 4 将静态路由重新分发到 EIGRP 路由进程：

redistribute static [**metric** bandwidth | delay | reliability | loading | mtu] [**route-map** map_name]

示例：

```
ciscoasa(config-router): redistribute static [route-map map_name]
```

步骤 5 将路由从 OSPF 路由进程重新分发到 EIGRP 路由进程：

redistribute ospf pid [**match** {**internal | external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** 带宽延迟可靠性负载 mtu] [**route-map** map_name]

示例：

```
ciscoasa(config-router)# redistribute ospf pid [match {internal | external [1 | 2] |
nssa-external [1 | 2]}][route-map map_name]
```

步骤 6 将 BGP 路由进程中的路由重新分发到 EIGRP 路由进程：

redistribute bgp [**metric** bandwidth delay reliability load mtu] [**route-map map_name**]

示例：

```
ciscoasa(config-router)# redistribute bgp [route-map map_name]
```

步骤 7 将 ISIS 路由进程中的路由重新分发到 EIGRP 路由进程：

redistribute isis [**level-1 | level-2 | level-1-2**][**include-connected | metric number | metric-type | tag | route-map map_name**]

示例：

```
ciscoasa(config-router)# redistribute isis [level-1] [metric delay 20 [route-map map_name]]
```

定义 EIGRPv6 邻居

EIGRP Hello 数据包以组播数据包的形式发送。如果 EIGRP 邻居位于整个非广播网络（例如隧道）内，则必须手动定义该邻居。当手动定义 EIGRP 邻居时，Hello 数据包作为单播消息发送至该邻居。

过程

步骤 1 创建 EIGRP 路由进程，并进入此 EIGRP 进程的路由器配置模式：

ipv6 router eigrp as-num

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 参数是 EIGRP 路由进程的自治系统编号。

步骤 2 定义静态邻居：

neighbor *ip-addr* **interface** *if_name*

示例：

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# neighbor 2001:DB8:0:ABCD::1 interface interface1
```

ip-addr 参数是邻居的 IP 地址。

if-name 参数是按照 **nameif** 命令指定的接口名称，邻居通过该名称可用。可以为 EIGRP 路由进程定义多个邻居。

EIGRP 监控

可以使用以下命令监控 EIGRP 路由进程。有关命令输出的示例和说明，请参阅命令参考。此外，您可以禁用邻居变更消息和邻居警告消息的日志记录。

如要监控或禁用多个 EIGRP 路由统计信息，请输入以下命令之一：

- **router-id**

  显示此 EIGRP 进程的 router-id。

- **show eigrp** [*as-number*] **events** [{*start end*} | **type**]

  显示 EIGRP 事件日志。

- **show eigrp** [*as-number*] **interfaces** [*if-name*] [**detail**]

  显示参与 EIGRP 路由的接口。

- **show eigrp** [as-number] **neighbors** [**detail** | **static**] [*if-name*]

  显示 EIGRP 邻居表。

- **show eigrp** [*as-number*] **topology** [*ip-addr* [**mask**] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  显示 EIGRP 拓扑表。

- **show eigrp** [*as-number*] **traffic**

  显示 EIGRP 流量统计信息。

- **show mfib cluster**

  显示有关转发条目和接口的 MFIB 信息。

- **show route cluster**

  显示有关集群的其他路由同步详细信息。

- **no eigrp log-neighbor-changes**

  禁用邻居变更消息的日志记录。在路由器配置模式下为 EIGRP 路由进程输入此命令。

- **no eigrp log-neighbor-warnings**

  禁用邻居警告消息的日志记录。

- **show ipv6 eigrp** *as-number* **interface** *interface*

  显示 EIGRP IPv6 拓扑表。

- **show ipv6 eigrp** [*as-number*] **traffic**

  显示 EIGRP IPv6 流量统计信息。

- **show ipv6 eigrp** [as-number] **neighbors** [*if-name*]

  显示 EIGRP IPv6 邻居表。

- **show ipv6 eigrp interfaces** [*if-name*]

  显示与给定接口相关的邻居信息。

- **show ipv6 eigrp** [*as-number*] **topology** [*ipv6-address* [**mask**] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  显示 EIGRP IPv6 拓扑表。

- **show ipv6 eigrp** [*as-number*] **events** [{*start* - *end*} | **type**]

  显示 EIGRP IPV6 事件日志。

- **show ipv6 eigrp timers**

  显示已配置的呼叫计时器和保持计时器。

EIGRP 示例

以下示例显示如何通过各种可选进程启用和配置 EIGRP：

过程

步骤 1 要启用 EIGRP，请输入以下命令：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

步骤 2 要配置从中发送或接收 EIGRP 路由消息的接口，请输入以下命令：

```
ciscoasa(config-router)# passive-interface {default}
```

步骤 3 要定义 EIGRP 邻居，请输入以下命令：

```
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

步骤 4 要配置参与 EIGRP 路由的接口和网络，请输入以下命令：

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

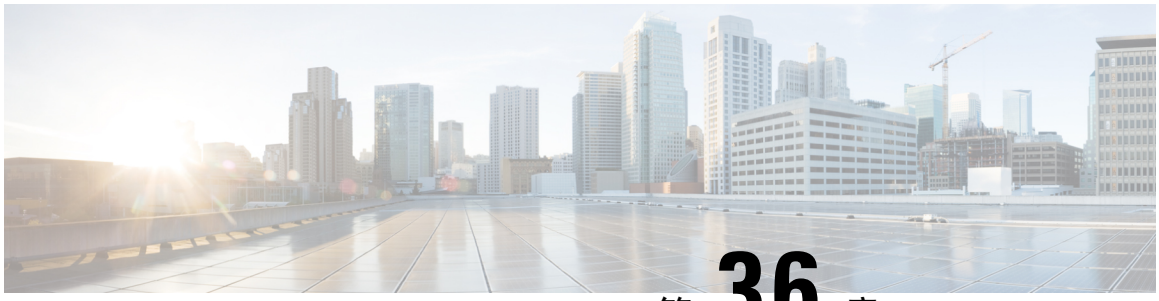
步骤 5 要更改用于 EIGRP 距离计算的接口延迟值，请输入以下命令：

```
ciscoasa(config-router)# exit
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# delay 200
```

EIGRP 的历史记录

表 *42: EIGRP* 的功能历史记录

功能名称	平台版本	功能信息
EIGRP 支持	7.0(1)	对于使用增强型内部网关路由协议 (EIGRP) 来路由数据、执行身份验证和重新分发及监控路由信息，添加了相应的支持。 引入了以下命令：**route eigrp**。
多情景模式下的动态路由	9.0(1)	在多情景模式下支持 EIGRP 路由。
集群	9.0(1)	对于EIGRP，在集群环境中支持批量同步、路由同步和第 2 层负载均衡。 引入或修改了以下命令：**show route cluster**、**debug route cluster**、**show mfib cluster**、**debug mfib cluster**。
EIGRP 自动汇总	9.2(1)	默认情况下，现已针对 EIGRP 禁用 Auto-Summary 字段。
EIGRPv6 支持	9.20(1)	对于使用增强型内部网关路由协议 (EIGRP) 来路由数据、执行身份验证和重新分发及监控路由信息，添加了 IPv6 支持。 我们引入了以下命令： **ipv6 eigrp**、 **ipv6 hello-interval eigrp**、 **ipv6 hold-time eigrp**、 **ipv6 split-horizon eigrp**、 **show ipv6 eigrp interface** 、 **show ipv6 eigrp traffic**、 **show ipv6 eigrp neighbors** 、 **show ipv6 eigrp interface**、 **ipv6 summary-address eigrp**、 **show ipv6 eigrp topology**、 **show ipv6 eigrp events** 、 **show ipv6 eigrp timers**、 **clear ipv6 eigrp** 和 **clear ipv6 router eigrp**。



第 36 章

组播路由

本章介绍如何将 ASA配置为使用组播路由协议。

- 关于组播路由， 第 1155 页
- 组播路由准则， 第 1158 页
- 启用组播路由， 第 1158 页
- 自定义组播路由， 第 1159 页
- PIM 监控， 第 1171 页
- 组播路由示例， 第 1172 页
- 组播路由的历史记录， 第 1172 页

关于组播路由

组播路由是一种带宽节省技术，通过同时向数千个公司收件人和家庭传送单一信息流来减少流量。使用组播路由的应用包括视频会议、公司通信、远程教育以及软件、股票报价和新闻的分发。

组播路由协议将源流量传递给多个接收者，而不会对源或接收者造成任何额外负担，而且是同类技术当中占用网络带宽最少的。组播数据包通过启用了协议无关组播 (PIM) 及其他支持性组播协议的 ASA 在网络中复制，是目前为止向多个接收者传输数据的最高效方式。

ASA 支持末节组播路由和 PIM 组播路由。但是，不能在一个 ASA 上都配置这两种路由。

注释 组播路由同时支持 UDP 和非 UDP 传输。但是，非 UDP 传输没有进行快速路径优化。

末节组播路由

末节组播路由提供动态主机注册并促进组播路由。如果针对末节组播路由进行了配置，ASA 将用作 IGMP 受托代理。ASA 将 IGMP 消息转发到上游组播路由器（上游组播路由器设置组播数据的传输），而不是完全参加组播路由。ASA 在为末节组播路由而配置后，就不能为 PIM 稀疏模式或双向模式而配置。您必须在参与 IGMP 末节组播路由的接口上启用 PIM。

ASA 同时支持 PIM-SM 和双向 PIM。PIM-SM 是一个组播路由协议，它使用基础单播路由信息库或支持组播的独立路由信息库。该协议会按组播组构建以单个交汇点 (RP) 为根的单向共享树，并且可以选择性地按组播源创建最短路径数。

PIM 组播路由

双向 PIM 是 PIM-SM 的一个变体，用于构建连接组播源和接收器的双向共享树。双向树使用每个组播拓扑链路上运行的专用转发器 (DF) 选择流程构建借助 DF，组播数据从源转发至交汇点 (RP)，然后联通共享树一起发送至接收器，而无需源特定的状态。DF 选择发生在 RP 发现期间，提供至 RP 的默认路由。

注释 如果 ASA 是 PIM RP，请使用 ASA 的未被转换的外部地址作为 RP 地址。

PIM 源特定组播支持

ASA 不支持 PIM 源特定组播 (SSM) 功能和相关配置。不过，ASA 允许与 SSM 相关的数据包通过，除非将其放置为最后一跳路由器。

SSM 被分类为数据传递机制，适用于一对多应用，如 IPTV。SSM 模型使用“通道”的概念，以 (S,G) 对表示，其中 S 表示源地址，G 表示 SSM 目标地址。通过使用组管理协议（如 IGMPv3）来实现订用通道。一旦SSM获悉某一特定的组播源，它将使接收客户端能直接从该源接收多播流，而不是从共享交汇点 (RP) 接收。SSM 中引入了访问控制机制，提供当前稀疏或疏-密模式实施无法提供的安全增强功能。

PIM-SSM 与 PIM-SM 不同，前者不使用 RP 或共享树。相反，组播组源地址上的信息将由接收方通过本地接收协议 (IGMPv3) 提供，并且用于直接构建源特定树。

PIM 自举路由器 (BSR)

PIM 自举路由器 (BSR) 是一个动态交汇点 (RP) 选择模型，它使用候选路由器执行 RP 功能以及中继组的 RP 信息。RP 功能包括 RP 发现并向 RP 提供默认路由。它执行此操作的方式是将一组设备配置为候选 BSR (C-BSR)，它们参与 BSR 选举过程，以从它们自身中选出一个 BSR。选择 BSR 后，配置为候选交汇点 (C-RP) 的设备将开始向选出的 BSR 发送其组映射。然后，BSR 会将组与 RP 的映射信息通过基于跳从 PIM 路由器传送至 PIM 路由器的 BSR 消息发至组播树下的其他所有设备。

此功能提供了一种动态获悉 RP 的方法，这在 RP 可能会定期关闭和启动的大型负载网络中非常重要。

PIM 引导程序路由器 (BSR) 术语

以下术语经常在 PIM BSR 配置中引用：

- 自举路由器 (BSR) - BSR 通过 PIM 逐跳向其他路由器通告交汇点 (RP) 信息。在多个候选 BSR 中，在选举过程后会选择单个 BSR。此自举路由器的主要目的是将所有候选 RP (C-RP) 通告收

集到称为 RP-set 的数据库中，并以 BSR 消息的形式定期（每 60 秒）将此数据库发送到该网络中的其他路由器。

- 自举路由器 (BSR) 消息— BSR 消息会组播到 TTL 为 1 的 All-PIM-Routers 组。收到这些消息的所有 PIM 邻居会将它们重新传输（TTL 同样为 1）到除收到消息的接口之外的所有接口。BSR 消息包含 RP 集合和当前活动 BSR 的 IP 地址。这是 C-RP 了解在何处单播其 C-RP 消息的方式。
- 候选自举路由器 (C-BSR) - 配置为候选 BSR 的某个设备会参与 BSR 选举机制。具有最高优先级的 C-BSR 会被选举作为 BSR。C-BSR 的最高 IP 地址作为决定因素。BSR 选举过程是优先的，例如，如果出现具有更高优先级的新 C-BSR，它会触发新的选举过程。
- 候选交汇点 (C-RP) - RP 作为组播数据源和接收器的交汇场所。配置为 C-RP 的设备会通过单播定期将组播组映射信息直接通告到选举的 BSR。这些消息包含组范围、C-RP 地址和保持时间。当前 BSR 的 IP 地址从网络中所有路由器收到的定期 BSR 消息获取。这样，BSR 可了解当前正在运行且可访问的 RP。

注释 ASA 不充当 C-RP，即使 C-RP 是 BSR 流量的强制性要求也是如此。仅路由器可以充当 C-RP。因此，对于 BSR 测试功能，您必须将路由器添加到拓扑。

- BSR 选举机制 - 每个 C-BSR 都会生成包含 BSR 优先级字段的引导程序消息 (BSM)。该域中的路由器会在整个域中泛洪传播 BSM。C-BSR 收到具有比自身优先级更高的 C-BSR 时，会在特定时间内抑制进一步发送 BSM。剩余的单个 C-BSR 会成为选举的 BSR，而且其 BSM 会通知域中的所有其他路由器它是选举的 BSR。

组播组概念

组播基于组概念。任意一组接收者对接收特定数据流表现出兴趣。这样的组没有任何物理边界或地理边界 - 主机可位于互联网上的任何位置。有兴趣接收流向特定组的数据的主机必须使用 IGMP 加入该组。要接收数据流，主机必须是该组的成员。

组播地址

组播地址指定已加入某个组的任意一组 IP 主机，并希望接收发送到此组的流量。

集群

组播路由支持集群。在跨网络 EtherChannel 集群中，在快速路径转发建立之前，控制单元会发送所有的组播数据包和数据包。在建立快速路径转发后，数据单元可能会转发组播数据包。所有数据流都是全流量。同时还支持末节转发流。由于跨网络 EtherChannel 集群中仅有一台设备接收组播数据包，因此，重定向到控制单元较为常见。 在独立接口集群中，设备不会独立工作。所有的数据和路由数据包均由控制单元处理和转发。数据单元会丢弃已发送的所有数据包。

组播路由准则

情景模式

在单情景模式中受支持。

防火墙模式

仅在路由防火墙模式下受支持。不支持透明防火墙模式。

IPv6

不支持 IPv6。

组播组

保留 224.0.0.0 和 224.0.0.255 之间的地址范围用于路由协议和其他拓扑发现或维护协议，例如网关发现和组成员报告。因此，不支持来自地址范围 224.0.0/24 的互联网组播路由；为保留地址启用组播路由时，未创建 IGMP 组。

集群

在集群中，对于 IGMP 和 PIM，仅在主设备上支持此功能。

其他准则

- 必须针对入站接口配置访问配置规则，以允许流量到达组播主机（如 224.1.2.3）。但不能为该规则指定目标接口，或者不能使其在初始连接验证过程中适用于组播连接。
- 流量区域中的接口上不支持 PIM/IGMP 组播路由。
- 请勿将 ASA 同时配置为交汇点 (RP) 和第一跳路由器。
- HSRP 备用 IP 地址不参与 PIM 邻居关系。因此，如果通过 HSRP 备用 IP 地址路由 RP 路由器 IP，则 ASA中组播路由不起作用。因此，要使组播流量成功通过，请确保 RP 地址的路由不是 HSRP 备用 IP 地址，而是将路由地址配置为接口 IP 地址。

启用组播路由

在 ASA 上启用组播路由，默认情况下将在所有数据接口上启用 IGMP 和 PIM，但不会在绝大多数型号的管理接口上启用 IGMP 和 PIM（请参阅 管理插槽/端口接口，第 660 页 了解不允许通过流量的接口）。IGMP 用于了解直连子网上是否存在组成员。主机通过发送 IGMP 报告消息加入组播组。PIM 用于维护转发表，以转发组播数据报。

要在管理接口上启用组播路由，必须在该管理接口上明确设置组播边界。

注释 组播路由仅支持 UDP 传输层。

下表列出了特定组播表的最大条目数。一旦达到这些限制，系统将会丢弃所有新条目。

- MFIB - 30,000
- IGMP 组 - 30,000
- PIM 路由 - 72,000

过程

启用组播路由：

multicast-routing

示例：

```
ciscoasa(config)# multicast-routing
```

组播路由表中的条目数量受 ASA 上 RAM 容量的限制。

自定义组播路由

本节介绍如何自定义组播路由。

配置末节组播路由和转发 IGMP 消息

注释 末节组播路由不与 PIM 稀疏和双向模式同时受支持。

作为至末节区域的网关的 ASA 不需要参与 PIM 稀疏模式或双向模式。相反，可以将该 ASA 配置为 IGMP 受托代理，并使其会从连接到一个接口的主机将 IGMP 消息转发到另一个接口上的上游组播路由器。要将 ASA 配置为 IGMP 代理，请转发主机加入并使消息从末节区域接口发送至上游接口。您还必须在参与末节模式组播路由的接口上启用 PIM。

过程

配置末节组播路由和转发 IGMP 消息：

igmp forward interface if_name

示例：

```
ciscoasa(config-if)# igmp forward interface interface1
```

配置静态组播路由

配置静态组播路由可以将组播流量与单播流量分隔开。例如，如果源和目标之间的路由不支持组播路由，可以通过如下方法来解决这个问题：使用GRE隧道在它们之间配置两个组播设备，并通过该隧道发送组播数据包。

使用 PIM 时，ASA 期望用于接收数据包的接口和用于将单播数据包发送回到源的接口是同一个接口。在某些情况下（例如，绕过不支持组播路由的路由），您可能希望单播数据包和组播数据包使用不同的路径。

静态组播路由不能通告或重分布。

过程

步骤 1 配置静态组播路由：

mroute src_ip src_mask {input_if_name | *rpf_neighbor*} [distance]

示例：

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
```

步骤 2 配置末节区域的静态组播路由：

mroute src_ip src_mask input_if_name [**dense** output_if_name] [distance]

示例：

```
ciscoasa(config)# mroute src_ip src_mask input_if_name [dense output_if_name] [distance]
```

末节组播路由仅支持 **dense** *output_if_name* 关键字-参数对。

配置 IGMP 功能

IP 主机使用 IGMP 向直接连接的组播路由器报告其组成员身份。IGMP 用于在特定 LAN 上的一个组播组中动态注册单个主机。主机通过向其本地组播路由器发送 IGMP 消息来识别组成员身份。在 IGMP 下，路由器监听 IGMP 消息，并定期发出查询以发现特定子网上处于活动状态或非活动状态的组。

本节介绍如何逐个接口配置可选的 IGMP 设置。

禁用接口上的 IGMP

您可以禁用特定接口上的 IGMP。如果知道特定接口上没有组播接口，并且想要防止 ASA 通过该接口发送主机查询消息，则此信息很有用。

过程

禁用接口上的 IGMP：

no igmp

示例：

```
ciscoasa(config-if)# no igmp
```

要重新启用接口上的 IGMP，请使用 **igmp** 命令。

注释
接口配置中仅显示 **no igmp** 命令。

配置 IGMP 组成员身份

您可以将 ASA 配置成为组播组的成员。配置 ASA 加入组播组会使上游路由器维护该组的组播路由表信息，并保持该组的路径处于活动状态。

注释 如果要将特定组的组播数据包转发给接口，且无需ASA将这些数据包接受为该组的一部分，请参阅配置静态加入的 IGMP 组，第 1162 页。

过程

将 ASA 配置为组播组的成员：

igmp join-group group-address

示例：

```
ciscoasa(config-if)# igmp join-group mcast-group
```

group-address 参数是该组的 IP 地址。

注释

igmp join-group 命令使让PIM 能够向源或汇聚点 (RP) 发送加入请求，前提是使用此命令的防火墙是应用该命令的接口上的 PIM 指定路由器 (DR)。

配置静态加入的 IGMP 组

有时，组成员因某些配置而无法报告其在组中的成员关系，或者网段上可能不存在组成员。但是，您仍希望将该组的组播流量发送到该网段。您可以通过配置静态加入的 IGMP 组将该组的组播流量发送到网段。

输入 **igmp static-group** 命令。ASA 不接收组播数据包，而是将其转发至指定的接口。

过程

静态配置 ASA 以加入接口上的组播组：

igmp static-group

示例：

```
ciscoasa(config-if)# igmp static-group group-address
```

group-address 参数是该组的 IP 地址。

注释
igmp static-group 命令使让PIM 能够向源或汇聚点 (RP) 发送加入请求，前提是使用此命令的防火墙是应用该命令的接口上的 PIM 指定路由器 (DR)。

控制对组播组的访问

您可以通过使用访问控制列表控制对组播组的访问。

过程

步骤 1 为组播流量创建标准 ACL：

access-list name **standard** [**permit | deny]** ip_addr mask

示例：

```
ciscoasa(config)# access-list acl1 standard permit 192.52.662.25
```

您可以为一个 ACL 创建多个条目。您可以使用扩展或标准 ACL。

ip_addr mask 参数是被允许或拒绝的组播组的 IP 地址。

步骤 2 创建扩展的 ACL：

access-list name **extended** [**permit | deny]** protocol src_ip_addr src_mask dst_ip_addr dst_mask

示例：

```
ciscoasa(config)# access-list acl2 extended permit protocol
src_ip_addr src_mask dst_ip_addr dst_mask
```

dst_ip_addr 参数是被允许或拒绝的组播组的 IP 地址。

步骤 3 将 ACL 应用于接口：

igmp access-group acl

示例：

```
ciscoasa(config-if)# igmp access-group acl
```

acl 参数是标准或扩展 IP ACL 的名称。

限制接口上的 IGMP 状态数量

您可以对每个接口限制 IGMP 成员身份报告造成的 IGMP 状态数量。超出所配置限制的成员身份报告不会输入到 IGMP 缓存中，多余成员身份报告的流量不会转发。

过程

限制接口上的 IGMP 状态数量：

igmp limit number

示例：

```
ciscoasa(config-if)# igmp limit 50
```

有效值的范围为 0 到 5000，默认值为 。

将此值设置为 0 可防止添加获悉的组，但仍允许手动定义成员身份（使用 **igmp join-group** 和 **igmp static-group** 命令）。此命令的 **no** 形式将恢复默认值。

注释 当您更改接口上具有活动加入的 IGMP 限制时，新限制不适用于现有组。仅当将新组添加到接口或 IGMP 加入计时器到期时，ASA 才会验证限制。要应用新的限制并立即生效，必须在接口上禁用并重新启用 IGMP。

修改发送到组播组的查询消息

ASA 发送查询消息，以发现哪些组播组有成员位于与接口连接的网络上。成员以 IGMP 报告消息作出响应，以表明自己想要接收特定组的组播数据包。查询消息会发送到全系统组播组，该组的地址为 224.0.0.1，生存时间值为 1。

这些消息会定期发送，从而刷新 ASA 上存储的成员身份信息。如果 ASA 发现组播组中没有本地成员仍与接口相连接，它会停止向连接的网络转发该组的组播数据包，并会向数据包源发送回删除消息。

默认情况下，子网上的 PIM 指定路由器负责发送查询消息。默认情况下，每 125 秒发送一次消息。

默认情况下，更改查询响应时间时，IGMP 查询中通告的最大查询响应时间为 10 秒。如果 ASA 不在此时间内接收对主机查询的响应，它就会删除该组。

注释 **igmp query-timeout** 和 **igmp query-interval** 命令需要 IGMP 版本 2。

如要更改查询间隔时间、查询响应时间和查询超时值，请执行以下步骤：

过程

步骤 1 设置查询间隔时间（以秒为单位）：

igmp query-interval 秒

示例：

```
ciscoasa(config-if)# igmp query-interval 30
```

有效值的范围为 1 到 3600；默认值为 125。

如果 ASA 不能在指定超时值（默认值为 255 秒）内在接口上收到查询消息，ASA 将会成为指定路由器并开始发送查询消息。

步骤 2 更改查询的超时值：

igmp query-timeout 秒

示例：

```
ciscoasa(config-if)# igmp query-timeout 30
```

有效值的范围为 60 到 300；默认值为 225。

步骤 3 更改最大查询响应时间：

igmp query-max-response-time 秒

有效值的范围为 1 到 25；默认值为 10。

示例：

```
ciscoasa(config-if)# igmp query-max-response-time 20
```

更改 IGMP 版本

默认情况下，ASA 运行 IGMP 版本 2；此版本启用了多项附加功能，例如 **igmp query-timeout** 和 **igmp query-interval** 命令。

子网上所有的组播路由器必须支持同一版本的 IGMP。ASA 不会自动检测版本 1 路由器并切换到版本 1。但是，可以在子网上结合使用 IGMP 版本 1 和版本 2 主机；当存在 IGMP 版本 1 主机时，运行 IGMP 版本 2 的 ASA 可正常工作。

过程

控制要在接口上运行的 IGMP 版本：

igmp version {**1** | **2**}

示例：

```
ciscoasa(config-if)# igmp version 2
```

配置 PIM 功能

路由器使用 PIM 来维护转发表，以便用于转发组播图。如果在 ASA 上启用组播路由，PIM 和 IGMP 将会在所有接口上自动启用。

注释 PAT 不支持 PIM。PIM 协议不使用端口，PAT 只能与使用端口的协议配合使用。

本节介绍如何配置可选的 PIM 设置。

启用和禁用接口上的 PIM

可以在特定接口上启用或禁用 PIM。

过程

步骤 1 在特定接口上启用或重新启用 PIM：

pim

示例：

```
ciscoasa(config-if)# pim
```

步骤 2 在特定接口上禁用 PIM：

no pim

示例：

```
ciscoasa(config-if)# no pim
```

注释
接口配置中仅显示 **no pim** 命令。

配置静态交汇点地址

常见 PIM 稀疏模式中或 bidir 域中的所有路由器均需要了解 PIM RP 地址。使用 **pim rp-address** 命令可静态配置该地址。

注释 ASA 不支持自动 RP。必须使用 **pim rp-address** 命令来指定 RP 地址。

您可以配置ASA来充当多个组的RP。ACL中指定的组范围确定PIM RP组映射。如果未指定ACL，则一个组的 RP 将应用于整个组播组范围 (224.0.0.0/4)。

过程

在特定接口上启用或重新启用 PIM：

pim rp-address ip_address [acl] [**bidir**]

ip_address 参数是分配为 PIM RP 的路由器的单播 IP 地址。

acl 参数是定义应将该 RP 用于哪些组播组的标准 ACL 的名称或编号。请勿在使用此命令时一起使用主机 ACL。

排除 **bidir** 关键字会导致这些组在 PIM 稀疏模式下运行。

注释
无论实际的双向配置是怎样的，ASA 在 PIM 问候消息中始终通告双向功能。

示例：

```
ciscoasa(config)# pim rp-address 10.86.75.23 [acl1] [bidir]
```

配置指定路由器优先级

指定路由器 (DR) 负责将 PIM 注册消息、加入消息和删除消息发送到 RP。如果网段上有多个组播路由器，将会根据 DR 优先级来选择 DR。如果多台设备具有同样的 DR 优先级，则具有最高 IP 地址的设备将会成为 DR。

默认情况下，ASA 的 DR 优先级为 1。您可以更改此值。

过程

更改指定路由器优先级：

pim dr-priority num

示例：

```
ciscoasa(config-if)# pim dr-priority 500
```

num 参数可以是 1 至 4294967294 的任意 数字。

配置和过滤 PIM 注册消息

当 ASA 作为 RP 时，您可以禁止特定的组播源注册到 ASA，从而防止未授权的源注册到 RP。Request Filter 窗格可用于定义 ASA 将会从其接受 PIM 注册消息的组播源。

过程

配置 ASA 以筛选 PIM 注册消息：

pim accept-register {**list** acl | **route-map** map-name}

示例：

```
ciscoasa(config)# pim accept-register {list acl1 | route-map map2}
```

在此示例中，ASA 筛选 PIM 注册消息 *acl1* 和路由映射 *map2*。

配置 PIM 消息间隔

路由器查询消息用于选择 PIM DR。PIM DR 负责发送路由器查询消息。默认情况下，每隔 30 秒发送一次路由器查询消息。此外，ASA 每隔 60 秒发送一次 PIM 加入消息或删除消息。

过程

步骤 1 发送路由器查询消息：

pim hello-interval seconds

示例：

```
ciscoasa(config-if)# pim hello-interval 60
```

seconds 参数的有效值范围为 1 到 3600 秒。

步骤 2 更改 ASA 发送 PIM 加入消息或删除消息的时间（以秒为单位）：

pim join-prune-interval seconds

示例：

```
ciscoasa(config-if)# pim join-prune-interval 60
```

seconds 参数的有效值范围为 10 到 600 秒。

过滤 PIM 邻居

您可以定义可成为 PIM 邻居的路由器。通过筛选可成为 PIM 邻居的路由器，可以实现以下目的：

- 防止未授权的路由器成为 PIM 邻居。
- 防止连接的末节路由器加入到 PIM。

过程

步骤 1 使用标准 ACL 定义要加入到 PIM 的路由器：

access-list pim_nbr deny *router-IP_addr PIM neighbor*

示例：

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

在此示例中，以下 ACL 与 **pim neighbor-filter** 命令配合使用可防止 10.1.1.1 路由器成为 PIM 邻居。

步骤 2 筛选邻居路由器：

pim neighbor-filter pim_nbr

示例：

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim neighbor-filter pim_nbr
```

此示例防止 10.1.1.1 路由器在接口 GigabitEthernet0/3 上成为 PIM 邻居。

配置双向邻居过滤器

Bidirectional Neighbor Filter 窗格显示在 ASA 上配置的 PIM 双向邻居过滤器（如有）。PIM 双向邻居过滤器是定义可参与 DF 选举的邻居设备的 ACL。如果接口未配置 PIM 双向邻居过滤器，则没有限制。如果配置了 PIM 双向邻居过滤器，则只有 ACL 允许的邻居可参与 DF 选举过程。

如果 PIM 双向邻居过滤器配置应用于 ASA，名称为 *interface-name*_multicast 的运行配置中会显示 ACL，其中，*interface-name* 是应用组播边界过滤器的接口的名称。如果已存在使用该名称的 ACL，将会给名称加上一个数字（例如，inside_multicast_1）。此 ACL 定义可成为 ASA 的 PIM 邻居的设备。

双向 PIM 允许组播路由器保持减少的状态信息。要选择 DF，必须为 bidir 双向启用分片中的所有组播路由器。

PIM 双向邻居过滤器允许指定应参与 DF 选举的路由器，同时仍允许所有路由器加入到稀疏模式域，从而实现从纯稀疏模式网络到 bidir 网络的过渡。支持 bidir 的路由器可以从它们本身当中选择 DF，即使分片上有非 bidir 路由器。非 bidir 路由器上的组播边界可防止 bidir 组中的 PIM 消息和数据泄漏到 bidir 子集云中或从 bidir 子集云泄漏出去。

如果启用了 PIM 双向邻居过滤器，ACL 允许的路由器将被视为具有双向功能。因此，以下说法均是正确的：

- 如果一个获允许的邻居不支持 bidir，将不会发生 DF 选举。
- 如果一个被拒绝的邻居支持 bidir，将不会发生 DF 选举。
- 如果一个被拒绝的邻居不支持 bidir，可能会发生 DF 选举。

过程

步骤 1 使用标准 ACL 定义要加入到 PIM 的路由器：

access-list pim_nbr deny *router-IP_addr PIM neighbor*

示例：

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

在此示例中，以下 ACL 与 **pim neighbor-filter** 命令配合使用可防止 10.1.1.1 路由器成为 PIM 邻居。

步骤 2 筛选邻居路由器：

pim bidirectional-neighbor-filter pim_nbr

示例：

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidirectional neighbor-filter pim_nbr
```

此示例防止 10.1.1.1 路由器在接口 GigabitEthernet0/3 上成为 PIM 双向邻居。

将 ASA 配置为候选 BSR

可以将 ASA 配置为候选 BSR

过程

步骤 1 配置路由器以宣布其候选者为引导程序路由器 (BSR)：

pim bsr-candidate *interface_name* [*hash_mask_length* [*priority*]]

示例：

```
ciscoasa(config)# pim bsr-candidate inside 12 3
```

步骤 2 （可选）将 ASA 配置为边界引导程序路由器：

interface *interface_name*

pim bsr-border

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# pim bsr-border
```

在接口上配置此命令时，不会通过接口发送或接收引导程序路由器 (BSR) 消息。

配置组播边界

地址范围定义了域边界，从而使具有 IP 地址相同的 RP 的域不会相互泄漏。可在大型域内的子网边界以及域与互联网之间的边界上执行范围界定。

您可以在接口上为组播组地址设置管理权限界定的边界。IANA 已将 239.0.0.0 到 239.255.255.255 的组播地址范围指定为可使用管理性界定的地址。此地址范围可在不同组织管理的域中重复使用。此类地址被视为本地地址，而不是全局唯一地址。

标准ACL定义受影响地址的范围。设置边界后，不允许组播数据包从任一方向流经边界。边界允许同一个组播组地址在不同的管理域中重复使用。

您可以通过输入 **filter-autorp** 关键字在使用管理权限界定的边界配置、检查和筛选 Auto-RP 发现消息和通知消息。Auto-RP 数据包中被边界 ACL 拒绝的任意 Auto-RP 组范围通知都会被删除。仅在 Auto-RP 组范围中的所有地址获边界 ACL 允许的情况下，Auto-RP 组范围通知才可以通过边界。如果有任何地址未获允许，在 Auto-RP 消息转发前，将会筛选整个组范围并将其从 Auto-RP 消息中删除。

过程

配置组播边界：

multicast boundary acl [**filter-autorp**]

示例：

```
ciscoasa(config-if)# multicast boundary acl1 [filter-autorp]
```

PIM 监控

可以使用以下命令监控 PIM 路由进程。有关命令输出的示例和说明，请参阅命令参考。

如要监控或禁用多个 PIM 路由统计信息，请输入以下命令之一：

- **show pim bsr-router**

  显示引导程序路由器信息。

- **show mroute**

  显示组播路由表的内容。

- **show mfib summary**

  显示有关 IPv4 PIM 组播转发信息库条目数及接口数的概要信息。

- **show mfib active**

  显示组播转发信息库 (MFIB) 中有关主用组播源向组播组发送信息的速率。

- **show pim group-map**

  显示组对 PIM 模式映射。要显示组的选举 RP，请指定组地址或名称。

- **show pim group-map rp-timers**

  显示每个组对 PIM 模式映射条目的计时器到期时间和正常运行时间。

- **show pim neighbor**

  显示协议无关组播 (PIM) 邻居。

组播路由示例

以下示例显示如何使用各个可选过程启用和配置组播路由：

1. 启用组播路由：

```
ciscoasa(config)# multicast-routing
```

2. 配置静态组播路由：

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
ciscoasa(config)# exit
```

3. 将 ASA 配置为组播组的成员：

```
ciscoasa(config)# interface
ciscoasa(config-if)# igmp join-group group-address
```

组播路由的历史记录

表 *43:* 组播路由的功能历史记录

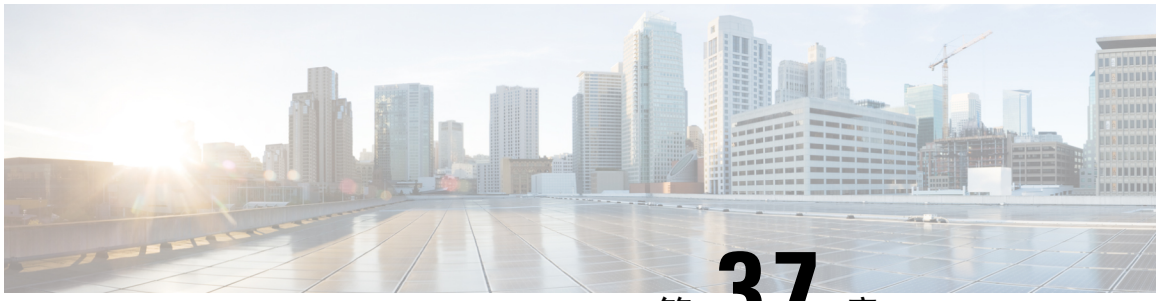
功能名称	平台版本	功能信息
组播路由支持	7.0(1)	增加了对于组播路由数据、身份验证以及使用组播路由协议重新发布和监控路由信息的支持。 引入了 **multicast-routing** 命令。

功能名称	平台版本	功能信息
支持集群功能	9.0(1)	增加了集群支持。 引入了以下命令：**debug mfib cluster**、**show mfib cluster**。
支持协议无关组播 - 源特定组播 (PIM-SSM) 直接通过	9.5(1)	添加了对启用组播路由时允许 PIM-SSM 数据包通过的支持，除非 ASA 为最后一跳路由器。这使得可以更加灵活地选择组播组，同时还能抵御不同的攻击；主机仅接收来自显式请求的源的流量。 我们未更改任何命令。
独立于协议的组播自举路由器 (BSR)	9.5(2)	添加了对新动态交汇点 (RP) 选择模式的支持，该功能使用备选路由器来执行交汇点功能以及中继组的交汇点信息。此功能提供动态获取交汇点 (RP) 的方法，这一点对于 RP 可定期断开和连接的大型复杂网络非常重要。 引入了以下命令：clear pim group-map、debug pim bsr、pim bsr-border、pim bsr-candidate、show pim bsr-router、show pim group-map rp-timers
增加了 igmp limit	9.15(1) 同样在 *9.12(4)* 中	igmp limit 从 500 增加到 5000。 新增/修改的命令：**igmp limit**。

第 VI 部分

AAA 服务器和本地数据库

- AAA 和本地数据库， 第 1177 页
- 用于 AAA 的 RADIUS 服务器， 第 1189 页
- 用于 AAA 的 TACACS+ 服务器， 第 1209 页
- 用于 AAA 的 LDAP 服务器， 第 1217 页
- 用于 AAA 的 RSA SecurID 服务器， 第 1229 页



第 37 章

AAA 和本地数据库

本章介绍身份验证、授权和记帐（AAA，也称为“3A”）。AAA 是一组服务，用于控制对计算机资源的访问、执行策略、评估使用情况并提供对服务进行计费所需的信息。这些过程对于高效进行网络管理和安全性而言至关重要。

本章还介绍如何为 AAA 功能配置本地数据库。对于外部 AAA 服务器，请参阅与您的服务器类型对应的章节。

- 关于 AAA 和本地数据库， 第 1177 页
- 本地数据库准则， 第 1182 页
- 在本地数据库中添加用户帐户， 第 1182 页
- 监控本地数据库， 第 1184 页
- 本地数据库的历史记录， 第 1184 页

关于 AAA 和本地数据库

本节介绍 AAA 和本地数据库。

身份验证

身份验证提供了一种识别用户的方法，这种方法通常先请用户输入有效用户名和有效密码，然后再授予访问权限。AAA 服务器将用户的身份验证凭证与数据库中存储的其他用户凭证进行比较。如果凭证匹配，则允许用户访问网络。如果凭证不匹配，则身份验证失败，并拒绝网络访问。

您可以将 ASA 配置为对以下项进行身份验证：

- 与 ASA 的所有管理连接，包括以下会话：
  - Telnet
  - SSH
  - 串行控制台
  - 使用 HTTPS 的 ASDM
  - VPN 管理访问

- **enable** 命令
- 网络接入
- VPN 接入

授权

授权是执行策略的过程：确定允许用户访问哪些类型的活动、资源或服务。对用户进行身份验证后，可能会授权该用户执行各种类型的访问或活动。

您可以配置 ASA 以便对下列各项进行授权：

- 管理命令
- 网络接入
- VPN 接入

会计

记账用于测量用户在访问期间使用的资源量，这可以包括系统时间长度或者用户在会话期间发送或接收的数据量。记账是通过记录会话统计信息和使用量信息来执行的，这些信息用于进行授权控制、计费、趋势分析、资源利用率和容量规划活动。

身份验证、授权和记账之间的交互

您可以单独使用身份验证功能，也可以将其与授权和记账功能配合使用。授权始终要求先对用户进行身份验证。您可以单独使用记账功能，也可以将其与身份验证和授权功能配合使用。

AAA 服务器和服务器组

AAA 服务器是用于进行访问控制的网络服务器。身份验证用于识别用户。授权用于实施策略，这些策略确定经过身份验证的用户能够访问哪些资源和服务。记账对时间和数据资源进行追踪，这些资源用于计费和分析。

如果要使用外部 AAA 服务器，必须先为外部服务器使用的协议创建 AAA 服务器组，然后将该服务器添加到该组。您可以为每个协议创建多个组，并为要使用的所有协议创建单独的组。每个服务器组都专门用于一种类型的服务器或服务。

有关如何创建组的详细信息，请参阅以下主题：

- 配置 RADIUS 服务器组，第 1201 页
- 配置 TACACS+ 服务器组，第 1211 页
- 配置 LDAP 服务器组，第 1223 页
- 配置 RSA SecurID AAA 服务器组，第 1230 页

有关使用 HTTP 表单的详细信息，请参阅 VPN 配置指南。

注释 从 ASA 9.22.1 起，不支持 Kerberos 协议。您不能再将 Kerberos 用于 AAA 服务。建议您使用下表 44: AAA 服务器支持的服务中列出的其他受支持服务器。

下表总结了支持的服务器类型及其用途，包括本地数据库。

表 *44: AAA* 服务器支持的服务

服务器类型和服务	身份验证	授权	记账
本地数据库			
管理员	是	是	否
VPN 用户	是	否	不兼容
防火墙会话（AAA 规则）	是	是	否
RADIUS			
管理员	是	是	是
VPN 用户	是	是	是
防火墙会话（AAA 规则）	是	是	是
TACACS+			
管理员	是	是	是
VPN 用户	是	不支持	是
防火墙会话（AAA 规则）	是	是	是
LDAP			
管理员	是	否	不兼容
VPN 用户	是	是	否
防火墙会话（AAA 规则）	是	否	不兼容
SDI (RSA SecurID)			
管理员	是	否	不兼容
VPN 用户	是	否	不兼容
防火墙会话（AAA 规则）	是	否	不兼容

服务器类型和服务	身份验证	授权	记账
HTTP 形式			
管理员	否	不兼容	不兼容
VPN 用户	是	否	不兼容
防火墙会话（AAA 规则）	否	不兼容	不兼容

注意

- RADIUS - 管理员的记帐不包括命令记帐。
- RADIUS - 防火墙会话的授权仅支持用户特定的访问列表，这些列表在 RADIUS 身份验证响应中接收或指定。
- TACACS+ - 管理员会计包括命令会计。
- HTTP 形式 - 仅用于无客户端 SSL VPN 用户会话的身份验证和 SSO 操作。

关于本地数据库

ASA 维护了一个本地数据库，您可以使用用户配置文件填充该数据库。您可以使用本地数据库代替 AAA 服务器来提供用户身份验证、授权和记帐。

您可以使用本地数据库实现下列功能：

- ASDM 按用户访问
- 控制台身份验证
- Telnet 和 SSH 身份验证
- **enable** 命令身份验证

  此设置仅用于 CLI 访问，并不影响思科 ASDM 登录。
- 命令授权

  如果您使用本地数据库打开命令授权，则ASA将参考用户权限级别来确定可用的命令。否则，通常不使用权限级别。默认情况下，所有命令的权限级别均为 0 或 15。
- 网络访问身份验证
- VPN 客户端身份验证

对于多情景模式，您可以在系统执行空间中配置用户名，以便在 CLI 中使用 **login** 命令提供个人登录；但是，您不能在系统执行空间中配置任何使用本地数据库的 AAA 规则。

注释 您不能使用本地数据库进行网络访问授权。

回退支持

本地数据库可以用作多项功能的回退方法。此行为旨在帮助您避免意外被锁定而无法登录 ASA。

用户登录时，将从配置中指定的第一个服务器开始逐个访问组中的服务器，直到有服务器作出响应为止。如果组中的所有服务器都不可用，并且您已将本地数据库配置为回退方法（仅用于管理身份验证和授权），则 ASA 将尝试使用本地数据库。如果未配置任何回退方法，则 ASA 将继续尝试使用 AAA 服务器。

对于需要回退支持的用户，我们建议您确保本地数据库中的用户名和密码与AAA服务器上的用户名和密码匹配。这种做法将提供透明的回退支持。由于用户无法确定是AAA服务器还是本地数据库正在提供服务，因此，如果AAA服务器上使用的用户名和密码与本地数据库中的用户名和密码不同，用户将无法确定应提供哪个用户名和密码。

本地数据库支持下列回退功能：

- 控制台和启用密码身份验证 - 如果组中的服务器全部不可用，则 ASA 将使用本地数据库对管理访问进行身份验证，这还可以包括启用密码身份验证。
- 命令授权 - 如果组中的 TACACS+ 服务器全部不可用，则使用本地数据库根据权限级别进行命令授权。
- VPN 身份验证和授权 - 支持 VPN 身份验证和授权，以便在通常支持这些 VPN 服务的 AAA 服务器不可用时，启用对 ASA 的远程访问。如果管理员的 VPN 客户端指定了配置为回退到本地数据库的隧道组，只要本地数据库配置了必要的属性，即使AAA服务器组不可用，也可以建立 VPN 隧道。

组中存在多个服务器时的回退方式

如果在服务器组中配置了多个服务器，并且对于该服务器组允许回退到本地数据库，则该组中没有任何服务器对来自ASA的身份验证请求作出响应时，将会进行回退。为了说明这一点，请考虑以下场景：

您配置了一个 LDAP 服务器组，其中依次包含两个 Active Directory 服务器，即服务器 1 和服务器 2。当远程用户登录时，ASA 将尝试向服务器 1 进行身份验证。

如果服务器 1 作出了身份验证失败响应（例如找不到用户），则 ASA 不会尝试向服务器 2 进行身份验证。

如果服务器 1 在超时期限内未作出响应（或者尝试进行身份验证的次数超过配置的最大值），则 ASA 尝试服务器 2。

如果组中的两个服务器均未作出响应，并且 ASA 配置为回退到本地数据库，则 ASA 将尝试向本地数据库进行身份验证。

本地数据库准则

在使用本地数据库进行身份验证或授权时，请确保避免被锁定而无法登录 ASA。

在本地数据库中添加用户帐户

要向本地数据库添加用户，请执行以下步骤：

过程

步骤 1 创建用户帐户。

username *username* [**password** *password*] [**privilege** *priv_level*]

示例：

```
ciscoasa(config)# username exampleuser1 password madmaxfuryroadrules privilege 1
```

username *username* 关键字是长度为 3 到 64 个字符的字符串，可以任意组合使用 ASCII 可打印字符（字符代码 32-126），但是空格和问号除外。 **password** 密码 关键词是一个区分大小写的密码，长度为 8 到 127 个字符，可以任意组合使用 ASCII 可打印字符（字符代码 32-126），但是以下除外。

- 无空格
- 没有问号
- 不能使用三个或三个以上连续或重复的 ASCII 字符。例如，以下密码将被拒绝：
  - **abc**user1
  - 用户**543**
  - 用户**aaaa**
  - 用户2**666**

例如，如果您使用 SSH 公钥身份验证，则您可能想创建用户名而不创建密码。**privilege***priv_level* 关键字用于设置范围为 0 到 15 的权限级别。默认值为 2。此权限级别与命令授权一起使用。

注意
如果未使用命令授权（**AAA 授权控制台 LOCAL** 命令），则默认级别 2 允许对特权 EXEC 模式进行管理访问。如果要限制对特权 EXEC 模式的访问，请将权限级别设置为 0 或 1，或者使用 **service-type** 命令。

上面的语法中并未显示这些不常用的选项：**nopassword** 关键字用于创建可以接受任何密码的用户帐户；此选项不安全，因此不建议使用。

encrypted 关键字（在 9.6 和早期版本中，用于 32 个字符或以下的密码）或 **pbkdf2** 关键字（在 9.6 和更高版本中，用于长度超过 32 个字符的密码；在 9.7 和更高版本中，用于所有长度的密码）表示密码已被加密（使用基于 MD5 的散列或 PBKDF2（基于密码的密钥派生功能 2）散列）。请注意，现有密码将继续使用基于 MD5 的散列方法，除非您输入新的密码。当您在 **username** 命令中定义密码后，出于安全目的，ASA 会在将其保存到配置时进行加密。输入 **show running-config** 命令后，**username**命令不会显示实际密码；它将显示加密的密码，后跟 **encrypted** 或 **pbkdf2** 关键字。例如，如果输入密码“test”，则 **show running-config** 命令输出内容将与以下内容类似：

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

只有在您剪切和粘贴配置文件，以便 在另一 ASA 中使用，而且您使用相同的密码时， 才会真的在 CLI 上输入 **encrypted** 或 **pbkdf2** 关键字。

步骤 2 （可选）配置用户名属性。

username 用户名 **attributes**

示例：

```
ciscoasa(config)# username exampleuser1 attributes
```

username 参数是您在第一步中创建的用户名。

默认情况下，使用此命令添加的 VPN 用户没有属性或组策略关联。您必须使用 **username attributes** 命令明确配置所有值。有关更多信息，请参阅《VPN 配置指南》。

步骤 3 （可选）如果使用 **aaa authorization exec** 命令配置了管理授权，请配置用户级别。

service-type {**admin** | **nas-prompt** | **remote-access**}

示例：

```
ciscoasa(config-username)# service-type admin
```

admin 关键字允许完全访问 **aaa authentication console LOCAL** 命令指定的所有服务。**admin** 关键字是默认值。

在配置 **aaa authentication** {**telnet** | **ssh** | **serial**} **console** 命令时， **nas-prompt** 关键字将允许访问 CLI，但如果配置 **aaa authentication http console** 命令，则拒绝 ASDM 配置访问。允许 ASDM 监控访问。如果使用 **aaa authentication enable console** 命令启用了身份验证，则用户无法使用 **enable** 命令（或 **login** 命令）访问特权 EXEC 模式。

remote-access 关键字会拒绝管理访问。您无法使用 **aaa authentication console** 命令指定的任何服务（不包括 **serial** 关键字；允许进行串行访问）。

步骤 4 （可选） 有关按每个用户对与 ASA 的 SSH 连接进行公钥身份验证的信息，请参阅配置 SSH 访问，第 1237 页。

步骤 5 （可选） 如果要使用此用户名进行 VPN 身份验证，则可以为用户配置许多 VPN 属性。有关更多信息，请参阅《VPN 配置指南》。

示例

以下示例向管理员用户帐户分配权限级别 15：

```
ciscoasa(config)# username admin password farscape1 privilege 15
```

以下示例启用管理授权，创建具有密码的用户帐户，进入用户名配置模式，并指定**service-type**为 **nas-prompt**：

```
ciscoasa(config)# aaa authorization exec authentication-server
ciscoasa(config)# username user1 password gOrgeOus
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type nas-prompt
```

监控本地数据库

请参阅以下命令来监控本地数据库。

- **show aaa-server**

  此命令可显示已配置的数据库统计信息。使用 **clear aaa-server statistics** 命令可清除 AAA 服务器统计信息。

- **show running-config aaa-server**

  此命令可显示 AAA 服务器运行配置。使用 **clear configure aaa-server** 命令可清除 AAA 服务器配置。

本地数据库的历史记录

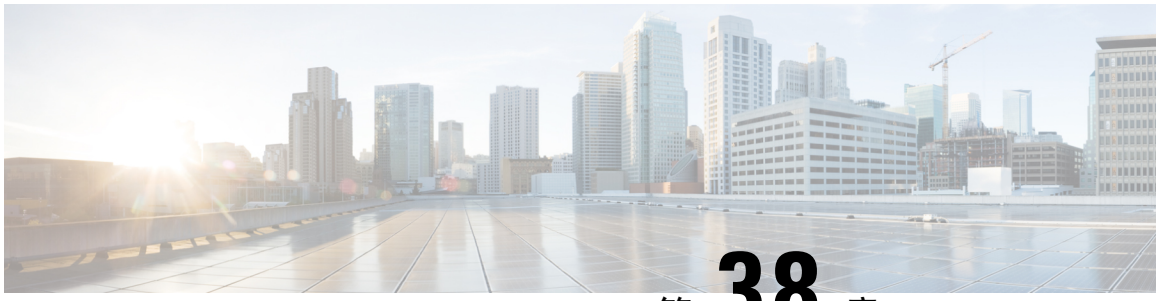
表 *45:* 本地数据库的历史记录

功能名称	平台版本	说明
AAA 的本地数据库配置	7.0(1)	介绍如何配置本地数据库以供 AAA 使用。 引入了以下命令： **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type**、**aaa authentication** {**telnet** | **ssh** | **serial**} **console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**show running-config aaa-server**、**show aaa-server**、**clear configure aaa-server**、**clear aaa-server statistics**。

功能名称	平台版本	说明
对 SSH 公钥身份验证的支持	9.1(2)	对于与 ASA 的 SSH 连接，您现在可以基于每个用户启用公钥身份验证。您可以指定公钥文件 (PKF) 格式的密钥或 Base64 密钥。PKF 密钥的长度可达 4096 位。对于由于过长而导致 ASA 不支持使用 Base64 格式（限长 2048 位）的密钥，请使用 PKF 格式。 引入了以下命令：**ssh authentication**。 在 *8.4(4.1)* 中也可用；*PKF* 密钥格式支持仅在 *9.1(2)* 中提供。
本地 **username** 和 **enable** 密码支持更长的密码（最多 127 个字符）	9.6(1)	您现在可以创建最多 127 个字符的本地 **username** 和 **enable** 密码（过去的限制为 32 个字符）。在创建长度超过 32 个字符的密码时，它将使用 PBKDF2（基于密码的密钥派生功能 2）散列存储在配置中。较短的密码将继续使用基于 MD5 的散列处理方法。 修改了以下命令：**enable**、**username**
SSH 公钥身份验证改进	9.6(2)	在更早的版本中，您在启用 SSH 公钥身份验证 (**ssh authentication**) 时，可以不必启用基于本地用户数据库的 AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。该配置现在已修复，您必须明确启用 AAA SSH 身份验证。要禁止用户使用密码而不是私钥，现在您可以创建未定义任何密码的用户名。 修改了以下命令：**ssh authentication**、**username**。
对所有本地 **username** 和 **enable** 密码使用 PBKDF2 散列算法	9.7(1)	配置中存储的所有长度的本地 **username** 和 **enable** 密码都将使用 PBKDF2 (基于密码的密钥派生函数 2) 散列算法。以前，32 个字符或以下的密码使用基于 MD5 的哈希处理方法。已经存在的密码仍将继续使用基于 MD5 的哈希值，但您输入的新密码除外。如需下载准则，请参阅一般操作配置指南中的“软件和配置”一章。 修改了以下命令：**enable**、**username**

功能名称	平台版本	说明
对使用 SSH 公钥身份验证的用户和具有密码的用户分别进行单独的身份验证	9.6(3)/9.8(1)	在 9.6(2) 以前的版本中，您在启用 SSH 公钥身份验证 (**ssh authentication**) 时，可以不必明确启用基于本地用户数据库的 AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。在 9.6(2) 中，ASA 要求明确启用 AAA SSH 身份验证。在此版本中，您不再需要明确启用 AAA SSH 身份验证；当您为用户配置 **ssh authentication** 命令时，默认情况下会为使用此类型身份验证的用户启用本地身份验证。此外，在明确配置 AAA SSH 身份验证时，此配置将仅适用于具有密码的用户名，并且可以使用任何 AAA 服务器类型（例如 **aaa authentication ssh console radius_1**）。例如，某些用户可以使用公钥身份验证（使用本地数据库），而其他用户则可配合使用密码和 RADIUS。 未修改任何命令。
更强的本地用户和启用密码要求	9.17(1)	对于本地用户和启用密码，添加了以下密码要求： • 密码长度 - 至少为 8 个字符。以前，最小值为 3 个字符。 • 重复和连续字符 - 不允许使用三个或三个以上连续的连续或重复 ASCII 字符。例如，以下密码将被拒绝： • **abc**user1 • 用户**543** • 用户**aaaa** • 用户2**666** 新增/修改的命令： **enable password**、**username**
本地用户锁定更改	9.17(1)	ASA 可以在登录尝试失败达到可配置次数之后锁定账户。此功能不适用于权限级别为 15 的用户。此外，用户将被无限期锁定，直到管理员解锁其账户。现在，用户将在 10 分钟后解锁，除非管理员在此之前使用 **clear aaa local user lockout** 命令。权限级别为 15 的用户现在也受锁定设置的影响。 新增/修改的命令：**aaa local authentication attempts max-fail** 、**show aaa local user**

功能名称	平台版本	说明
SSH 和 Telnet 密码更改提示	9.17(1)	本地用户首次使用 SSH 或 Telnet 登录 ASA 时，系统会提示他们更改密码。在管理员更改密码后，系统还会提示他们进行首次登录。但是，如果 ASA 重新加载，则系统不会提示用户，即使是首次登录也是如此。 新增/修改的命令：**show aaa local user**



第 38 章

用于 AAA 的 RADIUS 服务器

本章介绍如何配置用于 AAA 的 RADIUS 服务器。

- 关于用于 AAA 的 RADIUS 服务器， 第 1189 页
- AAA 的 RADIUS 服务器准则， 第 1200 页
- 配置用于 AAA 的 RADIUS 服务器， 第 1201 页
- 为 AAA 监控 RADIUS 服务器， 第 1207 页
- 用于 AAA 的 RADIUS 服务器的历史记录， 第 1208 页

关于用于 AAA 的 RADIUS 服务器

ASA 支持以下符合 RFC 标准的用于 AAA 的 RADIUS 服务器：

- 思科安全 ACS 3.2、4.0、4.1、4.2 和 5.x
- 思科身份服务引擎 (ISE)
- RSA 身份验证管理器 5.2、6.1 和 7.x 中的 RSA RADIUS
- Microsoft

受支持的身份验证方法

ASA 支持为 RADIUS 服务器使用以下身份验证方法：

- PAP - 适用于所有连接类型。
- CHAP 和 MS-CHAPv1 - 适用于 L2TP-over-IPsec 连接。
- MS-CHAPv2 - 适用于 L2TP-over-IPsec 连接和常规 IPsec 远程访问连接（当启用密码管理功能时）。您也可以通过无客户端连接使用 MS-CHAPv2。
- 身份验证代理模式 - 适用于 RADIUS-to-Active-Directory、RADIUS-to-RSA/SDI、RADIUS-to-Token 服务器和 RSA/SDI-to-RADIUS 连接。

注释 要启用 MS-CHAPv2 作为 ASA 与 RADIUS 服务器之间进行 VPN 连接所用的协议，则必须在隧道组常规属性中启用密码管理。启用密码管理会生成一个从 ASA 向 RADIUS 服务器的 MS-CHAPv2 身份验证请求。有关详细信息，请参阅 **password-management** 命令的描述。

如果在隧道组中使用双重身份验证并启用密码管理，则主身份验证请求和辅助身份验证请求包含 MS-CHAPv2 请求属性。如果 RADIUS 服务器不支持 MS-CHAPv2，则可以通过使用 **no mschapv2-capable** 命令将该服务器配置为发送非 MS-CHAPv2 身份验证请求。

VPN 连接的用户授权

ASA 可以使用 RADIUS 服务器进行 VPN 远程访问和防火墙直接转发代理会话的用户授权（按用户使用动态 ACL 或 ACL 名称）。要实施动态 ACL，必须将 RADIUS 服务器配置为支持动态 ACL。在用户进行身份验证时，RADIUS 服务器向 ASA 发送可下载的 ACL 或 ACL 名称。设备会根据 ACL 允许或拒绝对指定服务的访问。当身份验证会话到期时，ASA 会删除 ACL。

除了 ACL 以外，ASA 还支持 VPN 远程访问和防火墙直接转发代理会话的权限授权与设置的许多其他属性。

支持的 RADIUS 属性集

ASA 支持以下 RADIUS 属性集：

- RFC 2138 和 2865 中定义的身份验证属性。
- RFC 2139 和 2866 中定义的记帐属性。
- RFC 2868 和 6929 中定义的用于隧道协议支持的 RADIUS 属性。
- RADIUS 供应商 ID 9 确定的思科 IOS 供应商特定属性 (VSA)。
- RADIUS 供应商 ID 3076 确定的思科 VPN 相关 VSA。
- RFC 2548 中定义的 Microsoft VSA。

支持的 RADIUS 授权属性

授权是指执行权限或属性的过程。如果已配置权限或属性，则定义为身份验证服务器的 RADIUS 服务器会执行权限或属性。这些属性具有供应商 ID 3076。

下表列出了可用于用户授权的受支持 RADIUS 属性。

注释 RADIUS 属性名称不包含 cVPN3000 前缀。思科安全 ACS 4.x 支持这一新的命名法，但 ACS 4.0 之前版本中的属性名称仍然包含 cVPN3000 前缀。ASA 基于属性数字 ID（而非属性名称）实施 RADIUS 属性。

下表中列出的所有属性均为从 RADIUS 服务器发送到 ASA 的下游属性，但以下属性除外：146、150、151 和 152。这些属性编号是从 ASA 发送到 RADIUS 服务器的上游属性。RADIUS 属性 146 和 150 是从 ASA 发送到 RADIUS 服务器，以提出身份验证和请求授权。前面列出的所有四个属性都是从 ASA 发送到 RADIUS 服务器，以提出开始记账、临时更新和停止请求。8.4(3) 版本引入了上游 RADIUS 属性 146、150、151 和 152。

表 *46:* 支持的 *RADIUS* 授权属性

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
Access-Hours	支持	1	字符串	单值	时间范围的名称，例如工作时间
Access-List-Inbound	支持	86	字符串	单值	ACL ID
Access-List-Outbound	支持	87	字符串	单值	ACL ID
Address-Pools	支持	217	字符串	单值	IP 本地池的名称
Allow-Network-Extension-Mode	支持	64	布尔值	单值	0 = 已禁用 1 = 已启用
Authenticated-User-Idle-Timeout	支持	50	整数	单值	1-35791394 分钟
Authorization-DN-Field	支持	67	字符串	单值	可能的值：UID、OU、O、CN、L、SP、T、N、GN、SN、I、GENQ、DNQ、SE use-entire-name
Authorization-Required		66	整数	单值	0 = 否 1 = 是
Authorization-Type	支持	65	整数	单值	0 = 无 1 = RADIUS 2 = LDAP
Banner1	支持	15	字符串	单值	要为思科 VPN 远程访问会话显示的横幅 IPsec IKEv1、 Secure Client SSL TLS/DTL Clientless SSL。
Banner2	支持	36	字符串	单值	要为思科 VPN 远程访问会话显示的横幅 IPsec IKEv1、 Secure Client SSL TLS/DTL Clientless SSL。如果进行了相应的配置，字符串会连接到 Banner1 字符串。
Cisco-IP-Phone-Bypass	支持	51	整数	单值	0 = 已禁用 1 = 已启用
Cisco-LEAP-Bypass	支持	75	整数	单值	0 = 已禁用 1 = 已启用

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
Client Type	支持	150	整数	单值	1 = 思科 VPN 客户端 (IKEv1) 2 = Secure Clie VPN 3 = 无客户端 SSL VPN 4 = 直接转发代 L2TP/IPsec SSL VPN 6 = Secure Client IPsec (IKEv2)
Client-Type-Version-Limiting	支持	77	字符串	单值	IPsec VPN 版本号字符串
DHCP-Network-Scope	支持	61	字符串	单值	IP 地址
Extended-Authentication-On-Rekey	支持	122	整数	单值	0 = 已禁用 1 = 已启用
Framed-Interface-Id	支持	96	字符串	单值	分配的 IPv6 接口 ID。与 Framed-IPv6-Prefix 用以创建完整的已分配 IPv6 地址。例如：Framed-Interface-ID =1:1:1:1与 Framed-IPv6-P =2001:0db8::/64 组合可提供分配的IP地址 2001:0db8::1:1:1:1。
Framed-IPv6-Prefix	支持	97	字符串	单值	分配的 IPv6 前缀和长度。与 Framed-Interfac 合以创建完整的已分配 IPv6 地址。例如：前 2001:0db8::/64 与 Framed-Interface-Id=1:1:1:1 提供IP地址 2001:0db8::1:1:1:1。通过分配前缀 为/128 的完整 IPv6 地址（例如，Framed-IPv6-Prefix=2001:0db8::1/128），可以 属性分配IP地址而不使用 Framed-Interface-Id
Group-Policy	支持	25	字符串	单值	为远程访问 VPN 会话设置组策略。对于 8.2. 及更高版本，请改用此属性而非 IETF-Radius- 您可以使用以下其中一种格式： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
IE-Proxy-Bypass-Local		83	整数	单值	0 = 无 1 = 本地
IE-Proxy-Exception-List		82	字符串	单值	换行符 (\n) 分隔的 DNS 域列表
IE-Proxy-PAC-URL	支持	133	字符串	单值	PAC 地址字符串
IE-Proxy-Server		80	字符串	单值	IP 地址
IE-Proxy-Server-Policy		81	整数	单值	1 = 无修改 2 = 无代理 3 = 自动检测 4 = 使用 设置
IKE-KeepAlive-Confidence-Interval	支持	68	整数	单值	10 到 300 秒

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
IKE-Keepalive-Retry-Interval	支持	84	整数	单值	2 到 10 秒
IKE-Keep-Alives	支持	41	布尔值	单值	0 = 已禁用 1 = 已启用
Intercept-DHCP-Configure-Msg	支持	62	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Allow-Passwd-Store	支持	16	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Authentication		13	整数	单值	0 = 无 1 = RADIUS 2 = LDAP（仅适用于 = NT 域 4 = SDI 5 = 内部 6 = RADIUS 到 Active Directory
IPsec-Auth-On-Rekey	支持	42	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Backup-Server-List	支持	60	字符串	单值	服务器地址（以空格分隔）
IPsec-Backup-Servers	支持	59	字符串	单值	1 = 使用客户端配置的列表 2 = 禁用并清除 表 3 = 使用备份服务器列表
IPsec-Client-Firewall-Filter-Name		57	字符串	单值	指定要作为防火墙策略推送到客户端的过 称
IPsec-Client-Firewall-Filter-Optional	支持	58	整数	单值	0 = 必需 1 = 可选
IPsec-Default-Domain	支持	28	字符串	单值	指定要发送到客户端的单个默认域名（1 符）。
IPsec-IKE-Peer-ID-Check	支持	40	整数	单值	1 = 必需 2 = 如果对等证书支持 3 = 不检
IPsec-IP-Compression	支持	39	整数	单值	0 = 已禁用 1 = 已启用
IPsec-Mode-Config	支持	31	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP	支持	34	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP-Port	支持	35	整数	单值	4001 到 49151。默认值为 10000。
IPsec-Required-Client-Firewall-Capability	支持	56	整数	单值	0 = 无 1 = 远程 FW Are-You-There (AYT) 略 2 = 策略推送的 CPP 4 = 来自服务器的
IPsec-Sec-Association		12	字符串	单值	安全关联的名称
IPsec-Split-DNS-Names	支持	29	字符串	单值	指定要发送到客户端的辅助域名列表（1 符）。
IPsec-Split-Tunneling-Policy	支持	55	整数	单值	0 = 无拆分隧道 1 = 拆分隧道 2 = 允许本

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
IPsec-Split-Tunnel-List	支持	27	字符串	单值	指定用于描述分割隧道包含列表的网络或 AC 称。
IPsec-Tunnel-Type	支持	30	整数	单值	1 = LAN 到 LAN 2 = 远程访问
IPsec-User-Group-Lock		33	布尔值	单值	0 = 已禁用 1 = 已启用
IPv6-Address-Pools	支持	218	字符串	单值	IP 本地池 IPv6 的名称
IPv6-VPN-Filter	支持	219	字符串	单值	ACL 值
L2TP-Encryption		21	整数	单值	位图： 1 = 需要加密 2 = 40 位 4 = 128 位 8 无状态 15= 40/128 位加密/需要无状态
L2TP-MPPC-Compression		38	整数	单值	0 = 已禁用 1 = 已启用
Member-Of	支持	145	字符串	单值	逗号分隔的字符串，例如： `Engineering, Sales` 可在动态访问策略里使用的管理属性。不设 略。
MS-Client-Subnet-Mask	支持	63	布尔值	单值	IP 地址
NAC-Default-ACL		92	字符串		ACL
NAC-Enable		89	整数	单值	0 = 否 1 = 是
NAC-Revalidation-Timer		91	整数	单值	300 到 86400 秒
NAC-Settings	支持	141	字符串	单值	NAC 策略名称
NAC-Status-Query-Timer		90	整数	单值	30 到 1800 秒
Perfect-Forward-Secrecy-Enable	支持	88	布尔值	单值	0 = 否 1 = 是
PPTP-Encryption		20	整数	单值	位图： 1 = 需要加密 2 = 40 位 4 = 128 位 8 无状态 15= 40/128 位加密/需要无状态
PPTP-MPPC-Compression		37	整数	单值	0 = 已禁用 1 = 已启用
Primary-DNS	支持	5	字符串	单值	IP 地址
Primary-WINS	支持	7	字符串	单值	IP 地址
Privilege-Level	支持	220	整数	单值	介于 0 和 15 之间的整数。

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
Required-Client- Firewall-Vendor-Code	支持	45	整数	单值	1 = 思科系统（使用思科集成客户端） 2 = 3 = NetworkICE 4 = Sygate 5 = 思科系统 入侵防御安全代理）
Required-Client-Firewall-Description	支持	47	字符串	单值	字符串
Required-Client-Firewall-Product-Code	支持	46	整数	单值	思科系统公司产品： 1 = 思科入侵防御安全代理或思科集成客 Zone Labs 产品： 1 = Zone Alarm 2 = Zon 3 = Zone Labs Integrity NetworkICE 产品： 1 = BlackIce Defende Sygate 产品： 1 = Personal Firewall 2 = P Firewall Pro 3 = 安全代理
Required-Individual-User-Auth	支持	49	整数	单值	0 = 已禁用 1 = 已启用
Require-HW-Client-Auth	支持	48	布尔值	单值	0 = 已禁用 1 = 已启用
Secondary-DNS	支持	6	字符串	单值	IP 地址
Secondary-WINS	支持	8	字符串	单值	IP 地址
SEP-Card-Assignment		9	整数	单值	未使用
Session Subtype	支持	152	整数	单值	0 = 无 1 = 无客户端 2 = 客户端 3 = 仅客 Session Subtype 的适用条件是 Session Typ 性仅具有以下值：1、2、3 和 4。
Session Type	支持	151	整数	单值	0 = 无1 = Secure Client SSL VPN 2 = Secu IPSec VPN (IKEv2) 3 = 无客户端 SSL VP 户端邮件代理5 = 思科 VPN 客户端 (IKEv1) LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN
Simultaneous-Logins	支持	2	整数	单值	0 到 2147483647
Smart-Tunnel	支持	136	字符串	单值	智能隧道的名称
Smart-Tunnel-Auto	支持	138	整数	单值	0 = 已禁用 1 = 已启用 2 = 自动启动
Smart-Tunnel-Auto-Signon-Enable	支持	139	字符串	单值	智能隧道自动登录名称列表（附带域名）
Strip-Realm	支持	135	布尔值	单值	0 = 已禁用 1 = 已启用
SVC-Ask	支持	131	字符串	单值	0 = 已禁用 1 = 已启用 3 = 启用默认服务 认无客户端 （未使用 2 和 4）

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
SVC-Ask-Timeout	支持	132	整数	单值	5 到 120 秒
SVC-DPD-Interval-Client	支持	108	整数	单值	0 = 关 5-3600 秒
SVC-DPD-Interval-Gateway	支持	109	整数	单值	0 = 关） 5-3600 秒
SVC-DTLS	支持	123	整数	单值	0 = 错误 1 = 正确
SVC-Keepalive	支持	107	整数	单值	0 = 关 15-600 秒
SVC-Modules	支持	127	字符串	单值	字符串（模块的名称）
SVC-MTU	支持	125	整数	单值	MTU 值 256-1406 字节
SVC-Profiles	支持	128	字符串	单值	字符串（配置文件的名称）
SVC-Rekey-Time	支持	110	整数	单值	0 = 已禁用 1-10080 分钟
Tunnel Group Name	支持	146	字符串	单值	1 到 253 个字符
Tunnel-Group-Lock	支持	85	字符串	单值	隧道组的名称或“none”
Tunneling-Protocols	支持	11	整数	单值	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2T 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 互斥。 0 - 11、16 - 27、32 - 43、48 - 59 是合
Use-Client-Address		17	布尔值	单值	0 = 已禁用 1 = 已启用
VLAN	支持	140	整数	单值	0 到 4094
WebVPN-Access-List	支持	73	字符串	单值	访问列表名称
WebVPN ACL	支持	73	字符串	单值	设备上的 WebVPN ACL 的名称
WebVPN-ActiveX-Relay	支持	137	整数	单值	0 = 已禁用 Otherwise = 已启用
WebVPN-Apply-ACL	支持	102	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Auto-HTTP-Signon	支持	124	字符串	单值	保留
WebVPN-Citrix-Metaframe-Enable	支持	101	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Content-Filter-Parameters	支持	69	整数	单值	1 = Java ActiveX 2 = Java 脚本 4 = 映像 8 = 的 Cookie
WebVPN-Customization	支持	113	字符串	单值	自定义的名称
WebVPN-Default-Homepage	支持	76	字符串	单值	URL，例如 http://example-example.com

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
WebVPN-Deny-Message	支持	116	字符串	单值	有效字符串（最多 500 个字符）
WebVPN-Download_Max-Size	支持	157	整数	单值	0x7fffffff
WebVPN-File-Access-Enable	支持	94	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Browsing-Enable	支持	96	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Entry-Enable	支持	95	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	支持	78	字符串	单值	带可选通配符 (*) 的逗号分隔的 DNS/IP（ *.cisco.com、192.168.1.*、wwwin.cisco.co
WebVPN-Hidden-Shares	支持	126	整数	单值	0 = 无 1 = 可见
WebVPN-Home-Page-Use-Smart-Tunnel	支持	228	布尔值	单值	已启用（如果无客户端主页将通过智能隧道
WebVPN-HTML-Filter	支持	69	位图	单值	1 = Java ActiveX 2 = 脚本 4 = 映像 8 = C
WebVPN-HTTP-Compression	支持	120	整数	单值	0 = 关 1 = Deflate 压缩
WebVPN-HTTP-Proxy-IP-Address	支持	74	字符串	单值	逗号分隔的 DNS/IP:端口，带 http= 或 https 如 http=10.10.10.10:80、https=11.11.11.11:
WebVPN-Idle-Timeout-Alert-Interval	支持	148	整数	单值	0 到 30 0 = 已禁用。
WebVPN-Keepalive-Ignore	支持	121	整数	单值	0 到 900
WebVPN-Macro-Substitution	有	223	字符串	单值	无限制。
WebVPN-Macro-Substitution	有	224	字符串	单值	无限制。
WebVPN-Port-Forwarding-Enable	支持	97	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	支持	98	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-HTTP-Proxy	支持	99	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-List	支持	72	字符串	单值	端口转发列表名称
WebVPN-Port-Forwarding-Name	支持	79	字符串	单值	字符串名称（例如，“Corporate-Apps”） 此文本将替换无客户端门户主页上的默认 “Application Access”。
WebVPN-Post-Max-Size	支持	159	整数	单值	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	支持	149	整数	单值	0 到 30 0 = 已禁用。

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
WebVPN Smart-Card-Removal-Disconnect	支持	225	布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-Smart-Tunnel	支持	136	字符串	单值	智能隧道的名称
WebVPN-Smart-Tunnel-Auto-Sign-On	支持	139	字符串	单值	智能隧道自动登录名称列表（附带域名）
WebVPN-Smart-Tunnel-Auto-Start	支持	138	整数	单值	0 = 已禁用 1 = 已启用 2 = 自动启动
WebVPN-Smart-Tunnel-Tunnel-Policy	支持	227	字符串	单值	“e networkname”、“i networkname”或“a 一，其中 networkname 是指智能隧道网络列表 称，e表示不包含的隧道，i表示指定的隧道， 所有隧道。
WebVPN-SSL-VPN-Client-Enable	支持	103	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSL-VPN-Client-Keep- Installation	支持	105	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSL-VPN-Client-Required	支持	104	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSO-Server-Name	支持	114	字符串	单值	有效字符串
WebVPN-Storage-Key	支持	162	字符串	单值	
WebVPN-Storage-Objects	支持	161	字符串	单值	
WebVPN-SVC-Keepalive-Frequency	支持	107	整数	单值	15 到 600 秒，0 = 关闭
WebVPN-SVC-Client-DPD-Frequency	支持	108	整数	单值	5 到 3600 秒，0 = 关闭
WebVPN-SVC-DTLS-Enable	支持	123	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-DTLS-MTU	支持	125	整数	单值	MTU 值为 256 到 1406 个字节。
WebVPN-SVC-Gateway-DPD-Frequency	支持	109	整数	单值	5 到 3600 秒，0 = 关闭
WebVPN-SVC-Rekey-Time	支持	110	整数	单值	4 到 10080 分钟，0 = 关闭
WebVPN-SVC-Rekey-Method	支持	111	整数	单值	0（关闭）、1 (SSL)、2（新隧道）
WebVPN-SVC-Compression	支持	112	整数	单值	0（关闭）、1（Deflate 压缩）
WebVPN-UNIX-Group-ID (GID)	支持	222	整数	单值	有效 UNIX 组 ID
WebVPN-UNIX-User-ID (UID)	支持	221	整数	单值	有效 UNIX 用户 ID
WebVPN-Upload-Max-Size	支持	158	整数	单值	0x7fffffff
WebVPN-URL-Entry-Enable	支持	93	整数	单值	0 = 已禁用 1 = 已启用

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
WebVPN-URL-List	支持	71	字符串	单值	URL 列表名称
WebVPN-User-Storage	支持	160	字符串	单值	
WebVPN-VDI	支持	163	字符串	单值	设置列表

支持的 IETF RADIUS 授权属性

下表列出了支持的 IETF RADIUS 属性。

表 *47:* 支持的 *IETF RADIUS* 属性

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
IETF-Radius-Class	支持	25		单值	对于 8.2.x 版本及更高版本，我们建议使用 Group-Policy 属性 (VSA 3076，#25)： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称
IETF-Radius-Filter-Id	支持	11	字符串	单值	在 ASA 中定义的 ACL 名称，仅适用于全隧道 IPs 和 SSL VPN 客户端。
IETF-Radius-Framed-IP-Address	支持	n/a	字符串	单值	IP 地址
IETF-Radius-Framed-IP-Netmask	支持	n/a	字符串	单值	IP 地址掩码
IETF-Radius-Idle-Timeout	支持	28	整数	单值	秒
IETF-Radius-Service-Type	支持	6	整数	单值	秒。可能的 Service Type 值： • .Administrative - 允许用户访问配置提示符。 • .NAS-Prompt - 允许用户访问 exec 提示符。 • .remote-access - 允许用户访问网络
IETF-Radius-Session-Timeout	支持	27	整数	单值	秒

RADIUS 记帐连接断开原因代码

如果 ASA 在发送数据包时遇到连接断开问题，则会返回以下代码：

连接断开原因代码
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

AAA 的 RADIUS 服务器准则

本节介绍您在配置用于 AAA 的 RADIUS 服务器之前应检查的准则和限制。

- 在单模式下可以有最多 200 个服务器组，在多模式下每个情景可以有 4 个服务器组。

- 在单模式下每个组可以有最多 16 个服务器，在多模式下每个组可以有 8 个服务器。
- RADIUS 负载的最大长度为 4096 字节。

配置用于 AAA 的 RADIUS 服务器

本节介绍如何配置用于 AAA 的 RADIUS 服务器。

过程

步骤 1 将 ASA 属性加载到 RADIUS 服务器。用于加载属性的方法取决于您使用的 RADIUS 服务器类型：

- 对于思科 ACS：服务器已集成这些属性。您可以跳过此步骤。
- 对于来自其他供应商的 RADIUS 服务器（例如 Microsoft 互联网身份验证服务）：必须手动定义每个 ASA 属性。要定义属性，请使用属性名称或编号、类型、值和供应商代码 (3076)。

步骤 2 配置 RADIUS 服务器组，第 1201 页。

步骤 3 向组中添加 RADIUS 服务器，第 1205 页。

配置 RADIUS 服务器组

如果您要将外部 RADIUS 服务器用于身份验证、授权或记帐，则必须先为每个 AAA 协议创建至少一个 RADIUS 服务器组，然后向每个服务器组添加一个或多个服务器。

过程

步骤 1 创建 RADIUS AAA 服务器组。

aaa-server *group_name* **protocol radius**

示例：

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)#
```

当您输入 **aaa-server protocol** 命令时，系统将会进入 aaa-server 组配置模式。

步骤 2 （可选。）指定在尝试下一服务器前，会向组中带有 RADIUS 服务器的失败的 AAA 事务最大数量发送的请求的最大数量。

max-failed-attempts *number*

范围为 1 至 5。默认值为 3。

如果您使用本地数据库（仅用于管理访问）配置了回退方法，并且组中的所有服务器都无法响应，或者其响应无效，则会将该组视为无响应，并将尝试回退方法。该服务器组会在10分钟（默认值）内保持标记为无响应，以确保该时段内其他AAA请求不会尝试联系该服务器组，而是立即使用回退方法。要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。

如果没有回退方法，则 ASA 将继续重试该组中的服务器。

示例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

步骤 3 （可选。）指定用于重新激活组中的故障服务器的方法（重新激活策略）。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

其中：

- **depletion** [**deadtime** *minutes*] 仅在组中的所有服务器都处于非活动状态后才重新激活故障服务器。这是默认重新激活模式。可以指定从禁用组内最后一个服务器到随后重新启用所有服务器所经过的时长（0 到 1440 分钟之间）。仅当配置回退到本地数据库时，失效时间时间才适用；身份验证将在本地尝试，直到失效时间结束。默认值为 10 分钟。
- **timed** 在 30 秒钟的停机时间后重新激活出现故障的服务器。

示例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

步骤 4 （可选。）向组中的所有服务器发送记帐消息。

accounting-mode simultaneous

如要恢复仅向活动服务器发送消息的默认设置，请输入 **accounting-mode single** 命令。

示例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

步骤 5 （可选。）启用 RADIUS 临时记帐更新消息的定期生成。

interim-accounting-update [**periodic** [*hours*]]

ISE 将基于其从 NAS 设备（如 ASA）收到的记帐记录，保留一个活动会话的目录。不过，如果 ISE 为期 5 天没有接收到该会话仍处于活动状态的任何指示（记帐消息或终端安全评估事务处理），则它将删除从其数据库中删除该会话记录。为了确保长期VPN连接不被删除，请将该组配置为针对所有活动会话向 ISE 发送定期临时记帐更新消息。

- **periodic**[*hours*] 允许为每个被配置为向有关服务器组发送审计记录的 VPN 会话定期生成和传输审计记录。可以选择包括发送这些更新的间隔（以小时为单位）。默认值为 24 小时，范围为 1 至 120。

- （无参数。）如果使用不带 **periodic** 关键字的此命令，则 ASA 仅会在将 VPN 隧道连接添加到无客户端 VPN 会话时发送临时审计更新消息。发生此情况时，将生成记帐更新，以便将新分配的 IP 地址通知给 RADIUS 服务器。

示例：

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

步骤 6 （可选。）为 AAA 服务器组启用 RADIUS 动态授权（ISE 授权更改，CoA）服务。

dynamic-authorization [**port** 编号]

可以选择是否指定端口。默认值为 1700，范围为 1024 至 65535。

当您在 VPN 隧道中使用服务器组时，RADIUS 服务器组将注册接收 CoA 通知，并且 ASA 会侦听用于从 ISE 获取 CoA 策略更新的端口。仅当您在远程访问 VPN 中结合 ISE 使用此服务器组时，才能启用动态授权。

示例：

```
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

步骤 7 （可选。）如果您不想将 ISE 用于授权，则请为 RADIUS 服务器组启用仅授权模式。（仅当您在远程访问 VPN 中结合 ISE 使用此服务器组时，才能启用仅授权模式。）

authorize-only

这表示当此服务器组用于授权时，RADIUS 访问请求消息将会构建为“仅授权”请求，而不是为 AAA 服务器定义的已配置的密码方法。如果您使用 **radius-common-pw** 命令为 RADIUS 服务器配置公用密码，则它将被忽略。

例如，如果您想将证书用于身份验证而不是此服务器组，则应使用仅授权模式。您仍可将此服务器组用于授权和在 VPN 隧道中记帐。

示例：

```
ciscoasa(config-aaa-server-group)# authorize-only
```

步骤 8 （可选。）将可下载 ACL 与来自 RADIUS 数据包的思科 AV 对中收到的 ACL 进行合并。

merge-dacl {**before-avpair** | **after-avpair**}

示例：

```
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

此选项仅适用于 VPN 连接。对于 VPN 用户，ACL 的形式可以是思科 AV 对 ACL、可下载 ACL 和在 ASA 上配置的 ACL。此选项确定可下载 ACL 和 AV 对 ACL 是否会合并，并且不适用于在 ASA 上配置的任何 ACL。

默认设置为 **no merge dacl**，此值指定可下载 ACL 将不与思科 AV 对 ACL 合并。如果同时收到 AV 对和可下载 ACL，则优先使用 AV 对。

before-avpair 选项指定可下载 ACL 条目应放置在思科 AV 对条目之前。

after-avpair 选项指定可下载 ACL 条目应放置在思科 AV 对条目之后。

示例

以下示例显示如何通过单个服务器添加一个 RADIUS 组：

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit
```

以下示例显示如何为动态授权(CoA)更新和每小时定期记帐配置ISE服务器组。其中包括使用 ISE 配置密码身份验证的隧道组配置。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

以下示例显示如何使用ISE为本地证书验证和授权配置隧道组。包括服务器组配置中的仅授权命令，因为不会将服务器组用于身份验证。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

向组中添加 RADIUS 服务器

要向组中添加 RADIUS 服务器，请执行以下步骤：

过程

步骤 1 确定 RADIUS 服务器及其所属的 AAA 服务器组。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

示例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

如果不指定 **(***interface_name***)**，则 ASA 默认使用**内部**接口。

步骤 2 指定 ASA 如何处理可下载 ACL 中收到的来自 RADIUS 服务器的网络掩码。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

示例：

```
ciscoasa(config-aaa-server-host)# acl-netmask-convert standard
```

关键字 **auto-detect** 指定 ASA 应尝试确定所使用的网络掩码表达式的类型。如果 ASA 检测到通配符网络掩码表达式，则会将其转换为标准网络掩码表达式。

standard 关键字指定 ASA 假定从 RADIUS 服务器接收的可下载 ACL 中仅包含标准网络掩码表达式。因而不会对通配符网络掩码表达式进行转换。

wildcard 关键字指定 ASA 假定从 RADIUS 服务器接收的可下载 ACL 中仅包含通配符网络掩码表达式，并会在下载 ACL 时将所有通配符网络掩码表达式转换为标准网络掩码表达式。

步骤 3 指定用于所有通过 ASA 访问 RADIUS 授权服务器的用户的公用密码。

radius-common-pw 字符串

示例：

```
ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc
```

string 参数区分大小写，其字母数字关键字最长为 127 个字符，用作 RADIUS 服务器所有授权交易的公用密码。

步骤 4 对 RADIUS 服务器启用 MS-CHAPv2 身份验证请求。

mschapv2-capable

示例：

```
ciscoasa(config-aaa-server-host)# mschapv2-capable
```

步骤 5 指定与服务器的连接尝试超时值。

timeout 秒

指定服务器的超时间隔（1-300 秒）；默认值为 10 秒。对于每个 AAA 事务，ASA 将重试连接尝试（基于 **retry-interval** 命令中定义的间隔），直到达到超时。如果连续失败事务数量达到 AAA 服务器组中 max-failed-attempts 命令上指定的上限，则将会停用 AAA 服务器，并且ASA 将开始向另一台 AAA 服务器（如果已配置）发送请求。

示例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

步骤 6 配置针对上一个命令中指定的特定 AAA 服务器重试尝试之间的时长。

retry-interval 秒

示例：

```
ciscoasa(config-aaa-server-host)# retry-interval 8
```

seconds 参数指定请求的重试间隔（1-10 秒）。这是 ASA 在重试连接请求之前等待的时间。

注释
对于 RADIUS 协议，如果服务器回复“无法访问 ICMP 端口”消息，则系统会忽略 retry-interval 设置，并且 AAA 服务器会立即进入故障状态。如果这是 AAA 组中的唯一服务器，则会重新激活该服务器并向其发送另一个请求。这是预期行为。

步骤 7 将记帐消息发送到组中的所有服务器。

accounting-mode simultaneous

示例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

如要恢复仅向活动服务器发送消息的默认设置，请输入 **accounting-mode single** 命令。

步骤 8 将身份验证端口指定为端口 1645 或者指定用于用户身份验证的服务器端口。

authentication-port 端口

示例：

```
ciscoasa(config-aaa-server-host)# authentication-port 1646
```

步骤 9 将记帐端口指定为端口 1646 或者指定用于主机记帐的服务器端口。

accounting-port 端口

示例：

```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```

步骤 10 指定用于向 ASA 验证 RADIUS 服务器的服务器密钥值。您配置的服务器密钥应与在 RADIUS 服务器中配置的密钥相匹配。如果您不知道服务器密钥值，请询问 RADIUS 服务器管理员。最大长度为 64 个字符。

key

示例：

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

您配置的服务器密钥应与在 RADIUS 服务器中配置的密钥相匹配。如果您不知道服务器密钥值，请询问 RADIUS 服务器管理员。最大长度为 64 个字符。

示例

以下示例显示如何将 RADIUS 服务器添加到现有 RADIUS 服务器组：

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# radius-common-pw myexaplepasswordabc123
ciscoasa(config-aaa-server-host)# mschapv2-capable
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accounting-mode simultaneous
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# authorization-port 1645
ciscoasa(config-aaa-server-host)# key mysecretkeyexampleiceage2
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

为 AAA 监控 RADIUS 服务器

请参阅以下命令来为 AAA 监控 RADIUS 服务器的状态：

- **show aaa-server**

  此命令可显示配置的 RADIUS 服务器统计信息。您可以使用 **clear aaa-server statistics** 命令将计数器重置为零。

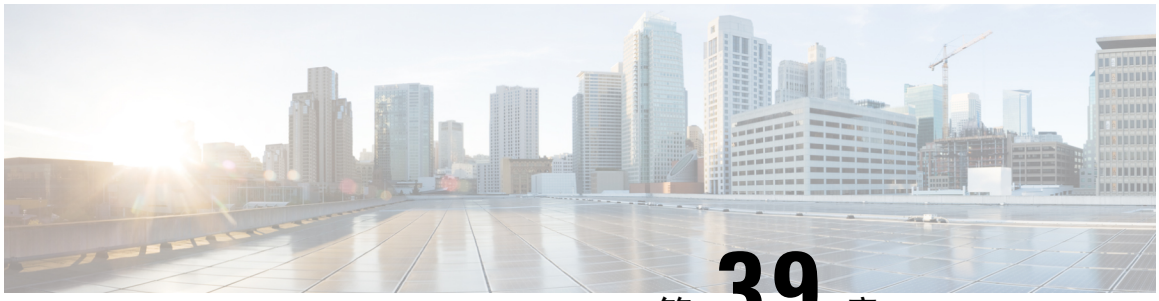
- **show running-config aaa-server**

  此命令可显示 RADIUS 服务器运行配置。

用于 AAA 的 RADIUS 服务器的历史记录

表 *48:* 用于 *AAA* 的 *RADIUS* 服务器的历史记录

功能名称	平台版本	说明
用于 AAA 的 RADIUS 服务器	7.0(1)	说明如何配置用于 AAA 的 RADIUS 服务器。 引入了以下命令： **aaa-server protocol**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**show aaa-server**、**show running-config aaa-server**、**clear aaa-server statistics**、**authentication-port**、**accounting-port**、**retry-interval**、**acl-netmask-convert**、**clear configure aaa-server**、**merge-dacl**、**radius-common-pw**、**key**。
在来自 ASA 的 RADIUS 访问请求和计费请求数据包中发送主要的供应商特有属性 (VSA)	8.4(3)	四个新 VSA - 通过来自 ASA 的 RADIUS 访问请求数据包发送 Tunnel Group Name (146) 和 Client Type (150)。通过来自 ASA 的 RADIUS 记帐请求数据包发送 Session Type (151) 和 Session Subtype (152)。为所有类型的记帐请求数据包（Start、Interim-Update 和 Stop）发送全部四个属性。RADIUS 服务器（例如 ACS 和 ISE）可以执行授权和策略属性，或者将这些属性用于记帐和收费。
每个组的 AAA 服务器组和服务器的数量上限都增加了。	9.13(1)	您可以配置更多 AAA 服务器组。在单情景模式下，您可以配置 200 AAA 服务器组（前一个限制为100）。在多情景模式下，您可以配置 8（前一个限制为4个）。 此外，在多情景模式下，您可以每组配置8个服务器（每个组的前一个限制为 4 个服务器）。单情景模式的每组限制 16，保持不变。 修改了以下命令以接受这些新限制：**aaa-server**、**aaa-server host**。



第 39 章

用于 AAA 的 TACACS+ 服务器

本章介绍如何配置 AAA 中使用的 TACACS+ 服务器。

- 关于用于 AAA 的 TACACS+ 服务器，第 1209 页
- 用于 AAA 的 TACACS+ 服务器准则，第 1210 页
- 配置 TACACS+ 服务器，第 1211 页
- 监控用于 AAA 的 TACACS+ 服务器，第 1214 页
- 用于 AAA 的 TACACS+ 服务器的历史记录，第 1215 页

关于用于 AAA 的 TACACS+ 服务器

ASA 支持使用以下协议进行 TACACS+ 服务器身份验证：ASCII、PAP、CHAP 和 MS-CHAPv1。

TACACS+ 属性

ASA 可支持 TACACS+ 属性。TACACS+ 属性可分隔身份验证、授权和记帐功能。该协议支持两种类型的属性：强制属性和可选属性。服务器和客户端都必须能够理解强制属性，而且必须将强制属性应用于用户。可选属性是否能被理解，或是否会被使用不作要求。

注释 要使用 TACACS+ 属性，请确保您已在 NAS 上启用 AAA 服务。

下表列出适用于直接转发代理连接的受支持的 TACACS+ 授权响应属性。

表 *49:* 支持的 *TACACS+* 授权响应属性

属性	说明
acl	确定要应用于连接的本地配置的 ACL。
idletime	指示经过身份验证的用户会话终止前可以处于非活动状态的时长（以分钟为单位）。

属性	说明
timeout	指示经过身份验证的用户会话终止前，身份验证凭据可以保持活动状态的时长（以分钟为单位）。

下表列出支持的 TACACS+ 记帐属性。

.

表 *50:* 支持的 *TACACS+* 记帐属性

属性	说明
bytes_in	指定此连接过程中传输的输入字节的数量（仅停止记录）
bytes_out	指定此连接过程中传输的输出字节的数量（仅停止记录）。
cmd	定义执行的命令（仅命令记帐）。
disc-cause	指定标识连接断开原因的数值代码（仅停止记录）。
elapsed_time	定义连接所消耗的秒数（仅停止记录）。
foreign_ip	指定隧道连接的客户端的 IP 地址。定义用于直接转发代理连接的最低安全性接口上的地址。
local_ip	指定对于隧道连接，客户端已连接到的 IP 地址。定义用于直接转发代理连接的最高安全性接口上的地址。
NAS port	包含连接的会话 ID。
packs_in	指定此连接过程中传输的输入数据包的数量。
packs_out	指定此连接过程中传输的输出数据包的数量。
priv-level	设置为命令记帐请求的用户权限级别，否则设置为 1。
rem_iddr	指示客户端的 IP 地址。
service	指定所使用的服务。对于仅进行命令记帐的情况，始终设置为“shell”。
task_id	指定记帐事务的唯一任务 ID。
username	指定用户的名称。

用于 AAA 的 TACACS+ 服务器准则

本节介绍您在配置用于 AAA 的 TACACS+ 服务器之前应检查的准则和限制。

IPv6

AAA 服务器可以使用 IPv4 或 IPv6 地址。

其他准则

- 在单模式下可以有最多 200 个服务器组，在多模式下每个情景可以有 4 个服务器组。
- 在单模式下每个组可以有最多 16 个服务器，在多模式下每个组可以有 8 个服务器。
- 对于在 ASA 设备模式下运行的 FPR1000、FPR2100 或 FPR3100 系列，必须遵守以下用户名约定：
  - 必须是 Linux 有效的用户名。
  - 必须仅使用小写字母。
  - 可以包含字母数字字符、句点 (.) 或连字符 (-)。
  - 必须不包含其他特殊字符，例如 at 符号 (@) 和斜线 (/)。

配置 TACACS+ 服务器

本节介绍如何配置 TACACS+ 服务器。

过程

步骤 1 配置 TACACS+ 服务器组，第 1211 页。

步骤 2 向组中添加 TACACS+ 服务器，第 1213 页。

配置 TACACS+ 服务器组

如果要将 TACACS+ 服务器用于身份验证、授权或记帐，则必须先创建至少一个 TACACS+ 服务器组，然后向每个服务器组添加一台或多台服务器。您可以按名称标识 TACACS+ 服务器组。

要添加 TACACS+ 服务器组，请执行以下步骤：

过程

步骤 1 确定服务器组名称和协议。

aaa-server *server_tag* **protocol tacacs+**

示例：

```
ciscoasa(config)# aaa-server servergroup1 protocol tacacs+
```

当您输入 **aaa-server protocol** 命令时，系统将会进入 aaa-server 组配置模式。

步骤 2 指定在尝试下一服务器前，会向组中带有 AAA 服务器的失败的 AAA 事务最大数量发送的请求的最大数量。

max-failed-attempts 编号

示例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 参数的范围可介于 1 到 5 之间。默认值为 3。

如果您使用本地数据库（仅用于管理访问）配置了回退方法，并且组中的所有服务器都无法响应，或者其响应无效，则会将该组视为无响应，并将尝试回退方法。该服务器组会在10分钟（默认值）内保持标记为无响应，以确保该时段内其他AAA请求不会尝试联系该服务器组，而是立即使用回退方法。要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。

如果没有回退方法，则 ASA 将继续重试该组中的服务器。

步骤 3 指定用于重新激活组中的故障服务器的方法（重新激活策略）。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

示例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

depletion 关键字仅在组中的所有服务器都处于非活动状态后才会重新激活故障服务器。

deadtime *minutes* 关键字参数对用于指定从禁用组中的最后一个服务器到随后重新启用所有服务器所经过的时间，范围介于 0 到 1440（以分钟为单位）之间。仅当配置回退到本地数据库时，失效时间时间才适用；身份验证将在本地尝试，直到失效时间结束。默认值为 10 分钟。

timed 关键字可在 30 秒停机时间后重新激活故障服务器。

步骤 4 将记帐消息发送到组中的所有服务器。

accounting-mode simultaneous

示例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

如要恢复仅向活动服务器发送消息的默认设置，请输入 **accounting-mode single** 命令。

示例

以下示例显示，如何添加拥有一台主用服务器和一台备用服务器的一个 TACACS+ 组。

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

向组中添加 TACACS+ 服务器

要将 TACACS+ 服务器添加到服务器组，请执行以下操作：

过程

步骤 1 确定 TACACS+ 服务器，以及该服务器所属的服务器组。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

示例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

如果不指定 **(***interface_name***)**，则 ASA 默认使用内部。

服务器可以使用 IPv4 或 IPv6 地址。

步骤 2 指定与服务器的连接尝试超时值。

timeout 秒

指定服务器的超时间隔（1-300 秒）；默认值为 10 秒。对于每个 AAA 事务，ASA 将重试连接尝试（基于 **retry-interval** 命令中定义的间隔），直到达到超时。如果连续失败事务数量达到 AAA 服务器组中 max-failed-attempts 命令上指定的上限，则将会停用 AAA 服务器，并且ASA 将开始向另一台 AAA 服务器（如果已配置）发送请求。

示例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

步骤 3 指定服务器端口作为端口号 49，或 ASA 与 TACACS+ 服务器进行通信所用的 TCP 端口号。

server-port *port_number*

示例：

```
ciscoasa(config-aaa-server-host)# server-port 49
```

步骤 4 指定服务器密钥值，该密钥值用于面向 TACACS+ 服务器对 NAS 进行身份验证。

key

示例：

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

此密钥值是一个区分大小写的字母数字关键字，最大长度为 127 个字符，它的值与 TACACS+ 服务器上的密钥相同。超出127个字符后的所有字符都会被忽略。该密钥会在客户端和服务器之间使用，用于加密它们之间传输的数据，该密钥在客户端和服务器系统上必须相同。该密钥不能包含空格，但允许包含其他的特殊字符。

监控用于 AAA 的 TACACS+ 服务器

请参阅以下用于监控用于 AAA 的 TACACS+ 服务器的命令：

- **show aaa-server**

  此命令可显示已配置的 TACACS+ 服务器统计信息。输入 **clear aaa-server statistics** 命令可清除 TACACS+ 服务器统计信息。

- **show running-config aaa-server**

  此命令可显示 TACACS+ 服务器运行配置。输入 **clear configure aaa-server** 命令可清除 TACACS+ 服务器配置。

用于 AAA 的 TACACS+ 服务器的历史记录

表 *51:* 用于 *AAA* 的 *TACACS+* 服务器的历史记录

功能名称	平台版本	说明
TACACS+ 服务器	7.0(1)	介绍如何配置用于 AAA 的 TACACS+ 服务器。 引入了以下命令： **aaa-server protocol**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**aaa authorization exec authentication-server**、**server-port**、**key**、**clear aaa-server statistics**、**clear configure aaa-server**、**show aaa-server**、**show running-config aaa-server**、**username**、**service-type**、**timeout**。
包含 IPv6 地址、用于 AAA 的 TACACS+ 服务器	9.7(1)	现在可以将 IPv4 或 IPv6 地址用于 AAA 服务器。
每个组的 AAA 服务器组和服务器的数量上限都增加了。	9.13(1)	您可以配置更多 AAA 服务器组。在单情景模式下，您可以配置 200 AAA 服务器组（前一个限制为100）。在多情景模式下，您可以配置 8（前一个限制为4个）。 此外，在多情景模式下，您可以每组配置 8 个服务器（每个组的前一个限制为 4 个服务器）。单情景模式的每组限制 16，保持不变。 修改了以下命令以接受这些新限制：**aaa-server**、**aaa-server host**。

第 40 章

用于 AAA 的 LDAP 服务器

本章介绍如何配置 AAA 中使用的 LDAP 服务器。

- 关于 LDAP 和 ASA，第 1217 页
- AAA 的 LDAP 服务器准则，第 1220 页
- 配置用于 AAA 的 LDAP 服务器，第 1221 页
- 监控用于 AAA 的 LDAP 服务器，第 1227 页
- 用于 AAA 的 LDAP 服务器的历史记录，第 1228 页

关于 LDAP 和 ASA

ASA 与大多数 LDAPv3 目录服务器兼容，包括：

- Sun Microsystems JAVA System Directory Server，目前是 Oracle Directory Server Enterprise Edition 的一部分，以前称为 Sun ONE Directory Server
- Microsoft Active Directory
- Novell
- OpenLDAP

默认情况下，ASA 会自动检测其是否连接到 Microsoft Active Directory、Sun LDAP、Novell、OpenLDAP 或通用 LDAPv3 目录服务器。但是，如果自动检测无法确定 LDAP 服务器类型，则可以手动对其进行配置。

身份验证如何与 LDAP 配合使用

在身份验证过程中，ASA 将充当用户的 LDAP 服务器的客户端代理，并以明文形式或通过使用 SASL 协议对 LDAP 服务器执行身份验证。默认情况下，ASA 以明文形式将身份验证参数（通常是用户名和密码）传递到 LDAP 服务器。

ASA 仅支持 Digest-MD5 SASL 机制。利用这种机制，ASA 会用根据用户名和密码计算出的 MD5 值响应 LDAP 服务器。

对用户成功执行 LDAP 身份验证后，LDAP 服务器将返回已通过身份验证的用户的属性。对于 VPN 身份验证，这些属性通常包括已应用于 VPN 会话的授权数据。在此情况下，使用 LDAP 即可一步完成身份验证和授权。

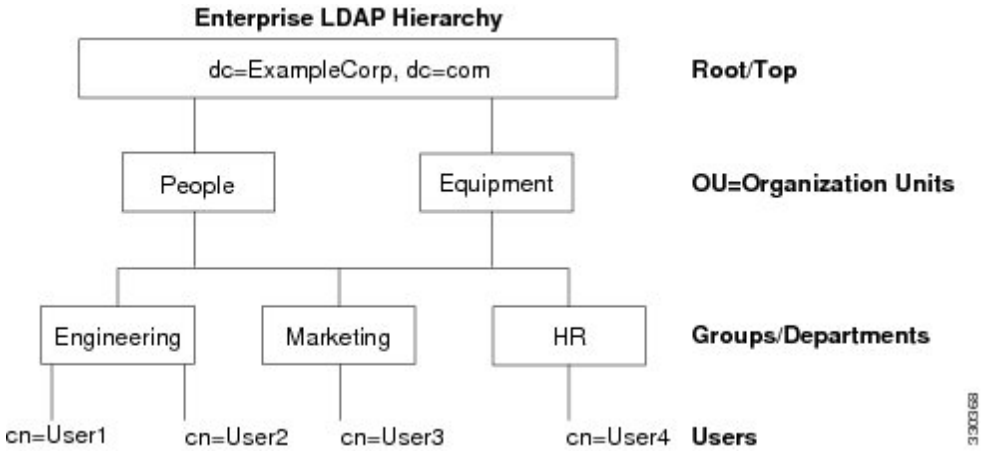
注释 有关 LDAP 协议的详细信息，请参阅 RFC 1777、2251 和 2849。

LDAP 层次结构

您的 LDAP 配置应反映贵组织的逻辑层次结构。例如，假设贵公司 Example Corporation 的一名员工名为 Employee1。Employee1 在 Engineering 组工作。您的 LDAP 层次结构可能有一个或多个级别。您可能决定设置一个单级别层次结构，在其中 Employee1 被视为 Example Corporation 的一名成员。您也可以设置一个多级别层次结构，在其中 Employee1 被视为 Engineering 部门的一名成员，该部门是一个称为 People 的组织单位的成员，而该组织单位本身是 Example Corporation 的成员。有关多级别层次结构的示例，请参阅下图。

虽然多级层次结构包含较多详细信息，但在单级层次结构中搜索结果返回的速度更快。

图 *81:* 多级 *LDAP* 层次结构



搜索 LDAP 层次结构

通过 ASA，可以在 LDAP 层次结构中定制搜索。在 ASA 上配置以下三个字段，以定义在 LDAP 层次结构中开始搜索的位置、搜索范围和查找的信息类型。这些字段共同将层次结构的搜索仅限于包含用户权限的部分。

- LDAP Base DN 定义服务器从 ASA 收到授权请求时应开始在 LDAP 层次结构中搜索用户信息的位置。
- Search Scope 定义在 LDAP 层次结构中的搜索范围。搜索继续在层次结构中 LDAP Base DN 下方的多个级别进行。您可以选择使服务器仅搜索其正下方的级别，否则，它可能搜索整个子树。单级别搜索速度更快，但子树搜索更加广泛。

- Naming Attribute 定义唯一识别 LDAP 服务器中条目的 RDN。常用命名属性可以包括 cn（通用名称）、sAMAccountName 和 userPrincipalName。

该图显示 Example Corporation 的样本 LDAP 层次结构。鉴于该层次结构，您能够以不同的方式定义搜索。下表显示两种样本搜索配置。

在第一个配置示例中，当 Employee1 使用所需的 LDAP 授权建立 IPsec 隧道时，ASA 将向 LDAP 服务器发送一个搜索请求，指明其应在 Engineering 组中搜索 Employee1。此搜索速度很快。

在第二个配置示例中，ASA 发送一个搜索请求，指明服务器应在 Example Corporation 内搜索 Employee1。此搜索需要更长时间。

表 *52:* 搜索配置示例

编号	LDAP Base DN	搜索范围	命名属性	结果
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	一个级别	cn=Employee1	搜索速度较快
2	dc=ExampleCorporation,dc=com	子树	cn=Employee1	搜索时间较长

绑定到 LDAP 服务器

ASA 使用登录 DN 和登录密码与 LDAP 服务器建立信任（绑定）。执行 Microsoft Active Directory 只读操作（例如身份验证、授权或组搜索）时，ASA 可以使用权限较少的登录 DN 进行绑定。例如，登录 DN 可能是其 AD“Member Of”指定属于 Domain Users 的一部分的用户。对于 VPN 密码管理操作，登录 DN 需要提升的权限，而且必须是 Account Operators AD 组的一部分。

以下是登录 DN 的一个示例：

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA 支持以下身份验证 方法：

- 在端口 389 上使用未加密密码执行简单 LDAP 身份验证
- 在端口 636 上执行安全 LDAP (LDAP-S)
- 简单身份验证和安全层 (SASL) MD5

ASA 不支持自治身份验证。

注释 作为 LDAP 客户端，ASA 不支持传输自治绑定或请求。

LDAP 属性映射

ASA 可为以下选项使用 LDAP 目录对用户进行身份验证：

- VPN 远程访问用户
- 防火墙网络访问/直通代理会话
- 设置策略权限（也称为授权属性），例如 ACL、书签列表、DNS 或 WINS 设置，以及会话计时器。
- 在本地组策略中设置关键属性

ASA 使用 LDAP 属性映射将本地 LDAP 用户属性转换为 ASA 属性。您可以将这些属性映射绑定到 LDAP 服务器或将其删除。您还可以显示或清除属性映射。

LDAP 属性映射不支持多值属性。例如，如果用户是多个 AD 组的成员，并且 LDAP 属性映射与多个组匹配，则根据匹配条目的字母顺序选择值。

要正确使用属性映射功能，您需要了解 LDAP 属性名称和值，以及用户定义的属性名称和值。

频繁映射的 LDAP 属性的名称以及经常将其映射到的用户定义属性的类型包括：

- IETF-Radius-Class（ASA 8.2 或更高版本中的 Group_Policy）- 根据目录部门或用户组（例如，Microsoft Active Directory memberOf）属性值设置组策略。组策略属性将 IETF-Radius-Class 属性替换为 ASDM V6.2/ASA V8.2 或更高版本。
- IETF-Radius-Filter-Id - 将访问控制列表或 ACL 应用于 VPN 客户端、IPsec 和 SSL。
- IETF-Radius-Framed-IP-Address - 将已分配的静态 IP 地址分配到 VPN 远程访问客户端、IPsec 和 SSL。
- Banner1 - 在 VPN 远程访问用户登录时显示文本横幅。
- Tunneling-Protocols - 根据访问类型，允许或拒绝 VPN 远程访问会话。

注释 单一 LDAP 属性映射可以包含一个或多个属性。只能从特定 LDAP 服务器映射一个 LDAP 属性。

AAA 的 LDAP 服务器准则

本节包含您在配置 AAA 的 LDAP 服务器之前应检查的准则和限制。

IPv6

AAA 服务器可以使用 IPv4 或 IPv6 地址。

其他准则

- ASA 上配置的用于访问 Sun 目录的 DN 必须可以访问该服务器上的默认密码策略。建议使用目录管理员或具有目录管理员权限的用户作为 DN。或者，也可以将 ACL 放在默认密码策略上。
- 您必须通过 SSL 配置 LDAP，以便对 Microsoft Active Directory 和 Sun 服务器启用密码管理。
- ASA 不支持使用 Novell、OpenLDAP 和其他 LDAPv3 目录服务器进行密码管理。
- 自版本 7.1(x) 开始，ASA 将使用本地 LDAP 机制执行身份验证和授权，而不再需要思科机制。
- 在单模式下可以有最多 200 个服务器组，在多模式下每个情景可以有 4 个服务器组。
- 在单模式下每个组可以有最多 16 个服务器，在多模式下每个组可以有 8 个服务器。
- 当用户登录时，从您在配置中指定的第一个服务器开始，一次访问一个 LDAP 服务器，直到服务器响应为止。如果组中的所有服务器均不可用，在将本地数据库配置为回退方法（仅限管理身份验证和授权）时，ASA 将尝试本地数据库。如果没有回退方法，ASA 将继续尝试 LDAP 服务器。

配置用于 AAA 的 LDAP 服务器

本节介绍如何配置用于 AAA 的 LDAP 服务器。

过程

步骤 1 配置 LDAP 属性映射。请参阅配置 LDAP 属性映射，第 1221 页。

步骤 2 添加 LDAP 服务器组。请参阅配置 LDAP 服务器组，第 1223 页。

步骤 3 （可选）从 LDAP 服务器中配置独立和不同于身份验证机制的授权。请参阅使用 LDAP 为 VPN 配置授权，第 1226 页。

配置 LDAP 属性映射

要配置 LDAP 属性映射，请执行以下步骤：

过程

步骤 1 创建未填充的 LDAP 属性映射表。

ldap-attribute-map *map-name*

示例：

```
ciscoasa(config)# ldap-attribute-map att_map_1
```

步骤 2 将用户定义的属性名称部门映射到思科属性。

map-name *user-attribute-name Cisco-attribute-name*

示例：

```
ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class
```

步骤 3 将用户定义的映射值部门映射到用户定义的属性值和思科属性值。

map-value *user-attribute-name Cisco-attribute-name*

示例：

```
ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1
```

步骤 4 确定服务器及其所属的 AAA 服务器组。

aaa-server *server_group* [*interface_name*] **host** *server_ip*

示例：

```
ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4
```

步骤 5 将属性映射绑定到 LDAP 服务器。

ldap-attribute-map *map-name*

示例：

```
ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1
```

示例

下列显示如何基于名为 accessType 的 LDAP 属性将管理会话限制到 ASA。accessType 属性可能具有下列值之一：

- VPN
- admin
- helpdesk

下列显示每个值与 ASA 支持的其中一个有效 IETF-Radius-Service-Type 属性的对应关系：remote-access（服务类型 5）Outbound、admin（服务类型 6）Administrative 和 nas-prompt（服务类型 7）NAS Prompt。

```
ciscoasa(config)# ldap attribute-map MGMT
ciscoasa(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
ciscoasa(config-ldap-attribute-map)# map-value accessType VPN 5
ciscoasa(config-ldap-attribute-map)# map-value accessType admin 6
ciscoasa(config-ldap-attribute-map)# map-value accessType helpdesk 7

ciscoasa(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
ciscoasa(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password test
ciscoasa(config-aaa-server-host)# ldap-login-dn CN=Administrator,CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# server-type auto-detect
ciscoasa(config-aaa-server-host)# ldap-attribute-map MGMT
```

以下示例说明如何显示思科 LDAP 属性名称的完整列表：

```
ciscoasa(config)# ldap attribute-map att_map_1
ciscoasa(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
  Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
 :
 :
  X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

配置 LDAP 服务器组

要创建和配置 LDAP 服务器组，然后向该组中添加 LDAP 服务器，请执行以下步骤：

开始之前

您必须先添加属性映射，然后才能向 LDAP 服务器组中添加 LDAP 服务器。

过程

步骤 1 确定服务器组名称和协议。

aaa-server *server_tag* **protocol ldap**

示例：

```
ciscoasa(config)# aaa-server servergroup1 protocol ldap
ciscoasa(config-aaa-server-group)#
```

当您输入 **aaa-server protocol** 命令时，系统将会进入 aaa-server 组配置模式。

步骤 2 指定在尝试下一服务器前，会向组中带有 LDAP 服务器的失败的 AAA 事务最大数量发送的请求的最大数量。

max-failed-attempts 编号

示例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 参数的范围为 1 至 5。默认值为 3。

如已使用本地数据库（仅限管理访问）配置了回退方法来配置回退机制，并且组中的所有服务器均无法响应，或其响应无效，则将该组视为无响应，并会尝试回退方法。该服务器组会在10分钟（默认值）内保持标记为无响应，以确保该时段内其他AAA请求不会尝试联系该服务器组，而是立即使用回退方法。要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。

如果没有回退方法，则 ASA 将继续重试该组中的服务器。

步骤 3 指定用于重新激活组中的故障服务器的方法（重新激活策略）。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

示例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

depletion 关键字用于仅在组中的所有服务器都处于非活动状态后才重新激活故障服务器。

deadtime *minutes* 关键字参数对用于指定从禁用组中的最后一个服务器到随后重新启用所有服务器所经过的时间，范围介于 0 到 1440（以分钟为单位）之间。仅当配置回退到本地数据库时，失效时间时间才适用；身份验证将在本地尝试，直到失效时间结束。默认值为 10 分钟。

timed 关键字用于在 30 秒的停机时间后重新激活故障服务器。

步骤 4 识别 LDAP 服务器以及其所属的 AAA 服务器组。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

示例：

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

如果不指定 **(***interface_name***)**，则 ASA 默认使用**内部**接口。

当您输入 **aaa-server host** 命令时，系统将会进入 aaa-server 主机配置模式。根据需要，请使用主机配置模式命令进一步配置 AAA 服务器。

下表列出了可用于 LDAP 服务器的命令，以及新的 LDAP 服务器定义是否具有该命令的默认值。如果未提供默认值（以“-”表示），请使用命令指定该值。

表 *53:* 主机模式命令和默认值

命令	默认值	说明
ldap-attribute-map	-	—
ldap-base-dn	—	—
ldap-login-dn	—	—
ldap-login-password	—	—
ldap-naming-attribute	—	—
ldap-over-ssl	636	如果未设置，则 ASA 将 sAMAccountName 用于 LDAP 请求。无论是使用 SASL 还是明文，都可以通过 SSL 来保护 ASA 与 LDAP 服务器之间的通信。如果未配置 SASL，则强烈建议通过 SSL 来保护 LDAP 通信。 您可以使用 **reference-identity** 子模式命令配置 ASA 用于验证 LDAPS (SSL) 服务器身份的引用身份名称。配置后，ASA 将使用下配置的匹配条件验证 aaa-ldap 服务器 **crypto ca reference-identity** <*name*>。如果在证书使用者名称或 SAN 中找不到匹配项，或者如果使用 reference-identity 指定的主机未解析，则终止连接。
ldap-scope	-	—
sasl-mechanism	—	—
server-port	389	-
server-type	autodiscovery	如果自动检测无法确定 LDAP 服务器类型，并且您知道服务器是 Microsoft、Sun 或通用 LDAP 服务器，则可以手动配置服务器类型。
ssl-client-certificate	-	ASA 应作为客户端证书提供给 LDAP 服务器的证书。如果将 LDAP 服务器配置为验证客户端证书，则需要此证书。您还必须启用 **ldap-over-ssl**。如果不配置证书，当 LDAP 服务器要求时，ASA 不会提供证书。如果 LDAP 服务器配置为需要对等证书，则安全 LDAP 会话将无法完成，并且身份验证/授权请求将失败。
timeout	10 秒	-

示例

以下示例说明如何配置名为 watchdogs 的 LDAP 服务器组并向该组中添加 LDAP 服务器。由于示例未定义重试间隔或 LDAP 服务器侦听的端口，因此 ASA 使用这两个服务器特定参数的默认值。

```
ciscoasa(config)# aaa-server watchdogs protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

使用 LDAP 为 VPN 配置授权

成功进行 LDAP 用户身份验证以进行 VPN 访问后，ASA 将查询 LDAP 服务器，服务器将返回 LDAP 属性。这些属性通常包括应用于 VPN 会话的授权数据。以这种方式使用 LDAP 可一步完成身份验证和授权。

但是，有些情况下可能需要获得与身份验证机制分开而且不同的 LDAP 目录服务器的授权。例如，如果使用 SDI 或证书服务器执行身份验证，则不返回授权信息。对于这种情况下的用户授权，您可在身份验证成功后查询 LDAP 目录，分两步完成身份验证和授权。

如要使用 LDAP 设置 VPN 用户授权，请执行以下步骤。

过程

步骤 1 创建一个名为 remotegrp 的 IPsec 远程访问隧道组。

tunnel-group *groupname*

示例：

```
ciscoasa(config)# tunnel-group remotegrp
```

步骤 2 将服务器组和隧道组进行关联。

tunnel-group *groupname* **general-attributes**

示例：

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

步骤 3 将新隧道组分配到先前创建的 AAA 服务器组以进行授权。

authorization-server-group *group-tag*

示例：

```
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

示例

虽然有可用于特定要求的其他授权相关命令和选项，但以下示例说明用于使用 LDAP 进行用户授权的命令。然后，示例将创建一个名为 remote-1 的 IPsec 远程访问隧道组，并将新隧道组分配到先前创建的 ldap_dir_1 AAA 服务器组以进行授权：

```
ciscoasa(config)# tunnel-group remote-1 type ipsec-ra
ciscoasa(config)# tunnel-group remote-1 general-attributes
ciscoasa(config-general)# authorization-server-group ldap_dir_1
ciscoasa(config-general)#
```

在完成此配置工作后，接着您可以通过输入以下命令，配置其他的 LDAP 授权参数，如目录密码、搜索目录的起点和目录搜索的范围：

```
ciscoasa(config)# aaa-server ldap_dir_1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
ciscoasa(config-aaa-server-host)# ldap-login-dn obscurepassword
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)#
```

监控用于 AAA 的 LDAP 服务器

有关监控用于 AAA 的 LDAP 服务器的信息，请参阅以下命令：

- **show aaa-server**

  此命令显示已配置的 AAA 服务器统计信息。使用 **clear aaa-server statistics** 命令可清除 AAA 服务器统计信息。

- **show running-config aaa-server**

  此命令可显示 AAA 服务器运行配置。使用 **clear configure aaa-server** 命令可清除 AAA 服务器配置。

用于 AAA 的 LDAP 服务器的历史记录

表 *54: AAA* 服务器的历史记录

功能名称	平台版本	说明
用于 AAA 的 LDAP 服务器	7.0(1)	LDAP 服务器介绍对 AAA 的支持以及如何配置 LDAP 服务器。 引入了以下命令： **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type**、**ldap attribute-map**、**aaa-server protocol**、**aaa authentication telnet | ssh | serial**} **console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**authorization-server-group**、**tunnel-group**、**tunnel-group general-attributes**、**map-name**、**map-value**、**ldap-attribute-map**。
用于 AAA 的使用 IPv6 地址的 LDAP 服务器	9.7(1)	现在可以将 IPv4 或 IPv6 地址用于 AAA 服务器。
每个组的 AAA 服务器组和服务器的数量上限都增加了。	9.13(1)	您可以配置更多 AAA 服务器组。在单情景模式下，您可以配置 200 AAA 服务器组（前一个限制为100）。在多情景模式下，您可以配置 8（前一个限制为4个）。 此外，在多情景模式下，您可以每组配置 8 个服务器（每个组的前一个限制为 4 个服务器）。单情景模式的每组限制 16，保持不变。 修改了以下命令以接受这些新限制：**aaa-server**、**aaa-server host**。
相互 LDAPS 身份验证。	9.18(1)	您可以为 ASA 配置客户端证书，以便在请求证书进行身份验证时提供给 LDAP 服务器。此功能在通过 SSL 使用 LDAP 时适用。如果 LDAP 服务器配置为需要对等证书，则安全 LDAP 会话将无法完成，并且身份验证/授权请求将失败。 添加了以下命令：**ssl-client-certificate**。

第 41 章

用于 AAA 的 RSA SecurID 服务器

以下主题介绍如何配置 AAA 中使用的 RSA SecurID 服务器。RSA SecureID 服务器也称为 SDI 服务器，因为 SDI 是用于与其通信的协议。您可以使用 RSA SecurID 服务器对管理连接，网络访问和 VPN 用户访问进行身份验证。

- 关于 RSA SecurID 服务器，第 1229 页
- 用于 AAA 的 RSA SecurID 服务器准则，第 1229 页
- 配置用于 AAA 的 RSA SecurID 服务器，第 1230 页
- 监控用于 AAA 的 RSA SecurID 服务器，第 1233 页
- 用于 AAA 的 RSA SecurID 服务器的历史记录，第 1233 页

关于 RSA SecurID 服务器

您可以直接使用 RSA SecurID 服务器进行身份验证，也可以间接使用 RSA SecurID 服务器作为身份验证的第二因素。在后一种情况下，您需要在 SecurID 服务器和 RADIUS 服务器之间配置与 SecurID 服务器的关系，并将 ASA 配置为使用 RADIUS 服务器。

但是，如果要直接针对 SecurID 服务器进行身份验证，则需要为 SDI 协议（用于与这些服务器通信的协议）创建 AAA 服务器组。

使用 SDI 时，在创建 AAA 服务器组时只需指定主 SecurID 服务器。ASA 将在首次连接到服务器时检索 sdiconf.rec 文件，该文件列出所有 SecurID 服务器副本。然后，如果主服务器不响应，ASA 可以使用这些副本进行身份验证。

此外，您必须在 RSA 身份验证管理器中将 ASA 注册为身份验证代理。注册 ASA 之前，身份验证尝试将失败。

用于 AAA 的 RSA SecurID 服务器准则

- 在单模式下可以有最多 200 个服务器组，在多模式下每个情景可以有 8 个服务器组。
- 在单模式下每个组可以有最多 16 个服务器，在多模式下每个组可以有 8 个服务器。当用户登录时，从您在配置中指定的第一个服务器开始，一次访问一个服务器，直到服务器响应为止。

配置用于 AAA 的 RSA SecurID 服务器

以下主题介绍如何配置RSA SecurID服务器组。然后，您可以在配置管理访问或VPN时使用这些组。

配置 RSA SecurID AAA 服务器组

如果要使用与RSA SecurID服务器的直接通信进行身份验证，必须首先至少创建一个SDI服务器组，并向每个组添加一个或多个服务器。如果在与 RADIUS 服务器的代理关系中使用的是 SecurID 服务器，则无需在 ASA 上配置 SDI AAA 服务器组。

过程

步骤 1 创建 SDI AAA 服务器组并进入 aaa-server-group 配置模式。

aaa-server *server_group_name* **protocol sdi**

示例：

```
ciscoasa(config)# aaa-server watchdog protocol sdi
```

步骤 2 （可选。）指定在尝试下一服务器前，会向组中带有 AAA 服务器的失败的 AAA 事务最大数量发送的请求的最大数量。

max-failed-attempts 编号

示例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 参数的范围可介于 1 到 5 之间。默认值为 3。

如果您使用本地数据库（仅用于管理访问）配置了回退方法，并且组中的所有服务器都无法响应，或者其响应无效，则会将该组视为无响应，并将尝试回退方法。该服务器组会在10分钟（默认值）内保持标记为无响应，以确保该时段内其他AAA请求不会尝试联系该服务器组，而是立即使用回退方法。要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。

如果没有回退方法，则 ASA 将继续重试该组中的服务器。

步骤 3 （可选。）指定用于重新激活组中的故障服务器的方法（重新激活策略）。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

示例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

depletion 关键字仅在组中的所有服务器都处于非活动状态后才会重新激活故障服务器。该模式为默认模式。

deadtime *minutes* 关键字参数对用于指定从禁用组中的最后一个服务器到随后重新启用所有服务器所经过的时间，范围介于 0 到 1440（以分钟为单位）之间。仅当配置回退到本地数据库时，失效时间时间才适用；身份验证将在本地尝试，直到失效时间结束。默认值为 10 分钟。

timed 关键字可在 30 秒停机时间后重新激活故障服务器。

将 RSA SecurID 服务器添加到 SDI 服务器组

在使用 SDI 服务器组之前，必须至少向该组添加一个 RSA SecurID 服务器。

SDI 服务器组中的服务器使用身份验证和服务器管理协议 (ACE) 与 ASA 通信。

过程

步骤 1 将 RSA SecurID 服务器添加到 SDI 服务器组。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

示例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

如果不指定接口，则 ASA 默认使用**内部**接口。

您可以使用 IPv4 或 IPv6 地址。

步骤 2 指定与服务器的连接尝试超时值。

timeout 秒

指定服务器的超时间隔（1-300 秒）；默认值为 10 秒。对于每个 AAA 事务，ASA 将重试连接尝试（基于 **retry-interval** 命令中定义的间隔），直到达到超时。如果连续失败事务数量达到 AAA 服务器组中 **max-failed-attempts** 命令上指定的上限，则将会停用 AAA 服务器，并且ASA 将开始向另一台 AAA 服务器（如果已配置）发送请求。

示例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

步骤 3 指定重试间隔，即系统在重试连接请求之前等待的时间。

retry-interval 秒

您可以指定 1-10 秒。默认值为 10 秒。

示例：

```
ciscoasa(config-aaa-server-host)# retry-interval 6
```

步骤 4 如果服务器端口与默认 RSA SecurID 端口 (TCP / 5500) 不同，请指定服务器端口。ASA 在此端口上联系 RSA SecurID 服务器。

server-port *port_number*

示例：

```
ciscoasa(config-aaa-server-host)# server-port 5555
```

导入 SDI 节点密钥文件

您可以手动导入 RSA 身份验证管理器 (SecurID) 服务器生成的 node-secret 文件。

过程

步骤 1 从 RSA 身份验证管理器服务器导出节点密钥文件。有关详细信息，请参阅 RSA 身份验证管理器文档。

步骤 2 将节点加密文件的解压版本放在可从 ASA 访问的服务器上，或将其复制到 ASA 本身。

服务器必须支持以下传输协议之一：FTP、HTTP、HTTPS、SCP、SMB、TFTP。

步骤 3 导入节点密钥文件。

aaa sdi import-node-secret *filepath rsa_server_address password*

其中：

- *filepath* 是从 RSA 身份验证管理器导出的未压缩节点密钥文件的完整路径。本地系统上的文件可以编址为 disk0:、disk1: 或 flash:。对于远程服务器上的文件，请使用标准 URL 表示法，例如 ftp://。
- *rsa_server_address* 是节点密钥所属的 RSA 身份验证管理器服务器的 IP 地址或完全限定主机名。
- 密码是导出文件时用于保护文件的密码。

示例：

```
ciscoasa# aaa sdi import-node-secret nodesecret.rec rsaam.example.com mysecret
nodesecret.rec imported successfully
ciscoasa#
```

监控用于 AAA 的 RSA SecurID 服务器

您可以使用以下命令监控和清除 RSA SecurID 相关信息。

- **show aaa-server**

  显示 AAA 服务器统计信息。使用 **clear aaa-server statistics** 命令清除服务器统计信息。

- **show running-config aaa-server**

  显示为系统配置的 AAA 服务器。使用 **clear configure aaa-server** 命令删除 AAA 服务器配置。

- **show aaa sdi node-secrets**

  显示哪些 RSA SecurID 服务器具有导入的节点密钥文件。使用 **clear aaa sdi node-secret** 命令删除节点密钥文件。

用于 AAA 的 RSA SecurID 服务器的历史记录

功能名称	平台版本	说明
SecurID 服务器	7.2(1)	支持 AAA 的 SecurID 服务器进行管理身份验证。以前版本的 VPN 身份验证版本支持 SecurID。
用于AAA 的 IPv6 地址	9.7(1)	现在可以将 IPv4 或 IPv6 地址用于 AAA 服务器。
每个组的 AAA 服务器组和服务器的数量上限都增加了。	9.13(1)	您可以配置更多 AAA 服务器组。在单情景模式下，您可以配置 200 AAA 服务器组（前一个限制为100）。在多情景模式下，您可以配置 8（前一个限制为4个）。 此外，在多情景模式下，您可以每组配置 8 个服务器（每个组的前一个限制为 4 个服务器）。单情景模式的每组限制 16，保持不变。 修改了以下命令以接受这些新限制：**aaa-server**、**aaa-server host**。
从用于 SDI AAA 服务器组的 RSA 身份验证管理器手动导入节点密钥文件。	9.15(1)	您可以导入从RSA身份验证管理器导出的节点密钥文件，以用于 SDI AAA 服务器组。 添加了以下命令：**aaa sdi import-node-secret**、**clear aaa sdi node-secret**、**show aaa sdi node-secrets**。

第 VII 部分

系统管理

- 管理访问， 第 1237 页
- 软件和配置， 第 1285 页
- 系统事件的响应自动化， 第 1329 页
- 测试和故障排除， 第 1341 页

第 42 章

管理访问

本章介绍如何通过 Telnet、SSH 和 HTTPS（使用 ASDM）访问 ASA 进行系统管理，如何对用户进行身份验证和授权以及如何创建登录横幅。

- 配置管理远程访问，第 1237 页
- 为系统管理员配置 AAA，第 1254 页
- 监控设备访问，第 1274 页
- 管理访问的历史记录，第 1277 页

配置管理远程访问

本节介绍如何为 ASDM、Telnet 或 SSH 配置 ASA 访问，以及其他管理参数，例如登录横幅。

配置 SSH 访问

如要确定客户端 IP 地址并定义允许使用 SSH 连接至 ASA 的用户，请执行以下步骤：请参阅以下准则：

- 要访问 ASA 接口以进行 SSH 访问，亦无需允许主机 IP 地址的访问规则。您只需按照本部分配置 SSH。
- 除了进入 ASA 时所经由的接口以外，不支持对其他接口进行 SSH 访问。例如，如果 SSH 主机位于外部接口上，则只能直接向外部接口发起管理连接。此规则的唯一例外是通过 VPN 连接（仅 ASA SSH 协议栈支持）。请参阅配置 VPN 隧道上的管理访问，第 1249 页。
- ASA 允许每个情景/单模式最多有 5 个并发 SSH 连接，在所有情景中最多分为 100 个连接。但是，由于配置命令可能会锁定正在更改的资源，因此您应一次在一个SSH会话中进行更改，以确保正确应用所有更改。
- 默认情况下，ASA 使用CiscoSSH 堆栈，它基于。您可以改为启用专有 ASA SSH 堆栈。CiscoSSH 支持：
  - FIPS 合规性
  - 定期更新，包括来自思科和开源社区的更新

请注意，思科SSH堆栈不支持：

- 通过VPN通过SSH连接到其他接口（管理访问）
- EDDSA密钥对
- FIPS模式下的RSA密钥对

如果需要这些功能，则应使用 ASA SSH 堆栈。

- 要使用 ASA **copy** 命令与 SCP 服务器复制文件或从 SCP 服务器复制文件，必须执行以下操作：
  - （仅限 CiscoSSH 堆栈） 使用 **ssh** 命令在 ASA 上为 SCP 服务器子网/主机启用 SSH 访问。
  - 使用 **crypto key generate** 命令生成密钥对（仅适用于物理 ASA）。
- 不再支持 SSH 默认用户名。使用 SSH 以及 **pix** 或 **asa** 用户名和登录密码无法再连接至 ASA。要使用 SSH，您必须使用 **aaa authenticationsshconsoleLOCAL** 命令配置 AAA 身份验证；然后通过输入 **username** 命令定义本地用户。如果要使用 AAA 服务器而不是本地数据库进行身份验证，建议也将本地身份验证配置为备用方法。
- 仅支持 SSH 版本 2。

开始之前

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统配置切换至情景配置，请输入 **changeto context** *name*。

过程

步骤 1 （可选） 使用 ASA SSH 堆栈而不是默认 CiscoSSH 堆栈。

no ssh stack ciscossh

要返回到 CiscoSSH 堆栈，请使用 **ssh stack ciscossh**。

步骤 2 生成 SSH 必需的密钥对（仅适用于物理 ASA）。

对于 ASA virtual，会在部署后自动创建密钥对。

a) 生成密钥对。

crypto key generate {**eddsa edwards-curve ed25519** | **ecdsa elliptic-curve** *size* |**rsa modulus** *size*}

示例：

```
ciscoasa(config)# crypto key generate ecdsa elliptic-curve 521
```

- **eddsa edwards-curve ed25519**-密钥大小为256位。 不支持CiscoSSH堆栈。
- size-以位为单位的大小为256、384或521。**ecdsa elliptic-curve**

• size-大小（以位为单位）为2048、3072或4096。**rsa modulus**

指定的密钥大小越大，生成密钥对所需的时间就越长。SSH按以下顺序尝试密钥：EdDSA，ECDSA，然后是RSA。使用 **show crypto key mypubkey** {**eddsa** | **ecdsa** | **rsa**} 命令查看密钥。SSH使用的密钥称为<Default- type -Key>。

b) （可选）如果您不想使用默认密钥顺序（EdDSA，ECDSA和RSA），请确定要使用的密钥对。

ssh key-exchange hostkey {**rsa** | **eddsa** | **ecdsa**}

如果选择RSA，则必须使用2048或更大的密钥。为了实现升级兼容性，仅在使用默认密钥顺序时才支持较小的密钥。

示例：

```
ciscoasa(config)# ssh key-exchange hostkey ecdsa
```

步骤 3 将密钥保存到永久性闪存中。

write memory

示例：

```
ciscoasa(config)# write memory
```

步骤 4 在本地数据库中创建可用于 SSH 访问的用户。您也可以使用 AAA 服务器进行用户访问，但建议使用本地用户名。

username *name* [**password** *password*] **privilege** *level*

示例：

```
ciscoasa(config)# username admin password Far$cape1999 privilege 15
```

默认情况下，特权级别为 2；输入介于 0 和 15 之间的级别，其中 15 具有所有特权。如果要强制用户使用公共密钥身份验证而不是密码身份验证 (**ssh authentication**)，您可能需要不使用密码创建用户。若您在 **username** 命令中配置公钥身份验证以及密码，则如果您在此程序中明确配置 AAA 身份验证，用户可使用任一种方法登录。**注意**：请勿使用 **username** 命令 **nopassword** 选项，；**nopassword** 选项允许输入任何密码，而不是无密码。

步骤 5 （可选） 允许用户使用公钥身份验证代替/以及密码身份验证，并在 ASA 上输入公钥：

username 名称 **attributes**

ssh authentication {**pkf** | **publickey** *key*}

示例：

```
ciscoasa(config)# username admin attributes
ciscoasa(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: "256-bit ED25519, converted by dean@dwinchester-mac from "
AAAAC3NzaC1lZDI1NTE5AAAAIDmIeTNfEOnuH0094p1MKX80fW2O216g4trnf7gwWe5Q
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
```

对于本地 **username**，您可以启用公钥身份验证代替/以及密码身份验证。您可以使用任何可生成 ssh-rsa、ssh-ed25519 或 ecdsa-sha2-nistp 原始密钥（不带证书）的 SSH 密钥生成软件（如 ssh keygen）生成公钥/私钥对。在 ASA 上输入该公钥。然后，SSH 客户端使用私钥（以及用于创建密钥对的密码）连接至 ASA。

对于 **pkf** 密钥，系统将提示您粘贴 PKF 格式的密钥，最长 4096 位。此格式用于由于过长而无法以 Base64 格式内嵌粘贴的密钥。例如，可以使用 ssh keygen 生成 4096 位的密钥，然后将其转换为 PKF，并使用 **pkf** 关键字作为密钥提示。**注意**：您可以将 **pkf** 选项与故障转移一起使用，但 PKF 密钥不会自动复制到备用系统。您必须输入 **write standby** 命令才能同步 PKF 密钥。

对于密钥，密钥是Base64编码的公钥。**publickey** 您可以使用任何可生成 ssh-rsa、ssh-ed25519 或 ecdsa-sha2-nistp 原始密钥（不带证书）的 SSH 密钥生成软件（如 ssh keygen）生成密钥对。

步骤 6 （对于密码访问）启用 SSH 访问的本地（或 AAA 服务器)身份验证：

aaa authentication ssh console {**LOCAL** | *server_group* [**LOCAL**]}

示例：

```
ciscoasa(config)# aaa authentication ssh console LOCAL
```

对于使用 **ssh authentication** 命令的用户名，此命令不影响本地公钥身份验证。ASA 隐式地使用本地数据库进行公钥身份验证。此命令仅影响具有密码的用户名。如果要允许本地用户使用公钥认证或密码，则需要使用此命令显式地配置本地身份验证以允许密码访问。

步骤 7 确定 ASA 从其接受每个地址或子网的连接的 IP 地址，以及可在其上使用 SSH 的接口。

ssh *source_IP_address mask source_interface*

- *source_interface* - 指定任何已命名的接口。对于网桥组，请指定网桥组成员接口。对于仅 VPN 管理访问（请参阅 配置 VPN 隧道上的管理访问，第 1249 页），请指定命名的 BVI 接口。

与 Telnet 不同，您可以在最低安全级别的接口上使用 SSH。

示例：

```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

步骤 8 （可选） 设置在 ASA 断开 SSH 会话之前，会话可空闲的持续时间。

ssh timeout 分钟

示例：

```
ciscoasa(config)# ssh timeout 30
```

设置超时时间，范围为 1 到 60 分钟。默认值为 5 分钟。在大多数情况下，默认持续时间都太短，应增加为直到完成所有前期测试和故障排除所需的时间。

步骤 9 （可选） 启用安全复制 (SCP) 服务器。

ssh scopy enable

SCP 服务器没有目录支持。缺少目录支持会限制远程客户端访问 ASA 内部文件。

SCP 服务器不支持横幅或通配符。

步骤 10 （可选） 配置 SSH 密码加密算法：

ssh cipher encryption {**all** | **fips** | **high** | **low** | **medium** | **custom** *colon-delimited_list_of_encryption_ciphers*}

示例：

```
ciscoasa(config)# ssh cipher encryption custom 3des-cbc:aes128-cbc:aes192-cbc
```

默认值为 **medium**。密码按其列出的顺序使用。对于预定义列表，从最高安全级别到最低安全级别列出。

- **all** 关键字指定使用所有密码：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes192-ctr aes256-ctr
- **custom** 关键字指定自定义密码加密配置字符串，以冒号分隔。
- **fips** 关键字指定仅符合 FIPS 的密码：aes128-cbc aes256-cbc
- **high** 关键字指定仅高强度密码：aes256-cbc aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr
- **low** 关键字指定低、中和高强度密码：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- **medium** 关键字指定中和高强度密码（默认设置）：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr

步骤 11 （可选） 配置 SSH 密码完整性算法：

{|||||||||冒号分隔的list_of_integrity_ciphers} **ssh cipher integrityallfipshighlowmediumcustom**

示例：

```
ciscoasa(config)# ssh cipher integrity custom hmac-sha1-96:hmac-md5
```

默认值为 **high**。

- **all** 关键字指定使用所有密码：hmac-sha1 hmac-sha1-96 (Deprecated) hmac-md5 (Deprecated) hmac-md5-96 (Deprecated) hmac-sha2-256
- **custom** 关键字指定自定义密码加密配置字符串，以冒号分隔。
- **fips** 关键字指定仅符合 FIPS 的密码：hmac-sha1 hmac-sha2-256

- **high** 关键字指定仅高 强度密码： hmac-sha2-256
- **low** 关键字指定低、中和高强度密码：hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96 hmac-sha2-256
- **medium** 关键字指定中和高强度密码：hmac-sha1 hmac-sha1-96 (Deprecated) hmac-sha2-256

步骤 12 （可选） (Admin context only) - 设置 Diffie-Hellman (DH) 密钥交换模式：

ssh key-exchange group {**curve25519-sha256** | **dh-group14-sha1** | **dh-group14-sha256** | **ecdh-sha2-nistp256**}

示例：

```
ciscoasa(config)# ssh key-exchange group dh-group14-sha1
```

默认为 **dh-group14-sha256**

DH密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥配合使用，以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。您只能在管理情景中设置密钥交换；此值供所有情景使用。

示例

以下示例展示如何使用 PKF 格式的密钥进行身份验证：

```
ciscoasa(config)# crypto key generate rsa modulus 4096
ciscoasa(config)# write memory
ciscoasa(config)# username exampleuser1 password examplepassword1 privilege 15
ciscoasa(config)# username exampleuser1 attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config)#
```

以下示例将在 Linux 或 Macintosh 系统上为 SSH 生成一个共享密钥，并将其导入 ASA：

1. 在计算机上生成 4096 位的 RSA 公钥和私钥：

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
|  o o            |
| ooooo           |
+-----------------+
```

2. 将密钥转换为 PKF 格式：

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by john@jcrichton-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+561+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3. 将密钥复制到剪贴板。
4. 在 ASDM 中，依次选择 **配置** > **设备管理** > **用户/AAA** > **用户帐户**，选择用户名，然后点击**编辑**。点击 **Public Key Using PKF** 并将密钥粘贴到窗口中：
5. 验证用户是否可以通过 SSH 连接到 ASA。对于密码，请输入您在创建密钥对时指定的 SSH 密钥密码。

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

系统将显示以下对话框，以供您输入密码：

同时，终端会话将显示以下内容：

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

以下示例显示与 ASA 的 SCP 会话。从外部主机上的客户端执行 SCP 文件传输。例如，在 Linux 中输入以下命令：

scp -v -pw *password* [*path*/]*source_filename*
username@asa_address:{**disk0**|**disk1**}:/[*path*/]*dest_filename*

-v 表示详细，如果您未指定 **-pw**，则会提示您输入密码。

配置 Telnet 访问

要识别允许使用 Telnet 连接至 ASA 的客户端 IP 地址，请执行以下步骤。请参阅以下准则：

- 如要访问 ASA 接口进行 Telnet 访问，也不需要允许主机 IP 地址的访问规则，您只需根据本部分配置 Telnet 访问。
- 除了进入 ASA 时所经由的接口以外，不支持对其他接口进行 Telnet 访问。例如，如果 Telnet 主机位于外部接口上，则只能发起直接到外部接口的 Telnet 连接。此规则的唯一例外是通过 VPN 连接。请参阅配置 VPN 隧道上的管理访问，第 1249 页。
- 除非使用 VPN 隧道中的 Telnet，否则无法使用 Telnet 访问最低安全级别的接口。
- 每个情景/单模式最多 5 个并发 Telnet 连接，在所有情景中最多分为 100 个连接。

开始之前

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统配置切换至情景配置，请输入 **changeto context** *name*。
- 要使用 Telnet 访问 ASA CLI，请输入通过 **password** 命令设置的登录密码。使用 Telnet 前必须手动设置该密码。

过程

步骤 1 识别 ASA 为位于特定接口的每个地址或子网接收连接的 IP 地址。

telnet *source_IP_address mask source_interface*

- *source_interface* - 指定任何已命名的接口。对于网桥组，请指定网桥组成员接口。对于仅 VPN 管理访问（请参阅 配置 VPN 隧道上的管理访问，第 1249 页），请指定命名的 BVI 接口。

如果只有一个接口，只要接口的安全级别为 100，您就可以配置 Telnet 以访问该接口。

示例：

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

步骤 2 设置 ASA 与 Telnet 会话断开连接之前，该会话可以持续空闲多长时间。

telnet timeout 分钟

示例：

```
ciscoasa(config)#  telnet timeout 30
```

设置超时时间，范围为 1 到 1440 分钟。默认值为 5 分钟。在大多数情况下，默认持续时间都太短，应增加为直到完成所有前期测试和故障排除所需的时间。

示例

下列显示如何让一台内部接口上的地址为 192.168.1.2 的主机访问 ASA：

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

下例显示如何允许 192.168.3.0 网络上的所有用户在内部接口上访问 ASA：

```
ciscoasa(config)# telnet 192.168.3.0. 255.255.255.255 inside
```

配置用于 ASDM 的 HTTPS 访问、其他客户端

如要使用 ASDM 或 CSM 等其他 HTTPS 客户端，则需要启用 HTTPS 服务器，并允许至 ASA 的 HTTPS 连接。HTTPS 访问已作为出厂默认配置的一部分启用。如要配置 HTTPS 访问，请执行以下步骤。请参阅以下准则：

- 要访问 ASA 接口以进行 HTTPS 访问，亦无需允许主机 IP 地址的访问规则。您只需按照本部分配置 HTTPS。但是，如果您配置 HTTP 重定向以将 HTTP 连接自动重定向至 HTTPS，则必须启用允许 HTTP 的访问规则；否则，该接口无法侦听 HTTP 端口。
- 除了进入ASA时所经由的接口以外，不支持对其他接口进行管理访问。例如，如果管理主机位于外部接口上，则只能直接向外部接口发起管理连接。此规则的唯一例外是通过VPN连接。请参阅配置 VPN 隧道上的管理访问，第 1249 页。
- 在单情景模式下，最多可以有 5 个 ASDM 并发会话。在多情景模式下，每个情景最多 5 个并发 ASDM 会话，在所有情景中最多分为 200 个 ASDM 实例。

  ASDM会话使用两个HTTPS连接：一个用于监控（始终存在），另一个用于进行配置更改（仅当进行更改时才存在）。例如，多情景模式系统限制为 200 个 ASDM 会话表示 HTTPS 会话数限制为 400。
- ASA 允许在单情景模式或每个情景（如果可用）中最多允许 6 个并发非 ASDM HTTPS 会话，所有情景中最多允许 100 个 HTTPS 会话。
- 如果在同一接口上同时启用 SSL (**webvpn** > **启用** 接口) 和 HTTPS 访问，则可以从 **https://***ip_address* 访问 Secure Client，从 **https://***ip_address***/admin**访问端口 443。如果还启用了 **aaa 身份验证 http 控制台**，则必须为 ASDM 访问指定其他端口。

开始之前

- 在多情景模式下，请在情景执行空间中完成本程序。要从系统配置切换至情景配置，请输入 **changeto context** *name*。

过程

步骤 1 识别 ASA 为位于特定接口的每个地址或子网接收 HTTPS 连接的 IP 地址。

http *source_IP_address mask source_interface*

- *source_interface* - 指定任何已命名的接口。对于网桥组，请指定网桥组成员接口。对于仅 VPN 管理访问（请参阅 配置 VPN 隧道上的管理访问，第 1249 页），请指定命名的 BVI 接口。

示例：

```
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

步骤 2 启用 HTTPS 服务器。

http server enable [*port*]

示例：

```
ciscoasa(config)# http server enable 444
```

默认情况下，端口为 443。如果更改端口号，请务必将其包括在 ASDM 访问 URL 中。例如，如果将端口号更改为 444，请输入以下 URL：

https://10.1.1.1:444

步骤 3 允许基于非浏览器的 HTTPS 客户端访问 ASA 上的 HTTPS 服务。默认情况下，允许 ASDM、CSM 和 REST API。

http server basic-auth-client *user_agent*

- *user_agent* - 在 HTTP 请求的 HTTP 报头中指定客户端的用户代理字符串。您可以指定完整字符串或部分字符串；部分字符串必须与用户代理字符串的开头匹配。建议使用完整的字符串以提高安全性。请注意，文件夹名称区分大小写。

  例如，**curl** 将匹配以下用户代理字符串：

  curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2

  curl 将不匹配以下用户代理字符串：

  abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2

  CURL 将不匹配以下用户代理字符串：

  curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2

使用单独的命令输入每个客户端字符串。 许多专业客户端（例如，python 库、curl 和 wget）不支持跨站请求伪造 (CSRF) 基于令牌的身份验证，因此，您需要特别允许这些客户端使用 ASA 基本身份验证方法。出于安全考虑，您应该只允许所需的客户端。

示例：

```
ciscoasa(config)# http server basic-auth-client curl
```

步骤 4 （可选） 设置连接和会话超时。

http server idle-timeout分钟

http server session-timeout分钟

http connection idle-timeout秒

- **http server idle-timeout**分钟 - 设置 ASDM 连接的空闲超时，范围为 1-1440 分钟。默认值为 20 分钟。ASA 会断开在设置的时间段内处于空闲状态的 ASDM 连接。
- **http server session-timeout**分钟 - 设置 ASDM 会话的会话超时，范围为 1-1440 分钟。此超时默认处于禁用状态。ASA 会断开超过设置时间段的 ASDM 会话。
- **http connection idle-timeout***seconds* - 设置所有 HTTPS 连接（包括 ASDM、WebVPN 和其他客户端）的空闲超时，范围为 10-86400 秒。此超时默认处于禁用状态。ASA 会断开在设置的时间段内处于空闲状态的连接。如果同时设置 **http server idle-timeout** 和 **http connection idle-timeout** 命令，则 **http connection idle-timeout** 优先执行。

示例：

```
ciscoasa(config)# http server idle-timeout 30
ciscoasa(config)# http server session-timeout 120
```

示例

以下示例显示如何启用HTTPS服务器并使内部接口上地址为192.168.1.2的主机访问ASDM：

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

以下示例显示如何使 192.168.3.0/24 网络上的所有用户可以访问内部接口上的 ASDM：

```
ciscoasa(config)# http 192.168.3.0 255.255.255.0 inside
```

为 ASDM 访问或无客户端 SSL VPN 配置 HTTP 重定向

您必须使用 HTTPS 连接至使用 ASDM 或无客户端 SSL VPN 的 ASA。为了方便起见，可以将 HTTP 管理连接重定向至 HTTPS。例如，通过重定向 HTTP，输入 **http://10.1.8.4/admin/** 或 **https://10.1.8.4/admin/** 均可访问位于该 HTTPS 地址的 ASDM 启动页面。

您可以重定向 IPv4 和 IPv6 流量。

开始之前

通常，您无需允许主机 IP 地址的访问规则。但是，对于 HTTP 重定向，您必须启用允许 HTTP 的访问规则；否则，该接口无法侦听 HTTP 端口。

过程

启用 HTTP 重定向：

http redirect *interface_name* [*port*]

示例：

```
ciscoasa(config)# http redirect outside 88
```

port 确定接口从其重定向 HTTP 连接的端口。默认值为 80。

配置 VPN 隧道上的管理访问

如果 VPN 隧道在一个接口上终止，但是您需要通过访问不同的接口来管理 ASA，则必须将该接口标识为管理访问接口。例如，如果从外部接口进入 ASA，通过此功能可以使用 ASDM、SSH、 或 Telnet 连接到内部接口；或者，当从外部接口进入时，可以 Ping 内部接口。

注释 如果使用 CiscoSSH 堆栈（默认设置），则 SSH 不支持此功能。

注释 SNMP 不支持此功能。 对于基于 VPN 的 SNMP，我们建议在环回接口上启用 SNMP。您无需启用管理访问功能即可在环回接口上使用 SNMP。环回接口也适用于 SSH。

除了进入 ASA 时所经由的接口以外，不支持对其他接口进行 VPN 访问。例如，如果 VPN 访问位于外部接口上，则只能直接向外部接口发起连接。应在 ASA 的可直接访问的接口上启用 VPN，并使用域名解析，以便您不必记住多个地址。

通过以下类型的 VPN 隧道可以实现管理访问： IPsec 客户端、IPsec 站点间的简单 VPN 和 Secure Client SSL VPN 客户端。

开始之前

- 管理专用接口不支持此功能。
- 当使用管理访问接口，并且配置身份 NAT 时，必须为 NAT 配置路由查询选项。有关详细信息，请参阅 ASA 防火墙 CLI 配置指南的相应版本中 *NAT* 示例和参考 一章中的“NAT 和 VPN 管理访问”部分。

过程

指定从另一个接口进入 ASA 时要访问的管理接口的名称。

management-access *management_interface*

对于 Easy VPN 和站点间隧道，可以指定命名 BVI（在路由模式下）。

示例：

```
ciscoasa(config)# management-access inside
```

更改控制台超时

控制台超时设置连接可保持处于特权 EXEC 模式下或配置模式下的时间；当达到超时时间后，会话将进入用户 EXEC 模式。默认情况下，会话不会超时。此设置不会影响可与控制台端口保持连接的时间，该连接永不超时。

过程

指定授权会话结束后的空闲时间（0-60，以分钟为单位）。

console timeout *number*

示例：

```
ciscoasa(config)# console timeout 0
```

默认超时为 0，表示会话不会超时。

自定义 CLI 提示符

利用为提示符添加信息这项功能，可以大体了解在您有多个模块时登录哪一台 ASA。故障转移起价你，如果两台 ASA 具有相同的主机名，则此功能非常有用。

在多情景模式中，您可以在登录到系统执行空间或管理情景时查看扩展的提示符。在非管理情景中，您仅可看到默认提示符，即主机名和情景名称。

默认情况下，提示符显示 ASA 的主机名。在多情景模式下，提示符还显示情景名称。在 CLI 提示符中可以显示以下项目：

cluster-unit	显示集群设备名称。集群中的每台设备都有一个唯一的名称。
context	（仅多情景模式）显示当前情景的名称。
domain	显示域名。
hostname	显示主机名。
priority	显示故障转移优先级 pri（主要）或 sec（辅助）。

state	显示设备的流量传递状态或角色。 对于故障转移，会面向 state 关键字显示以下值： • **act** - 已启用故障转移，设备正在传递流量。 • **stby** - 已启用故障转移，设备未在传递流量，并且处于备用、故障或其他非活动状态。 • **actNoFailover** - 未启用故障转移，设备正在传递流量。 • **stbyNoFailover** - 未启用故障转移，设备未在传递流量。这可能会在待机设备上存在阈值以上的接口故障时发生。 对于集群，会显示控制和数据的值。

过程

通过输入以下命令自定义 CLI 提示符：
prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]}

示例：

```
ciscoasa(config)# prompt hostname context slot state priority
ciscoasa/admin/pri/act(config)#
```

输入关键字的顺序确定提示符中各元素的顺序（各元素以斜线 (/) 分隔）。

配置登录横幅

您可以配置在用户连接至 ASA 时、在用户登录之前或在用户进入特权 EXEC 模式之前将显示的消息。

开始之前

- 从安全角度来看，重要的是横幅阻止未经授权的访问。请勿使用“欢迎”或“请”等措辞，因为它们像是在邀请入侵者。以下横幅为未经授权的访问设置正确的语调：

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- 在添加横幅后，如果有以下情况，可能会关闭至 ASA 的 Telnet 或 SSH 会话：
  - 没有足够的系统内存可用来处理横幅消息。
  - 在尝试显示横幅消息时发生 TCP 写入错误。

- 有关横幅消息的准则，请参阅 RFC 2196。

过程

添加在以下三个时间之一要显示的横幅：在用户首次连接时 (message-of-the-day (motd))，在用户登录时 (login)，以及在用户访问特权 EXEC 模式时 (exec)。

banner {**exec** | **login** | **motd**} *text*

示例：

```
ciscoasa(config)# banner motd Only authorized access is allowed to $(hostname).
```

当用户连接至 ASA 时，系统首先显示 message-of-the-day 横幅，然后显示 login 横幅和提示符。在用户成功登录 ASA 后，系统将显示 exec 横幅。

如要添加一行以上，请将**banner** 命令放在每行之前。

对于横幅文本：

- 允许包含空格，但使用 CLI 时无法输入制表符。
- 除了 RAM 和闪存对横幅长度的限制外，无其他长度限制。
- 通过包含字符串 **$(hostname)** 和 **$(domain)**，可以动态添加 ASA 的主机名或域名。
- 如果在系统配置中配置横幅，可以通过在情景配置中使用 **$(system)** 字符串来在情景中使用该横幅文本。

示例

以下示例显示如何添加 message-of-the-day 横幅：

```
ciscoasa(config)# banner motd Only authorized access is allowed to $(hostname).

ciscoasa(config)# banner motd Contact me at admin@example.com for any issues.
```

设置管理会话配额

可以在 ASA 上建立允许的最大同时 ASDM、SSH 和 Telnet 会话数量。如果达到最大值，则不允许其他会话，并生成系统日志消息。如要防止系统锁定，则管理会话配额机制无法阻止控制台会话。

注释 在多情景模式下，如果最大 ASDM 会话数固定为 5，则无法配置会话数。

注释 如果您还为最大管理会话（SSH等）的每个情景设置资源限制，则将使用较低的值。

开始之前

在多情景模式下，请在情景执行空间中完成本程序。要从系统切换至情景配置，请输入 **changeto context**名称 命令。

过程

步骤 1 请输入以下命令：

quota management-session [**ssh** | **telnet** | **http** | **user**] *number*

- **ssh**-设置最大SSH会话数（介于1和5之间）。默认值为 5。
- **telnet**-设置最大Telnet会话数，介于1和5之间。默认值为 5。
- **http**-设置最大HTTPS（ASDM）会话数，介于1和5之间。默认值为 5。
- **user**-设置每个用户的最大会话数，介于1和5之间。默认值为 5。
- number-设置介于0（无限制）和10000之间的会话总数。 当不带任何其他关键字输入时，此参数设置介于1到15之间的会话总数。默认值为 15。

示例：

```
ciscoasa(config)# quota management-session ssh 3
ciscoasa(config)# quota management-session telnet 1
ciscoasa(config)# quota management-session http 4
ciscoasa(config)# quota management-session user 2
```

步骤 2 查看当前正在使用的会话。

show quota management-session [**ssh** | **telnet** | **http** | **user**]

示例：

```
ciscoasa(config)#show quota management-session

#Sessions               ConnectionType                 Username
1                             SSH                      cisco
2                             TELNET                   cisco
1                             SSH                      cisco1
```

为系统管理员配置 AAA

本部分介绍如何为系统管理员配置身份验证、管理授权和命令授权。

配置管理验证

配置用于 CLI 和 ASDM 访问的身份验证。

关于管理验证

如何登录 ASA 取决于是否启用身份验证。

关于 SSH 身份验证

请参阅以下行为了解在有身份验证和无身份验证的情况下进行 SSH 访问：

- 无身份验证时 - 在无身份验证的情况下，SSH 不可用。
- 身份验证 - 如果启用身份验证，请输入在 AAA 服务器或本地用户数据库中所定义的用户名和密码。对于公钥身份验证，ASA 仅支持本地数据库。 如果配置 SSH 公钥身份验证，则 ASA 隐式使用本地数据库。当您使用用户名和密码登录时，只需要明确配置 SSH 身份验证。您将进入用户 EXEC 模式。

关于 Telnet 身份验证

有关在使用身份验证和不使用身份验证的情况下的 Telnet 访问，请参阅以下行为：

- 无身份验证 - 如果不为 Telnet 启用任何身份验证，请勿输入用户名；您应该输入登录密码（使用 **password** 命令设置）。没有默认密码，因此您必须设置一个，才能通过 Telnet 连接到 ASA。您将进入用户 EXEC 模式。
- 有身份验证 - 如果启用 Telnet 身份验证，请输入在 AAA 服务器或本地用户数据库中所定义的用户名和密码。您将进入用户 EXEC 模式。

关于 ASDM 身份验证

有关在使用身份验证和不使用身份验证的情况下的 ASDM 访问，请参阅以下行为。您还可以配置证书身份验证，而不管是否使用 AAA 身份验证。

- 无身份验证 - 默认情况下，可以使用空的用户名以及通过 **enable password** 命令设置的启用密码（默认为空）登录 ASDM。建议您尽快更改启用密码，不要再保持空白状态；请参阅 设置主机名、域名及启用密码和 Telnet 密码，第 815 页。首次在CLI中输入命令时，系统会提示您更改密码；登录ASDM时不会强制执行此行为。 **enable** 请注意，如果在登录屏幕输入用户名和密码（而不是将用户名留空），则 ASDM 将检查本地数据库是否有匹配项。
- 证书身份验证 -（仅限单个、路由模式）您可以要求用户具备有效的证书。输入证书用户名和密码，ASA 会根据 PKI 信任点对证书进行验证。

- AAA 身份验证 - 启用 ASDM (HTTPS) 身份验证时，需要输入 AAA 服务器或本地用户数据库中定义的用户名和密码。不能再使用空用户名和启用密码登录 ASDM。
- AAA 身份验证加证书身份验证 -（仅限单个、路由模式）启用 ASDM (HTTPS) 身份验证时，需要输入 AAA 服务器或本地用户数据库中定义的用户名和密码。如果用户名和密码对于证书身份验证是不同的，系统将提示您输入它们。您可以选择预填充从证书派生的用户名。

关于串行身份验证

请参阅以下行为了解在有身份验证和无身份验证的情况下访问串行控制台端口：

- 无身份验证 - 如果不为串行访问启用任何身份验证，则不输入用户名或密码。您将进入用户 EXEC 模式。
- 身份验证 - 如果为串行访问启用身份验证，请输入在 AAA 服务器或本地用户数据库中所定义的用户名和密码。您将进入用户 EXEC 模式。

关于 Enable 身份验证

如要在登录后进入特权 EXEC 模式，请输入 **enable** 命令。此命令的工作方式取决于是否启用身份验证：

- No Authentication - 如果不配置 enable 身份验证，在输入 **enable** 命令时输入系统启用密码（通过 **enable password**命令设置），该密码默认留空。第一次输入 **enable** 命令时，系统会提示您更改密码。但是，如果不使用 enable 身份验证，在输入 **enable** 命令后，则不再以特定用户身份登录，这会影响基于用户的功能，如命令授权。为了保留用户名，请使用 enable 身份验证。
- Authentication - 如果配置 enable 身份验证，ASA 会提示您输入在 AAA 服务器或本地用户数据库上定义的用户名和密码。当执行命令授权时此功能特别有用，因为用户名在确定用户可以输入的命令时非常重要。

对于使用本地数据库的 enable 身份验证，可以使用 **login** 命令，来代替 **enable** 命令。**login** 命令会保留用户名，但不需要配置开启身份验证。

注意 如果您将可以访问 CLI 但您不希望其进入特权 EXEC 模式的用户添加到本地数据库中，则应该配置命令授权。在无命令授权的情况下，如果用户的权限级别为 2 或更高（2 是默认值），则用户可以在 CLI 使用自己的密码访问特权 EXEC 模式（以及所有命令）。或者，您可以使用 AAA 服务器而不是本地数据库进行身份验证，或将所有本地用户都设置为 1 级，以阻止使用 login 命令，这样就可以控制谁可以使用系统启用密码访问特权 EXEC 模式。

从主机操作系统到 ASA 的会话

有些平台支持将 ASA 作为单独的应用运行：例如，Catalyst 6500 上的 ASASM 或 Firepower 4100/9300 上的 ASA。对于从主机操作系统到 ASA 的会话，您可以配置串行和 Telnet 身份验证，具体取决于连接类型。

多情景模式下，无法在系统配置中配置任何 AAA 命令。但是，如果在管理员情景中配置 Telnet 或串行身份验证，则身份验证也适用于这些会话。在此情况下，使用管理员情景 AAA 服务器或本地用户数据库。

配置用于 CLI 和 ASDM访问的身份验证

开始之前

- 配置 Telnet、SSH 或 HTTP 访问。
- 对于外部身份验证，请配置 AAA 服务器组。对于本地身份验证，请向本地数据库添加用户。
- HTTP 管理身份验证不支持 AAA 服务器组的 SDI 协议。
- 此功能不影响使用 **ssh authentication** 命令对本地用户名进行 SSH 公共密钥身份验证。ASA 隐式使用本地数据库进行公共密钥身份验证。此功能仅影响用户名与密码。如果要允许本地用户进行公共密钥身份验证或使用密码，您需要使用此程序显式配置本地身份验证，以允许进行密码访问。

过程

对用户进行管理访问的身份验证。

aaa authentication {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

示例：

```
ciscoasa(config)# aaa authentication ssh console radius_1 LOCAL
ciscoasa(config)# aaa authentication http console radius_1 LOCAL
ciscoasa(config)# aaa authentication serial console LOCAL
```

telnet 关键字控制 Telnet 访问。**ssh** 关键字控制 SSH 访问（仅密码；公共密钥身份验证隐式使用本地数据库）。**http** 关键字控制 ASDM 访问。**serial** 关键字控制控制台端口访问。

如果使用 AAA 服务器组进行身份验证，可以将 ASA 配置为在 AAA 服务器不可用时使用本地数据库作为回退方法。指定服务器组名后跟 **LOCAL**（区分大小写）。建议在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为ASA提示符不会给出使用何种方法的任何指示。或者，您可以只输入 **LOCAL**，以将本地数据库用作主要的身份验证方法（不使用回退）。

配置 Enable 身份验证（特权 EXEC 模式）

您可以在用户输入 **enable** 命令时对他们进行身份验证。

开始之前

请参阅关于 Enable 身份验证，第 1255 页。

过程

选择以下选项之一用于对用户进行身份验证：

- 如要使用 AAA 服务器或本地数据库对用户进行身份验证，请输入以下命令：

  aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]}

  示例：

  ```
  ciscoasa(config)# aaa authentication enable console LOCAL
  ```

  系统提示用户输入用户名和密码。

  如果使用 AAA 服务器组进行身份验证，可以将 ASA 配置为在 AAA 服务器不可用时使用本地数据库作为回退方法。指定服务器组名后跟 **LOCAL**（区分大小写）。建议在本地数据库中使用与 AAA 服务器相同的用户名和密码，因为 ASA 提示符不会给出使用何种方法的任何指示。

  或者，您可以只输入 **LOCAL**，以将本地数据库用作主要的身份验证方法（不使用回退）。

- 如要以本地数据库中用户的身份登录，请输入以下命令：

  login

  示例：

  ```
  ciscoasa# login
  ```

  ASA 提示输入用户名和密码。在输入密码后，ASA 将该用户置于本地数据库指定的权限级别中。

  用户可以使用自己的用户名和密码登录来访问特权 EXEC 模式，因此无需为每个人提供系统使能口令。如要允许用户在登录后访问特权 EXEC 模式（以及所有命令），请将用户权限级别设置为 2（默认）到 15。如果配置本地命令授权，则用户只能输入分配给该权限级别或更低级别的命令。

配置 ASDM 证书身份验证

无论是否有 AAA 身份验证，您都可以要求进行证书身份验证。ASA 将针对 PKI 信任点验证证书。

开始之前

仅在单个路由模式中支持此功能。

过程

步骤 1 启用证书身份验证：

http authentication-certificate *interface_name*[**match** *certificate_map_name*]

示例：

```
ciscoasa(config)# crypto ca certificate map map1 10
ciscoasa(config-ca-cert-map)# subject-name emailAddress www.example.com
ciscoasa(config)# http authentication-certificate outside match map1
```

您应为每个接口配置证书身份验证，使得受信任/内部接口上的连接无需提供证书。您可以多次使用该命令，以在多个接口上启用证书身份验证。

若要要求证书匹配证书映射，请指定 **match** 关键字和映射名称。使用 **crypto ca certificate map** 命令配置映射。

步骤 2 （可选） 设置 ASDM 用于从证书派生用户名的属性：

http username-from-certificate{*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**} [**pre-fill-username**]

示例：

```
ciscoasa(config)# http username-from-certificate CN pre-fill-username
```

默认情况下，ASDM 使用 CN OU 属性。

- *primary-attr* 参数指定要用于派生用户名的属性。*secondary-attr* 参数指定要与主要属性配合用于派生用户名的其他属性。您可以使用以下属性：
  - C - 国家/地区
  - CN - 公用名
  - DNQ - DN 限定符
  - emailAddress - 邮件地址
  - GENQ - 世代限定符
  - GN - 名
  - I - 首字母
  - L - 位置
  - N - 名称
  - O - 组织
  - OU - 组织单位
  - SER - 序列号

- SN - 姓氏
- SP - 州/省
- T - 职位
- UID - 用户 ID
- UPN - 用户主体名称

- **use-entire-name** 关键字使用完整 DN 名称。
- **use-script** 关键字使用 ASDM 生成的 Lua 脚本。
- **pre-fill-username** 关键字在提示身份验证时预填充用户名。如果用户名与您最初输入的不同，系统将显示一个新对话框，其中含有预填充的用户名。然后，您可以输入身份验证的密码。

使用管理授权控制 CLI 和 ASDM 访问

ASA 使您可以在管理用户和远程访问用户进行身份验证时对他们加以区分。用户角色的区分可防止远程访问 VPN 和网络访问用户建立到 ASA 的管理连接。

开始之前

RADIUS 或 LDAP（映射的）用户

当用户通过 LDAP 进行身份验证时，可将本地 LDAP 属性及其值映射到 ASA 属性来提供特定授权功能。配置具有 0 和 15 之间的值的特权级别的 Cisco VSA CVPN3000-Privilege-Level。然后，使用 **ldap map-attributes** 命令将 LDAP 属性映射到 Cisco VAS CVPN3000-Privilege-Level。

当 RADIUS IETF **service-type** 属性作为 RADIUS 身份验证和授权请求的结果在访问接受消息中进行发送时，其用于表示授予通过身份验证的用户的服务类型

在访问接受消息中发送 RADIUS Cisco VSA **privilege-level** 属性 (Vendor ID 3076, sub-ID 220) 时，该属性用于表示用户的权限级别。

TACACS+ 用户

使用“service=shell”请求授权，服务器以 PASS 或 FAIL 作为响应。

本地用户

为给定用户名设置 **service-type** 命令。默认情况下，service-type 是 admin，允许对 **aaa authenticationconsole** 命令指定的任何服务进行完全访问。

管理授权属性

请参阅下表，了解管理授权的AAA服务器类型和有效值。ASA 使用这些值来确定管理访问的级别。

管理级别	RADIUS/LDAP（映射的）属性	TACACS+ 属性	本地数据库属性
完全访问 - 允许完全访问**aaa authenticationconsole** 命令所指定的任何服务	Service-Type 6（管理），Privilege-Level 1	PASS，特权级别 1	admin
部分访问 - 允许在您配置**aaa authenticationconsole** 命令时访问 CLI 或 ASDM。但是，如果您使用**aaa authenticationenableconsole** 命令配置 **enable** 身份验证，则 CLI 用户无法使用 **enable** 命令访问 EXEC 特权模式。	Service-Type 7（NAS 提示），Privilege-Level 2 及更高级别 Framed (2) 和 Login (1) 服务类型按同一方式处理。	PASS，特权级别 2 及更高级别	nas-prompt
No Access - 拒绝管理访问。用户无法使用由 **aaa authenticationconsole** 命令 选项指定的任何服务（不包括 **serial**关键字；允许串行访问）。远程访问（IPsec 和 SSL）用户仍可对其远程访问会话进行身份验证并终止会话。所有其他服务类型（Voice、FAX 等）按同一方式处理。	Service-Type 5（出站）	FAIL	remote-access

其他准则

- 串行控制台访问不包含在管理授权中。
- 您还必须为管理访问配置 AAA 身份验证才能使用此功能。请参阅配置用于 CLI 和 ASDM访问的身份验证，第 1256 页。
- 如果您使用外部身份验证，则必须在启用此功能之前预配置 AAA 服务器组。
- HTTP 授权仅在单个路由模式下受支持。

过程

步骤 1 为 Telnet 和 SSH 启用管理授权：

aaa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

auto-enable 关键字允许具有足够授权权限的管理员在登录时自动进入特权 EXEC 模式。

示例：

```
ciscoasa(config)# aaa authentication ssh console RADIUS
ciscoasa(config)# aaa authorization exec authentication-server auto-enable
```

步骤 2 为 HTTPS (ASDM) 启用管理授权：

aaa authorization http console {**authentication-server** | **LOCAL**}

示例：

```
ciscoasa(config)# aaa authentication http console RADIUS
ciscoasa(config)# aaa authorization http console authentication-server
```

步骤 3

示例

以下示例显示如何定义 LDAP 属性映射。在本示例中，安全策略指定正在通过 LDAP 进行身份验证的用户将用户记录字段或参数标题和公司分别到映射 IETF-RADIUS service-type 和 privilege-level。

```
ciscoasa(config)# ldap attribute-map admin-control
ciscoasa(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
ciscoasa(config-ldap-attribute-map)# map-name company
```

以下示例向 LDAP AAA 服务器 应用 LDAP 属性映射：

```
ciscoasa(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
ciscoasa(config-aaa-server-host)# ldap attribute-map admin-control
```

配置命令授权

如果要控制对命令的访问，可以通过ASA配置命令授权，在其中确定可供用户使用的命令。默认情况下，登录时可以访问用户 EXEC 模式，此模式仅提供最小数量的命令。输入 **enable** 命令时（或在使用本地数据库时输入 **login** 命令时），可以进入特权 EXEC 模式并访问高级命令（包括配置命令）。

可以使用两种命令授权方法之一：

- 本地权限级别
- TACACS+ 服务器权限级别

关于命令授权

您可以启用命令授权，以便只有授权用户可以输入命令。

支持的命令授权方法

可以使用两种命令授权方法之一：

- 本地权限级别 - 在 ASA 上配置命令权限级别。当本地、RADIUS 或 LDAP（如果将 LDAP 属性映射到 RADIUS 属性）用户面向 CLI 访问进行身份验证时，ASA 会为该用户指定由本地数据库、RADIUS 或 LDAP 服务器定义的权限级别。用户可以访问分配的权限级别及以下级别的命令。请注意，所有用户首次登录时都会进入用户 EXEC 模式（命令级别为 0 或 1）。用户需要使用 **enable** 命令再次进行身份验证才能进入特权 EXEC 模式（命令级别为 2 或更高），或使用 **login** 命令登录（仅限本地数据库）。

注释 您可以在本地数据库中没有任何用户，以及没有 CLI 也没有 **enable** 身份验证的情况下，使用本地命令授权。输入 **enable** 命令时，您需要输入系统启用密码，ASA 会为您指定级别 15。然后，您可以为每个级别创建启用密码，以便在输入 **enable** *n*（2 至 15）时，ASA 为您指定级别 *n*。除非启用本地命令授权，否则不使用这些级别。

- TACACS+ 服务器权限级别 - 在 TACACS+ 服务器上，配置用户或组在进行 CLI 访问的身份验证后可以使用的命令。用户在 CLI 输入的每个命令都使用 TACACS+ 服务器进行验证。

安全情景和命令授权

每个情景的 AAA 设置相互独立，不同情景之间不会共享这些设置。

配置命令授权时，必须分别配置每个安全情景。此配置能够实现对不同安全情境执行不同的命令授权。

当在安全情景之间切换时，管理员应知道登录时指定的用户名允许的命令在新情景会话中可能有所差异，或在新情景中可能根本无法配置该命令授权。如果管理员不知道安全情境之间的命令授权可能有所差异，就可能会对其造成困扰。

注释 系统执行空间不支持 AAA 命令；因此，命令授权在系统执行空间不可用。

命令权限级别

默认情况下，会为以下命令分配 0 级权限，为所有其他命令分配 15 级权限。

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**

- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

如果将任何配置模式命令移到低于 15 的级别，请确保也将“**configure**”命令移到同一级别，否则用户将无法进入配置模式。

配置本地命令授权

通过本地命令授权可以为 16 个权限级别（0 到 15）之一分配命令。默认情况下，会向每个命令分配 0 级或 15 级权限。您可以将每个用户定义在特定权限级别，每个用户可以输入分配的权限级别或以下级别的任何命令。ASA 支持在本地数据库、RADIUS 服务器或 LDAP 服务器（如果将 LDAP 属性映射到 RADIUS 属性）中定义的用户权限级别。

过程

步骤 1 将命令分配到权限级别。

privilege [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** *command*

示例：

```
ciscoasa(config)# privilege show level 5 command filter
```

对要重新分配的每个命令重复此命令。

此命令中的选项如下：

- **show** | **clear** | **cmd** - 这些可选关键字可用于仅为命令的显示、清除或配置形式设置权限。命令的配置形式通常是导致配置更改的形式，或者是以未修改的命令形式（无 **show**或 **clear** 前缀），或者是以 **no** 形式。如果不使用其中一个关键字，则会影响命令的所有形式。
- **level***level* - 介于 0 和 15 之间的级别。
- **mode** {**enable** | **configure**} - 如果某个命令可以在用户 EXEC 模式或特权 EXEC 模式下以及配置模式下输入，并且该命令在每个模式下执行不同的操作，则可以分别设置其在这些模式下的权限级别：
  - **enable** - 指定用户 EXEC 模式和特权 EXEC 模式。
  - **configure** - 指定配置模式，可以使用 **configure terminal** 命令进行访问。
- **command***command* - 将要配置的命令。您只能配置主命令的权限级别。例如，可以配置所有 **aaa** 命令的级别，但是不可以单独配置 **aaa authentication** 命令和 **aaa authorization** 命令的级别。

步骤 2 （可选） 为命令授权启用 AAA 用户。如果没有此命令，则 ASA 仅支持本地数据库用户的权限级别，并将所有其他类型的用户默认设置为 15 级。

aaa authorization exec authentication-server [auto-enable]

示例：

```
ciscoasa(config)# aaa authorization exec authentication-server
```

此命令还将启用管理授权。请参阅使用管理授权控制 CLI 和 ASDM 访问 ，第 1259 页。

步骤 3 启用使用本地命令权限级别：

aaa authorization command LOCAL

示例：

```
ciscoasa(config)# aaa authorization command LOCAL
```

在设置命令权限级别时，除非使用此命令来配置命令授权，否则不会进行命令授权。

示例

filter 命令具有以下形式：

- **filter**（表示为 **configure** 选项）
- **show running-config filter**
- **clear configure filter**

您可以为每种形式分别设置权限级别，或通过忽略此选项为所有形式设置同一权限级别。以下示例显示如何分别设置每种形式：

```
ciscoasa(config)# privilege show level 5 command filter
ciscoasa(config)# privilege clear level 10 command filter
ciscoasa(config)# privilege cmd level 10 command filter
```

或者， 以下示例显示如何将所有 filter 命令设置为同一级别：

```
ciscoasa(config)# privilege level 5 command filter
```

show privilege 命令分隔显示的形式。

以下示例显示 **mode** 关键字的使用。必须从用户 EXEC 模式输入 **enable** 命令，而可在配置模式中访问的 **enable password** 命令则要求最高的权限级别：

```
ciscoasa(config)# privilege cmd level 0 mode enable command enable
ciscoasa(config)# privilege cmd level 15 mode cmd command enable
```

```
ciscoasa(config)# privilege show level 15 mode cmd command enable
```

以下示例显示 使用 **configure** 关键字的附加命令 **mode** 命令：

```
ciscoasa(config)# privilege show level 5 mode cmd command configure
ciscoasa(config)# privilege clear level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode enable command configure
```

注释 此最后一行用于 **configure terminal** 命令。

在 Commands TACACS+ 服务器上配置命令

您可以在思科安全访问控制服务器 (ACS) TACACS+ 服务器上，为组或为单个用户将命令配置为共享配置文件组件。对于第三方 TACACS+ 服务器，请参阅服务器文档了解有关命令授权支持的详细信息。

请参阅以下在思科安全 ACS 3.1 版本中配置命令的准则；其中许多原则也适用于第三方服务器。

- ASA 将待授权的命令作为外壳命令发送，因此请在 TACACS+ 服务器上将命令配置为外壳命令。

注释 思科安全 ACS 可能包括名为“pix-shell”的命令类型。请勿将此类型用于 ASA 命令授权。

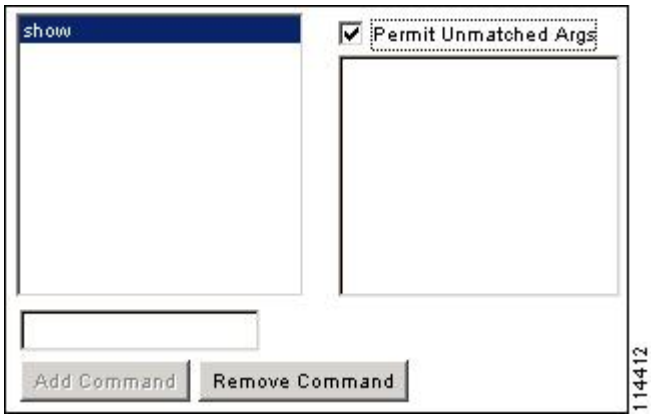
- 命令的第一个词被视为主命令。所有附加的单词都被视为参数，需要在其前面放置 **permit** 或 **deny**。

  例如，如要允许 **show running-configuration aaa-server** 命令，请向命令字段添加 **show running-configuration**，然后在参数字段键入 **permit aaa-server**。

- 通过选中 **Permit Unmatched Args** 复选框，可以允许未明确拒绝的所有命令参数。

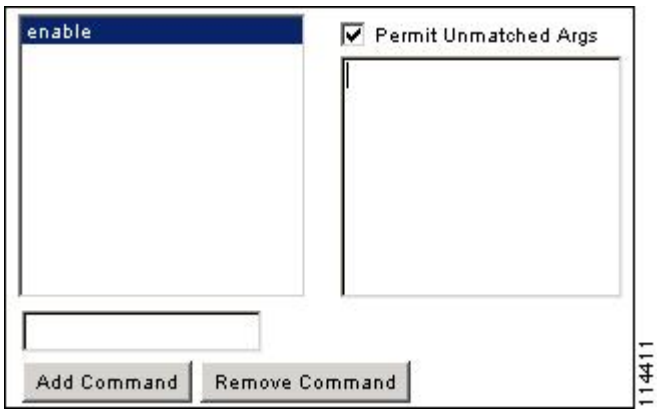
  例如，您可以仅配置 **show** 命令，那么将允许所有 **show** 命令。建议使用此方法，这样您就无需预测命令的每个变体（包括缩写和问号），其显示 CLI 的使用情况（请参阅下图）。

图 *82:* 允许所有相关命令



- 对于单个单词的命令，即使命令没有参数，也必须允许不匹配的参数，例如 **enable** 或 **help**（请参见下图）。

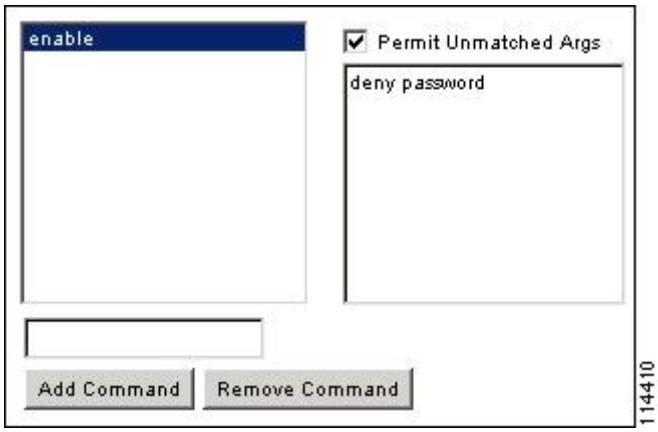
图 *83:* 允许单个单词的命令



- 如要禁止某些参数，请输入参数并在前面放置 **deny**。

  例如，如要允许 **enable**，但不允许 **enable password**，请在命令字段中输入 **enable**，在参数字段内输入 **deny password**。确保选中 **Permit Unmatched Args** 复选框，这样仍能允许单独使用的 **enable**（请参见下图）。

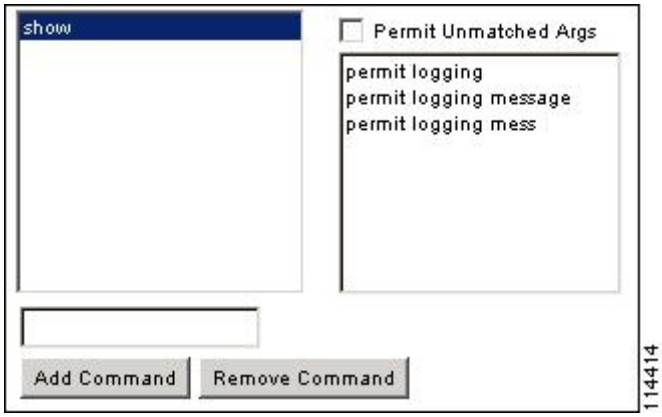
图 *84:* 禁止参数



- 当您在命令行中缩写命令时，ASA 会将前缀和主命令扩展为全文，但对附加的参数却按照您输入的原样发送到 TACACS+ 服务器。

  例如，如果您输入 **sh log**，那么 ASA 将整个 **show logging** 命令发送到 TACACS+ 服务器。但是，如果您输入 **sh log mess**，那么 ASA 将 **show logging mess** 命令发送到 TACACS+ 服务器，而不是发送扩展的 **show logging message** 命令。您可以配置同一个参数的多种拼法以便预测其缩写（请参阅下图）。

图 *85:* 指定缩写



- 建议您允许所有用户使用以下基本命令：
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**
  - **login**

- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

配置 TACACS+ 命令授权

如果启用TACACS+命令授权，且用户在CLI上输入命令，ASA会将命令和用户名发送到TACACS+服务器以确定命令是否已授权。

在启用 TACACS+ 命令授权之前，请务必以 TACACS+ 服务器上定义的用户身份登录 ASA，并确保您具有必要的命令授权来继续配置 ASA。例如，您应该以获得所有命令授权的管理员用户身份登录。否则，可能会意外锁定。

在您确定配置会按预期方式运行之前，请勿保存配置。如果您因错误被锁定，通常可以通过重启 ASA 来恢复访问。

请确保您的TACACS+系统完全稳定且可靠。必要的可靠性级别通常需要您具有完全冗余的TACACS+服务器系统和完全冗余的与 ASA 的连接性。例如，在您的 TACACS+ 服务器池中包括一个与接口 1 连接的服务器和另一个与接口 2 连接的服务器。您还可以将本地命令授权配置为在 TACACS+ 服务器不可用时的回退方法。

如要使用 TACACS+ 服务器配置命令授权，请执行以下步骤：

过程

输入以下命令：

aaa authorization command *tacacs+_server_group* [**LOCAL**]

示例：

```
ciscoasa(config)# aaa authorization command tacacs+_server_group [LOCAL]
```

您可以将 ASA 配置为在 TACACS+ 服务器不可用时使用本地数据库作为回退方法。如要启用回退，请指定服务器组名后跟 **LOCAL**（**LOCAL** 区分大小写）。建议在本地数据库中使用与 TACACS+ 服务器相同的用户名和密码，因为ASA提示符不会给出使用何种方法的任何指示。请确保在本地数据库和命令权限级别中配置用户。

为本地数据库用户配置密码策略

使用本地数据库配置用于CLI或ASDM访问的身份验证时，可以配置密码策略来要求用户在指定时间后更改密码并规定密码标准，例如最短长度和更改后的最小字符数。

密码策略仅适用于使用本地数据库的管理用户，而不适用于可以使用本地数据库的其他流量类型（例如用于网络访问的VPN或AAA流量），也不适用于通过AAA服务器进行身份验证的用户。

配置密码策略后，当您更改密码（自己本人的或其他用户的）时，密码策略将应用于新密码。所有现有密码都将成为祖父。新策略将应用于使用**username**命令以及**change-password** 命令更改密码。

开始之前

- 使用本地数据库为 CLI 或 ASDM 访问配置 AAA 身份验证。
- 在本地数据库中制定用户名。

过程

步骤 1 （可选）设置远程用户的密码多久之后到期（以天为单位）。

password-policy lifetime 天

示例：

```
ciscoasa(config)# password-policy lifetime 180
```

注释
控制台端口的用户不会由于密码到期而锁定。

有效值为 0 到 65536 天。默认值为 0 天，表示密码不会到期。

密码到期之前七天，将会显示一条警告消息。在密码到期后，拒绝远程用户访问系统。如要在到期后访问，请执行以下操作之一：

- 请另一位管理员使用 **username** 命令更改密码。
- 登录到物理控制台端口更改密码。

步骤 2 （可选）设置与旧密码相比，新密码中必须更改的最小字符数。

password-policy minimum-changes *value*

示例：

```
ciscoasa(config)# password-policy minimum-changes 2
```

有效值为 0 和 64 个字符之间。默认值为 0。

字符匹配与位置无关，意味着只有新密码字符不在当前密码的任何地方出现时才视为被更改。

步骤 3 （可选）设置密码最小长度。

password-policy minimum-length 值

示例：

```
ciscoasa(config)# password-policy minimum-length 8
```

有效值为 3 和 64 个字符之间。建议最小密码长度为 8 个字符。

步骤 4 （可选）设置密码必须具有的最小大写字符数。

password-policy minimum-uppercase 值

示例：

```
ciscoasa(config)# password-policy  minimum-uppercase 3
```

有效值为 0 和 64 个字符之间。默认值为 0，表示无最小数。

步骤 5 （可选）设置密码必须具有的最小小写字符数。

password-policy minimum-lowercase 值

示例：

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

有效值为 0 和 64 个字符之间。默认值为 0，表示无最小数。

步骤 6 （可选）设置密码必须具有的最小数字字符数。

password-policy minimum-numeric *value*

示例：

```
ciscoasa(config)# password-policy minimum-numeric 1
```

有效值为 0 和 64 个字符之间。默认值为 0，表示无最小数。

步骤 7 （可选）设置密码必须具有的最小特殊字符数。

password-policy minimum-special 值

示例：

```
ciscoasa(config)# password-policy minimum-special 2
```

有效值为 0 和 64 个字符之间。特殊字符包括以下字符：!、@、#、$、%、^、&、*、“（”和“）”。默认值为 0，表示无最小数。

步骤 8 禁止重用密码：

password-policy reuse-interval 值

示例：

```
ciscoasa(config)# password-policy reuse-interval 5
```

您可以禁止重用与之前使用的密码（2 至 7 个之前的密码）相匹配的密码。之前的密码使用 **password-history** 命令以加密形式存储在每个用户名下的配置中；此命令用户不可配置。

步骤 9 禁止使用与用户名匹配的密码：

password-policy username-check

步骤 10 （可选）设置用户是否必须使用 **change-password** 命令更改密码，而不是让用户使用 **username** 命令更改密码。

password-policy authenticate enable

示例：

```
ciscoasa(config)# password-policy authenticate enable
```

默认设置为禁用：用户可以使用其中任一种方法更改密码。

如果启用此功能并尝试使用 **username** 命令更改密码，将会出现以下错误消息：

```
ERROR: Changing your own password is prohibited
```

也不能使用 **clear configure username** 命令删除自己的帐户。如果尝试这样做，系统将会显示以下错误消息：

```
ERROR: You cannot delete all usernames because you are not allowed to delete yourself
```

更改密码

如果在密码策略中配置了密码有效期，则需要在旧密码到期时将密码更改为新密码。如果启用密码策略身份验证，则要求用此密码更改方法。如果未启用密码策略身份验证，则既可以使用此方法也可以直接更改用户帐户。

如要更改用户名密码，请执行以下步骤：

过程

输入以下命令：

change-password [**old-password** *old_password* [**new-password** *new_password*]]

示例：

```
ciscoasa# change-password old-password j0hncr1chton new-password a3rynsun
```

如果未在命令中输入旧密码和新密码，ASA 会提示您输入。

启用和查看登录历史记录

默认情况下，登录历史记录将保存 90 天。可以禁用此功能，也可更改持续时间，最多 365 天。

开始之前

- 登录历史仅按设备保存；在故障转移和集群环境中，每台设备都仅保留其自己的登录历史记录。
- 在重新加载后，不会保留登录历史记录数据。
- 当您为一种或多种 CLI 管理方法（SSH、ASDM、串行控制台）启用本地 AAA 身份验证时，此功能将适用于本地数据库中或来自 AAA 服务器的用户名。ASDM 登录不会保存在历史中。

过程

步骤 1 设置登录历史记录持续时间：

aaa authentication login-history duration 天

示例：

```
ciscoasa(config)# aaa authentication login-history duration 365
```

可以将 *days* 设置为 1 到 365 之间。默认值为 90。要禁用登录历史记录，请输入 **no aaa authentication login-history**。

当用户登录时，他们将看到其自己的登录历史记录，如此 SSH 示例：

```
cugel@10.86.194.108's password:
The privilege level for user cugel is 15.  The privilege level at the previous login was
2.
User cugel logged in to ciscoasa at 21:04:10 UTC Dec 14 2016
Last login: 21:01:44 UTC Dec 14 2016 from ciscoasa console
Successful logins over the last 90 days: 6
Authentication failures since the last login: 0
Type help or '?' for a list of available commands.
ciscoasa>
```

步骤 2 查看登录历史记录：

show aaa login-history [**user** 名称]

示例：

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
Privilege level:                                    14
Privilege level changed from 11 to 14 at:           14:07:30 UTC Aug 21 2018
```

配置管理访问记帐

在 CLI 中输入 **show** 命令之外的任何命令时，可以将记帐消息发送到 TACACS+ 记帐服务器。您可以配置在用户登录时、输入 **enable** 命令时或者发出命令时记帐。

对于命令记帐，只能使用 TACACS+ 服务器。

如要配置管理访问和 enable 命令记帐，请执行以下步骤：

过程

步骤 1 输入以下命令：

aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

示例：

```
ciscoasa(config)# aaa accounting telnet console group_1
```

有效的服务器组协议是 RADIUS 和 TACACS+。

步骤 2 启用命令记帐。只有 TACACS+ 服务器支持命令记帐。

aaa accounting command [**privilege** *level*] *server-tag*

示例：

```
ciscoasa(config)# aaa accounting command privilege 15 group_1
```

privilege *level* 关键字参数对是最低权限级别，而 *server-tag* 参数是 ASA 应将命令记帐消息发送到的 TACACS+ 服务器组的名称。

从锁定中恢复

在某些情况下，当您打开命令授权或 CLI 身份验证时，可能会被锁定退出 ASA CLI。通常，重启 ASA 即可恢复访问。但是，如果您已经保存配置，则可能会被锁定。

下表列出了常见锁定条件以及如何从中恢复：

表 *55: CLI* 身份验证和命令授权锁定情景

功能	锁定条件	说明	解决方法： 单模	解决方法： 多模
本地 CLI 身份验证	未在本地数据库中配置用户。	如果本地数据库中没有用户，则您无法登录，并且无法添加任何用户。	登录并重置密码和 **aaa** 命令。	使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并添加用户。
TACACS+ 命令授权 TACACS+ CLI 身份验证 RADIUS CLI 身份验证	服务器关闭或无法访问，且没有配置回退方法。	如果服务器无法访问，则您无法登录或无法输入任何命令。	1. 登录并重置密码和 AAA 命令。 2. 将本地数据库配置为回退方法，这样您就不会在服务器关闭时被锁定。	1. 如果由于 ASA 上的网络配置不正确而无法访问服务器，请使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并重新配置网络设置。 2. 将本地数据库配置为回退方法，这样您就不会在服务器关闭时被锁定。
TACACS+ 命令授权	您以没有足够权限的用户身份或不存在的用户身份登录。	启用命令授权，但是随后发现用户无法再输入任何命令。	修复 TACACS+ 服务器用户帐户。 如果您没有访问 TACACS+ 服务器的权限并需要立即配置 ASA，可登录到维护分区并重置密码和 **aaa** 命令。	使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并完成配置更改。您也可以禁用命令授权，直到修复 TACACS+ 配置。
本地命令授权	您以没有足够权限的用户身份登录。	启用命令授权，但是随后发现用户无法再输入任何命令。	登录并重置密码和 **aaa** 命令。	使用会话从交换机登录 ASA。您可以从系统执行空间更改为情景并更改用户级别。

监控设备访问

请参阅以下命令来监控设备访问：

- **show running-config all privilege all**

  此命令显示所有命令的权限级别。

  对于 **show running-config all privilege all** 命令，ASA 将显示当前为每个 CLI 命令分配的权限级别。以下是此命令的输出示例：

```
ciscoasa(config)# show running-config all  privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
...
```

- **show running-config privilege level** 级别

  此命令显示特定权限级别的命令。level 参数是介于 0 和 15 之间的整数。

  以下示例显示 10 级权限的命令分配：

```
ciscoasa(config)# show running-config all privilege level 10
privilege show level 10 command aaa
```

- **show running-config privilege command** 命令

  此命令用于显示特定命令的权限级别。

  以下示例显示 **access-list** 命令的命令分配：

```
ciscoasa(config)# show running-config all privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

- **show curpriv**

  此命令用于显示当前登录的用户。

  以下是 **show curpriv** 命令的输出示例：

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

  下表显示 **show curpriv** 命令的输出。

表 *56: show curpriv* 命令输出说明

字段	说明
用户名 (Username)	用户名、如果您以默认用户身份登录，则名称是 enable_1（用户 EXEC）或 enable_15（特权 EXEC）。
Current privilege level	级别范围为 0 到 15。除非您配置本地命令授权并为中间权限级别分配命令，否则只能使用 0 级和 15 级。
Current Modes	可用的访问模式如下： • P_UNPR - 用户 EXEC 模式（0 级和 1 级） • P_PRIV - 特权 EXEC 模式（2 级到 15 级） • P_CONF - 配置模式

- **show quota management-session** [**ssh** | **telnet** | **http** | **username** *user*]

  此命令用于显示当前正在使用的会话。

  以下是 **show quota management-session** 命令的输出示例：

```
ciscoasa(config)#show quota management-session

#Sessions               ConnectionType                  Username
1                             SSH                        cisco
2                             TELNET                     cisco
1                             SSH                        cisco1
```

- **show aaa login-history** [**user** 名称]

  此命令用于显示每个用户的登录历史记录。

  以下是 **show aaa login-history** 命令的输出示例。

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
Privilege level:                                    14
Privilege level changed from 11 to 14 at:           14:07:30 UTC Aug 21 2018
```

管理访问的历史记录

表 *57:* 管理访问的历史记录

功能名称	平台版本	说明
CiscoSSH 堆栈现在为默认设置	9.19(1)	现在默认使用思科 SSH 堆栈。 新增/修改的命令：**ssh stack ciscossh**
环回接口支持 SSH 和 Telnet	9.18(2)	您现在可以添加环回接口并用于以下功能： • SSH • Telnet 新增/修改的命令：**interface loopback**、**ssh**、**telnet**
思科 SSH 堆栈	9.17(1)	ASA 使用专有 SSH 堆栈进行 SSH 连接。现在，您可以选择使用基于 OpenSSH 的 CiscoSSH 堆栈。默认堆栈继续为ASA堆栈。思科SSH支持： • FIPS 合规性 • 定期更新，包括来自思科和开源社区的更新 请注意，CiscoSSH 堆栈不支持以下功能： • 通过VPN通过SSH连接到其他接口（管理访问） • EdDSA 密钥对 • FIPS模式下的RSA密钥对 如果需要这些功能，应继续使用ASA SSH堆栈。 CiscoSSH 堆栈的 SCP 功能略有变化：要使用 ASA **copy** 命令将文件复制到 SCP 服务器或从 SCP 服务器复制文件，您必须使用**ssh**命令在 ASA 上为 SCP 服务器子网/主机启用 SSH 访问权限。 新增/修改的命令：**ssh stack ciscossh**
本地用户锁定更改	9.17(1)	ASA 可以在登录尝试失败达到可配置次数之后锁定账户。此功能不适用于权限级别为 15 的用户。此外，用户将被无限期锁定，直到管理员解锁其账户。现在，用户将在 10 分钟后解锁，除非管理员在此之前使用 **clear aaa local user lockout** 命令。权限级别为 15 的用户现在也受锁定设置的影响。 新增/修改的命令：**aaa local authentication attempts max-fail** 、**show aaa local user**

功能名称	平台版本	说明
SSH 和 Telnet 密码更改提示	9.17(1)	本地用户首次使用 SSH 或 Telnet 登录 ASA 时，系统会提示他们更改密码。在管理员更改密码后，系统还会提示他们进行首次登录。但是，如果 ASA 重新加载，则系统不会提示用户，即使是首次登录也是如此。 请注意，任何使用本地用户数据库的服务（例如 VPN）也必须使用在 SSH 或 Telnet 登录期间更改的新密码。 新增/修改的命令：**show aaa local user**
SSH 安全性改进	9.16（1）	SSH 现在支持以下安全性改进： • 主机密钥格式 - **crypto key generate** {**eddsa** | **ecdsa**}. 除了 RSA，我们还增加了对 EdDSA 和 ECDSA 主机密钥的支持。如果密钥存在，ASA 会尝试按以下顺序使用：EdDSA、ECDSA，然后是 RSA。如果使用 **ssh key-exchange hostkey rsa** 命令将 ASA 显式配置为使用 RSA 密钥，则必须生成 2048 位或更高位的密钥。为了实现升级兼容性，仅当使用默认主机密钥设置时，ASA才会使用较小的RSA主机密钥。RSA支持将在更高版本中删除。 • 密钥交换算法 - **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • 加密算法 -**ssh cipher encryption chacha20-poly1305@openssh.com** • 不再支持 SSH 版本 1 - 已删除 **ssh version** 命令。 新增/修改的命令： **crypto key generate eddsa**、 **crypto key zeroize eddsa**、 **show crypto key mypubkey**、 **ssh cipher encryption chacha20-poly1305@openssh.com**、 **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**}、 **ssh key-exchange hostkey**、 **ssh version**
SNMP 的管理访问	9.14(2)	在配置通过 VPN 隧道的管理访问时，在加密映射访问列表中包含外部接口的 IP 地址，作为通过站点间 VPN 进行安全 SNMP 轮询的 VPN 配置的一部分。
HTTPS 空闲超时设置	9.14(1)	现在，您可以为 ASA 的所有 HTTPS 连接设置空闲超时，包括 ASDM、WebVPN 和其他客户端。以前，使用 **http server idle-timeout** 命令只能设置 ASDM 空闲超时。如果同时设置两个超时，新命令优先执行。 新增/修改的命令：**http connection idle-timeout**

功能名称	平台版本	说明
SSH 加密密码现在按预定义列表的安全性从最高到最低的顺序列出	9.13(1)	SSH 加密密码现在按预定义列表（例如中等或高安全性）的安全性从最高到最低的顺序列出。在较早的版本中，它们是按从最低到最高的顺序列出的，这意味着低安全性密码的提议先于高安全性密码。 新增/修改的命令：**ssh cipher encryption**
仅限在管理情景中设置 SSH 密钥交换模式	9.12(2)	您必须在 Admin 情景中设置 SSH 密钥交换；所有其他情景将继承此设置。 新增/修改的命令：**ssh key-exchange**
现在登录时需要更改 **enable** 密码	9.12(1)	**enable** 默认密码为空。现在，如果您尝试在 ASA 上进入特权 EXEC 模式，系统会要求您将密码改为一个至少包含 3 个字符的值，而不能将密码留空。**no enable password** 命令今后将不受支持。 在 CLI 中，您可以使用 **enable** 命令、**login** 命令（用户权限级别应在 2 级以上）或者 SSH 或 Telnet 会话（如果启用 **aaa authorization exec auto-enable**）来进入特权 EXEC 模式。无论使用哪种方法，您都必须设置密码。 但是在登录 ASDM 时，则没有这项更改密码的要求。默认情况下，在 ASDM 中，您无需使用用户名和 **enable** 密码即可登录。 新增/修改的命令：**enable password**
可配置管理会话限制	9.12(1)	现在，您可以配置汇聚管理会话数、每用户管理会话数和每协议管理会话数的最大值。以前，您只能配置汇聚会话数。此功能不会影响控制台会话。需要注意的是，在多情景模式下，如果最大 HTTPS 会话数固定为 5，则无法配置会话数。此外，系统配置中也不再接受 **quota management-session** 命令，您只能在情景配置中进行此设置。现在，最大汇聚会话数为 15。如果您已将其配置为 0（无限制）或大于 16 的值，在升级设备时，此值会自动更改为 15。 新增/修改的命令： **quota management-session**、**show quota management-session**
管理权限级别更改通知	9.12(1)	现在，在您授予访问权限 (**aaa authentication enable console**) 或允许直接进行特权 EXEC 访问 (**aaa authorization exec auto-enable**) 后，如果用户已分配的访问权限级别在上次登录后发生更改，ASA 会向用户显示通知。 新增/修改的命令：**show aaa login-history**

功能名称	平台版本	说明
SSH 增强安全性	9.12(1)	请参阅以下 SSH 安全改进： • 支持 Diffie-Hellman 组 14 SHA256 密钥交换。此设置现在为默认值。先前默认值为组 1 SHA1。 • 支持 HMAC-SHA256 完整性加密。默认值现在是高安全性密码组（仅 hmac-sha2-256）。先前默认值为介质集。 新增/修改的命令：**ssh cipher integrity** 、**ssh key-exchange group dh-group14-sha256**
允许基于非浏览器的 HTTPS 客户端访问 ASA	9.12(1)	您可以允许基于非浏览器的 HTTPS 客户端访问 ASA 上的 HTTPS 服务。默认情况下，允许 ASDM、CSM 和 REST API。 新增/修改的命令：**http server basic-auth-client**
RSA 密钥对支持 3072 位密钥	9.9(2)	您现在可以将模数长度设为 3072。 新增或修改的命令：**crypto key generate rsa modulus**
网桥虚拟机 (BVI) 上的 VPN 管理访问	9.9(2)	现在，如果在 BVI 上启用了 VPN **management-access**，可以在该 BVI 上启用管理服务（例如 **telnet**、**http** 和 **ssh**）。对于非 VPN 管理访问，应在网桥组成员接口上继续配置这些服务。 新增或修改的命令：**https**、**telnet**、**ssh**、**management-access**
已弃用 SSH 版本 1	9.9(1)	SSH 版本 1 已弃用，未来不再发行。默认设置已从 SSH v1 和 v2 更改为仅 SSH v2。 新增/修改的命令：**ssh version**
对使用SSH公钥身份验证的用户和具有密码的用户分别进行单独的身份验证	9.6(3)/9.8(1)	在 9.6(2) 以前的版本中，您在启用 SSH 公钥身份验证 (**ssh authentication**)时，可以不必明确启用基于本地用户数据库的AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。在 9.6(2) 中，ASA 要求明确启用 AAA SSH 身份验证。在此版本中，您不再需要明确启用 AAA SSH 身份验证；当您为用户配置 **ssh authentication** 命令时，默认情况下会为使用此类型身份验证的用户启用本地身份验证。此外，在明确配置 AAA SSH 身份验证时，此配置将仅适用于具有密码的用户名，并且可以使用任何 AAA 服务器类型（例如 **aaa authentication ssh console radius_1**）。例如，某些用户可以使用公钥身份验证（使用本地数据库），而其他用户则可配合使用密码和 RADIUS。 未修改任何命令。

功能名称	平台版本	说明
登录历史记录	9.8(1)	默认情况下，登录历史记录将保存 90 天。可以禁用此功能，也可更改持续时间，最多365天。仅当为一种或多种管理方法（SSH、ASDM、Telnet 等）启用本地 AAA 身份验证时，此功能才适用于本地数据库中的用户名。 引入了以下命令：**aaa authentication login-history**、**show aaa login-history**
禁止重复使用密码以及禁止使用与某一用户名匹配的密码的密码策略实施	9.8(1)	现在，可以禁止重复使用过去的密码（最多7代），还可以禁止使用与某一用户名匹配的密码。 引入了以下命令：**password-history**、**password-policy reuse-interval**、**password-policy username-check**
ASDM 的 ASA SSL 服务器模式匹配	9.6(2)	对于通过证书进行身份验证的 ASDM 用户，您现在可以要求证书与证书映射匹配。 修改了以下命令：**http authentication-certificate match**
SSH 公钥身份验证改进	9.6(2)	在更早的版本中，您在启用 SSH 公钥身份验证 (**ssh authentication**) 时，可以不必启用基于本地用户数据库的 AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。该配置现在已修复，您必须明确启用 AAA SSH 身份验证。要禁止用户使用密码而不是私钥，现在您可以创建未定义任何密码的用户名。 修改了以下命令：**ssh authentication**、**username**。
ASDM 管理授权	9.4(1)	现在可以单独为 HTTP 访问与 Telnet 和 SSH 访问配置管理授权。 引入了以下命令：**aaa authorization http console**
证书配置中的 ASDM 用户名	9.4(1)	当启用 ASDM 证书身份验证 (**http authentication-certificate**) 时，可以配置 ASDM 从证书提取用户名的方式；还可以在出现登录提示时启用用户名预填充功能。 引入了以下命令：**http username-from-certificate**
改进的一次性密码身份验证	9.2(1)	有足够授权权限的管理员可以通过输入自己的身份验证凭证一次进入特权 EXEC 模式。**aaa authorization exec** 命令中添加了 **auto-enable** 选项。 修改了以下命令：**aaa authorization exec**。
对 IPV6 的 HTTP 重定向支持	9.1(7)/9.6(1)	现在，在为 ASDM 接入或无客户端 SSL VPN 启用 HTTP 重定向到 HTTPS 时，可将已发送的流量重定向到 IPv6 地址。 向以下命令添加了功能：**http redirect**

功能名称	平台版本	说明
可配置 SSH 加密和完整性密码	9.1(7.4)、9.3(3)、9.6(1)	用户可在执行 SSH 加密管理时选择密码模式，并可配置 HMAC 和加密来改变密钥交换算法。根据您的应用，您可能希望将密码变得更加严格或更不严格。请注意，安全复制的性能部分取决于所使用的加密密码。默认情况下，ASA 会按顺序协商以下其中一种算法：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr。如果选择建议的第一种算法 (3des-cbc)，则性能会远远慢于 128-cbc 等更高效的算法。例如，要更改所需的密码，请使用 **ssh cipher encryption custom aes128-cbc**。 引入了以下命令：**ssh cipher encryption, ssh cipher integrity**。
SSH 的 AES-CTR 加密	9.1(2)	ASA 中的 SSH 服务器实施现在支持 AES-CTR 模式加密。
改进的 SSH 重新生成密钥间隔	9.1(2)	在连接时间达到 60 分钟后或数据流量达到 1 GB 后，SSH 连接重新生成密钥。 引入了以下命令：**show ssh sessions detail**。
对于在多情景模式下的 ASASM，支持从交换机进行 Telnet 和虚拟控制台身份验证。	8.5(1)	虽然从多情景模式下的交换机连接至 ASASM 将连接至系统执行空间，但是可以在管理员情景中配置身份验证来监管这些连接。
使用本地数据库时，支持管理员密码策略	8.4(4.1)、9.1(2)	使用本地数据库配置用于 CLI 或 ASDM 访问的身份验证时，可以配置密码策略来要求用户在指定时间后更改密码并规定密码标准，例如最短长度和更改后的最小字符数。 引入了以下命令：**change-password**、**password-policy lifetime**、**password-policy minimum changes**、**password-policy minimum-length**、**password-policy minimum-lowercase**、**password-policy minimum-uppercase**、**password-policy minimum-numeric**、**password-policy minimum-special**、**password-policy authenticate enable**、**clear configure password-policy**、**show running-config password-policy**。
支持 SSH 公钥身份验证	8.4(4.1)、9.1(2)	对于与 ASA 的 SSH 连接，您可以基于每个用户启用公钥身份验证。您可以指定公钥文件 (PKF) 格式的密钥或 Base64 密钥。PKF 密钥的长度可达 4096 位。对于由于过长而导致 ASA 不支持使用 Base64 格式（限长 2048 位）的密钥，请使用 PKF 格式。 引入了以下命令：**ssh authentication**。 仅在 *9.1(2)* 及更高版本中支持 *PKF* 密钥格式。
支持用于 SSH 密钥交换的 Diffie-Hellman 组 14	8.4(4.1)、9.1(2)	已添加支持 Diffie-Hellman 组 14 进行 SSH 密钥交换。以前，只支持组 1。 引入了以下命令：**ssh key-exchange**。

功能名称	平台版本	说明
支持的管理会话最大数量	8.4(4.1)、9.1(2)	您可以设置并发 ASDM、SSH 和 Telnet 会话的最大数量。 引入了以下命令：**quota management-session**、**show running-config quota management-session**、**show quota management-session**。
提高了 SSH 安全性；不再支持 SSH 默认用户名。	8.4(2)	从 8.4(2) 开始，您无法再使用 pix 或 asa 用户名和登录密码通过 SSH 连接至 ASA。如要使用 SSH，必须使用 **aaa authentication ssh console LOCAL** 命令 (CLI) 或“配置 \> 设备管理 \> 用户/AAA \> AAA 访问 \> 身份验证 (ASDM)”来配置 AAA 身份验证；然后通过输入 **username** 命令 (CLI) 或依次选择“配置 \> 设备管理 \> 用户/AAA \> 用户帐户 (ASDM)”来定义本地用户。如果要使用 AAA 服务器而不是本地数据库进行身份验证，建议也将本地身份验证配置为备用方法。
管理访问	7.0(1)	引入了此功能。 引入了以下命令： **show running-config all privilege all**、**show running-config privilege level**、**show running-config privilege command**、**telnet**、**telnet timeout**、**ssh**、**ssh timeout**、**http**、**http server enable**、**asdm image disk**、**banner**、**console timeout**、**icmp**、**ipv6 icmp**、**management access**、**aaa authentication console**、**aaa authentication enable console**、**aaa authentication telnet | ssh console**、**service-type**、**login**、**privilege**、**aaa authentication exec authentication-server**、**aaa authentication command LOCAL**、**aaa accounting serial | telnet | ssh | enable console**、**show curpriv**、**aaa accounting command privilege**。

第 43 章

软件和配置

本章介绍如何管理 ASA 软件和配置。

- 升级软件，第 1285 页
- 使用 ROMMON 加载映像（ISA 3000），第 1285 页
- 升级 ROMMON 映像（ISA 3000），第 1287 页
- 降级软件，第 1288 页
- 管理文件，第 1293 页
- 设置 ASA 映像、ASDM 和启动配置，第 1302 页
- 备份和恢复配置或其他文件，第 1305 页
- Cisco Secure Firewall 3100/4200上的热插拔 SSD，第 1322 页
- 禁用 USB 端口，第 1324 页
- 软件和配置的历史记录，第 1326 页

升级软件

有关完整的升级过程，请参阅《思科 ASA 升级指南》。

使用 ROMMON 加载映像（ISA 3000）

要使用 TFTP 从 ROMMON 模式下将软件映像加载到 ASA，请执行以下步骤。

过程

步骤 1 根据访问 ISA 3000 控制台，第 11 页中的说明连接到 ASA 控制台端口。

步骤 2 关闭 ASA，然后重新启动。

步骤 3 在启动过程中，当系统提示您进入 ROMMON 模式时，请按 **Escape** 键。

步骤 4 在 ROMMOM 模式下，定义 ASA 的接口设置，包括 IP 地址、TFTP 服务器地址、网关地址、软件映像文件和端口，如下所示：

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

注释
请确保已存在网络连接。

interface 命令在 ASA 5506-X、ASA 5508-X、ASA 5516-X 和 ISA 3000 平台上将被忽略，您必须从管理 1/1 接口对这些平台执行 TFTP 恢复。

步骤 5 验证您的设置：

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

步骤 6 对 TFTP 服务器执行 ping 操作：

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

步骤 7 保存网络设置，以备将来使用：

```
rommon #8> sync
Updating NVRAM Parameters...
```

步骤 8 加载软件映像：

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21
```

```
Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

成功加载软件映像后，ASA 会自动退出 ROMMON 模式。

步骤 9 从ROMMON 模式启动 ASA 不会在重新加载时保留系统映像；您仍需将映像下载到闪存。有关完整的升级过程，请参阅《思科 ASA 升级指南 》。

升级 ROMMON 映像（ISA 3000）

按照以下步骤升级 ISA 3000 的 ROMMON 映像。对于 ASA 型号，系统上的 ROMMON 版本必须为 1.1.8 或更高版本。我们建议您将引擎升级到最新版本。

您只能升级到新版本；无法降级。

注意 适用于 1.1.15 的 ASA 5506-X，5508-X 和 5516-X ROMMON 升级，以及适用于 1.0 的 ISA 3000 ROMMON 升级。并且，1.0.5 的 ISA 3000 ROMMON 升级时间为过去 ROMMON 版本的两倍，大约需要 15 分钟。升级流程中**请勿**重启设备 。如果升级未在 30 分钟内完成或升级失败，请联系思科技术支持； **请勿**重启或重置设备。

开始之前

从Cisco.com 获取新的ROMMON映像，并将其放在服务器上以复制到ASA。ASA 支持FTP、TFTP、SCP、HTTP(S) 和 SMB 服务器。请从以下网址下载映像：

- ISA 3000：https://software.cisco.com/download/home/286288493/type

过程

步骤 1 将 ROMMON 映像复制到 ASA 闪存。此程序显示 FTP 副本；输入 **copy ?**，使用其他服务器类型的语法。

copy ftp://[*username*:*password*@]*server_ip*/**asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

步骤 2 要查看当前版本，请输入 **show module** 命令并在 MAC 地址范围表中查看 Mod 1 的输出中的固件版本：

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
```

```
---- -------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

步骤 3 升级 ROMMON 映像：

upgrade rommon disk0:asa5500-firmware-*xxxx*.SPA

示例：

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

步骤 4 当出现提示时，确认重新加载 ASA。

ASA 将升级 ROMMON 映像，然后重新加载操作系统。

降级软件

在许多情况下，您可以降级ASA软件并从以前的软件版本恢复备份配置。降级方法取决于您的ASA平台。

降级的准则和限制

降级前请参阅以下准则：

- **没有对集群的官方零停机降级支持**-但是，在某些情况下，零停机降级将起作用。关于降级，请参阅以下已知问题；请注意，可能会有其他需要您重新加载集群设备的问题，这会导致停机。
  - **降级到具有集群功能的 9.9(1) 以前版本**- 9.9(1) 及更高版本包含备份分发方面的改进。如果您的集群中有 3 个或更多个设备，您必须执行以下步骤：
    1. 从集群中删除所有辅助设备（使得集群仅包含主设备）。
    2. 将 1 个辅助设备降级，然后重新加入集群。
    3. 禁用主设备上的集群功能；将其降级，然后重新加入集群。
    4. 一次一个，将剩余的辅助设备降级，然后重新加入集群。
  - **在启用集群站点冗余时降级到 9.9(1) 以前的版本**- 如果您想要降级（或如果您想要将 9.9(1) 以前版本的设备添加到集群），您应该禁用站点冗余。否则，您会看到副作用，例如运行旧版本的设备上出现虚拟转发数据流。
  - **在集群和加密映射的情况下从 9.8(1) 降级**- 如果配置了加密映射，则在从 9.8(1) 降级时，将没有零停机时间降级支持。应在降级之前清除加密映射配置，在降级之后再重新应用该配置。
  - **在将集群设备运行状态检查设置为 0.3 到 0.7 秒的情况下从 9.8(1) 降级**- 如果在将保持时间 (**health-check holdtime**) 设置为 0.3 - 0.7 秒后降级 ASA 软件，则此设置将恢复为 3 秒的默认值，因为不支持新设置。
  - **在集群的情况下从 9.5(2) 或更高版本降级到 9.5(1) 或早期版本 (CSCuv82933)**-在从 9.5(2) 降级时，将没有零停机时间降级支持。您必须大致在同一时间重新加载所有设备，这样当设备恢复在线时可形成新的集群。如果您等待所有设备按顺序重新加载完，则无法形成集群。
  - **在集群的情况下从 9.2(1) 或更高版本降级到 9.1 或早期版本**- 不支持零停机时间降级。
- **从 9.22 或更高版本降级的问题** - 如果使用 usb-port disable 命令禁用 USB 端口，但随后降级到更早的版本，则该端口将保持禁用状态，且在不擦除NVRAM的情况下无法重新启用该端口（FXOS 本地-mgmt **erase secure all** 命令）。
- **从 9.18 或更高版本降级问题**- 9.18 中的行为发生变化，其中 **访问组** 命令将在其 **访问组** 命令之前列出。如果降级， **访问组** 命令将被拒绝，因为它尚未加载 **访问组** 命令。即使您之前已启用 **forward-reference enable** 命令，也会出现此结果，因为该命令现在已被删除。在降级之前，请确保手动复制所有 **访问组** 命令，然后在降级后重新输入这些命令。
- **从9.10（1）降级以进行智能许可**-由于智能代理中的更改，如果您进行降级，则必须将设备重新注册到思科智能软件管理器。新的智能代理使用加密文件，因此您需要重新注册才能使用旧智能代理所需的未加密文件。
- **使用 PBKDF2（基于密码的密钥派生功能 2）散列处理，利用密码降级到 9.5 和早期版本**- 9.6 以前的版本不支持 PBKDF2 散列处理。在 9.6(1) 中，长度超过 32 个字符的 **enable** 和 **username** 密码使用 PBKDF2 散列处理。在 9.7(1) 中，所有长度的新密码都将使用 PBKDF2 散列处理（现有密码继续使用 MD5 散列处理）。如果降级，则 **enable** 密码将恢复为默认值（空白）。用户名不会正确解析，并将删除 **username** 命令。必须重新创建本地用户。

- **对于 ASA Virtual从版本 9.5(2.200) 降级-** ASA virtual 不会保留许可注册状态。您需使用 **license smart register idtoken id_token force** 命令重新注册（对于 ASDM：请参阅 **Configuration > Device Management > Licensing > Smart Licensing** 页面，并使用 **Force registration** 选）；从智能软件管理器中获取 ID 令牌。
- **即使备用设备运行的软件版本不支持原始隧道协商的密码套件，也会将 VPN 隧道复制到备用设备**—此情景在降级时出现。在此情况下，请断开 VPN 连接，然后再重新连接。

降级后删除了不兼容的配置

当您降级到旧版本时，更高版本中引入的命令将从配置中删除。在降级之前，无法自动根据目标版本检查配置。您可以按版本查看何时在ASA新功能中添加了新命令。https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.html

您可以在使用命令降级后查看被拒绝的命令。**show startup-config errors** 如果可以在实验设备上执行降级，则可以使用此命令预览效果，然后在生产设备上执行降级。

在某些情况下，ASA会在升级时自动将命令迁移到新表单，因此根据您的版本，即使您没有手动配置新命令，降级也可能会受到配置迁移的影响。我们建议您对旧配置进行备份，可供您在降级时使用。在升级到 8.3 的情况下，将自动创建备份 (<old_version>_startup_cfg.sav)。其他迁移不会创建备份。有关可能影响降级的自动命令迁移的详细信息，请参阅《ASA 升级指南》中的“特定于版本的准则和迁移”。

另请参阅中的已知降级问题。降级的准则和限制，第 1288 页

例如，运行9.8（2）版本的ASA包括以下命令：

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
```

当您降级到9.0（4）时，您将在启动时看到以下错误：

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
                                  ^
ERROR: % Invalid input detected at '^' marker.

username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                               ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
                                       ^
ERROR: % Invalid input detected at '^' marker.
```

在本例中，在版本9.5（2）中添加了对access-list extended命令中sctp的支持，在版本9.6（1）中添加了对username命令中pbkdf2的支持，并在snmp-server user命令中支持engineID是在9.5（3）版本中添加的。

降级 Firepower 1000、Cisco Secure Firewall 1200/3100/4200

通过将 ASA 版本设置为旧版本，将备份配置恢复为启动配置，然后重新加载，可以降级 ASA 软件版本。

开始之前

此程序需要在升级之前对ASA进行备份配置，以便可以恢复旧配置。如果不恢复旧配置，则可能存在表示新功能或更改功能不兼容的命令。加载旧软件版本时，将会拒绝任何新命令。

过程

步骤 1 使用独立部署，故障转移或集群部署的ASA升级指南中的升级程序加载旧ASA软件版本。https://www.cisco.com/c/en/us/td/docs/security/asa/upgrade/asa-upgrade/asa-appliance-asav.html在这种情况下，请指定旧ASA版本而不是新版本。重要提示：请不要重新加载ASA。

步骤 2 在ASA CLI中，将备份ASA配置复制到启动配置。对于故障转移，请在主用设备上执行此步骤。此步骤会将命令复制到备用设备。

copy *old_config_url* **startup-config**

请务必不要使用;将运行配置保存到启动配置。此命令将覆盖您的备份配置。**write memory**

示例：

```
ciscoasa# copy disk0:/9.13.1_cfg.sav startup-config
```

步骤 3 重新加载 ASA。

ASA CLI

reload

ASDM

依次选择 **Tool** > **System Reload**。

降级 Firepower 4100/9300

您可以通过将备份配置恢复为启动配置，将 ASA 版本设置为旧版本，然后重新加载来降级 ASA 软件版本。

开始之前

- 此程序需要在升级之前对ASA进行备份配置，以便可以恢复旧配置。如果不恢复旧配置，则可能存在表示新功能或更改功能不兼容的命令。加载旧软件版本时，将会拒绝任何新命令。

- 确保旧ASA版本与当前FXOS版本兼容。否则，请在恢复旧ASA配置之前先将FXOS降级。只需确保降级的FXOS也与当前ASA版本兼容（在降级之前）。如果无法实现兼容性，我们建议您不要执行降级。

过程

步骤 1 在ASA CLI中，将备份ASA配置复制到启动配置。对于故障转移或集群，请在主用/控制设备上执行此步骤。此步骤会将命令复制到备用/数据单元。

copy *old_config_url* **startup-config**

请务必不要使用;将运行配置保存到启动配置。此命令将覆盖您的备份配置。**write memory**

示例：

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

步骤 2 在FXOS中，使用 机箱管理器或FXOS CLI，按照独立，故障转移或集群部署的ASA升级指南中的升级程序使用旧ASA软件版本。在这种情况下，请指定旧ASA版本而不是新版本。

步骤 3 如果您还降级FXOS，请使用 机箱管理器 或FXOS CLI将旧的FXOS软件版本设置为当前版本，使用独立部署，故障转移或集群部署的ASA升级指南中的升级程序。

降级 ISA 3000

降级功能提供了 ASA 5500-X and ISA 3000 型号完成以下功能的快捷方式：

- 清除引导映像配置 (**clear configure boot**)。
- 将引导映像设置为旧映像 (**boot system**)。
- （可选）输入新的激活密钥 (**activation-key**)。
- 将运行配置保存到启动 (**write memory**)。此操作会将 BOOT 环境变量设置为旧映像，因此，当您重新加载时，将会加载旧映像。
- 将旧配置备份复制到启动配置 (**copy***old_config_url***startup-config**)。
- 正在重新加载 (**reload**)。

开始之前

- 此程序需要在升级之前对 ASA 进行备份配置，以便可以恢复旧配置。

过程

ASA CLI：降级软件并恢复旧配置。

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

示例：

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

/noconfirm 选项用于在不进行提示的情况下执行降级。*image_url* 是旧映像在 disk0、disk1、tftp、ftp 或 smb 上的路径。*old_config_url* 是到已保存的预迁移配置的路径。如果需要恢复至 8.3 版本之前的激活密钥，则可输入旧的激活密钥。

管理文件

查看闪存中的文件

您可以查看闪存中的文件，并参阅有关文件的信息。

过程

步骤 1 查看闪存中的文件：

dir [**disk***n***:**]

disk0: 是内部存储器。其他驱动器编号表示外部存储，例如 USB 驱动器、SSD 或 SD 卡。

示例：

```
hostname# dir

Directory of disk0:/
500    -rw-  4958208     22:56:20 Nov 29 2004  cdisk.bin
2513   -rw-  4634        19:32:48 Sep 17 2004  first-backup
2788   -rw-  21601       20:51:46 Nov 23 2004  backup.cfg
2927   -rw-  8670632     20:42:48 Dec 08 2004  asdmfile.bin
```

步骤 2 查看有关特定文件的扩展信息：

show file information [path:/]*filename*

示例：

```
hostname# show file information cdisk.bin

disk0:/cdisk.bin:
  type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)
```

所列的文件大小仅用作示例。

默认路径是内部闪存的根目录 (disk0:/)。

从闪存中删除文件

您可以从闪存中删除不再需要的文件。

过程

从闪存中删除文件：

delete disk*n***:** *filename*

disk0: 是内部存储器。其他驱动器编号表示外部存储，例如 USB 驱动器、SSD 或 SD 卡。

默认情况下，如果未指定路径，将从当前工作目录中删除文件。删除文件时，可以使用通配符。系统会提示您要删除的文件的文件名，然后您必须确认删除。

擦除闪存文件系统

要清除闪存文件系统，请执行以下步骤：

过程

步骤 1 根据 访问 ISA 3000 控制台，第 11 页 中的说明连接到 ASA 控制台端口。

步骤 2 关闭 ASA，然后重新启动。

步骤 3 在启动过程中，当系统提示您进入 ROMMON 模式时，请按 **Escape** 键。

步骤 4 输入 **erase** 命令，这会覆盖所有文件并清除文件系统，包括隐藏的系统文件：

rommon #1> **erase** [**disk0:** | **disk***n***:** | **usb:**]

disk0: 是内部存储器。其他驱动器编号表示外部存储。较新的型号使用 **usb:** 作为外部 USB 驱动器。

配置文件访问

ASA 可以使用 FTP 客户端、安全复制客户端或 TFTP 客户端。您也可以将 ASA 配置为安全复制服务器，以便可以在计算机上使用安全复制客户端。

配置 FTP 客户端模式

ASA 可使用 FTP 在 FTP 服务器中上传或下载映像文件或配置文件。在被动 FTP 中，客户端同时启动控制连接和数据连接。服务器（被动模式下数据连接的接收方）通过它用于侦听特定连接的端口号进行响应。

过程

将 FTP 模式设置为被动：

ftp mode passive

示例：

```
ciscoasa(config)# ftp mode passive
```

配置 ASA 安全复制服务器

当 ASA 被用作 SCP 客户端时，可以使用 **copy** 命令来配置 SCP 设置。

SCP 的性能部分取决于所使用的加密密码。默认情况下，ASA 会按顺序协商以下其中一种算法：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr。如果选择建议的第一种算法 (3des-cbc)，则性能会远远慢于 128-cbc 等更高效的算法。要更改建议的密码，可使用 **ssh cipher encryption** 命令；例如，**ssh cipher encryption custom aes128-cbc**

开始之前

- ASA 许可证必须具有强加密 (3DES/AES) 许可证，才能支持 SSH V2 连接。
- 除非另有规定，否则对于多情景模式，请在系统执行空间中完成本程序。要从该情景更改到系统执行空间，请输入 **changeto system** 命令。如果您尚未进入系统配置模式，请在 窗格中双击主用设备 IP 地址下的 **System**。
- 对于 SCP 服务器，请根据 配置 SSH 访问 ，第 1237 页在 ASA 上启用 SSH。

过程

步骤 1 （可选）ASA 为与之连接的每个 SCP 服务器存储 SSH 主机密钥。如果需要，可以手动管理密钥。

ssh pubkey-chain [**no**]**server** *ip_address* {**key-string** *key_string* **exit**| **key-hash** {**md5** | **sha256**} *fingerprint*}

示例：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
ciscoasa(config-ssh-pubkey-server)# show running-config ssh pubkey-chain
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256 f1:22:49:47:b6:76:74:b2:db:26:fb:13:65:d8:99:19:
e7:9e:24:46:59:be:13:7f:25:27:70:9b:0e:d2:86:12
```

对于每个服务器，可以指定 SSH 主机的 **key-string**（公钥）或 **key-hash**（散列值）。

key_string 是远端对等体的采用 Base64 编码的 RSA 公钥。您可以从打开的 SSH 客户端（即 .ssh/id_rsa.pub 文件）获得公钥值。在您提交采用 Base64 编码的公钥之后，系统会通过 SHA-256 对其进行散列处理。

key-hash{**md5** | **sha256**}*fingerprint* 可用于输入已经过散列处理的密钥（使用 MD5 或 SHA-256 密钥）；例如，您从 **show** 命令输出复制的密钥。

步骤 2 （可选） 启用或禁用 SSH 主机密钥检查。对于多情景模式，在管理情景中输入此命令。

[**no**] **ssh stricthostkeycheck**

示例：

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?

Address or name of remote host [10.86.95.9]?

Destination username [cisco]?

Destination password []? cisco123

Destination filename [x]?
```

默认情况下，系统会启用此选项。当启用此选项时，如果ASA中尚未存储主机密钥，系统会提示您接受或拒绝主机密钥。当禁用此选项时，如果以前未存储主机密钥，ASA 会自动接受主机密钥。

示例

以下示例为 10.86.94.170 上的服务器添加经过散列处理的主机密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256 65:d9:9d:fe:1a:bc:61:aa:
64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

以下示例为 10.7.8.9 上的服务器添加主机字符串密钥：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:
46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

配置 ASA TFTP 客户端路径

TFTP 是一种简单的客户端/服务器文件传输协议，RFC 783 和 RFC 1350 第 2 修订版对其进行了说明。您可以将 ASA 配置为 TFTP 客户端，以便它可以与 TFTP 服务器之间进行双向文件复制。按照这种方式，您可以备份配置文件并将其传播到多台 ASA。

按照本节所述可以预定义 TFTP 服务器的路径，从而无需在诸如 **copy** 和 **configure net** 等命令中输入该路径。

过程

预定义用于 **configure net** 和 **copy** 命令的 TFTP 服务器地址和文件名。

tftp-server *interface_name server_ip filename*

示例：

```
ciscoasa(config)# tftp-server inside 10.1.4.7 files/config1.cfg
ciscoasa(config)# copy tftp: test.cfg

Address or name of remote host [10.1.4.7]?

Source filename [files/config1.cfg]?config2.cfg

Destination filename [test.cfg]?

Accessing tftp://10.1.4.7/files/config2.cfg;int=outside...
```

输入命令时，可以覆盖文件名；例如，当使用 **copy** 命令时，可以利用预定义的 TFTP 服务器地址，但仍然在交互式提示符处输入任意文件名。

对于 **copy** 命令，输入 **tftp:** 以使用 tftp-server 值而非 **tftp://***url*。

将文件复制到 ASA

本节介绍如何复制应用映像、ASDM 软件、配置文件，或者任何其他需要从 TFTP、FTP、SMB、HTTP、HTTPS、SCP 服务器或从优盘等驱动器下载至内部或外部闪存的文件。

准则

- **disk0:** 是内部存储器。其他驱动器编号表示外部存储，例如 USB 驱动器、SSD 或 SD 卡。
- 确保 USB 驱动器已格式化为 EXT2/3/4 或 VFAT/FAT32。
- 您不能在闪存中的同一目录下具有两个名称相同但字母大小写不同的文件。例如，如果尝试将文件 Config.cfg 下载至包含 config.cfg 文件的位置，则会收到以下错误消息：

```
%Error opening disk0:/Config.cfg (File exists)
```

开始之前

- 对于多情景模式，您必须处于系统执行空间中。
- 要使用 ASA **copy** 命令与 SCP 服务器复制文件或从 SCP 服务器复制文件，必须执行以下操作：
  - （仅限 CiscoSSH 堆栈）使用 **ssh** 命令在 ASA 上为 SCP 服务器子网/主机启用 SSH 访问。
  - 使用 **crypto key generate** 命令生成密钥对（仅适用于物理 ASA）。

过程

使用以下服务器类型之一复制文件。

- 从 TFTP 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **tftp:**//*server*[/*path*]/*src_filename* **disk***n***:**/[*path*/]*dest_filename*

  示例：

```
ciscoasa# copy tftp://10.1.1.67/files/context1.cfg disk0:/context1.cfg

Address or name of remote host [10.1.1.67]?

Source filename [files/context1.cfg]?

Destination filename [context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- 从 FTP 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **ftp:**//[*user*[**:***password*]**@**]*server*[/*path*]/*src_filename* **disk***n***:**/[*path*/]*dest_filename*

示例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/context1.cfg
disk0:/contexts/context1.cfg

Address or name of remote host [10.1.1.67]?

Source username [jcrichton]?

Source password [aeryn]?

Source filename [files/context1.cfg]?

Destination filename [contexts/context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- 从 HTTP(S) 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* **disk***n***:/**[*path/*]*dest_filename*

  示例：

```
ciscoasa# copy https://asun:john@10.1.1.67/files/moya.cfg disk0:/contexts/moya.cfg

Address or name of remote host [10.1.1.67]?

Source username [asun]?

Source password [john]?

Source filename [files/moya.cfg]?

Destination filename [contexts/moya.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- 从 SMB 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* **disk***n***:/**[*path/*]*dest_filename*

  示例：

```
ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- 从 SCP 服务器进行复制：

  ;int=*interface* 选项会绕过路由查找，并始终使用指定接口来访问 SCP 服务器。

copy [**/noconfirm**] [*interface_name*]
scp://[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] **disk***n***:/**[*path/*]*dest_filename*

示例：

```
ciscoasa# copy scp://pilot@10.86.94.170/test.cfg disk0:/test.cfg

Address or name of remote host [10.86.94.170]?

Source username [pilot]?

Destination filename [test.cfg]?

The authenticity of host '10.86.94.170 (10.86.94.170)' can't be established.
RSA key fingerprint is
<65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19>(SHA256).
Are you sure you want to continue connecting (yes/no)? yes

Please use the following commands to add the hash key to the configuration:
  ssh pubkey-chain
    server 10.86.94.170
      key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19


Password: <type in password>
!!!!!!
6006 bytes copied in 8.160 secs (750 bytes/sec)
```

- 从 USB 或内部或外部驱动器复制：

  copy [**/noconfirm**] **disk***n***:/**[*path*]*/src_filename* **disk***n***:/**[*path/*]*dest_filename*

  示例：

```
ciscoasa# copy /noconfirm disk1:/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

将文件复制到启动配置或运行配置

您可以将文本文件从TFTP、FTP、SMB、HTTP(S)或SCP服务器或者从闪存下载至运行配置或启动配置。

开始之前

将配置复制到运行配置时，会合并这两个配置。合并会将新配置中的所有新命令添加到运行配置中。如果配置相同，则不会发生任何更改。如果命令冲突或命令影响情景的运行，则合并的影响取决于命令。可能会发生错误，也可能出现意外结果。

（可选）指定ASA与服务器进行通信所使用的接口。如果不指定接口，ASA将查看仅管理路由表；如果没有匹配，则会查看数据路由表。

过程

要将文件复制到启动配置或运行配置，请针对相应的下载服务器，输入以下命令之一：

- 从 TFTP 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **tftp://***server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  示例：

  ```
  ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config
  ```

- 从 FTP 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  示例：

  ```
  ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/old-startup.cfg startup-config
  ```

- 从 HTTP(S) 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* {**startup-config** | **running-config**}

  示例：

  ```
  ciscoasa# copy https://asun:john@10.1.1.67/files/new-running.cfg running-config
  ```

- 从 SMB 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  示例：

  ```
  ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/new-running.cfg running-config
  ```

- 从 SCP 服务器进行复制：

  copy [**/noconfirm**] [*interface_name*] **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] {**startup-config** | **running-config**}

  示例：

```
ciscoasa# copy scp://pilot:moya@10.86.94.170/new-startup.cfg startup-config
```

;Int=interface*interface* 选项 会绕过路由查询并始终使用指定的接口 到达 SCP 服务器。

示例

例如，要从 TFTP 服务器复制配置，请输入以下命令：

```
ciscoasa# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

要从 FTP 服务器复制配置，请输入以下命令：

```
ciscoasa# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

要从 HTTP 服务器复制配置，请输入以下命令：

```
ciscoasa# copy http://209.165.200.228/configs/startup.cfg startup-config
```

设置 ASA 映像、ASDM 和启动配置

如果您有多个 ASA 或 ASDM 映像，则应指定要启动的映像。如果不设置映像，则会使用默认启动映像，并且该映像可能不是计划使用的映像。对于启动配置，您可以选择在可见文件系统中指定文件，而不是隐藏目录。

请参阅以下模型准则：

- Firepower 4100/9300 机箱 - ASA 升级由 FXOS 管理；您无法在 ASA 操作系统中升级 ASA，因此不要对 ASA 映像使用此过程。您可以单独升级 ASA 和 FXOS，并且它们是单独列在 FXOS 目录列表中。ASA 包始终包括 ASDM。
- 设备模式下的 Firepower 1000、Cisco Secure Firewall 1200/3100/4200 - ASA、ASDM 和 FXOS 映像被捆绑成一个单个的包。ASA 使用此过程进行管理软件包更新。虽然这些平台使用 ASA 来识别要引导的映像，但基础机制与传统 ASA 不同。有关详细信息，请参阅下面的命令说明。
- 模型的 ASDM - ASDM 可以从 ASA 操作系统内部升级，因此您无需只使用捆绑的 ASDM 映像。对于 Firepower 4100/9300， 手动上传的 ASDM 映像不会出现在 FXOS 映像列表中；您必须从 ASA 管理 ASDM 映像。

注释 升级 ASA 捆绑包时，捆绑包中的 ASDM 映像将替换 ASA 上以前的 ASDM 捆绑包映像，因为它们具有相同的名称 (**asdm.bin**)。但是，如果您手动选择了您上传的其他 ASDM 映像（例如，**asdm-782.bin**），那么即使捆绑包升级之后，您仍可继续使用该映像。为了确保您运行的是兼容版本的 ASDM，您应该在升级捆绑包之前先升级 ASDM，或者应该在升级 ASA 捆绑包之前，或将 ASA 重新配置为使用捆绑的 ASDM 映像 (**asdm.bin**)。

- ASA Virtual - ASA virtual 包的初始部署会将 ASA 映像放在只读的 boot:/ 分区中。升级 ASA virtual 时，可以在闪存中指定不同的映像。请注意，如果您随后清除配置 (**clear configure all**)，则 ASA virtual 将还原为加载原始部署映像。初始部署 ASA virtual 包还包括它在闪存中放置的 ASDM 映像。您可以单独升级 ASDM 映像。
- **disk0:** 是内部存储器。其他驱动器编号表示外部存储，例如 USB 驱动器、SSD 或 SD 卡。

请参阅以下默认设置：

- ASA 映像：
  - 设备模式下的 Firepower 1000,Cisco Secure Firewall 1200/3100/4200 - 启动先前运行的启动映像。
  - ISA 3000 - 启动 ASA 在内部闪存中找到的第一个应用映像。
  - ASA Virtual - 启动您在首次部署时创建的只读 boot:/ 分区中的映像。
  - Firepower 4100/9300 机箱— FXOS 系统确定要引导的 ASA 映像。不能使用此过程来设置 ASA 映像。
- 所有 ASA 上的 ASDM 映像 - 启动 ASA 在内部闪存中找到的第一个 ASDM 映像，或者，如果此位置不存在映像，则在外部闪存中查找。
- 启动配置 - 默认情况下，ASA 从隐藏文件形式的启动配置进行引导。

过程

步骤 1 设置 ASA 启动映像位置：

boot system *url*

示例：

```
ciscoasa(config)# boot system disk0:/images/asa921.bin
```

URL 可以是：

- **disk** *n*:/[*path*/]*filename*

- **tftp://**[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*

  并非所有型号都支持 TFTP 选项。

设备模式下的 Firepower 1000Cisco Secure Firewall 1200/3100/4200：您只能输入一个 **boot system** 命令。如果要升级到新映像，则必须输入 **no boot system** 以删除您设置的上一个映像。请注意，您的配置中不能有 **boot system** 命令；例如，如果您从 ROMMON 安装了映像，有新设备，或者手动删除了该命令。此 **boot system** 命令会在您输入时执行操作：系统验证并解压缩映像，并将其复制到引导位置（FXOS 管理的 disk0 上的内部位置）。重新加载 ASA 时，系统将加载新图像。如果在重新加载之前改变主意，可以输入 **no boot system** 命令从引导位置删除新映像，这样当前映像将继续运行。输入此命令后，您甚至可以从 ASA 闪存中删除原始映像文件，ASA 将从引导位置正确引导；但是，我们建议将要使用的任何映像保留在闪存中，因为 **boot system** 命令仅适用于闪存中的映像。与其他模型不同，启动配置中的此命令不会影响启动映像，并且实质上是有修饰的。最后加载的启动图像将始终在重新加载时运行。如果在输入此命令后未保存配置，则在重新加载时，旧命令将存在于您的配置中，即使新映像已启动。请务必保存配置，以便配置保持同步。您只能从思科下载站点使用原始文件名加载图像。如果更改文件名，将不会加载。您还可以通过加载威胁防御映像来重新映像到 威胁防御。在这种情况下，系统会提示您立即重新加载。

ASA virtual 和 ISA 3000：您可以输入最多四个 **boot system** 命令条目，以指定要按顺序从中引导的不同映像；ASA 将引导其成功找到的第一个映像。当输入 **boot system** 命令时，该命令会在列表的底部添加一个条目。要对启动条目重新排序，必须使用 **clear configure boot system** 命令删除所有条目，然后按所需顺序重新输入这些条目。只能配置一个 **boot system tftp** 命令，并且该命令必须是配置的第一个命令。

注释
如果 ASA 陷入不断启动的循环中，则可以将 ASA 重新引导至 ROMMON 模式下。有关 ROMMON 模式的详细信息，请参阅查看调试消息，第 1345 页。

示例：

```
asa(config)# boot system disk0:/cisco-asa-fp2k.9.13.2.SPA
The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.13.2 will do the following:
   - upgrade to the new platform version 2.7.2
   - upgrade to the CSP ASA version 9.13.2
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
asa(config)#
```

步骤 2 设置要启动的 ASDM 映像：

asdm image disk*n***:/**[*path*/]*filename*

示例：

```
ciscoasa(config)# asdm image disk0:/images/asdm721.bin
```

如果不指定要启动的映像，即使仅安装了一个映像，ASA 也会在运行配置中插入 **asdm image** 命令。为了避免自动更新（如已配置）发生问题，以及避免在每次启动时都搜索映像，您应在启动配置中指定要启动的 ASDM 映像。

步骤 3 （可选）将启动配置设置为一个已知文件，而不是默认的隐藏文件。

boot config disk*n:/*[*path*/]*filename*

当您使用不适合隐藏目录的大型配置时，此功能非常重要。如果保存大型配置并看到以下错误消息，请务必使用此命令将配置保存到新文件：

%错误写入。nvram:/startup-config（设备上没有剩余空间）

示例：

```
ciscoasa(config)# boot config disk0:/configs/startup1.cfg
```

备份和恢复配置或其他文件

我们建议您对配置和其他系统文件进行定期备份以防止系统故障。

执行全面系统备份或还原

以下程序介绍如何将配置和映像备份至 tar.gz 文件并将该文件传输到本地计算机。

开始备份或恢复之前

- 在您启动备份或恢复之前，您在备份或恢复位置应至少有 300 MB 的可用磁盘空间。
- 如果您在备份期间或之后进行任何配置更改，则这些更改将不会包含在备份中。如果在进行备份后更改配置，然后执行恢复后的，则会覆盖此配置更改。因此，ASA 的行为可能会有所不同。
- 一次只能启动一个备份或恢复。
- 只能将配置恢复为与执行原始备份时相同的 ASA 版本。无法使用恢复工具将配置从一个 ASA 版本迁移到另一个版本。如果需要迁移配置，ASA 会在加载新 ASA OS 时自动升级驻留的启动配置。
- 如果使用集群，则只能备份或恢复启动配置、运行配置和身份证书。必须为每台设备单独创建和恢复备份。
- 如果使用故障转移，则必须为主用设备和备用设备单独创建和恢复备份。

- 如果您针对ASA设置主密码，则需要该主密码短语来恢复您使用此程序创建的备份配置。如果您不知道ASA的主密码，请参阅配置主密码，第824页，以了解在继续备份之前如何重置该密码。
- 如果导入PKCS12数据（使用 **crypto ca trustpoint** 命令）并且信任点使用RSA密钥，则会为导入的密钥对分配与信任点相同的名称。由于此限制，如果在恢复ASDM配置后为信任点及其密钥对指定其他名称，则启动配置将与原始配置相同，但运行配置将包含其他密钥对名称。这意味着，如果对密钥对和信任点使用不同的名称，则无法恢复原始配置。要解决此问题，请确保对信任点及其密钥对使用同一名称。
- 无法使用CLI进行备份及使用ASDM进行恢复，反之亦然。
- 每个备份文件包含以下内容：
  - 运行配置
  - 启动配置
  - 所有安全映像

    思科安全桌面和主机扫描映像

    思科安全桌面和主机扫描设置

    Secure Client (SVC) 映像和配置文件

    Secure Client (SVC) 自定义和转换
  - 身份证书（包括绑定到身份证书的RSA密钥对；独立密钥除外）
  - VPN预共享密钥
  - SSL VPN配置
  - 应用配置文件自定义框架 (APCF)
  - 书签
  - 自定义
  - 动态访问策略 (DAP)
  - 插件
  - 连接配置文件的预填充脚本
  - 代理自动配置
  - 转换表
  - Web内容
  - 版本信息

备份系统

本程序介绍如何执行完整系统备份。

过程

步骤 1 备份系统：

backup [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

示例：

```
ciscoasa# backup location disk0:/sample-backup]
Backup location [disk0:/sample-backup]?
```

如果不指定 **interface** *name*，ASA 将查看仅管理路由表；如果没有匹配，则会查看数据路由表。

在系统执行空间中的多情景模式下，输入 **context** 关键字以备份指定的情景。每个情景必须单独备份；也就是说，针对每个文件重新输入 **backup** 命令。

在VPN证书和预共享密钥的备份期间，需要由**passphrase**关键字标识的密钥才可对证书进行编码。必须提供要用于编码和解码PKCS12格式的证书的密码。备份仅包含绑定到证书的RSA密钥对，不包括任何独立证书。

备份 **location** 可以是本地磁盘或远程 URL。如果不提供位置，则会使用以下默认名称：

- 单模式 - disk0:*hostname*.backup.*timestamp*.tar.gz
- 多模式 - disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz

步骤 2 按照提示操作：

示例：

```
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco.
You will be required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file
is used to restore to a device with a different master passphrase,
you will need to provide the current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
```

```
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

恢复备份

您可以指定要在您的本地计算机上从 zip 备份 tar.gz 文件恢复的配置和映像。

过程

步骤 1 从备份文件恢复系统。

restore [**/noconfirm**] [**context** *ctx-name*] [**passphrase** *value*] [**location** *path*]

示例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
```

当使用**context**关键字恢复多个情景时，必须单独恢复每个备份的情景文件；也就是说，为每个文件重新输入 **restore** 命令。

步骤 2 按照提示操作：

示例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?

Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version,
some configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption.
Master passphrase is required to restore running configuration,
startup configuration and VPN pre-shared keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
```

```
Backing up [SSL VPN Configurations: Customization] ⋯ Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] ⋯ Done!
Backing up [SSL VPN Configurations: Plug-in] ⋯ Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] ⋯ Done!
Backing up [SSL VPN Configurations: Proxy auto-config] ⋯ Done!
Backing up [SSL VPN Configurations: Translation table] ⋯ Done!
Backing up [SSL VPN Configurations: Web Content] ⋯ Done!
Backing up [Anyconnect(SVC) client images and profiles] ⋯ Done!
Backing up [Anyconnect(SVC) customizations and transforms] ⋯ Done!
Backing up [Cisco Secure Desktop and Host Scan images] ⋯ Done!
Backing up [UC-IME tickets] ⋯ Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to
this device, please note them for future reference.

ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside,
the IP is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside,
the IP is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations.
Do not overwrite configuration file if you want to preserve the old http-
and https-proxy configurations.

Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates.
The default is cisco. If the passphrase is not correct, certificates will not be restored.

No passphrase was provided for identity certificates.
Using the default value: cisco. If the passphrase is not correct,
certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

配置自动备份和恢复 (ISA 3000)

在 ISA 3000 上，每次使用保存配置时，都可以使用 **write memory**将自动备份配置到特定位置。

通过自动恢复，您可以轻松地使用在 SD 闪存卡上加载的完整配置来配置新设备。默认出厂配置中启用自动恢复。

配置自动备份 (ISA 3000)

在 ISA 3000 上，每次使用保存配置时，都可以使用 **write memory**将自动备份配置到特定位置。

开始之前

此功能在 ISA 3000 上不可用。

过程

步骤 1 设置备份包参数：

backup-package backup [**interface** *name*] **location** {**disk***n***:** | *url*} [**passphrase** *string*]

- **interface** *name* - 指定接口访问备份 URL（如果指定了设备外存储）。如果不指定接口名称，ASA 将查看仅管理路由表；如果没有匹配，则会查看数据路由表。
- **location** {**disk***n***:** | *url*} - 指定用于备份数据的存储介质。您可以指定 URL 或本地存储。disk0 是内部闪存驱动器；disk1 是 USB 1 上的可选 USB 记忆棒；disk2 是 USB 2 上的可选 USB 记忆棒。disk3 是 SD 存储卡。请注意，自动恢复的默认设置使用 disk3。
- **passphrase** *string* - 设置用于保护备份数据的密码。请注意，自动恢复的默认设置使用“cisco”作为密码。

默认情况下，这些设置也会与手动 **backup** 命令一起使用。请参阅 备份系统，第 1307 页。请注意，如果在启用自动备份或恢复时使用手动 **backup** 命令，则系统会保存指定名称的备份文件，以及自动备份和恢复使用的“auto-backup-asa.tgz”名称。

示例：

```
ciscoasa(config)# backup-package backup location disk3: passphrase cisco
```

步骤 2 启动自动模式进行备份和恢复：

backup-package backup auto

使用 **write memory** 时保存配置时，系统会自动将配置保存到备份位置以及启动配置。备份文件的名称为“auto-backup-asa.tgz”。要禁用自动备份，请使用此命令的 **no** 形式。

示例：

```
ciscoasa(config)# backup-package backup auto
```

配置自动恢复 (ISA 3000)

自动恢复模式可在没有任何用户干预的情况下恢复设备上的系统配置。例如，将包含已保存备份配置的 SD 存储卡插入新设备，然后打开设备电源。设备启动后会检查 SD 卡，以确定是否需要恢复系

统配置。（仅当备份文件具有不同设备的“指纹”时，才会启动恢复。在备份或恢复操作期间，备份文件的指纹会更新为与当前设备匹配。因此，如果设备已完成恢复，或者已创建自己的备份，则系统会跳过自动恢复。）如果指纹显示需要恢复，则设备会替换系统配置（startup-config、running-config、SSL VPN配置等；有关备份内容的详细信息，请参阅 备份系统，第 1307 页）。当设备完成启动时，系统会运行保存的配置。

自动恢复在默认出厂配置中启用，因此您可以轻松地使用加载到 SD 存储卡上的完整配置来配置新设备，而无需执行设备的任何预配置。

由于设备需要在启动过程中尽早决定是否需要恢复系统配置，因此它会检查 ROMMON 变量来确定设备是否处于自动恢复模式，并获取备份配置的位置。使用以下 ROMMON 变量：

- **RESTORE_MODE =** {**auto** |**manual**}

  默认为**自动**。

- **RESTORE_LOCATION =** {**disk0:** | **disk1:** | **disk2:** | **disk3:**}

  默认值为 **disk3:**。

- **RESTORE_PASSPHRASE** = 密钥

  默认值为 **cisco**。

要更改自动恢复设置，请完成以下程序。

开始之前

- 此功能在 ISA 3000 上不可用。
- 如果使用默认恢复设置，则需要安装 SD 存储卡（部件号 SD-IE-1GB =）。
- 如果需要恢复默认配置以确保启用自动恢复，请使用 **configure factory default** 命令。此命令仅在透明防火墙模式下可用，因此，如果您处于路由防火墙模式，请首先使用 **firewall transparent** 命令。

过程

步骤 1 设置恢复包参数。

backup-package restore location {**disk***n***:** | *url*} [**passphrase** *string*]

- **location disk***n***:** - 指定用于恢复数据的存储介质。disk0 是内部闪存驱动器；disk1 是 USB 1 上的可选 USB 记忆棒；disk2 是 USB 2 上的可选 USB 记忆棒。disk3 是 SD 存储卡。默认值为 disk3。
- **passphrase** *string* - 设置用于读取备份数据的密码。默认值为“cisco”。

默认情况下，这些设置也会与手动 **restore** 命令一起使用。请参阅 备份系统，第 1307 页。

示例：

```
ciscoasa(config)# backup-package restore location disk1: passphrase $upe3rnatural
```

步骤 2 启动或禁用自动模式进行恢复。

[**no**] **backup-package restore auto**

恢复的文件的名称为“auto-backup-asa.tgz”。

示例：

```
ciscoasa(config)# no backup-package restore auto
```

备份单模式配置或多模式系统配置

在单情景模式下，或是在多情景模式下的系统配置中，可以将启动配置或运行配置复制到外部服务器或本地闪存。

开始之前

（可选）指定ASA与服务器进行通信所使用的接口。如果不指定接口，ASA将查看仅管理路由表；如果没有匹配，则会查看数据路由表。

过程

使用以下服务器类型之一来备份配置：

- 复制到 TFTP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **tftp://***server*[*/path*]*/dst_filename*

  示例：

  ```
  ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg
  ```

- 复制到 FTP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  示例：

  ```
  ciscoasa# copy startup-config ftp://jcrichton:aeryn@10.1.1.67/files/new-startup.cfg
  ```

- 复制到 SMB 服务器：

copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

示例：

```
ciscoasa# copy /noconfirm running-config smb://chiana:dargo@10.1.1.67/new-running.cfg
```

- 复制到 SCP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*[**;int=***interface_name*]

  示例：

```
ciscoasa# copy startup-config
scp://pilot:moya@10.86.94.170/new-startup.cfg
```

  ;Int=interface*interface* 选项 会绕过路由查询并始终使用指定的接口 到达 SCP 服务器。

- 复制到本地闪存：

  copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  示例：

```
ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg
```

  请确保目标目录存在。如果不存在，请先使用 **mkdir** 命令创建该目录。

备份闪存中的情景配置或其他文件

通过在系统执行空间中输入以下命令之一来复制本地闪存中的情景配置或其他文件。

开始之前

（可选）指定ASA与服务器进行通信所使用的接口。如果不指定接口，ASA将查看仅管理路由表；如果没有匹配，则会查看数据路由表。

过程

使用以下服务器类型之一备份情景配置：

- 从闪存复制到 TFTP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **tftp://***server*[*/path*]*/dst_filename*

  示例：

```
ciscoasa# copy disk0:/asa-os.bin tftp://10.1.1.67/files/asa-os.bin
```

- 从闪存复制到 FTP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  ftp://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  示例：

  ```
  ciscoasa# copy disk0:/asa-os.bin ftp://jcrichton:aeryn@10.1.1.67/files/asa-os.bin
  ```

- 从闪存复制到 SMB 服务器：

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  smb://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  示例：

  ```
  ciscoasa# copy /noconfirm copy disk0:/asdm.bin
  smb://chiana:dargo@10.1.1.67/asdm.bin
  ```

- 从闪存复制到 SCP 服务器：

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  scp://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*[**;int=***interface_name*]

  示例：

  ```
  ciscoasa# copy disk0:/context1.cfg
  scp://pilot:moya@10.86.94.170/context1.cfg
  ```

  ;Int=interface*interface* 选项 会绕过路由查询并始终使用指定的接口 到达 SCP 服务器。

- 从闪存复制到本地闪存：

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  示例：

  ```
  ciscoasa# copy /noconfirm disk1:/file1.cfg disk0:/file1.cfgnew-running.cfg
  ```

  请确保目标目录存在。如果不存在，请先使用 **mkdir** 命令创建该目录。

在情景中备份情景配置

在多情景模式下，您可以从情景中执行以下备份操作：

过程

步骤 1 将运行配置复制到已连接至情景网络的启动配置服务器：

```
ciscoasa/contexta# copy running-config startup-config
```

步骤 2 将运行配置复制到已连接至情景网络的 TFTP 服务器：

```
ciscoasa/contexta# copy running-config tftp:/server[/path]/filename
```

从终端显示复制配置

过程

步骤 1 将配置列显到终端：

more system:running-config

步骤 2 请复制此命令的输出，然后将配置粘贴到文本文件。

使用 Export 和 Import 命令备份附加文件

对您的配置至关重要的其他文件可能包括以下文件：

- 您使用 **import webvpn** 命令导入的文件。目前，这些文件包括自定义、URL 列表、网络内容、插件和语言转换文件。
- DAP 策略 (dap.xml)。
- CSD 配置 (data.xml)。
- 数字密钥和证书。
- 本地 CA 用户数据库和证书状态文件。

通过 CLI 可以使用 **export** 和 **import** 命令备份和恢复配置的各个元素。

要备份这些文件，比如您使用 **import webvpn** 命令或证书导入的文件，请执行以下步骤。

过程

步骤 1 运行适用的 **show** 命令，如下所示：

```
ciscoasa # show import webvpn plug-in
ica
rdp
ssh, telnet
vnc
```

步骤 2 对于要备份的文件，请运行 **export** 命令（在本示例中为 rdp 文件）：

```
ciscoasa # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

使用脚本备份和恢复文件

您可以使用脚本来备份和恢复 ASA 上的配置文件，包括通过 **import webvpn** CLI 命令导入的所有扩展文件、CSD 配置 XML 文件和 DAP 配置 XML 文件。出于安全原因，我们不建议对数字密钥和证书或者本地 CA 密钥执行自动备份。

本部分对此操作提供说明，并包含您可以按原样使用或根据环境要求修改后使用的样本脚本。此样本脚本特定于 Linux 系统。要将其用于 Microsoft Windows 系统，需要运用此样本的逻辑对其进行修改。

注释 或者，可以使用 **backup** 和 **restore** 命令。有关详细信息，请参阅执行全面系统备份或还原，第 1305 页。

在开始使用备份和恢复脚本之前

要使用脚本来备份和恢复 ASA 配置，请先执行以下任务：

- 使用 Expect 模块安装 Perl。
- 安装可以访问 ASA 的 SSH 客户端。
- 安装 TFTP 服务器，以将文件从 ASA 发送到备份站点。

另一个选项是使用商用工具。您可以将此脚本的逻辑运用于此类工具。

运行脚本

要运行备份和恢复脚本，请执行以下步骤：

过程

步骤 1 将脚本文件下载或剪切并粘贴到系统上的任意位置。

步骤 2 在命令行中，输入 **Perl***scriptname*，其中 *scriptname* 是脚本文件的名称。

步骤 3 按 **Enter** 键。

步骤 4 系统会提示您输入每个选项的值。或者，可以在输入 **Perl***scriptname* 命令时，按 **Enter** 键之前输入选项的值。无论采用哪种方式，脚本都要求输入每个选项的值。

步骤 5 脚本会开始运行，显示其发出的命令，这可以为您提供 CLI 记录。您可以在日后恢复时使用这些 CLI，这在您希望仅恢复一两个文件时特别有用。

样本脚本

```
#!/usr/bin/perl
#Description: The objective of this script is to show how to back up
configurations/extensions.
# It currently backs up the running configuration, all extensions imported via "import
webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
#       -h: ASA hostname or IP address
#       -u: User name to log in via SSH
#       -w: Password to log in via SSH
#       -e: The Enable password on the security appliance
#       -p: Global configuration mode prompt
#       -s: Host name or IP address of the TFTP server to store the configurations
#       -r: Restore with an argument that specifies the file name. This file is produced
during backup.
#If you don't enter an option, the script will prompt for it prior to backup.
#
#Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

#global variables
%options=();
$restore = 0; #does backup by default
$restore_file = '';
$asa = '';
$storage = '';
$user = '';
$password = '';
$enable = '';
$prompt = '';
$date = `date +%F`;
chop($date);
my $exp = new Expect();

getopts("h:u:p:w:e:s:r:",\%options);
do process_options();

do login($exp);
do enable($exp);
```

```
if ($restore) {
   do restore($exp,$restore_file);
}
else {
   $restore_file = "$prompt-restore-$date.cli";
   open(OUT,">$restore_file") or die "Can't open $restore_file\n";
   do running_config($exp);
   do lang_trans($exp);
   do customization($exp);
   do plugin($exp);
   do url_list($exp);
   do webcontent($exp);
   do dap($exp);
   do csd($exp);
   close(OUT);
}
do finish($exp);

sub enable {
   $obj = shift;
   $obj->send("enable\n");
   unless ($obj->expect(15, 'Password:')) {
      print "timed out waiting for Password:\n";
   }
   $obj->send("$enable\n");
   unless ($obj->expect(15, "$prompt#")) {
      print "timed out waiting for $prompt#\n";
   }
}

sub lang_trans {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn translation-table\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /Translation Tables/;
     next unless (/^.+\s+.+$/);
     ($lang, $transtable) = split(/\s+/,$_);
     $cli = "export webvpn translation-table $transtable language $lang
$storage/$prompt-$date-$transtable-$lang.po";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub running_config {
  $obj = shift;
  $obj->clear_accum();
  $cli ="copy /noconfirm running-config $storage/$prompt-$date.cfg";
  print "$cli\n";
  $obj->send("$cli\n");
  $obj->expect(15, "$prompt#" );
}
```

```
sub customization {
  $obj = shift;
  $obj->clear_accum();
  $obj->send("show import webvpn customization\n");
  $obj->expect(15, "$prompt#" );
  $output = $obj->before();
  @items = split(/\n+/, $output);

  for (@items) {
    chop;
    next if /^Template/ or /show import/ or /^\s*$/;
    $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
  }
}

sub plugin {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn plug-in\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/;
     $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub url_list {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn url-list\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/ or /No bookmarks/;
     $cli="export webvpn url-list $_ $storage/$prompt-$date-urllist-$_.xml";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}
```

```
sub dap {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir dap.xml\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub csd {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir sdesktop\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub webcontent {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn webcontent\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /No custom/;
     next unless (/^.+\s+.+$/);
     ($url, $type) = split(/\s+/,$_);
     $turl = $url;
     $turl =~ s/\/\+//;
     $turl =~ s/\+\//-/;
     $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub login {
    $obj = shift;
    $obj->raw_pty(1);
```

```
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user\@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:" )) {
        die "timeout waiting for password:\n";
    }

    $obj->send("$password\n");

    unless ($obj->expect(15, "$prompt>" )) {
        die "timeout waiting for $prompt>\n";
    }
}

sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";

}

sub restore {
   $obj = shift;
   my $file = shift;
   my $output;
   open(IN,"$file") or die "can't open $file\n";
   while (<IN>) {
      $obj->send("$_");
      $obj->expect(15, "$prompt#" );
      $output = $obj->before();
      print "$output\n";
   }
   close(IN);
}

sub process_options {
  if (defined($options{s})) {
      $tstr= $options{s};
      $storage = "tftp://$tstr";
  }
  else {
      print "Enter TFTP host name or IP address:";
      chop($tstr=<>);
      $storage = "tftp://$tstr";
  }
  if (defined($options{h})) {
      $asa = $options{h};
  }
  else {
      print "Enter ASA host name or IP address:";
      chop($asa=<>);
  }

  if (defined ($options{u})) {
      $user= $options{u};
  }
  else {
      print "Enter user name:";
      chop($user=<>);
  }

  if (defined ($options{w})) {
      $password= $options{w};
  }
  else {
```

```
        print "Enter password:";
        chop($password=<>);
    }
    if (defined ($options{p})) {
        $prompt= $options{p};
    }
    else {
        print "Enter ASA prompt:";
        chop($prompt=<>);
    }
    if (defined ($options{e})) {
        $enable = $options{e};
    }
    else {
        print "Enter enable password:";
        chop($enable=<>);
    }

    if (defined ($options{r})) {
       $restore = 1;
       $restore_file = $options{r};
    }
}
```

Cisco Secure Firewall 3100/4200上的热插拔 SSD

如果您有两个SSD，它们会在您启动时形成RAID。防火墙启动时，您可以在CLI上执行以下任务：

- 热插拔其中一个 SSD - 如果 SSD 出现故障，您可以更换它。请注意，如果您只有一个 SSD，则无法在防火墙开启时将其删除。
- 删除一个 SSD - 如果您有两个 SSD，可以删除一个。
- 添加第二个 SSD - 如果您有一个 SSD，可以添加第二个 SSD 并形成 RAID。

⚠

注意 请勿在未使用此程序从 RAID 中移除 SSD 的情况下将其移除。可能会导致数据丢失。

过程

步骤 1 删除其中一个 SSD。

a) 从 RAID 中删除 SSD。

raid remove-secure local-disk {**1** | **2**}

remove-secure 关键字将从 RAID 中删除 SSD，禁用自加密磁盘功能，并对 SSD 执行安全擦除。如果您只想从 RAID 中删除 SSD 并保持数据不变，可以使用 **remove** 关键字。

示例：

```
ciscoasa(config)# raid remove-secure local-disk 2
```

b) 监控 RAID 状态，直到 SSD 不再显示在清单中。

show raid

从 RAID 中删除 SSD 后， **可操作性** 和 **驱动器状态** 将显示为 **降级**。第二个驱动器将不再列为成员磁盘。

示例：

```
ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
```

```
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) 从机箱中取出 SSD。

步骤 2 添加 SSD。

a) 将 SSD 物理添加到空插槽。

b) 将 SSD 添加到 RAID。

raid add local-disk {**1** | **2**}

将新 SSD 同步到 RAID 可能需要几个小时，在此期间防火墙完全正常运行。您甚至可以重新启动，同步将在启动后继续。使用 **show raid** 命令显示状态。

如果您安装的 SSD 以前在另一个系统上使用过，并且仍处于锁定状态，请输入以下命令：

raid add local-disk {**1** | **2**} *psid*

Psid 印在 SSD 背面的标签上。或者，您可以重新启动系统，SSD 将被重新格式化并添加到 RAID。

禁用 USB 端口

默认情况下，type-A USB 端口已启用。出于安全考虑，您可能希望禁用 USB 端口访问。以下型号支持禁用 USB：

- Firepower 1000 系列
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

准则

- 启用或禁用 USB 端口需要 重新加载。
- 如果 USB 端口被禁用，并且您降级到不支持此功能的版本，则端口将保持禁用状态，并且在不清除 NVRAM 的情况下无法重新启用端口（FXOS local-mgmt **erase secure all** 命令）。
- 如果执行 ROMMON **factory-reset** 或 FXOS local-mgmt **erase secure**，USB 端口将重新启用。
- 对于高可用性或集群，请禁用或启用主用设备或控制节点上的 USB 端口。命令将复制到其他节点。但是，您需要重新加载每台设备才能使更改生效。

注释 此功能不会影响 USB 控制台端口（如果有）。

过程

步骤 1 禁用 USB 端口。

usb-port disable

write memory

reload

要重新启用 USB 端口，请输入 **no usb-port disable**。

示例：

```
ciscoasa(config)# usb-port disable
Requesting USB disable. This may take 30 seconds to complete.
Please execute 'write memory' and reboot the system to apply
any operational state changes.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 19d02ee0 671dbe24 88193adb bccb8147

12382 bytes copied in 0.530 secs
[OK]

ciscoasa(config)# reload
Proceed with reload? [confirm]
```

步骤 2 查看端口状态。

show usb-port

管理状态显示 USB 端口配置。运行状态显示当前操作。例如，如果禁用 USB 端口但不重新加载，则管理状态将显示为禁用，而运行状态将显示为启用。

示例：

```
ciscoasa(config)# show usb-port
USB Port info
---------------
Admin State: disabled
Oper State: disabled
```

软件和配置的历史记录

功能名称	平台版本	功能信息
安全复制客户端和服务器	9.1(5)/9.2(1)	ASA 现在支持安全复制 (SCP) 客户端和服务器，从而与 SCP 服务器进行双向文件传输。 引入了以下命令：**ssh pubkey-chain**、**server (ssh pubkey-chain)**、**key-string**、**key-hash** 和 **ssh stricthostkeycheck**。 修改了以下命令：**copy scp**。
可配置 SSH 加密和完整性密码	9.1(7)9.4(3)9.5(3)9.6(1)	用户可在执行 SSH 加密管理时选择密码模式，并可配置 HMAC 和加密来改变密钥交换算法。根据您的应用，您可能希望将密码变得更加严格或更不严格。请注意，安全复制的性能部分取决于所使用的加密密码。默认情况下，ASA 会按顺序协商以下其中一种算法：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr。如果选择建议的第一种算法 (3des-cbc)，则性能会远远慢于 128-cbc 等更高效的算法。例如，要更改所需的密码，请使用 **ssh cipher encryption custom aes128-cbc**。 引入了以下命令：**ssh cipher encryption**、**ssh cipher integrity**
默认情况下会启用自动更新服务器证书验证	9.2(1)	现在，默认情况下会启用自动更新服务器证书验证；对于新的配置，必须明确禁用证书验证。如果您是从较早版本升级且未启用证书验证，则不会启用证书验证，并会显示以下警告： `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` 配置将被迁移，以明确不配置 验证。 **auto-update server no-verification** 修改了以下命令：**auto-update server** {**verify-certificate** | **no-verification**}。
使用 CLI 的系统备份和恢复	9.3(2)	您现在可以使用 CLI 来备份和恢复完整系统配置，包括映像和证书。 引入了以下命令：**backup** 和 **restore**。

功能名称	平台版本	功能信息
恢复和加载新的 ASA 5506W-X 映像	9.4(1)	我们现在支持恢复和加载新的 ASA 5506W-X 映像。 引入了以下命令：**hw-module module wlan recover image**。
ISA 3000 的自动备份和自动恢复	9.7(1)	可以使用 pre-set parameters in the backup 和 restore 命令中的预设参数来启用自动备份和/或自动恢复功能。这些功能的使用情形包括从外部介质的初始配置；设备更换；回滚到某一可操作状态。 引入了以下命令：**backup-package location**、**backup-package auto**、**show backup-package status**、**show backup-package summary**
思科 SSH 堆栈在使用 SCP 客户端时需要 SSH 访问权限	9.17(1)	如果使用 CiscoSSH 堆栈，要使用 ASA **copy** 命令将文件复制到 SCP 服务器或从 SCP 服务器复制文件，必须使用 **ssh** 命令在 SCP 服务器子网/主机上启用 ASA 访问。
Cisco Secure Firewall 3100 上的 SSD 支持 RAID	9.17(1)	SSD 是自加密驱动器 (SED)，如果您有 2 个 SSD，它们会形成软件 RAID。 新增/修改的命令：**raid, show raid, show ssd**
禁用 USB 端口	9.22(1)	默认情况下，type-A USB 端口已启用并且无法禁用。现在，您可以在以下机型上出于安全目的禁用 USB 端口访问： • Firepower 1000 • Cisco Secure Firewall 1200 • Cisco Secure Firewall 3100 • Cisco Secure Firewall 4200 此设置存储在固件中，并且需要重新加载。此外，如果 USB 端口被禁用，并且您降级到不支持此功能的版本，则端口将保持禁用状态，并且在不清除 NVRAM 的情况下无法重新启用端口。 **注释** 此功能不会影响 USB 控制台端口（如果有）。 新增/修改的命令：**usb-port disable**、**show usb-port**

第 44 章

系统事件的响应自动化

本章介绍如何配置嵌入式事件管理器 (EEM)。

- 关于 EEM， 第 1329 页
- EEM 准则， 第 1330 页
- 配置 EEM， 第 1331 页
- EEM 示例， 第 1338 页
- 监控 EEM， 第 1339 页
- EEM 的历史记录， 第 1340 页

关于 EEM

EEM 服务使您可以调试问题并提供用于故障排除的通用日志记录。这项服务由两个部分组成：EEM 响应或侦听的事件，以及定义操作和 EEM 所响应事件的事件管理器小程序。您可以配置多个事件管理器小程序来响应不同的事件和执行不同的操作。

支持的事件

EEM 支持以下事件：

- 系统日志 - ASA 使用系统日志消息 ID 标识触发事件管理器小程序的系统日志消息。您可以配置多个系统日志事件，但系统日志消息 ID 可能不会在一个事件管理器小程序内重叠。
- 计时器 - 可以使用计时器触发事件。对于每个事件管理器小程序，每个计时器只能配置一次。每个事件管理器小程序最多可以有三个计时器。计时器的三种类型如下：
  - 看门狗（定期）计时器在小程序操作完成后的指定时间段后触发事件管理器小程序，并会自动重新启动。
  - 倒数（一次性）计时器在指定时间段后立即触发事件管理器小程序，且通常不会重新启动，除非删除并重新添加它们。
  - 绝对（一天一次）计时器促使事件在每天的指定时间发生一次，并会自动重新启动。时间格式为 hh:mm:ss。

对于上述类型的每个事件管理器小程序，只能配置一个计时器事件。

- 无 - 当您使用 CLI 或 ASDM 手动运行事件管理器小程序时，会触发 None 事件。
- 故障 - 当 ASA 出现故障时，触发故障事件。在某些情况下，会触发强制崩溃：

  如果 ASA 配置为在块耗尽时重新加载，并且 ASA 在配置的持续时间内保持内存不足，则它会发出系统日志并收集故障排除数据。ASA 强制崩溃并触发重新加载过程以释放内存块。在 HA 设置中，在这种情况下，会触发故障转移。在集群设置中，节点离开集群。

  不管 **output** 命令的值是什么， **action** 命令都会定向至 crashinfo 文件。输出会在 **show tech** 命令之前生成。

事件管理器小程序上的操作

当事件管理器小程序被触发时，会执行事件管理器小程序上的操作。每个操作都具有用于指定操作序列的编号。该序列号在事件管理器小程序中必须是唯一的。您可以为一个事件管理器小程序配置多个操作。命令是典型的 CLI 命令，例如 **show blocks**。

输出目标

您可以使用 **output** 命令将操作输出发送到指定的位置。一次只能启用一个输出值。默认值为 **output none**。此值会丢弃 **action** 命令的任何输出。命令在全局配置模式下作为权限级别为 15（最高）的用户来运行。此命令可能不接受任何输入，因为它处于禁用状态。您可以将 **action** CLI 命令的输出发送到以下三个位置之一：

- **None** - 这是默认位置，会丢弃输出
- **Console** - 此位置将输出发送到 ASA 控制台
- **File** - 此位置将输出发送到文件。以下四个文件选项可用：
  - **Create a unique file** - 每次调用事件管理器小程序时，此选项会创建具有唯一名称的新文件
  - **Create/overwrite a file** - 每次调用事件管理器小程序时，此选项会覆盖指定的文件。
  - **Create/append to a file** - 每次调用事件管理器小程序时，此选项会附加到指定的文件。如果指定的文件不存在，则会创建文件。
  - **Create a set of files** - 此选项会创建一组具有唯一名称的文件，每次调用事件管理器小程序时，都会轮换这些文件。

EEM 准则

本节介绍在配置 EEM 之前应检查的准则和限制。

情景模式准则

不支持多情景模式。

其他准则

- 在发生崩溃期间，ASA 的状态一般是未知的。在这种情况下运行某些命令可能不安全。
- 事件管理器小程序的名称不能包含空格。
- 不能修改 None 事件和 Crashinfo 事件参数。
- 因为系统日志消息会发送到 EEM 中进行处理，因此可能会影响性能。
- 每个事件管理器小程序的默认输出均为 **output none**。要更改此设置，必须输入其他输出值。
- 只能为每个事件管理器小程序定义一个输出选项。

配置 EEM

EEM 的配置由以下任务组成：

过程

步骤 1 创建事件管理器小应用程序并配置事件，第 1331 页。
步骤 2 配置操作和操作输出的目标，第 1333 页。
步骤 3 运行事件管理器小程序，第 1335 页。
步骤 4 跟踪内存分配和内存使用，第 1335 页。

创建事件管理器小应用程序并配置事件

要创建事件管理器小程序并配置事件，请执行以下步骤：

过程

步骤 1 创建事件管理器小程序并进入事件管理器小程序配置模式。

event manager applet 名称

示例：

```
ciscoasa(config)# event manager applet exampleapplet1
```

name 参数最多可包含 32 个字母数字字符。不允许使用空格。

要删除事件管理器小应用程序，请输入此命令的 **no** 形式。

步骤 2 描述事件管理器小程序。

description 文本

示例：

```
ciscoasa(config-applet)# description applet1example
```

text 参数最多可以包含 256 个字符如果用引号将说明文本引起来，说明文本可包含空格。

步骤 3 要配置指定事件，请输入以下命令之一。要删除已配置的事件，请输入相应命令的 **no** 形式。

- 要配置系统日志事件，请确定一条或一系列触发事件管理器小程序的系统日志消息。

  event syslog id *nnnnnn* [*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

  示例：

  ```
  ciscoasa(config-applet)# event syslog id 106201
  ```

  nnnnnn 参数标识系统日志消息 ID。**occurs** *n* 关键字-参数对指示系统日志消息必须发生多长时间，事件管理器小应用程序 才会被调用。默认情况为每 0 秒出现 1 次。有效值为 1 到 4294967295。**period** *seconds* 关键字-参数对指示事件必须发生的秒数， 并将事件管理器小应用程序 的调用频率限制为在配置的时间内最多调用一次。有效值为 0 到 604800。值 0 表示未定义时间段。

- 要将事件配置为在每个配置的时间段内发生一次并自动重新启动，请输入以下命令。

  event timer watchdog time 秒

  示例：

  ```
  ciscoasa(config-applet)# event timer watchdog time 30
  ```

  秒数的范围为 1 - 604800。

- 要将事件配置为发生一次且不会重新启动（除非删除然后重新添加事件），请输入以下命令。

  event timer countdown time 秒

  示例：

  ```
  ciscoasa(config-applet)# event timer countdown time 60
  ```

  秒数的范围为 1 - 604800。使用此命令的 **no** 形式会删除倒计时计时器事件。

  注释
  如果这是启动配置，当您重新启动时此计时器将会重新运行。

- 要将事件配置为在指定时间一天发生一次并自动重新启动，请输入以下命令。

  event timer absolute time 小时*:*分钟*:*秒

  示例：

  ```
  ciscoasa(config-applet)# event timer absolute time 10:30:20
  ```

  时间格式为 hh:mm:ss。事件范围为 00:00:00（午夜）至 23:59:59。

- ASA 出现崩溃时会触发崩溃事件。

  event crashinfo

  示例：

  ```
  ciscoasa(config-applet)# event crashinfo
  ```

  不管 **output** 命令的值是什么， **action** 命令都会定向至 crashinfo 文件。输出会在 **show tech** 命令之前生成。

配置操作和操作输出的目标

要配置操作和操作输出的特定发送目标，请执行以下步骤：

过程

步骤 1 在事件管理器小程序上配置操作。

action *n* **cli command** “*command*”

示例：

```
ciscoasa(config-applet)# action 1 cli command “show version”
```

n 选项是操作 ID。有效 ID 的范围为 0 到 4294967295。*command* 选项的值必须位于引号中；否则，如果命令由多个单词组成，则会发生错误。命令在全局配置模式下作为权限级别为 15（最高）的用户来运行。此命令可能不接受任何输入，因为它处于禁用状态。如果命令可用，请使用选项。**noconfirm**

步骤 2 选择一个可用的输出目标选项。使用相应命令的 **no** 形式可删除输出目标。

- **None** 选项会丢弃 **action** 命令的任何输出（这是默认设置）：

  output none

  示例：

```
ciscoasa(config-applet)# output none
```

- **Console** 选项将 **action** 命令的输出发送到控制台。

  output console

  示例：

  ```
  ciscoasa(config-applet)# output console
  ```

  注释
  运行此命令会影响性能。

- **New File** 选项为调用的每个事件管理器小程序将 **action** 命令的输出发送到新文件。

  output file new

  示例：

  ```
  ciscoasa(config-applet)# output file new
  ```

  文件名的格式为 eem-*applet-timestamp*.log，其中， *applet* 是事件管理器小程序的名称， *timestamp* 是注有日期的时间戳，其格式为 YYYYMMDD-hhmmss。

- **New Set of Rotated Files** 选项可创建一组会轮换的文件。当要写入新文件时，最旧的文件会被删除，且所有的后续文件都会在写入第一个文件之前进行重新编号。

  output file rotate *n*

  示例：

  ```
  ciscoasa(config-applet)# output file rotate 50
  ```

  最新的文件以 0 表示，最旧的文件 以最高编号 (*n*-1) 表示。*n* 选项是轮换值。有效值范围为 2 到 100。文件名格式为 eem-*applet-x*.log，其中，*applet* 是小程序的名称，*x* 是文件编号。

- **Single Overwritten File** 选项将 **action** 命令输出写入到一个文件中，每次写入都会覆盖原有文件。

  output file overwrite *filename*

  示例：

  ```
  ciscoasa(config-applet)# output file overwrite examplefile1
  ```

  filename 参数是本地（至 ASA）文件名。此命令也可以使用 FTP、TFTP 和 SMB 目标文件。

- **Single Appended File** 选项将 **action** 命令输出写入到一个文件中，每次写入时都会附加到原有文件。

  output file append *filename*

示例：

```
ciscoasa(config-applet)# output file append examplefile1
```

filename 参数是本地（对于 ASA 而言）文件名。

运行事件管理器小程序

要运行事件管理器小程序，请执行以下步骤：

过程

运行事件管理器小程序。

event manager run *applet*

示例：

```
ciscoasa# event manager run exampleapplet1
```

如果运行尚未配置 **event none** 命令的事件管理器小程序，将会发生错误。*applet* 参数是事件管理器小程序的名称。

跟踪内存分配和内存使用

要记录内存分配和内存使用情况，请执行以下步骤：

过程

步骤 1 启用内存日志记录。

memory logging [1024-4194304] [**wrap**] [**size** [1-2147483647]] [**process** *process-name*] [**context** *context-name*]

示例：

```
ciscoasa(config)# memory logging 202980
```

唯一必填参数是内存日志记录缓冲区中的条目数。**wrap** 选项用于通知内存日志记录实用程序在封装时保存缓冲区。缓冲区只能保存一次。

如果内存日志记录缓冲区 wrap 多次，会被覆写。当缓冲区 wrap 时，系统会将触发器发送到事件管理器，以启用数据保存。**size** 选项用于监控特定大小。**process** 选项用于监控特定流程。

注释
Checkheaps 进程被当作一个进程完全忽略，因为它以非标准方式使用内存分配器。

context 选项按给定名称为给定虚拟情景记录内存日志记录。

要更改内存日志记录参数，必须将其禁用，然后重新启用。

步骤 2 显示内存日志记录结果。

```
show memory logging [brief | wrap]
show memory logging include [address] [caller] [operator] [size] [process] [time] [context]
```

示例：

```
ciscoasa# show memory logging
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] time=[13:26:33.407] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542
0x000000000131911a 0x0000000000442bfd process=[ci/console] time=[13:26:33.407] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542
0x000000000182774d 0x000000000182cc8a process=[CMGR Server Process]
time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process]
time=[13:26:35.964] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000021246ef 0x0000000001827098
0x000000000182c08d 0x000000000182c262 process=[CMGR Server Process]
time=[13:26:37.964] oper=[free]
addr=0x00007fff224b9460 size=40 @ 0x00000000021246ef 0x000000000182711b
0x000000000182c08d 0x000000000182c262 process=[CMGR Server Process]
time=[13:26:38.464] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542
0x000000000182774d 0x000000000182cc8a process=[CMGR Server Process]
time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process]
```

```
time=[13:26:38.464] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[ci/console] time=[13:26:38.557] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542
0x000000000131911a 0x0000000000442bfd process=[ci/console] time=[13:26:38.557] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b

ciscoasa# show memory logging include process operation size
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] oper=[malloc] size=72 process=[ci/console] oper=[free]
size=72 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR Server Process] oper=[malloc] size=512 process=[CMGR Server Process]
oper=[free] size=512 process=[CMGR Server Process] oper=[malloc] size=40
process=[CMGR Server Process] oper=[free] size=16 process=[CMGR Server Process]
oper=[free] size=40 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR Server Process] oper=[malloc] size=512 process=[CMGR Server Process]
oper=[free] size=512 process=[CMGR Server Process] oper=[malloc] size=40
process=[ci/console] oper=[malloc] size=72 process=[ci/console]
oper=[free] size=72 ciscoasa# show memory logging brief
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
```

无需任何选项，**show memory logging** 即可显示统计信息以及记录的操作。**brief** 选项仅显示统计信息。**wrap** 选项显示封装后的缓冲区，然后清除数据，以免出现重复数据或保存重复数据。**include** 选项仅包含输出中的指定字段。您可以按任意顺序指定字段，但它们始终以下列顺序显示：

1. Process
2. Time
3. Context（除非在单模式下）
4. Operation（free/malloc/等）
5. Address

6. Size
7. Callers

输出格式如下：

process=[XXX] time=[XXX] context=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

最多显示 4 个主叫方地址。操作类型列于示例所示的输出（...的数量）中。

步骤 3 响应内存日志记录包装事件。

event memory-logging-wrap

示例：

```
ciscoasa(config)# event manager applet memlog
ciscoasa(config)# event memory-logging-wrap
ciscoasa(config)# action 0 cli command "show memory logging wrap"
ciscoasa(config)# output file append disk0:/memlog.log
```

示例显示了记录所有内存分配的小程序。当为内存日志记录启用包装时，内存日志记录器向事件管理器发送事件以触发配置的小程序。

EEM 示例

以下示例显示这样的事件管理器小程序：每小时记录一次有关阻止泄露情况信息，并将输出写入到一组会轮换的日志文件中，从而保存一天的日志：

```
ciscoasa(config)# event manager applet blockcheck
ciscoasa(config-applet)# description “Log block usage”
ciscoasa(config-applet)# event timer watchdog time 3600
ciscoasa(config-applet)# output rotate 24
ciscoasa(config-applet)# action 1 cli command “show blocks old”
```

以下示例显示这样的事件管理器小程序：在每天凌晨 1 点重新启动 ASA，根据需要保存配置：

```
ciscoasa(config)# event manager applet dailyreboot
ciscoasa(config-applet)# description “Reboot every night”
ciscoasa(config-applet)# event timer absolute time 1:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command “reload save-config noconfirm”
```

以下示例显示在午夜与凌晨 3 点之间禁用给定接口的事件管理器小程序。

```
ciscoasa(config)# event manager applet disableintf
```

```
ciscoasa(config-applet)# description “Disable the interface at midnight”
ciscoasa(config-applet)# event timer absolute time 0:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command “interface GigabitEthernet 0/0”
ciscoasa(config-applet)# action 2 cli command “shutdown”
ciscoasa(config-applet)# action 3 cli command “write memory”

ciscoasa(config)# event manager applet enableintf
ciscoasa(config-applet)# description “Enable the interface at 3am”
ciscoasa(config-applet)# event timer absolute time 3:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command “interface GigabitEthernet 0/0”
ciscoasa(config-applet)# action 2 cli command “no shutdown”
ciscoasa(config-applet)# action 3 cli command “write memory”
```

监控 EEM

请参阅以下命令以监控 EEM：

- **clear configure event manager**

  此命令可删除事件管理器的运行配置。

- **clear configure event manager applet** *appletname*

  此命令可从配置中删除已命名的事件管理器小程序。

- **show counters protocol eem**

  此命令可显示事件管理器的计数器。

- **show event manager**

  此命令可显示有关已配置的事件管理器小程序的信息，包括命中次数和上一次调用事件管理器小程序的时间。

- **show memory logging**、**show memory logging include**

  这些命令可显示关于内存分配和内存使用情况的统计信息。

- **show running-config event manager**

  此命令可显示事件管理器的运行配置。

EEM 的历史记录

表 *58: EEM* 的历史记录

功能名称	平台版本	说明
嵌入式事件管理器 (EEM)	9.2(1)	EEM 服务使您可以调试问题并提供用于故障排除的通用日志记录。这项服务由两个部分组成：EEM 响应或侦听的事件，以及定义操作和 EEM 所响应事件的事件管理器小程序。您可以配置多个事件管理器小程序来响应不同的事件和执行不同的操作。 引入或修改了以下命令：**event manager applet**、**description**、**event syslog id**、**event none**、**event timer** {**watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss*}、**event crashinfo**、**action cli command**、**output** {**none** | **console** | **file** {**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*}}、**show running-config event manager**、**event manager run**、**show event manager**、**show counters protocol eem**、**clear configure event manager**、**debug event manager**、**debug menu eem**。
EEM 的内存跟踪	9.4(1)	添加了一项新的调试功能来记录内存分配和内存使用情况，以响应内存日志记录封装事件。 我们引入或修改了以下命令：**memory logging**、**show memory logging**、**show memory logging include** 和 **event memory-logging-wrap**。

第 45 章

测试和故障排除

本章介绍如何对 ASA 进行故障排除和测试基本连接。

- 恢复启用密码和 Telnet 密码，第 1341 页
- 查看调试消息，第 1345 页
- 数据包捕获，第 1345 页
- 查看崩溃转储，第 1351 页
- 查看核心转储，第 1351 页
- CPU 使用情况和报告，第 1351 页
- 测试配置，第 1356 页
- 监控连接，第 1368 页
- 测试和故障排除的历史记录，第 1368 页

恢复启用密码和 Telnet 密码

忘记启用密码或 Telnet 密码时，可在 ASA virtual 和 ISA 3000 模式下恢复这些密码。必须使用 CLI 执行该任务。

注释 您无法恢复在其他平台上丢失的密码。您只能恢复出厂默认配置，并将密码重置为默认值。如需了解 Firepower 4100/9300，请参阅《FXOS 配置指南》。对于其他模型，请参阅 FXOS 故障排除指南。

恢复 ISA 3000 上的密码

要恢复 ISA 3000 平台上的密码，请执行以下步骤：

过程

步骤 1 连接到 ASA 控制台端口。

步骤 2 关闭 ASA，然后重新启动。

步骤 3 启动后，当系统提示进入 ROMMON 模式时按下 **Escape** 键。

步骤 4 要更新配置寄存器值，请输入以下命令：

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

ASA 将显示当前的配置注册值以及配置选项列表。记录当前配置寄存器值，以便稍后恢复。

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ...... auto-boot index 1 image in disks
```

步骤 5 通过输入以下命令重新加载 ASA：

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASA 加载默认配置，而非启动配置。

步骤 6 通过输入以下命令访问特权 EXEC 模式：

```
ciscoasa# enable
```

步骤 7 系统提示输入密码时，请按 **Enter** 键。

密码为空。

步骤 8 通过输入以下命令加载启动配置：

```
ciscoasa# copy startup-config running-config
```

步骤 9 通过输入以下命令访问全局配置模式：

```
ciscoasa# configure terminal
```

步骤 10 通过输入以下命令，根据需要在默认配置中更改密码：

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
```

```
ciscoasa(config)# username name password password
```

步骤 11 通过输入以下命令加载默认配置：

```
ciscoasa(config)# no config-register
```

默认配置寄存器值为 0x1。有关配置寄存器的详细信息，请参阅命令参考。

步骤 12 通过输入以下命令，将新密码保存至启动配置：

```
ciscoasa(config)# copy running-config startup-config
```

恢复 ASA Virtual上的密码或映像

要恢复 ASA virtual 上的密码或映像，请执行以下步骤：

过程

步骤 1 将运行的配置复制到 ASA virtual 上的备份文件：

copy running-config *filename*

示例：

```
ciscoasa# copy running-config backup.cfg
```

步骤 2 重新启动 ASA virtual：

reload

步骤 3 从 GNU GRUB 菜单，按向下箭头，选择 <**filename**> **with no configuration load** 选项，然后按 **Enter** 键。文件名为 ASA virtual 上的默认启动映像文件名。默认启动映像永远不会通过 **fallback** 命令自动启动。然后加载选定的启动映像。

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

示例：

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

步骤 4 将备份配置文件复制到运行的配置。

copy *filename* **running-config**

示例：

```
ciscoasa (config)# copy backup.cfg running-config
```

步骤 5 重置密码。

enable password 密码

示例：

```
ciscoasa(config)# enable password cisco123
```

步骤 6 保存新配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

禁用 ISA 3000 硬件的密码恢复

注释 在 ASA virtual、 Cisco Secure Firewall 型号上无法禁用密码恢复。

要禁用密码恢复以确保非授权用户无法使用密码恢复机制来损害 ASA，请执行以下步骤。

开始之前

在 ASA 上，使用 **noservice password-recovery** 命令可防止您在配置完整无损的情况下进入 ROMMON 模式。当进入 ROMMON 模式时，ASA 会提示您擦除所有闪存文件系统。不先执行该擦除操作就无法进入 ROMMON 模式。如果您选择不擦除闪存文件系统，ASA 将重新加载。因为密码恢复取决于使用 ROMMON 模式并维护现有配置，所以该擦除可防止恢复密码。但是，禁用密码恢复可以防止未授权用户查看配置或插入不同的密码。在此情况下，要将系统恢复到操作状态，请加载新映像和备份配置文件（如可用）。

service password-recovery 命令显示在配置文件中，仅供参考。在 CLI 提示符处输入命令时，设置保存在 NVRAM 中。更改设置的唯一方法是在 CLI 提示符下输入命令。使用不同版本的命令加载新配置不会更改设置。如果在将 ASA 配置为启动时（准备密码恢复）忽略启动配置并禁用密码恢复，则 ASA 会更改设置以便照常加载启动配置。如果使用故障转移并将备用设备配置为忽略启动配置，则会对配置注册进行与 **no service password- recovery** 命令复制到备用设备时相同的更改。

过程

禁用密码恢复。

no service password-recovery

示例：

```
ciscoasa (config)# no service password-recovery
```

查看调试消息

由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科TAC进行故障排除会话过程中使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。要启用调试消息，请参阅命令参考中的 **debug** 命令。

数据包捕获

当对连接问题进行故障排除或监视可疑活动时，捕获数据包可能非常有用。如果要使用数据包捕获服务，我们建议您联系思科 TAC。

数据包捕获准则

情景模式

- 您可以配置某种情景内集群控制链路上的捕获；仅捕获与集群控制链路中发送的情景关联的数据包。
- 在多情景模式下，一个共享 VLAN 只能配置一个捕获，仅使用配置的最后一个捕获。
- 如果删除最后配置的（活动）捕获，则没有捕获会变成活动状态，即使您之前已在其他情景中配置捕获；您必须删除捕获并重新添加才能让它变成活动状态。
- 流入该捕获所关联的接口的所有流量都将被捕获，包括流向共享 VLAN 上的其他情景的流量。因此，如果您在情景 A 中为同时被情景 B 使用的 VLAN 启用捕获，则将同时捕获情景 A 和情景 B 的进口流量。
- 对于出口流量，将只捕获带活动捕获的情景的流量。唯一的例外是当您未启用ICMP检查时（因此 ICMP 流量在加速路径中没有会话）。在这种情况下，将捕获共享 VLAN 上所有情景的入口和出口 ICMP 流量。

其他准则

- 如果 ASA 收到的数据包带有格式不正确的 TCP 报头，并因 *invalid-tcp-hdr-length* ASP 丢弃原因而丢弃这些数据包，则接收这些数据包的接口上的**show capture** 命令输出不会显示这些数据包。
- 您只能捕获 IP 流量；不能捕获非 IP 数据包（如 ARP）。
- 对于内联 SGT 标记数据包，捕获的数据包包含您的 PCAP 查看器可能无法识别的其他 CMD 报头。
- 数据包捕获包括系统由于检测、NAT、TCP 规范化或其他调整数据包内容的功能而修改或注入到连接的数据包。
- 数据路径中注入的虚拟数据包的生命周期跟踪无法准确反映数据路径如何处理物理数据包。这种差异取决于注入的虚拟数据包的软件版本、配置和类型。以下配置设置可能导致差异：
  - 至少存在同一主机的 2 条 NAT 语句。
  - 连接的正向和反向流采用不同协议。例如，正向流采用 UDP 或 TCP，反向流采用 ICMP。
  - 正在启用 ICMP 错误检测。

捕获数据包

要捕获数据包，请执行以下步骤。

过程

步骤 1 启用数据包捕获功能以进行数据包嗅探和网络故障隔离。

capture *capture_name* [**type** {**asp-drop** [**all** | *drop-code*] | **tls-proxy** | **raw-data** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] {**interface** {*interface_name* | **asa_dataplane** | **asa_mgmt_plane** | **cplane**} } [**buffer** *buf_size*] [**ethernet-type** *type*] [**reeinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**file-size**] [**headers-only**] [**match** *protocol* {**host** *source-ip* | *source-ip mask* | **any** | **any4**|**any6**} [*operator src_port*] {**host** *dest_ip* |*dest_ip mask* | **any** | **any4**|**any6**} [*operator dest_port*]]

示例：

```
ciscoasa# capture captest interface inside
```

您必须为任何要捕获的数据包配置接口。在多个 **capture** 语句中使用同一个 *capture_name* 可捕获多种类型的流量。

type asp-drop 关键字可捕获加速安全路径丢弃的数据包。在集群中，还将捕获从一台设备转发到另一台设备时丢失的转发数据包。在多情景模式下，在系统执行空间中发出此选项时，将捕获所有丢弃的数据包；在某个情景中发出此选项时，将只捕获从属于该情景的接口中输入的丢弃数据包。

type raw-data 关键字可捕获入站和出站数据包。该设置为默认设置。

inline-tag *tag* 关键字参数对用于为特定 SGT 值指定标签，或保留不指定以捕获带任何 SGT 值的标记数据包。

buffer 关键字定义了用于存储数据包的缓冲区大小。字节缓冲区已满时，数据包捕获停止。用于集群中时，此值是指每台设备的大小，而不是所有设备的总和。**circular-buffer** 关键字可在缓冲区已满时从头开始覆盖缓冲区。

ethernet-type 关键字设置要捕获的以太网类型。支持的以太网类型包括 8021Q、ARP、IP、IP6、LACP、PPPOED、PPPOES、RARP 和 VLAN。802.1Q 或 VLAN 类型会出现异常。802.1Q 标记会被自动跳过，内部以太网类型用于匹配。IP 是默认以太网类型。

interface 关键字可设置要在其上使用数据包捕获的接口的名称。

要在数据层面捕获数据包，请使用 **asa_dataplane** 关键字。

要配置捕获文件的大小，请使用 **file-size** 关键字。文件大小可以介于 32 和 10000 MB 之间。

如果要仅捕获数据包的 L2、L3 和 L4 报头，但不捕获数据，请使用 **headers-only** 命令。

match 关键字通过匹配协议、源和目标 IP 地址以及可选端口进行捕获。此关键字最多可在一个命令中使用三次。**any** 关键字仅用于捕获 IPv4。您可以使用 **any4** 和 **any6** 关键字来分别捕获匹配的 IPv4 和 IPv6 网络流量。操作符可以是以下任意一项：

- lt - 小于
- gt - 大于
- eq - 等于

real-time 关键字可显示连续、实时捕获的数据包。

reinject-hide 关键字可指定不捕获任何重新注入的数据包，此关键字仅适用于集群分析环境。

注释
如果已配置 ACL 优化，则您无法在捕获中使用 **access-list** 命令。只能使用 **access-group** 命令。如果在此情况下尝试使用 **access-list** 命令，系统将显示错误。

步骤 2 捕获集群控制链路流量：

capture *capture_name* {**type lacp interface** *interface_id* [**buffer** *buf_size*] [**packet-length** *bytes*] [**circular-buffer**] [**real-time** [**dump**] [**detail**]]

capture *capture_name* **interface cluster** [**buffer** *buf_size*] [**cp-cluster**] [**ethernet-type** *type*] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**trace**] [**match** *protocol* {**host** *source-ip* | *source-ip mask* | **any** | **any4**|**any6**} [*operator src_port*] {**host** *dest_ip* |*dest_ip mask* | **any** | **any4**|**any6**} [*operator dest_port*]]

示例：

```
ciscoasa# capture ccl type lacp interface GigabitEthernet0/0
ciscoasa# capture ccl interface cluster match udp any eq 49495 any
ciscoasa# capture ccl interface cluster match udp any any eq 49495
```

您可以通过以下两种方式捕获集群控制链路流量：要捕获集群控制链路上的所有流量，请对接口名称使用 **cluster** 关键字。要仅捕获 cLACP 数据包，请指定 **type lacp**，并指定物理接口 ID 而不是接口

名称。集群控制链路上有两种类型的数据包：控制层面数据包和数据层面数据包，它们都包含转发的数据流量和集群 LU 消息。IP 地址报头中的 TTL 字段经过编码以区分这两种类型的数据包。捕获转发的数据包时，其集群尾部包含在捕获文件中以用于调试。

cp-cluster 关键字仅在集群控制链路上捕获控制平面数据包（无数据平面数据包）。此选项在多情景模式下的系统中很有用，在此模式下，您无法使用 ACL 来匹配流量。

步骤 3 捕获整个集群范围内的数据包：

cluster exec capture *capture_name* 参数

步骤 4 捕获交换机的出口流量数据包（仅在 Cisco Secure Firewall 4200 型号设备上支持）：

capture *capture_name* **switch interface** *interface_name* **direction egress**

注释
使用 **both** 参数为交换机同时创建出口和进口流量的捕获。

步骤 5 停止捕获数据包：

no capture *capture_name*

要终止实时捕获数据包，请输入 **Ctrl + c**。要永久删除捕获，请使用此命令的 **no** 形式。此实时选项仅适用于 **raw-data** 和 **asp-drop** 捕获。

步骤 6 要手动停止捕获数据包，不从缓冲区删除数据包，请执行以下操作：

capture 名称 **stop**

步骤 7 要再次开始捕获：

no capture 名称**stop**

步骤 8 捕获集群设备上的持久数据包跟踪：

cluster exec *capture_test* **persist**

步骤 9 清除持久数据包跟踪：

cluster exec *clear* **packet-trace**

步骤 10 捕获解密的 IPsec 数据包：

cluster exec *capture_test* **include-decrypted**

步骤 11 清除捕获：

clear capture *capture_name*

示例

控制平面数据包

进出控制平面的所有数据包的 TTL 为 255，且端口号 49495 用于集群控制平面侦听端口。以下示例展示如何为集群环境创建 LACP 捕获：

```
ciscoasa# capture lacp type lacp interface GigabitEthernet0/0
```

以下示例 显示如何为集群链路中的控制路径数据包 创建捕获：

```
ciscoasa# capture cp interface cluster match udp any eq 49495 any
ciscoasa# capture cp interface cluster match udp any any eq 49495
```

数据平面数据包

数据包包括从一台设备转发到另一台设备（其连接所有者）的数据包和集群LU消息。常规集群 LU 更新消息的 TTL 为 254，且存在 TTL 为 253 的特殊 LU 数据包。此特殊 LU 数据包仅适用于 TCP，而且它仅在导向器选择新的流所有者时发生；导向器会将请求数据包与 CLU_FULL 更新数据包一起发送回去。LU 数据包通过原始数据包的 L3/L4 报头填充，以避免接收器端出现潜在的竞争条件。转发的数据包的TTL小于4。以下示例显示如何为集群控制链路中的数据路径数据包创建捕获：要捕获所有集群间数据层面“流逻辑更新”消息，请使用端口 4193。

```
ciscoasa# access-list cc1 extended permit udp any any eq 4193
ciscoasa# access-list cc1 extended permit udp any eq 4193 any
ciscoasa# capture dp interface cluster access-list ccl
```

查看数据包捕获

您可以在 CLI 中、浏览器中查看数据包捕获，或将捕获下载至您选择的服务器。

过程

步骤 1 在 CLI 中查看捕获：

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

示例：

```
ciscoasa# show capture capin

 8 packets captured

 1: 03:24:35.526812       192.168.10.10 > 203.0.113.3: icmp: echo request
 2: 03:24:35.527224       203.0.113.3 > 192.168.10.10: icmp: echo reply
 3: 03:24:35.528247       192.168.10.10 > 203.0.113.3: icmp: echo request
 4: 03:24:35.528582       203.0.113.3 > 192.168.10.10: icmp: echo reply
 5: 03:24:35.529345       192.168.10.10 > 203.0.113.3: icmp: echo request
 6: 03:24:35.529681       203.0.113.3 > 192.168.10.10: icmp: echo reply
 7: 03:24:57.440162       192.168.10.10 > 203.0.113.3: icmp: echo request
 8: 03:24:57.440757       203.0.113.3 > 192.168.10.10: icmp: echo reply
```

access-list 关键字显示基于用于标识特定访问列表的 IP 或较高字段的数据包的信息。

cluster exec 关键字使您能够在一个设备中发出 **show capture** 命令，并同时在所有其他设备中运行该命令。

count 关键字显示指定数据的数据包的数量。

decode 关键字在 **isakmp** 类型的捕获应用于接口时非常有用。在解密后会捕获流过该接口的所有 ISAKMP 数据，并在解码字段后展示更多信息。数据包的解码输出取决于数据包的协议。通常，此命令支持 ICMP、UDP 和 TC P协议的 IP 解码。从版本 9.10(1) 开始，此命令还支持 GRE 和 IPinIP 的 IP 解码。

detail 关键字显示每个数据包的其他协议信息。

dump 关键字显示通过数据链路传输的数据包的十六进制转储。

packet-number 关键字以指定的数据包编号开始显示。

步骤 2 使用浏览器查看数据包捕获：

https://*ip_of_asa*/**admin/capture/***capture_name*/**pcap**

如果忽略 **pcap** 关键字，则仅提供等同于 **show capture** *capture_name* 命令输出的信息。

在多情景模式下，**copy capture** 命令仅在系统执行空间中可用。

步骤 3 将数据包捕获复制到服务器。此示例显示 FTP。

[**cluster exec**] **copy /pcap capture:**[*context-name*/]*capture_name* **ftp://***username***:***password***@***server_ip***/***path*

如果忽略 **pcap** 关键字，则仅提供等同于 **show capture** *capture_name* 命令输出的信息。

注释
将数据包捕获复制到磁盘时，请确保捕获文件名小于或等于63个字符。当文件名超过63个字符时，即使成功捕获数据包，但将捕获复制到磁盘时也会失败。

示例

以下示例显示 asp-drop 类型的捕获：

```
ciscoasa# capture asp-drop type asp-drop acl-drop
ciscoasa# show capture asp-drop

 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown

ciscoasa# show capture asp-drop

 2 packets captured
```

```
 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown
```

以下示例显示以太网类型的捕获：

```
ciscoasa# capture arp ethernet-type arp interface inside
ciscoasa# show cap arp

22 packets captured

   1: 05:32:52.119485       arp who-has 10.10.3.13 tell 10.10.3.12
   2: 05:32:52.481862       arp who-has 192.168.10.123 tell 192.168.100.100
   3: 05:32:52.481878       arp who-has 192.168.10.50 tell 192.168.100.10
   4: 05:32:53.409723       arp who-has 10.106.44.135 tell 10.106.44.244
   5: 05:32:53.772085       arp who-has 10.106.44.108 tell 10.106.44.248
   6: 05:32:54.782429       arp who-has 10.106.44.135 tell 10.106.44.244
   7: 05:32:54.784695       arp who-has 10.106.44.1 tell 11.11.11.112:
```

查看崩溃转储

如果 ASA 或 ASA virtual 崩溃，您可以查看崩溃转储信息。如果要解释崩溃转储，我们建议您联系思科 TAC。请参阅 命令参考中的 **show crashdump** 命令。

查看核心转储

核心转储是程序异常终止或崩溃时的运行程序快照。核心转储用于诊断或调试错误并保存崩溃以备将来进行非现场分析。思科 TAC 可能会要求您启用核心转储功能以对 ASA 或 ASA virtual上的应用或系统崩溃进行故障排除。请参阅 命令参考中的 **coredump** 命令。

CPU 使用情况和报告

“CPU 利用率”(CPU Utilization) 报告汇总了指定时间内使用的 CPU 百分比。通常，核心在非高峰时段运行大约 30% 至 40% 的总 CPU 容量，在高峰时段运行大约 60% 至 70% 的容量。

ASA Virtual 中的 vCPU 使用率

在 ASA virtual 上使用 **show cpu usage** 命令显示 CPU 利用率统计信息。ASA virtual vCPU 使用率显示了用于数据路径、控制点和外部进程的 vCPU 用量。

云服务提供商（例如 VMware、Azure、OCI 等）报告的 vCPU 使用情况包括所述的 ASA virtual 使用情况以及：

- ASA virtual 空闲时间
- 用于 ASA Virtual VM 的 %SYS 开销
- 在 vSwitch、vNIC 和 pNIC 之间移动数据包的开销。此开销可能会非常大。

CPU 使用率示例

在以下示例中，报告的 vCPU 使用率截然不同：

- ASA Virtual 报告：40%
- DP：35%
- 外部进程：5%
- vSphere 报告：95%
- ASA（如 ASA virtual 报告）：40%
- ASA 空闲轮询：10%
- 开销：45%

开销用于执行虚拟机监控程序功能，以及使用 vSwitch 在 NIC 与 vNIC 之间移动数据包。

由于 ESXi 服务器能够代表 ASA virtual 将其他计算资源用于开销，因此使用率可能会超过 100%。

VMware CPU 使用率报告

在 vSphere 中，点击“**虚拟机性能**”选项卡，然后点击“**高级**”以显示“**图表选项**”下拉列表，该列表将显示 VM 的每种状态的 vCPU 使用率（%USER、%IDLE、%SYS 等）。此信息有助于从 VMware 的角度了解使用 CPU 资源的位置。

在 ESXi 服务器外壳上（使用 SSH 访问外壳以连接主机），esxtop 是可用的。Esxtop 具有一个与 Linux **top** 命令类似的外观，为 vSphere 性能提供了 VM 状态信息，包括以下信息：

- vCPU、内存和网络使用率的详细信息
- 每个 VM 的每种状态的 vCPU 使用率
- 内存（运行时键入 M）和网络（运行时键入 N），以及统计信息和 RX 丢弃的数量

ASA Virtual 和 vCenter 图表

ASA virtual 与 vCenter 之间的 CPU 使用率 (%) 存在差异：

- vCenter 图表值始终大于 ASA virtual 值。
- vCenter 称之为 %CPU 使用率； ASA virtual 称之为 %CPU 利用率。

术语“%CPU 利用率”和“%CPU 使用率”表示不同的东西：

- CPU 利用率提供了物理 CPU 的统计信息。
- CPU 使用率提供了基于 CPU 超线程的逻辑 CPU 统计信息。但是，由于只使用一个 vCPU，因此超线程未打开。

vCenter 按如下方式计算 CPU 使用率 (%)：

当前使用的虚拟 CPU 的用量，以总可用 CPU 的百分比表示

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率

当比较以 MHz 为单位的使用率时，vCenter 和 ASA virtual 值是一致的。根据 vCenter 图，MHz % CPU 使用率的计算方式为：60/(2499 x 1 个 vCPU) = 2.4

Amazon CloudWatch CPU 使用情况报告

您可以查看指标资源管理器，以按标签和属性监控资源。执行以下步骤以查看特定实例的CPU利用率统计信息：

过程

步骤 1 打开 **CloudWatch** 控制台，然后在导航窗格中选择 **指标** 。

步骤 2 选择 **EC2** 指标命名空间，然后选择 **每实例指标** 维度。

步骤 3 在搜索字段中输入 **CPUUtilization** 并按 Enter 键。选择所需实例的行，以显示该实例的 **CPUUtilization** 指标图形。

有关更多信息，请参阅 Amazon CloudWatch 文档 。

ASA Virtual 和 Amazon CloudWatch Graphs

由于在 ASA virtual 和 CloudWatch 上计算 CPU 使用率的方式不同，因此 Amazon CloudWatch 图形数字高于数字。

ASA virtual 在轮询模式下运行时，每个 CPU 都会运行一个轻量级命令循环，而不是进入省电模式或任何其他空闲状态。通过保持每个核心始终处于活动状态，而不必打开/关闭或根据 Intel 电源状态调整其时钟，从而提高性能。

在 ASA virtual 内部，此活动被理解为空闲行为，并且 CPU 使用率已正确计算。但是，在 Amazon CloudWatch 上，空闲行为看起来像正常的 CPU 活动，因为所有 CPU 周期都有要运行的指令，这会导致 CloudWatch 显示高 CPU 使用率百分比 (85-90%)。

Azure CPU 使用率报告

执行以下步骤，使用 Azure Monitor 中的 VM Insights 查看所有受监控 VM 的 CPU 利用率：

过程

步骤 1 转到 Azure 门户，选择 **监控** ，然后在 **解决方案** 部分选择 **虚拟机** 。

步骤 2 选择 **性能** 选项卡以显示 **CPU Utilization %** 图表。此图表显示平均处理器使用率最高的前五台计算机。

执行以下步骤，直接从特定 Azure VM 查看 CPU 利用率百分比图表：

过程

步骤 1 转到 Azure 门户并选择 **虚拟机**。

步骤 2 从 VM 列表中，选择 VM。

步骤 3 在 **监控** 部分中，选择 **见解**。

步骤 4 选择 **Performance** 选项卡。

有关详细信息，请参阅 如何使用 VM Insights 绘制性能图表 。

ASA Virtual 和 Azure Graphs

ASA virtual 与 Azure 之间的 CPU 使用率 (%) 存在差异。Azure 图形数字始终高于 ASA virtual 数字，因为 Azure 将 CPU 使用率计算为活动使用的虚拟 CPU 的数量，指定为总可用 CPU 的百分比。

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率

Azure 还对访客操作系统请求的 CPU 数量进行速率限制。请考虑以下场景： ASA virtual 报告 CPU 使用率 40%，虚拟机监控程序报告 CPU 使用率 90%。现在，如果 ASA virtual 需要更高的处理能力，CPU 使用率可能会超过 80%，然后虚拟机监控程序可能会报告 CPU 使用率超过 95%。这会导致虚

拟机监控程序对 ASA virtual CPU 进行节流，即使 ASA virtual 只是在轮询模式下运行一个轻量级命令循环，表现出空闲行为。

Hyper-V CPU 使用率报告

除了查看可用云服务器的 CPU、RAM 和磁盘空间配置信息外，您还可以查看磁盘、I/O 和网络信息。使用这些信息可帮助您确定哪种云服务器适合您的需求。您可以通过命令行 nova 客户端或云控制面板 (Cloud Control Panel) 界面来查看可用的服务器。

在命令行中运行以下命令：

```
nova flavor-list
```

系统将显示所有可用的服务器配置。该列表包含了以下信息：

- ID - 服务器配置 ID
- 名称 - 按 RAM 大小和性能类型标记的配置名称
- Memory_MB - 配置的 RAM 量
- 磁盘 - 磁盘大小（以 GB 为单位）（对于一般用途的云服务器，即为系统磁盘的大小）
- 临时 - 数据磁盘的大小
- 交换 - 交换空间的大小
- VCPUs - 与配置关联的虚拟 CPU 的数量
- RXTX_Factor - 分配给连接到服务器的 PublicNet 端口、ServiceNet 端口和隔离网络（云网络）的带宽量（以 Mbps 为单位）
- Is_Public - 未使用

ASA Virtual 和 Hyper-V 图形

ASA Virtual 与 Hyper-V 之间的 CPU 使用率 (%) 存在差异：

- Hyper-V 图表值始终大于 ASA Virtual 值。
- Hyper-V 称之为 %CPU 使用率；ASA Virtual 称之为 %CPU 利用率。

术语“%CPU 利用率”和“%CPU 使用率”表示不同的东西：

- CPU 利用率提供了物理 CPU 的统计信息。
- CPU 使用率提供了基于 CPU 超线程的逻辑 CPU 统计信息。但是，由于只使用一个 vCPU，因此超线程未打开。

Hyper-V 按如下方式计算 CPU 使用率 (%)：

当前使用的虚拟 CPU 的用量，以总可用 CPU 的百分比表示

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率

注释 建议查看 ASA Virtual 报告，以获取准确的 CPU 使用率百分比。

OCI CPU 使用率报告

您可以使用计算实例指标（ **oci_computeagent**）查看 OCI 中的 CPU 利用率百分比。CPU 利用率指标显示 CPU 的活动级别，以占总时间的百分比表示。执行以下步骤以查看单个计算实例的指标图表：

过程

步骤 1 打开导航菜单，然后点击 **计算**下的 **实例** 。

步骤 2 点击实例，然后点击 **资源**下的 **指标** 。

步骤 3 在度量命名空间列表中选择 **oci_computeagent** 。

有关详细信息，请参阅 计算实例指标 。

ASA Virtual 和 OCI 图形

OCI 图形数字始终高于 ASA virtual 数字，因为 OCI 将 CPU 使用率计算为活动使用的虚拟 CPU 的数量，指定为可用 CPU 总数的百分比。

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率

测试配置

本节介绍如何为单模式 ASA 或每个安全情景测试连接，如何 ping ASA 接口，以及如何让一个接口上的主机 ping 到另一个接口上的主机。

测试基本连接：Ping 通地址

ping 是一种简单命令，可用于确定特定地址是否处于活动状态以及是否会做出响应。以下主题详细介绍此命令以及您可以使用此命令完成什么类型的测试。

使用 Ping 可测试的信息

当您 ping 设备时，系统会向设备发送数据包并且设备会返回回复。此过程可以让网络设备相互发现、识别和测试。

您可以使用 ping 来执行以下测试：

- 环回测试两个接口 - 可以在同一个 ASA 上从一个接口向另一个接口发起 ping，以外部环回测试方式来验证每个接口的基本“up”状态和操作。
- Ping 连接 ASA - 可以在其他 ASA 上 ping 某个接口，以验证其是否已打开并正在响应。
- Ping 通过 ASA - 可以通过在 ASA 的另一端 ping 某个设备来 ping 通过中间 ASA。数据包在每个方向传输时将通过两个中间 ASA 的接口。此操作会对中间设备的接口、操作和响应时间执行基本测试。
- Ping 测试网络设备的可疑操作 - 可以从某个 ASA 接口 ping 连接您怀疑运行不正常的网络设备。如果接口配置正确但没有收到回送，则可能是设备存在问题。
- Ping 测试中间通信 - 可以从某个 ASA 接口 ping 连接已知运行正常的网络设备. 如果接收到回送，任意中间设备的正确操作和物理连接都得以确认。

在 ICMP 和 TCP ping 之间进行选择

ASA 包括传统 ping，它会发送 ICMP 回送请求数据包并会在返回中获取回送回复数据包。如果所有相关网络设备都允许 ICMP 流量，这就是标准工具并且会正常运行。通过 ICMP ping，您可以 ping IPv4 或 IPv6 地址或主机名。

但是，某些网络会禁止 ICMP。如果您的网络禁止 ICMP，则可以改用 TCP ping 测试网络连接。对于 TCP ping，ping 会发送 TCP SYN 数据包，如果在响应中收到 SYN-ACK，则系统将 ping 视为成功。通过 TCP ping，您可以 ping IPv4 地址或主机名，但是不可以 ping IPv6 地址。

请记住，ICMP 或 TCP ping 成功只说明您使用的地址处于活动状态并会响应该特定类型的流量。这意味着基本连接正常工作。在设备上运行的其他策略可能会阻止特定类型的流量成功通过设备。

启用 ICMP

默认情况下，您可以从安全性高的端口 ping 到安全性低的端口。只需启用 ICMP 检测即可允许回程流量通行。如果要想从低到高进行 ping，则需要应用 ACL 来允许流量。

当 ping ASA 接口时，应用于接口的所有 ICMP 规则都必须允许回送请求数据包和回送响应数据包。ICMP 规则是可选的：如果您不配置这些规则，则系统会允许流入接口的所有 ICMP 流量。

此程序介绍要启用 ASA 接口的 ICMP ping 或通过 ASA 执行 ping，您可能需要完成的所有 ICMP 配置。

过程

步骤 1 确保 ICMP 规则允许回送请求/回送响应。

ICMP 规则是可选的，应用于直接发送到接口的 ICMP 数据包。如果不应用 ICMP 规则，系统会允许所有 ICMP 访问。在这种情况下，不需要进行任何操作。

但是，如果实施 ICMP 规则，请确保在每个接口上至少包含以下命令，将“inside”替换为设备上接口的名称。

```
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo inside
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo-reply inside
```

步骤 2 确保访问规则允许 ICMP。

当通过 ASA ping 主机时，访问规则必须允许 ICMP 流量流出和返回。访问规则必须至少允许回送请求数据包/回送回复 ICMP 数据包。您可以将这些规则添加为全局规则。

假设您已经向接口应用或全局应用访问规则，则只需将这些规则添加到相关 ACL，例如：

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any anyecho

ciscoasa(config)# access-list outside_access_in extendedpermit icmp any
anyecho-reply
```

或者，允许所有 ICMP 即可：

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any any
```

如果您没有访问规则，则还需要允许所需的其他流量类型，因为向接口应用任何访问规则都会增加一个隐式拒绝，因此会丢弃所有其他流量。使用 **access-group** 命令，向接口应用或全局应用 ACL。

如果仅为测试目的添加规则，则可以使用 **access-list** 命令的 **no** 形式 从 ACL 删除规则。如果整个 ACL 都仅用于测试目的，请使用 **no access-group** 命令从接口删除 ACL。

步骤 3 启用 ICMP 检测。

与 ping 接口相反，通过 ASA 执行 ping 时，需要执行 ICMP 检测。检测允许返回流量（即，回送回复数据包）返回到发起 ping 的主机，同时确保每个数据包都有一个响应，以防止特定类型的攻击。

您只要在默认全局检测策略中启用 ICMP 检测即可。

```
ciscoasa(config)# policy-map  global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect icmp
```

Ping 主机

要 ping 任何设备，只需输入 **ping** 和 IP 地址或主机名，例如 **ping 10.1.1.1** 或 **ping www.example.com**。对于 TCP ping，应包含 **tcp** 关键字和目标端口，例如 **ping tcp www.example.com 80**。这通常可满足您需要执行的任何测试要求。

ping 成功的输出示例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

如果 ping 失败，对于每次失败尝试，系统都会输出 ?，并且成功率会显示为低于 100%（完全失败显示 0%）：

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

但是，您还可以添加参数以控制 ping 的一些方面。以下是基本选项：

- ICMP ping。

  ping [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]

  其中：

  - *if_name* 会指定 ping 的源 IP 地址；但是，出口接口由使用数据路由表的路由查找确定。
  - *host* 是要 ping 的主机的 IPv4、IPv6 或主机名。
  - **repeat** *count* 是要发送的数据包的数量。默认值为 5。
  - **timeout** *seconds* 是在无响应的情况下每个数据包在超时之前等待的秒数。默认值为 2。
  - **data** *pattern* 是要用于所发送数据包中的十六进制模式。默认值为 0xabcd。
  - **size** *bytes* 是所发送数据包的长度。默认值为 100 字节。
  - **validate** 表示要验证回复数据。

- TCP ping。

  ping tcp [*if_name*] *host* [*port*] [**repeat** *count*] [**timeout** *seconds*] [**source** *host* [*ports*]

  其中：

  - *if_name* 会指定 ping 的源 IP 地址；但是，出口接口由使用数据路由表的路由查找确定。
  - *host* 是要 ping 的目标的 IPv4 地址或主机名。您不能将 TCP ping 用于 IPv6 地址。
  - *port* 是要 ping 的主机上的 TCP 端口。
  - **repeat** 和 **timeout** 与上述含义相同。
  - **source** *host port* 表示 ping 的源 IP 地址和端口。使用端口 0 可获取随机端口。

- 交互式 ping。

  ping

  输入不带参数的 ping 时，系统会提示您输入接口、目标和其他参数，包括不可用作关键字的扩展参数。如果您需要对 ping 数据包拥有广泛控制，请使用此方法。

系统地测试 ASA 连接

如果您要对 ASA 连接进行更系统的测试，可以采用以下一般程序。

开始之前

如果要查看程序中提及的系统日志消息，请启用日志记录（使用 **logging enable** 命令，或在 ASDM 中依次选择 **Configuration > Device Management > Logging > Logging Setup**）。

虽然不必要，但您还可以启用 ICMP 调试以在从外部设备 ping ASA 接口时，查看 ASA 控制台上的消息（您将无法查看通过 ASA 的 ping 的调试消息）。我们建议仅在故障排除过程中启用 ping 和调试消息，因为它们会影响性能。以下示例将启用 ICMP 调试，设置要发送到 Telnet 或 SSH 会话的系统日志消息并将它们发送到那些会话，以及启用日志记录。您也可以使用 **logging buffer debug** 命令代替 **logging monitor debug** 命令，将日志消息发送到缓冲区，稍后使用 **show logging** 命令进行查看。

```
ciscoasa(config)# debug icmp trace
ciscoasa(config)# logging monitor debug
ciscoasa(config)# terminal monitor
ciscoasa(config)# logging enable
```

在此配置下，如果从外部主机 (209.165.201.2) 成功 ping 到 ASA 外部接口 (209.165.201.1)，您会看到以下类似内容：

```
ciscoasa(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

输出显示 ICMP 数据包长度（32 字节）、ICMP 数据包的标识符 (1) 和 ICMP 序列号（ICMP 序列号从 0 起计，每次发送请求后序列号递增）。

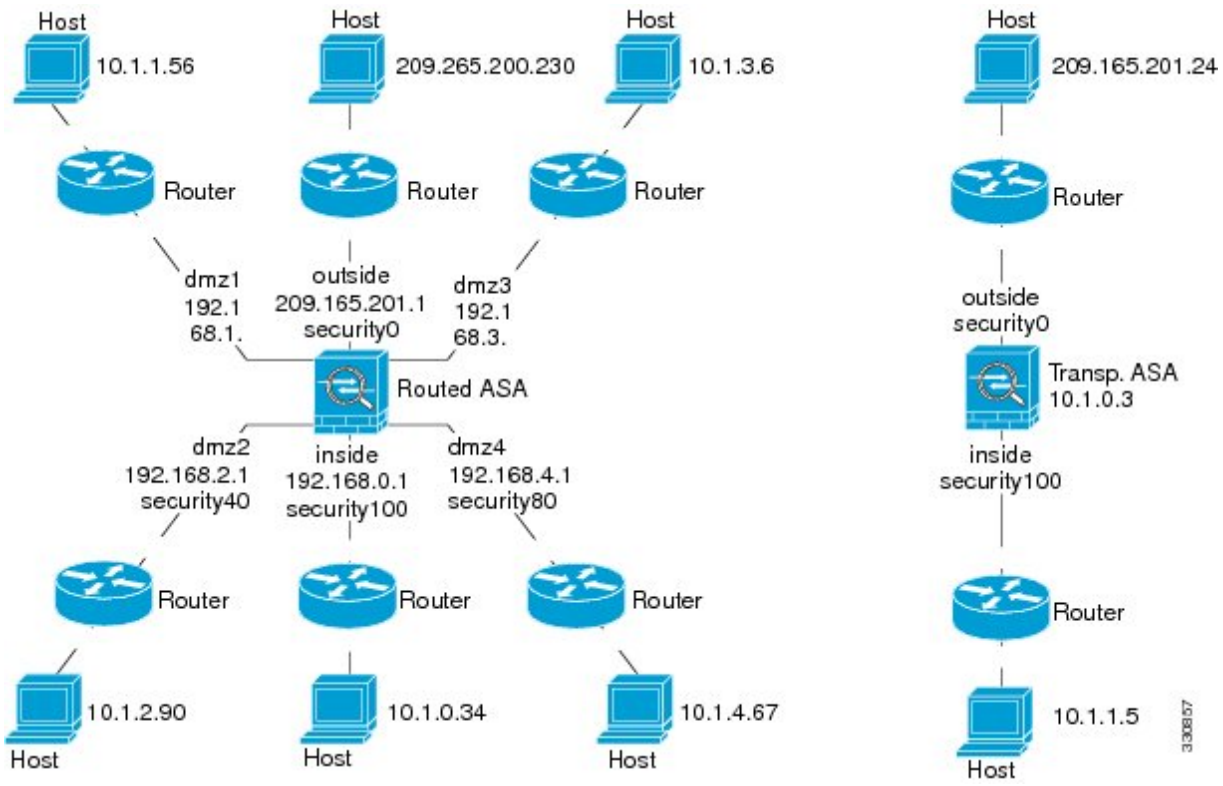
完成测试后，请禁用调试。保留此配置可能构成性能和安全风险。如果仅为了测试而启用日志记录，还可以禁用日志记录。

```
ciscoasa(config)# no debug icmp trace
ciscoasa(config)# no logging monitor debug
ciscoasa(config)# no terminal monitor
ciscoasa(config)# no logging enable
```

过程

步骤 1 绘制显示接口名称、安全级别和 IP 地址的单模式 ASA 或安全情景的示意图。示意图也应包括所有直接连接的路由器和一台主机，该主机位于用于 ping ASA 的路由器的另一侧。

图 *86:* 接口、路由器和主机的网络图



步骤 2 从直接连接的路由器 ping 每个 ASA 接口。对于透明模式，ping BVI IP 地址。此测试可确保 ASA 接口处于活动状态，并且接口配置正确。

如果 ASA 接口处于非活动状态、接口配置不正确，或 ASA 与路由器之间的交换机关闭（参阅下图），ping 操作可能会失败。在这种情况下，数据包不能到达 ASA，因此调试消息或系统日志消息不会显示。

图 *87: ASA* 接口的 *ping* 故障

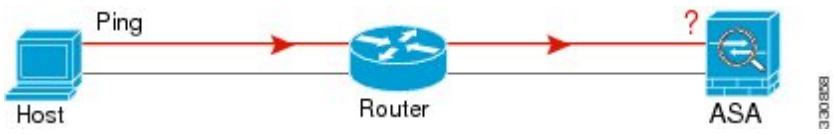
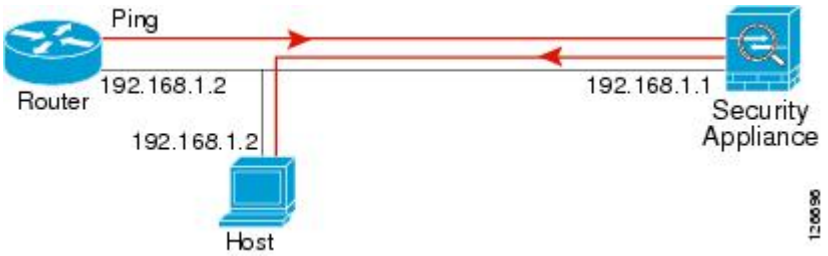


图 *88: IP* 寻址问题引发的 *Ping* 故障



如果 ping 回复没有返回到路由器，则可能存在交换机环路或冗余 IP 地址（参阅下图）。

步骤 3 从远程主机上 ping 每个 ASA 接口。对于透明模式，ping BVI IP 地址。此测试检查直接连接的路由器是否能在主机和 ASA 之间路由数据包，以及 ASA 是否可以正确地将数据包路由回主机。

如果 ASA 没有通过中间路由器返回路由到主机，ping 操作可能失败（参阅下图）。在这种情况下，调试消息显示 ping 成功，但系统会显示系统日志消息 110001，指示出现路由故障。

图 *89: ASA* 没有返回路由引发的 *ping* 故障

步骤 4 从 ASA 接口 ping 到已知正常运行的网络设备。

- 如果没有收到 ping，传输硬件或接口配置中可能存在问题。
- 如果 ASA 接口已正确配置但没有收到来自“已知良好的”设备的回送回复，接口硬件的接收功能可能存在问题。如果另一个具有“已知良好的”接收功能的接口可以在 ping 过该“已知良好的”设备后收到回送，则可以确认第一个接口硬件的接收功能存在问题。

步骤 5 从一个源接口的主机或路由器 ping 另一个接口上的主机或路由器。无论要检查多少接口对，都可以重复此步骤。如果使用 NAT，测试显示 NAT 运行正常。

如果 ping 成功，系统将显示系统日志消息确认路由模式的地址转换（305009 或 305011），并确认已创建一个 ICMP 连接（302020）。您还可以输入 **show xlate** 或 **show conns** 命令查看此信息。

如果 NAT 配置错误，ping 操作可能会失败。在这种情况下，系统会显示系统日志消息，指示 NAT 失败（305005 或 305006）。如果在没有静态转换的情况下从外部主机 ping 内部主机，您将会收到消息 106010。

图 *90: ASA* 未进行地址转换引发的 *ping* 故障

跟踪主机路由

如果您向某个 IP 地址发送流量时遇到问题，可以跟踪主机路由以确定网络路径是否有问题。

过程

步骤 1 使 ASA 在跟踪路由中可见，第 1363 页。
步骤 2 确定数据包路由，第 1364 页。

使 ASA 在跟踪路由中可见

默认情况下，ASA 不会作为跃点显示在跟踪路由中。要使其显示，您需要递减通过 ASA 的数据包上的生存时间，并增加对 ICMP 不可达消息的速率限制。

过程

步骤 1 创建 L3/L4 类映射，以确定要为其自定义连接设置的流量。

class-map 名称

match 参数

示例：

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
```

有关匹配语句的信息，请参阅防火墙配置指南中的“服务策略”一章。

步骤 2 添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

policy-map *name* **class** *name*

示例：

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

步骤 3 减小与类匹配的数据包的生存时间 (TTL)。

```
set connection decrement-ttl
```

步骤 4 如果编辑的是现有服务策略（例如，名为 global_policy 的默认全局策略），您即可跳过此步骤。否则，应在一个或多个接口上激活策略映射。

service-policy *policymap_name* {**global** | **interface** *interface_name* }

示例：

```
ciscoasa(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

步骤 5 增加对 ICMP 不可达消息的速率限制，以便 ASA 显示在跟踪路由输出中。

icmp unreachable rate-limit 速率**burst-size**大小

示例：

```
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 1
```

速率限制可为 1-100，1 为默认值。突发大小无意义，但必须为 1-10。

示例

以下示例为所有流量全局减小 TTL 并将 ICMP 不可达消息限制增至 50。

```
ciscoasa(config)# class-map global-policy
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class global-policy
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

确定数据包路由

使用 Traceroute 帮助您确定数据包到达目标地址所要经过的路由。跟踪路由通过向无效端口上的目标发送 UDP 数据包或 ICMPv6 回应来工作。由于端口无效，连接到该目标的路由器会以 ICMP 或 ICMPv6 超时消息做出响应，并向 ASA 报告该错误。

跟踪路由显示发送的每个探测的结果。每行输出以递增顺序对应一个 TTL 值。下表对输出符号进行了说明。

输出符号	说明
*	在超时期限内未收到对探测的响应。

输出符号	说明
U	没有通往目标的路由。
nn msec	各节点指定探测数的往返时间（以毫秒为单位）。
!N.	无法访问 ICMP 网络。对于 ICMPv6，地址超出范围。
!H	无法访问 ICMP 主机。
!P	无法访问 ICMP。对于 ICMPv6，端口不可访问。
!A	管理性禁止 ICMP。
?	未知 ICMP 错误。

过程

跟踪通往目标的路由：

traceroute [*destination_ip* | *hostname*} [**source** {*source_ip* | *source-interface*}] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

示例：

```
ciscoasa# traceroute 209.165.200.225

Type escape sequence to abort.
Tracing the route to 209.165.200.225

1 10.83.194.1 0 msec 10 msec 0 msec
2 10.83.193.65 0 msec 0 msec 0 msec
3 10.88.193.101 0 msec 10 msec 0 msec
4 10.88.193.97 0 msec 0 msec 10 msec
5 10.88.239.9 0 msec 10 msec 0 msec
6 10.88.238.65 10 msec 10 msec 0 msec
7 172.16.7.221 70 msec 70 msec 80 msec
8 209.165.200.225 70 msec 70 msec 70 msec

ciscoasa# traceroute 2002::130

Type escape sequence to abort.
Tracing the route to 2002::130

 1  5000::2 0 msec 0 msec 0 msec
 2  2002::130 10 msec 0 msec 0 msec
```

通常，您只需包含目标 IP 地址或主机名，例如 **traceroute www.example.com**。但是，如有必要，可以调整跟踪的特征：

- **source** {*source_ip* | *source-interface*} - 指定用作跟踪源的接口。您可以按名称或 IP 地址指定接口。对于 Ipv6，无法指定源接口；只能指定源 IP 地址。IPv6 地址仅当已在 ASA 上启用 IPv6 时有效。在透明模式下，您必须使用管理地址。

- **numeric** - 表示在跟踪路由上应显示的 IP 地址。如果没有此关键字，跟踪路由不会为地址执行 DNS 查找，并且如果您配置了 DNS，跟踪路由还包含 DNS 名称。
- **timeout** *timeout_value* - 在超时之前等待响应的时间。默认值为 3 秒。
- **probe** *probe_num* - 每个 TTL 级别发送的探测数量。默认值为 3。
- **ttl** *min_ttl max_ttl* - 探测的最小和最大生存时间值。默认最小值为 1，但也可以设置更高值来阻止显示已知跃点。最大默认值为 30。当数据包到达目标地址或达到最大值时，跟踪路由终止。
- **port** *port_value* - 要使用的 UDP 端口。默认值为 33434。
- **use-icmp** - 为探测发送 ICMP 数据包而不是 UDP 数据包。

使用数据包跟踪器测试策略配置

您可以通过根据源和目标寻址以及协议特征为数据包建模，测试您的策略配置。跟踪会执行策略查找以测试访问规则、NAT、路由等，以便查看系统会允许还是拒绝数据包。

通过这样测试数据包，您可以看到策略结果并测试系统是否会按照需要处理要允许或拒绝的流量类型。除了验证配置之外，您还可以使用跟踪器调试意外行为，例如数据包本应被允许，但却被拒绝的情况。

过程

步骤 1 此命令较为复杂，因此我们将它分成几个部分。首先从为跟踪选择接口和协议开始：

packet-tracer input *ifc_name* [**vlan-id***vlan_id*] {**icmp** | **tcp** | **udp** | **rawip** | **sctp**} [**inline-tag** *tag*] *...*

其中：

- **input** *ifc_name* - 开始跟踪的接口的名称。 对于网桥组，请指定网桥组成员接口名称。
- **vlan-id** *vlan_id* -（可选）。数据包跟踪器进入父接口的虚拟 LAN，稍后会被重定向至子接口。仅当输入接口进入接口不是子接口时，VLAN 身份才可用。有效值的范围为 1 到 4096。
- **icmp**、**tcp**、**udp**、**rawip**、**sctp** - 要使用的协议。“rawip”是原始 IP，即非 TCP/UDP 的 IP 数据包。
- **inline-tag** *tag* -（可选）。嵌入第 2 层 CMD 报头中的安全组标签值。有效值范围为 0 到 65533。

步骤 2 接下来，键入源地址和协议条件。

...{*src_ip* | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}*...*

其中：

- *src_ip* - 数据包跟踪的源 IPv4 或 IPv6 地址。

- **user** *username* - domain\user 格式的用户身份。跟踪中使用最近为用户映射的地址（如有）。
- **security-group** {**name** *name* | **tag** *tag*} - 基于 Trustsec 的 IP-SGT 查找的源安全组。您可以指定安全组名称或标签编号。
- **fqdn** *fqdn-string* - 源主机的完全限定域名，仅限 IPv4。

步骤 3 接下来，键入协议特征。

- ICMP - 输入 ICMP 类型 (1-255)、ICMP 代码 (0-255)，并且可以选择键入 ICMP 标识符。您必须对每个变量使用编号，例如，8 用于表示回送。

  type code... [*ident*]...
- TCP/UDP/SCTP - 输入源端口号。

  ...*src_port* ...
- Raw IP - 输入协议编号，0-255。

  …协议 ...

步骤 4 最后，键入目标地址条件、TCP/UDP 跟踪的目标端口，以及可选关键字，并按 **Enter** 键。

...dmac {*dst_ip* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *dst_port* [**detailed**] [**xml**]

其中：

- *dst_ip* - 数据包跟踪的目标 IPv4 或 IPv6 地址。
- **security-group** {**name** *name* **| tag** *tag*} - 适用于 Trustsec 的基于 IP-SGT 查找的目标安全组。您可以指定安全组名称或标签编号。
- **fqdn** *fqdn-string* - 目标主机的完全限定域名，仅限 IPv4。
- *Dst_port* - TCP/UDP/SCTP 跟踪的目标端口。请勿为 ICMP 或原始 IP 跟踪添加此值。
- *dmac* -（透明模式）目标 MAC 地址。
- **detailed** - 除了正常输出之外，还提供详细的跟踪结果信息。
- **xml** - 以 XML 格式显示跟踪结果。

步骤 5 键入 **persist** 选项，使数据包跟踪器跨集群设备调试数据包。

- 您可以通过使用 **transmit** 选项，允许模拟的数据包传出 ASA。
- 要跳过 ACL、VPN 筛选器、IPsec 欺骗和 uRPF 等安全检查，请使用 **bypass-checks** 选项。
- 使用 **decrypted** 选项，您可以将已解密的数据包注入 VPN 隧道，还可以模拟通过 VPN 隧道的数据包。

步骤 6 键入 **id** 和 **origin**，以用于跟踪集群设备中的特定数据包。

- **id** - 由启动跟踪的设备分配的标识号。

- **origin** - 指示启动跟踪的集群设备。

示例

以下示例跟踪从 10.100.10.10 到 10.100.11.11 的 HTTP 端口的 TCP 数据包。结果表明隐式拒绝访问规则将丢弃该数据包。

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11
 80

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

监控连接

要查看当前连接及其源、目标、协议等信息，请使用 **show conn all detail** 命令。

测试和故障排除的历史记录

功能名称	平台版本	说明
跟踪路由支持 IPv6	9.7(1)	**traceroute** 命令已修改为接受 IPv6 地址。 修改了以下命令：**traceroute**

功能名称	平台版本	说明
对于网桥组成员接口，支持使用 Packet Tracer	9.7(1)	现在，对于网桥组成员接口可以使用 Packet T 我们为 **packet-tracer** 命令添加了两个新选项 **dmac**
手动开始和停止数据包捕获	9.7(1)	您现在可以手动停止和开始捕获。 添加/修改的命令：**capture stop**
增强了数据包跟踪器和数据包捕获功能	9.9(1)	数据包跟踪器通过以下功能得到增强： • 在集群设备之间传递数据包时跟踪该数据 • 允许模拟数据包传出 ASA。 • 绕过对模拟数据包的安全检查。 • 将模拟数据包视为 IPSec/SSL 解密数据包 数据包捕获通过以下功能得到增强： • 在解密后捕获数据包。 • 捕获跟踪并将其保留在永久列表中。 新增或修改的命令：**cluster exec capture test include-decrypted**、**cluster exec capture test tr cluster exec clear packet-tracer**、**cluster exec packet-tracer id**、**cluster exec show packet-tra packet-tracer persist**、 **packet-tracer transmi packet-tracer decrypted**、**packet-tracer bypa**
无需使用 ACL 便可匹配 IPv6 流量的数据包捕获支持	9.10(1)	如果您在 **capture** 命令中使用 **match** 关键字，字仅匹配 IPv4 流量。现在，您可以指定 **any4** 键字，以捕获 IPv4 或 IPv6 流量。**any** 关键字 IPv4 流量。 新增/修改的命令：**capture match**
适用于 Forepower 9300/4100 的新**debug telemetry**命令。	9.14(1)	如果您使用的是 **debug telemetry** 命令，则会相关的调试消息。生成遥测报告时，调试有助的原因。 新增/修改的命令： **[no] debug telemetry**、**sh telemetry**

功能名称	平台版本	说明
ping 命令更改	9.18(2)	为了支持对环回接口执行 ping 操作，**ping** 命令现改行为。如果您在命令中指定接口，则源 IP 地址接口 IP 地址匹配，但实际出口接口将由使用数据路由查找来确定。 新增/修改的命令：**ping**
交换机的数据包捕获	9.20(1)	您现在可以配置以捕获交换机的出口和进口流量此选项仅适用于 Cisco Secure Firewall 4200 型号的 新增/修改的命令： **capture** *capture_name* **switch interface** *interface_n* **direction** { **both** | **egress** | **ingress** }]

第 VIII 部分

监控

- 日志记录， 第 1373 页
- SNMP， 第 1403 页
- 思科成功网络和遥测数据， 第 1439 页
- Anonymous Reporting 和 Smart Call Home， 第 1449 页

第 46 章

日志记录

本章介绍如何记录系统消息并将其用于故障排除。

- 关于日志记录，第 1373 页
- 日志记录准则，第 1381 页
- 配置日志记录，第 1382 页
- 监控日志，第 1397 页
- 日志记录示例，第 1398 页
- 日志记录功能历史记录，第 1399 页

关于日志记录

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。思科设备可以将其日志消息发送到 UNIX 样式的系统日志服务。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件打印消息。以这种形式记录日志可为日志提供受保护的长期存储。日志对常规故障排除及事件处理均有帮助。

ASA 系统日志提供有关对 ASA 进行监控和故障排除的信息。通过日志记录功能，可以执行以下操作：

- 指定应记录哪些系统日志消息。
- 禁用或更改系统日志消息的严重性级别。
- 指定系统日志消息应发送到的一个或多个位置，包括：
  - 内部缓冲区
  - 一个或多个系统日志服务器
  - ASDM
  - SNMP 管理站
  - 指定的电子邮件地址
  - 控制台

- Telnet 和 SSH 会话。

- 以组形式（例如，按严重性级别或消息类）配置和管理系统日志消息。
- 指定是否对系统日志生成应用速率限制。
- 指出在内部日志缓冲区已满时如何处理其内容：覆盖缓冲区、将缓冲区内容发送到 FTP 服务器，或者将内容保存到内部闪存。
- 按位置、严重性级别、类或自定义消息列表过滤系统日志消息。

多情景模式下的日志记录

每个安全情景包含自己的日志记录配置并生成其自己的消息。如果登录到系统或管理情景，然后更改为其他情景，则只能在会话中查看与当前情景相关的消息。

请在管理情景中查看在系统执行空间中生成的系统日志消息（包括故障转移消息）以及在管理情景中生成的消息。无法在系统执行空间中配置日志记录或查看任何日志记录信息。

可以将ASA配置为在每个消息中包含情景名称，从而帮助区分发送到单个系统日志服务器的情景消息。此功能有助于确定哪些消息来自管理情景，哪些消息来自系统；源于系统执行空间的消息使用设备 ID **system**，源于管理情景的消息使用管理情景的名称作为设备 ID。

系统日志消息分析

以下是可从各种系统日志消息审阅中获取的信息类型的一些示例：

- ASA 安全策略允许的连接。这些消息帮助确定安全策略中仍存在的漏洞。
- ASA 安全策略拒绝的连接。这些消息显示将哪些类型的活动定向到受保护内部网络。
- 使用 ACE 拒绝率日志记录功能显示在 ASA 上发生的攻击。
- IDS 活动消息可以显示已发生的攻击。
- 用户身份验证和命令使用情况提供安全策略更改的审计线索。
- 带宽使用情况消息显示每个已建立和中断的连接，以及各连接使用的持续时间和流量。
- 协议使用情况消息显示每个连接使用的协议和端口号。
- 地址转换审计线索消息记录建立或中断的 NAT 或 PAT 连接，如果接收到从网络内部到外部环境的恶意活动报告，这些消息会有所帮助。

系统日志消息格式

系统日志消息的结构如下：

```
[<PRI>] [Timestamp] [Device-ID] : %ASA-Class-Level-Message_number: Message_text
```

字段说明如下：

<PRI>	优先级值。在启用日志记录 EMBLEM 后，此值将显示在系统日志消息中。日志记录 EMBLEM 与 UDP 兼容，但与 TCP 不兼容。
时间戳	系统将显示事件的日期和时间。在启用时间戳日志记录后，如果时间戳被配置为 RFC 5424 格式，则系统日志消息中的所有时间戳都会以 UTC 显示时间，如 RFC 5424 标准所示。
Device-ID	通过用户界面启用登录 device-id 选项时配置的设备标识符字符串。如果启用，则在 EMBLEM 格式化系统日志消息中不会显示设备 ID。
分类	系统日志消息类提供一个按类型将系统日志消息分类的方法，相当于设备的特性或功能。例如，vpnc 类表示 VPN 客户端。
ASA	由 ASA 所生成消息的系统日志消息设备代码。值始终为 `ASA`。
级别	0 到 7。级别反映系统日志消息所描述情况的严重性 - 数字越小，情况越严重。
Message_number	用于标识系统日志消息的唯一六位数编号。所有消息都记录在 Cisco Secure Firewall ASA 系列系统日志消息指南中。
Message_text	用于描述情况的文本字符串。系统日志消息的这一部分有时包含 IP 地址、端口号或用户名。

启用了日志记录 EMBLEM、日志记录时间戳 rfc5424 和设备 ID 的系统日志消息示例。

```
<166>2018-06-27T12:17:46Z: %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

启用了日志记录时间戳 rfc5424 和设备 ID 的系统日志消息示例。

```
2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

系统日志消息的结构如下：

```
[<PRI>] [Timestamp] [Device-ID] : %ASA-Level-Message_number: Message_text
```

字段说明如下：

<PRI>	优先级值。在启用日志记录 EMBLEM 后，此值将显示在系统日志消息中。日志记录 EMBLEM 与 UDP 兼容，但与 TCP 不兼容。
时间戳	系统将显示事件的日期和时间。在启用时间戳日志记录后，如果时间戳被配置为 RFC 5424 格式，则系统日志消息中的所有时间戳都会以 UTC 显示时间，如 RFC 5424 标准所示。
Device-ID	通过用户界面启用登录 device-id 选项时配置的设备标识符字符串。如果启用，则在 EMBLEM 格式化系统日志消息中不会显示设备 ID。
ASA	由 ASA 所生成消息的系统日志消息设备代码。值始终为 `ASA`。
级别	0 到 7。级别反映系统日志消息所描述情况的严重性 - 数字越小，情况越严重。
Message_number	用于标识系统日志消息的唯一六位数编号。

Message_text	用于描述情况的文本字符串。系统日志消息的这一部分有时包含 IP 地址、端口号或用户名。

设备生成的所有系统日志消息都记录在 Cisco Secure Firewall ASA 系列系统日志消息指南中。

启用了日志记录 EMBLEM、日志记录时间戳 rfc5424 和设备 ID 的系统日志消息示例。

```
<166>2018-06-27T12:17:46Z: %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

启用了日志记录时间戳 rfc5424 和设备 ID 的系统日志消息示例。

```
2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

严重性级别

下表列出系统日志消息严重性级别。可以为各严重性级别分配自定义颜色，更轻松地在 ASDM 日志查看器中对其进行区分。要配置系统日志消息颜色设置，请依次选择**工具 > 首选项 > 系统日志**选项卡，或者在日志查看器中点击工具栏上的**颜色设置**。

表 *59:* 系统日志消息严重级别

级别号	严重性级别	说明
0	**应急**	系统不可用。
1	**警报**	需要立即采取措施。
2	**严重**	严重情况。
3	**错误**	错误情况。
4	**警告**	警告情况。
5	**通知**	正常但重大的情况。
6	**信息性**	消息仅供参考。
7	**调试**	消息仅供调试。 调试问题时，仅临时记录此级别的日志。此日志级别可能会生成太多消息，从而影响系统性能。

注释 ASA 和 不会生成严重性级别为零 (emergencies) 的系统日志消息。

系统日志消息过滤

您可以过滤生成的系统日志消息，以便仅将某些系统日志消息发送到特定输出目标。例如，您可以将ASA配置为将所有系统日志消息发送至一个输出目标，而将这些系统日志消息中的一部分发送至其他输出目标。

具体而言，您可以根据以下条件将系统日志消息定向到输出目标：

- 系统日志消息 ID 号
- 系统日志消息严重性级别
- 系统日志消息类（相当于一个功能区）

通过创建一个在设置输出目标时可以指定的消息列表来自定义这些条件。或者，可以将ASA配置为将一个特定的消息类发送至每种类型的输出目标，而不管消息列表是什么。

系统日志消息类

可以通过两种方法使用系统日志消息类：

- 指定整个类别的系统日志消息的输出位置。使用 **logging class** 命令。
- 创建指定消息类的消息列表。使用 **logging list** 命令。

系统日志消息类提供一个按类型将系统日志消息分类的方法，相当于设备的特性或功能。例如，RIP 类表示 RIP 路由。

特定类中的所有系统日志消息共享其系统日志消息 ID 号中相同的前三位数字。例如，所有以数字 611 开头的系统日志消息 ID 都与 vpnc（VPN 客户端）类相关联。与 VPN 客户端功能相关联的系统日志消息范围从 611101 至 611323。

此外，大多数 ISAKMP 系统日志消息都具有公用预置对象集来帮助识别隧道。这些对象在适用时前置于系统日志消息的描述性文本。如果在生成系统日志消息时对象未知，则不显示特定的 heading = value 组合。

对象的前缀如下：

Group = *groupname*, Username = *user*, IP = *IP_address*

其中组是隧道组，用户名是来自本地数据库或 AAA 服务器的用户名，IP 地址是远程访问客户端或第 2 层对等体的公用 IP 地址。

下表列出消息类以及每个类中的消息 ID 范围。

表 *60:* 系统日志消息类和关联的消息 *ID* 号

类别	定义	系统日志消息 ID 号
auth	用户身份验证	109、113
-	访问列表	106

类别	定义	系统日志消息 ID 号
-	应用防火墙	415
—	僵尸网络流量筛选	338
bridge	透明防火墙	110、220
ca	PKI 证书颁发机构	717
citrix	Citrix Client	723
-	集群	747
-	卡管理	323
config	命令界面	111、112、208、308
csd	安全桌面	724
cts	Cisco TrustSec	776
dap	动态访问策略	734
eap, eapoudp	用于网络准入控制的 EAP 或 EAPoUDP	333、334
eigrp	EIGRP 路由	336
电子邮件	邮件代理	719
-	环境监控	735
ha	故障转移	101、102、103、104、105、210、311、709
-	基于身份认证的防火墙	746
ids	入侵检测系统	400、733
-	IKEv2 工具包	750、751、752
ip	IP 堆栈	209、215、313、317、408
ipaa	IP 地址分配	735
ips	入侵保护系统	400、401、420
-	IPv6	325
-	许可	444
mdm-proxy	MDM 代理	802

类别	定义	系统日志消息 ID 号
nac	网络准入控制	731、732
nacpolicy	NAC 策略	731
nacsettings	配置 NAC 设置，以应用 NAC 策略	732
-	NAT 与 PAT	305
-	网络无线接入点	713
np	网络处理器	319
-	NP SSL	725
ospf	OSPF 路由	318、409、503、613
-	密码加密	742
-	电话代理	337
rip	RIP 路由	107、312
rm	资源管理器	321
-	Smart Call Home	120
session	用户会话	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
-	ScanSafe	775
ssl	SSL 堆栈	725
svc	SSL VPN 客户端	722
sys	System	199、211、214、216、306、307、315、414、604、605，606、610、612、614、615、701、711、741
-	威胁检测	733
标记交换	服务标记交换	779
transactional-rule-engine-tre	事务规则引擎	780
UC-IMS	UC-IMS	339

类别	定义	系统日志消息 ID 号
vm	VLAN 映射	730
vpdn	PPTP 和 L2TP 会话	213、403、603
vpn	IKE 和 IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN 客户端	611
vpnfo	VPN 故障转移	720
vpnlb	VPN 负载均衡	718
-	VXLAN	778
webfo	WebVPN 故障转移	721
webvpn	WebVPN 和 Secure Client	716

自定义消息列表

灵活地创建自定义消息列表，以对将哪些系统日志消息发送至哪个输出目标实施控制。在自定义系统日志消息列表中，可以使用以下任意或所有条件指定系统日志消息组：

- 严重性级别
- 消息 ID
- 系统日志消息 ID 范围
- 消息类

例如，可以使用消息列表执行以下操作：

- 选择严重性级别为 1 和 2 的系统日志消息，然后将其发送到一个或多个邮件地址。
- 选择与消息类（例如 ha）关联的所有系统日志消息，然后将其保存到内部缓冲区。

消息列表可以包含多个消息选择条件。 但是，必须使用新命令条目来添加各消息选择条件。可以创建包含重叠消息选择条件的消息列表。如果消息列表中的两个条件选择同一消息，则消息仅记录一次。

集群

系统日志消息是在集群环境中用于记帐、监控和故障排除的一种实用工具。集群中的每台ASA设备（最多允许八台设备）都是独立生成系统日志消息；然后，某些**logging**命令支持您控制报头字段，其中包括时间戳和设备 ID。系统日志服务器使用设备 ID 标识系统日志生成器。您可以使用 **logging**

device-id 命令来生成具有相同或不同设备 ID 的系统日志消息，以使消息看上去是来自集群中的相同或不同设备。

日志记录准则

本节介绍您在配置日志记录之前应审阅的准则和限制。

IPv6 准则

- 支持 IPv6。可以使用 TCP 或 UDP 发送系统日志。
- 确保配置用于发送系统日志的接口已经启用，支持 IPv6，并且可以通过指定接口到达系统日志服务器。
- 不支持通过 IPv6 进行安全登录。

其他准则

- 系统日志服务器必须运行一个名为 syslogd 的服务器程序。Windows 提供了一个系统日志服务器，作为其操作系统的组成部分。
- 系统日志服务器基于防火墙系统的 syslog-ng 进程运行。请勿使用外部配置文件，例如 SecureWorks 的 *scwx.conf* 文件。此类文件与设备不兼容。使用它们将导致解析错误，最终 syslog-ng 进程将失败。
- 要查看由 ASA 生成的日志，必须指定日志记录输出目标。如果启用日志记录而未指定日志记录输出目标，则 ASA 会生成消息，但不会将其保存到可对其进行查看的位置。必须单独指定每个不同的日志记录输出目标。例如，要将多个系统日志服务器指定为输出目标，请对每个系统日志服务器输入新命令。
- 不支持在备用设备上通过 TCP 发送系统日志。
- 如果您使用 TCP 作为传输协议，系统会打开与系统日志服务器的 4 个连接，以确保消息不会丢失。如果您使用系统日志服务器从大量设备收集消息，并且合并的连接开销对该服务器来说太大，请改用 UDP。
- 不能将两个不同的列表或类分配给不同的系统日志服务器或相同位置。
- 您最多可以配置 16 个系统日志服务器。不过，在多情景模式下，限制为每个情景 4 个服务器。
- 应该可以通过 ASA 到达系统日志服务器。应将该设备配置为拒绝可以从其到达系统日志服务器的接口上的 ICMP 不可达消息，并将系统日志发送到同一服务器。请确保已对所有严重性级别启用日志记录。要防止系统日志服务器崩溃，请抑制系统日志 313001、313004 和 313005 的生成。
- 用于系统日志的 UDP 连接数与硬件平台上的 CPU 数量和您配置的系统日志服务器数量直接相关。在任何时刻，UDP 系统日志连接的数量都等于 CPU 数量乘以已配置的系统日志服务器数量的积。这是预期行为。请注意，全局 UDP 连接空闲超时适用于这些会话，默认值为 2 分钟。如

果您想更快关闭这些会话，可以调整该设置，但超时适用于所有 UDP 连接，而不仅是系统日志。

- 使用自定义消息列表仅与访问列表命中相匹配时，对于已将其日志记录严重性级别提高至调试（级别 7）的访问列表不会生成访问列表日志。对于 **logging list** 命令，默认日志记录严重性级别设置为 6。此默认行为是程序设计的。将访问列表配置的日志记录严重性级别显式更改为调试时，还必须更改日志记录配置本身。

  以下是来自 **show running-config logging** 命令的不含访问列表命中的样本输出，因为其日志记录严重性级别已更改为调试：

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

  以下是来自 **show running-config logging** 命令的包含访问列表命中的样本输出：

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging buffered debugging
```

  在此情况下，访问列表配置不更改，并会显示访问列表命中数，如下例所示：

```
ciscoasa(config)# access-list global line 1 extended
permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended
permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

- 当ASA通过TCP发送系统日志时，在系统日志服务重新启动后，需要大约一分钟来启动连接。
- 从系统日志服务器收到的服务器证书的 Extended Key Usage 字段中必须包含“ServAuth”。此检查将仅针对非自签名证书进行，自签名证书在此字段中不提供任何值。

配置日志记录

本节介绍如何配置日志记录。

启用日志记录

要启用日志记录，请执行以下步骤：

过程

启用日志记录。

logging enable

示例：

```
ciscoasa(config)# logging enable
```

配置输出目标

要优化系统日志消息使用情况以进行故障排除和性能监控，建议指定一个或多个应发送系统日志消息的位置，包括内部日志缓冲区、一个或多个外部系统日志服务器、ASDM、SNMP 管理站、控制台端口、指定的邮件地址或 Telnet 和 SSH 会话。

在启用了仅管理访问的接口上配置系统日志记录时，数据平面相关日志（会丢弃系统日志ID 302015、302014、106023 和 304001），并且不会到达系统日志服务器。由于数据路径路由表没有管理接口路由，将会丢弃系统日志消息。因此，请确保您配置的接口已禁用仅管理访问

将系统日志消息发送至外部系统日志服务器

可以根据外部系统日志服务器上的可用磁盘空间将消息存档，并在保存日志记录数据后对其进行处理。例如，可以指定在记录特定类型的系统日志消息时要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

要将系统日志消息发送到外部系统日志服务器，请执行以下步骤：

过程

步骤 1 将 ASA 配置为向系统日志服务器发送消息。

可以将 ASA 配置为向 IPv4 或 IPv6 系统日志服务器发送消息。

logging host *interface_name syslog_ip* [**tcp**[*/port*] | **udp** [*/port*] [**format emblem**]]

示例：

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp/1026
ciscoasa(config)# logging host dmz1 2002::1:1 udp/2020
```

format emblem 关键字为系统日志服务器启用 EMBLEM 格式日志记录（仅限 UDP）。*interface_name* 参数指定访问系统日志服务器所通过的接口。*syslog_ip* 参数指定系统日志服务器的 IP 地址。**tcp**[*/port*] or**udp**[*/udp*] 关键字-参数对指定 ASA 应使用 TCP 或 UDP 将系统日志消息发送到系统日志服务器。

可以将 ASA 配置为使用 UDP 或 TCP（但不同时使用两者）将数据发送到系统日志服务器。如果未指定协议，则默认协议为 UDP。

警告
如果指定TCP，则在ASA发现日志服务器发生故障，出于安全原因，将会阻止通过ASA的新连接。要允许新连接而不考虑与 TCP 系统日志服务器的连接，请参阅第 3 步。

如果指定UDP，则无论系统日志服务器是否可运行，ASA都会继续允许新连接。这两个协议的有效端口值为 1025 至 65535。默认 UDP 端口为 514。默认 UDP 端口为 1470。

步骤 2 指定应将哪些系统日志消息发送到系统日志服务器。

logging trap {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging trap errors
```

可以指定严重性级别号（1 至 7）或名称。例如，如果将严重性级别设置为 3，则 ASA 会发送严重性级别为 3、2 和 1 的系统日志消息。可以指定标识要发送到系统日志服务器的系统日志消息的自定义消息列表。

步骤 3 （可选）禁用在 TCP 连接的系统日志服务器关闭时阻止新连接的功能。

logging permit-hostdown

示例：

```
ciscoasa(config)# logging permit-hostdown
```

如果将 ASA 配置为将系统日志消息发送至基于 TCP 的系统日志服务器，并且其中任何一个系统日志服务器关闭或日志队列已满，则会阻止到ASA的新连接。备份系统日志服务器，且日志队列不再已满后，将再次允许新连接。使用此命令，即使系统日志服务器无法运行，也可以允许新连接。

步骤 4 （可选）将日志记录设备设置为大多数 UNIX 系统期望的除 20 以外的值。

logging facility 编号

示例：

```
ciscoasa(config)# logging facility 21
```

启用安全日志记录

过程

通过在 logging host 命令中指定 **secure** 关键字启用安全日志记录。此外，还可以选择输入 **reference-identity**。

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**[**reference-identity** *reference_identity_name*]]

其中：

- **logging host** *interface_name syslog_ip* 指定系统日志服务器所在的接口以及系统日志服务器的 IP 地址。
- [**tcp**/*port* | **udp**/*port*] 指定系统日志服务器为获取系统日志消息所侦听的端口（TCP 或 UDP）。**tcp** 关键字指定 ASA 应使用 TCP 将系统日志消息发送到系统日志服务器。**udp** 关键字指定 ASA 应使用 UDP 将系统日志消息发送到系统日志服务器。
- **format emblem** 关键字为系统日志服务器启用 EMBLEM 格式日志记录。
- **secure** 关键字指定与远程日志记录主机的连接应仅对 TCP 使用 SSL/TLS。安全日志记录不支持 UDP；如果尝试使用此协议，则会发生错误。
- [**reference-identity** *reference_identity_name*] 基于先前配置的引用标识对象启用对证书的 RFC 6125 引用标识检查。有关引用标识对象的详细信息，请参阅配置引用标识，第 889 页。

示例：

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure  reference-identity
syslogServer
```

将 EMBLEM 格式的系统日志消息生成到系统日志服务器

要将 EMBLEM 格式的系统日志消息生成到系统日志服务器，请执行以下步骤：

过程

使用端口 514 通过 UDP 将 EMBLEM 格式的系统日志消息发送到系统日志服务器。

logging host *interface_name ip_address*{**tcp** [*/port*] | **udp** [*/ port*]] [**format emblem**]

示例：

```
ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
ciscoasa(config)# logging host interface_1 2001::1 udp format emblem
```

您可以配置 IPv4 或 IPv6 系统日志服务器。

format emblem 关键字为系统日志服务器启用 EMBLEM 格式日志记录（仅限 UDP）。*interface_name* 参数指定访问系统日志服务器所通过的接口。*ip_address* 参数指定系统日志服务器的 IP 地址。**tcp**[*/port*] or**udp**[*/udp*] 关键字和参数对指定 ASA 应使用 TCP 或 UDP 将系统日志消息发送到系统日志服务器。

可以将 ASA 配置为使用 UDP 或 TCP（但不同时使用两者）将数据发送到系统日志服务器。如果未指定协议，则默认协议为 UDP。

可以使用多个 **logging host** 命令指定将全部接收系统日志消息的其他服务器。如果配置两个或多个系统日志服务器，请确保对于所有日志记录服务器将日志记录严重性级别限于警告。

警告
如果指定TCP，则在ASA发现日志服务器发生故障，出于安全原因，将会阻止通过ASA的新连接。要在系统日志服务器发生故障时允许新连接，请参阅第 3 步（共 将系统日志消息发送至外部系统日志服务器，第 1383 页 步）。

如果指定UDP，则无论系统日志服务器是否可运行，ASA都会继续允许新连接。这两个协议的有效端口值为 1025 至 65535。默认 UDP 端口为 514。默认 UDP 端口为 1470。

注释
不支持在备用 ASA 上通过 TCP 发送系统日志。

将 EMBLEM 格式的系统日志消息生成到其他输出目标

要将 EMBLEM 格式的系统日志消息生成到其他输出目标，请执行以下步骤：

过程

将EMBLEM格式的系统日志消息发送到系统日志服务器之外的输出目标，例如Telnet或SSH会话。

logging emblem

示例：

```
ciscoasa(config)# logging emblem
```

将系统日志消息发送至内部日志缓冲区

您需要指定应将哪些系统日志记录消息发送到充当临时存储位置的内部日志缓冲区。新消息附加到列表的末尾。当缓冲区已满时（也就是说，当缓冲区换行时），除非ASA配置为将完整缓冲区保存到其他位置，否则在生成新消息时会覆盖旧消息。

要将系统日志消息发送到内部日志缓冲区，请执行以下步骤：

过程

步骤 1 指定应将哪些系统日志记录消息发送到充当临时存储位置的内部日志缓冲区。

logging buffered {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging buffered critical
ciscoasa(config)# logging buffered level 2
```

```
ciscoasa(config)# logging buffered notif-list
```

新消息附加到列表的末尾。当缓冲区已满时（也就是说，当缓冲区换行时），除非ASA配置为将完整缓冲区保存到其他位置，否则在生成新消息时会覆盖旧消息。要清空内部日志缓冲区，请输入 **clear logging buffer** 命令。

步骤 2 更改内部日志缓冲区的大小。默认缓冲区大小为 4 KB。

logging buffer-size 字节

示例：

```
ciscoasa(config)# logging buffer-size 16384
```

步骤 3 选择以下其中一个选项：

- 将新消息保存到内部日志缓冲区，并将完整日志缓冲区内容保存到内部闪存。

  logging flash-bufferwrap

  示例：

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

  注释
  如果缓冲区大小超过 2 MB，该命令将停止在闪存中写入数据，且不会发出任何警告。

- 将新消息保存到内部日志缓冲区，并将完整日志缓冲区内容保存到 FTP 服务器。

  logging ftp-bufferwrap

  示例：

  ```
  ciscoasa(config)# logging ftp-bufferwrap
  ```

  将缓冲区内容保存到其他位置时， ASA 会创建具有使用以下时间戳格式的名称的日志文件：

  ```
  LOG-YYYY-MM-DD-HHMMSS.TXT
  ```

  其中 *YYYY* 是年，*MM* 是月，*DD* 是月日期，*HHMMSS* 是时间（以小时、分钟和秒为单位）。

- 标识要存储日志缓冲区内容的 FTP 服务器。

  logging ftp-server *server pathusername password*

  示例：

  ```
  ciscoasa(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
  ```

server 参数指定外部 FTP 服务器的 IP 地址。*path* 参数指定要在其上保存日志缓冲区数据的 FTP 服务器上的目录路径。此路径相对于 FTP 根目录。*username* 参数指定可日志记录到 FTP 服务器中的用户名。*password* 参数指示所指定用户名的 密码。

- 将当前日志缓冲区内容保存到内部闪存。

  logging savelog [*savefile*]

  示例：

```
ciscoasa(config)# logging savelog latest-logfile.txt
```

更改可用于日志的内部闪存量

要更改可用于日志的内部闪存量，请执行以下步骤：

过程

步骤 1 指定可用于保存日志文件的最大内部闪存量。

logging flash-maximum-allocation *kbytes*

示例：

```
ciscoasa(config)# logging flash-maximum-allocation 1200
```

默认情况下，ASA 可以为日志数据使用最多 50 MB 的内部闪存。可供 ASA 用于保存日志数据的最小内部闪存量为 3 MB。flash-maximum-allocation 值的最大限制为 2 GB。

如果保存到内部闪存的日志文件会导致可用内部闪存量低于配置的最小限制，则ASA会删除最早的日志文件，以确保保存新日志文件后最小内存量保持可用。如果没有要删除的文件，或者如果在删除所有旧文件后可用内存仍然低于限制，则 ASA 将无法保存新日志文件。

步骤 2 指定必须可供 ASA 用于保存日志文件的最小内部闪存量。

logging flash-minimum-free *kbytes*

示例：

```
ciscoasa(config)# logging flash-minimum-free 4000
```

将系统日志消息发送给邮件消息

如要将系统日志消息发送到邮件地址，请执行以下步骤：

过程

步骤 1 指定应将哪些系统日志消息发送到邮件地址。

logging mail {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging mail high-priority
```

通过邮件发送时，系统日志消息显示在邮件的主题行中。因此，建议将此选项配置为通知管理员具有高严重性级别（例如 critical、alert 和 emergency）的系统日志消息。

步骤 2 指定在将系统日志消息发送到邮件地址时要使用的源邮件地址。

logging from-address *email_address*

示例：

```
ciscoasa(config)# logging from-address xxx-001@example.com
```

步骤 3 指定在将系统日志消息发送到邮件地址时要使用的收件人邮件地址。

logging recipient-address *e-mail_address*[*severity_level*]

示例：

```
ciscoasa(config)# logging recipient-address admin@example.com
```

步骤 4 指定在将系统日志消息发送到邮件地址时要使用的 SMTP 服务器。您可以提供主服务器和辅助服务器地址，以确保日志消息服务永不中断。或者，您也可以将接口与服务器关联，以识别要用于日志记录的路由表。如果未提供接口，ASA 将引用管理路由表，如果没有适当的路由条目，则会查看数据路由表。

smtp-server [*primary-interface*] *primary-smpt-server-ip-address* [[*backup-interface*]*backup-smpt-server-ip-address*]

示例：

```
ciscoasa(config)# smtp-server 10.1.1.24 10.1.1.34
ciscoasa(config)# smtp-server 10.1.1.24
ciscoasa(config)# smtp-server management 10.1.1.24 outside 10.1.1.34
ciscoasa(config)# smtp-server management 10.1.1.24
```

将系统日志消息发送到 ASDM

要将系统日志消息发送到 ASDM，请执行以下步骤：

过程

步骤 1 指定应将哪些系统日志消息发送到 ASDM。

logging asdm {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging asdm 2
```

ASA 为等待发送到 ASDM 的系统日志消息预留一个缓冲区，并在消息出现时将其保存在缓冲区中。ASDM 日志缓冲区是不同于内部日志缓冲区的缓冲区。当 ASDM 日志缓冲区已满时，ASA 将删除最早的系统日志消息以在缓冲区中为新系统日志消息腾出空间。删除最早的系统日志消息来为新系统日志消息腾出空间是 ASDM 中的默认设置。要控制 ASDM 日志缓冲区中保留的系统日志消息数，可以更改缓冲区的大小。

步骤 2 指定要在 ASDM 日志缓冲区中保留的系统日志消息数。

logging asdm-buffer-size *num_of_msgs*

示例：

```
ciscoasa(config)# logging asdm-buffer-size 200
```

输入 **clear logging asdm** 命令以清空 ASDM 日志缓冲区的当前内容。

配置日志记录队列

要配置日志记录队列，请执行以下步骤：

过程

指定 ASA 将系统日志消息发送到已配置的输出目标之前可以在其队列中保留的系统日志消息数。

logging queue *message_count*

示例：

```
ciscoasa(config)# logging queue 300
```

ASA 在内存中具有固定的块数，这些块可以分配用于在系统日志消息等待发送到已配置的输出目标时将其缓冲存储。所需的块数取决于系统日志消息队列的长度和所指定系统日志服务器的数量。默认队列大小为 512 条系统日志消息。队列大小仅受块内存可用性的限制。有效值为 0 至 8192 条消息，具体视平台而定。如果日志记录队列设置为 0，则队列的最大可配置大小为 8192 条消息。

将系统日志消息发送到控制台端口

要将系统日志消息发送到控制台端口，请执行以下步骤：

过程

指定应将哪些系统日志消息发送到控制台端口。

logging console { *severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging console errors
```

将系统日志消息发送到 SNMP 服务器

要启用到 SNMP 服务器的日志记录，请执行以下步骤。

过程

启用 SNMP 日志记录并指定要将哪些消息发送到 SNMP 服务器。

logging history [**rate-limit** *number interval* | **level** *level* | *logging_list* | *level*]

如果使用 **logging rate-limit** 命令来设置全局速率限制，则该命令优先于此命令中的 **rate-limit** 关键字。

示例：

```
ciscoasa(config)# logging history errors
```

```
ciscoasa(config)# logging history rate-limit 15 15 level critical
```

将系统日志消息发送到 Telnet 或 SSH 会话

要将系统日志消息发送到 Telnet 或 SSH 会话，请执行以下步骤：

过程

步骤 1 指定应将哪些系统日志消息发送到 Telnet 或 SSH 会话。

logging monitor {*severity_level* | *message_list*}

示例：

```
ciscoasa(config)# logging monitor 6
```

步骤 2 启用仅到当前会话的日志记录。

terminal monitor

示例：

```
ciscoasa(config)# terminal monitor
```

如果注销然后再次登录，则需要重新输入此命令。输入 **terminal no monitor** 命令以禁用到当前会话的日志记录。

配置系统日志消息

在系统日志显示或隐藏无效用户名

在系统日志消息中可显示或隐藏登录尝试未成功的无效用户名。在默认情况下，如果用户名无效或者有效性未知时，用户名会被隐藏。例如当用户意外键入密码而不是用户名时，在生成的系统日志消息中隐藏“用户名”会更为安全。您可能希望利用显示的无效用户名对登录问题进行故障排除。

过程

步骤 1 显示无效用户名：

no logging hide username

步骤 2 隐藏无效用户名：

logging hide username

在系统日志消息中包含日期和时间

要在系统日志消息中包含日期和时间，请执行以下步骤：

过程

指定系统日志消息应包含其生成日期和时间。

logging timestamp

示例：

```
ciscoasa(config)# logging timestamp
LOG-2008-10-24-081856.TXT
```

要从系统日志消息中删除日期和时间，请输入 **no logging timestamp** 命令。

禁用系统日志消息

要禁用指定的系统日志消息，请执行以下步骤：

过程

阻止 ASA 生成特定系统日志消息。

no logging message *syslog_id*

示例：

```
ciscoasa(config)# no logging message 113019
```

要重新启用已禁用的系统日志消息，请输入 **logging message** *syslog_id* 命令（例如，**logging message 113019**）。要重新启用所有已禁用系统日志消息的日志记录，请输入 **clear configure logging disabled** 命令。

更改系统日志消息的严重性级别

要更改系统日志消息的严重性级别，请执行以下步骤：

过程

指定系统日志消息的严重性级别。

logging message *syslog_id* **level** *severity_level*

示例：

```
ciscoasa(config)# logging message 113019 level 5
```

要将系统日志消息的严重性级别重置为其设置，请输入 **no logging message***syslog_id***level***severity_level* 命令（例如 **no logging message 113019 level 5**）。要将所有已修改的系统日志消息的严重性级别重置为其设置，请输入 **clear configure logging level** 命令。

在备用设备上阻止系统日志消息

过程

使用以下命令阻止在备用单元上正在生成的特定系统日志消息。

no logging message *syslog-id* **standby**

示例：

```
ciscoasa(config)# no logging message 403503 standby
```

取消阻止特定的系统日志消息，以确保在发生故障转移的情况下，故障转移备用ASA的系统日志消息保持同步。使用 **logging standby** 命令取消阻止以前阻止在备用设备上生成的特定系统日志消息。

注释
当主用和备用 ASA 同时记录的稳定状态期间，共享日志记录目标（例如系统日志服务器、SNMP 服务器和 FTP 服务器）上的流量翻倍。但是，在发生故障转移时，在切换阶段，备用 ASA 会生成更多事件，包括主用设备的切换入侵和连接事件。

在非 EMBLEM 格式系统日志消息中包含设备 ID

要在非 EMBLEM 格式系统日志消息中包含设备 ID，请执行以下步骤：

过程

将 ASA 配置为在非 EMBLEM 格式系统日志消息中包含设备 ID。只能为系统日志指定一种类型的设备 ID。

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

示例：

```
ciscoasa(config)# logging device-id hostname
ciscoasa(config)# logging device-id context-name
```

context-name 关键字指示应用作设备 ID 的当前情景的名称（仅适用于多情景模式）。如果在多情景模式下为管理情景启用日志记录设备 ID，则源于系统执行空间中的消息使用设备 ID **system**，源于管理情景中的消息使用管理情景的名称作为设备 ID。

注释
在 ASA 集群中，始终使用所选接口的控制单元 IP 地址。

cluster-id 关键字指定集群中单个 ASA 设备的启动配置中的唯一名称作为设备 ID。**hostname** 关键字指定应用作设备 ID 的 ASA 的主机名。**ipaddress** *interface_name* 关键字/参数对指定应将指定为 *interface_name* 的接口 IP 地址用作设备 ID。如果使用 **ipaddress** 关键字，则无论从哪个接口发送系统日志消息，设备 ID 都会成为指定的 ASA 接口 IP 地址。在集群环境中，**system** 关键字指示设备 ID 成为接口上的系统 IP 地址。此关键字为从设备发送的所有系统日志消息提供单个一致的设备 ID。**string** *text* 关键字/参数对指定应将 text 字符串用作设备 ID。字符串可以包含多达 16 个字符。

不能使用空格或以下任何字符：

- &（与号）
- ‘（单引号）
- “（双引号）
- <（小于）
- >（大于）
- ?（问号）

注释
如果启用，则在 EMBLEM 格式化系统日志消息和 SNMP 陷阱中不会显示设备 ID。

创建自定义事件列表

可以使用以下三个条件来定义事件列表：

- 事件类
- 严重性
- 消息 ID

要创建将发送到特定日志记录目标（例如，SNMP 服务器）的自定义事件列表，请执行以下步骤：

过程

步骤 1 指定用于选择要保存在内部日志缓冲区中的消息的条件。例如，如果将严重性级别设置为 3，则 ASA 会发送严重性级别为 3、2 和 1 的系统日志消息。

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[-*end_id*]}

示例：

```
ciscoasa(config)# logging list list-notif level 3
```

姓名参数指定列表的名称。**level***level* 关键字-参数对指定严重性级别。**class** *message_class* 关键字/参数对指定特定消息类。**message** *start_id* [-*end_id*] 关键字/参数对指定单个系统日志消息编号或编号范围。

注释
请勿使用严重性级别的名称作为系统日志消息列表的名称。禁止的名称包括 emergencies、alert、critical、error、warning、notification、informational 和 debugging。同样，请勿在事件列表名称的开头使用这些单词的前三个字符。例如，请勿使用以字符“err”开头的事件列表名称。

步骤 2 （可选）向列表中添加更多消息选择条件。

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[-*end_id*]}

示例：

```
ciscoasa(config)# logging list list-notif message 104024-105999
ciscoasa(config)# logging list list-notif level critical
ciscoasa(config)# logging list list-notif level warning class ha
```

输入与上一步中相同的命令，指定现有消息列表的名称和其他条件。为要添加到列表的每个条件输入新命令。例如，可以将在列表中包含系统日志消息的条件指定如下：

- 日志消息 ID 属于范围 104024 至 105999。
- 所有系统日志消息都具有 critical 或更高的严重性级别（emergency、alert 或 critical）。
- 所有 ha 类系统日志消息都具有 warning 或更高的严重性级别（emergency、alert、critical、error 或 warning）。

注释
如果系统日志消息满足以下任何条件，则会将其记录。如果系统日志消息满足其中多个条件，则该消息仅记录一次。

配置日志记录过滤器

将类中的所有系统日志消息发送到指定输出目标

要将类中的所有系统日志消息发送到指定输出目标，请执行以下步骤：

过程

覆盖指定的输出目标命令中的配置。例如，如果指定严重性级别为 7 的消息应该转至内部日志缓冲区，并且严重性级别为 3 的 ha 类消息应该转至内部日志缓冲区，则后者配置优先。

logging class *message_class* {**buffered** | **console** | **history** | **mail** | **monitor** | **trap**} [*severity_level*]

示例：

```
ciscoasa(config)# logging class ha buffered alerts
```

buffered、**history**、**mail**、**monitor** 和 **trap** 关键字指定应将此类中的系统日志消息发送到的输出目标。**history** 关键字启用 SNMP 日志记录。**monitor** 关键字启用 Telnet 和 SSH 日志记录。**trap** 关键字启用系统日志服务器日志记录。每个命令行条目选择一个目标。要指定类应转至多个目标，请为每个输出目标输入一个新命令。

限制系统日志消息生成速率

要限制系统日志消息生成速率，请执行以下步骤：

过程

在指定时间段内将指定的严重性级别（1 至 7）应用于消息集或单条消息（不是目标）。

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

示例：

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

速率限制会影响发送到所有已配置的目标的消息量。要将日志记录速率限制重置为默认值，请输入 **clear running-config logging rate-limit** 命令。要重置日志记录速率限制，请输入 **clear configure logging rate-limit** 命令。

监控日志

请参阅以下命令来监控日志记录状态。

- **show logging**

  此命令显示系统日志消息，包括严重性级别。

注释 可供查看的最大系统日志消息数为1000，这是默认设置。可供查看的最大系统日志消息数为 2000。

- **show logging message**

  此命令显示严重性级别已修改的系统日志消息和已禁用的系统日志消息的列表。

- **show logging message** *message_ID*

  此命令显示特定系统日志消息的严重性级别。

- **show logging queue**

  此命令显示日志记录队列和队列统计信息。

- **show running-config logging rate-limit**

  此命令显示当前日志记录速率限制设置。

- **配置 > 防火墙 > 访问规则**

  此窗格允许您根据搜索条件（规则十六进制ID）将日志记录的实时查看器过滤为特定日志。要查看结果，请选择规则并点击**显示日志 (Show Log)**。

日志记录示例

以下示例显示所显示的有关 **show logging** 命令的日志记录信息。

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address “10.1.1.1”
    Mail logging: disabled
    ASDM logging: disabled


ciscoasa (config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: enabled
    Console logging: disabled
```

```
Monitor logging: disabled
Buffer logging: level debugging, 330272 messages logged
Trap logging: level debugging, facility 20, 325464 messages logged
    Logging to inside 2001:164:5:1::123
Permit-hostdown logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

以下示例显示如何同时控制是否启用了系统日志消息以及指定的系统日志消息的严重性级别：

```
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)

ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (disabled)

ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)
```

日志记录功能历史记录

表 *61:* 日志记录功能历史记录

功能名称	平台版本	说明
日志记录	7.0(1)	通过各种输出目标提供 ASA 网络日志记录信息，并包括查看和保存日志文件的选项。
速率限制	7.0(4)	限制生成系统日志消息的速率。 引入了以下命令：**logging rate-limit**。
日志记录列表	7.2(1)	创建要在其他命令中用于按各种条件（日志记录级别、事件类和消息 ID）指定消息的日志记录列表。 引入了以下命令：**logging list**。
安全日志记录	8.0(2)	指定与远程日志记录主机的连接应使用 SSL/TLS。仅在所选的协议为 TCP 的情况下此选项才有效。 修改了以下命令：**logging host**。

功能名称	平台版本	说明
日志记录类	8.0(4) 至 8.1(1)	添加了对日志记录消息的 ipaa 事件类的支持。 修改了以下命令：**logging class**。
日志记录类和已保存的日志记录缓冲区	8.2(1)	添加了对日志记录消息的 dap 事件类的支持。 修改了以下命令：**logging class**。 添加了对清除已保存的日志记录缓冲区（ASDM、内部、FTP 和闪存）的支持。 引入了以下命令：**clear logging queue bufferwrap**。
密码加密	8.3(1)	添加了对密码加密的支持。 修改了以下命令：**logging ftp server**。
日志查看器	8.3(1)	向日志查看器中添加了源 IP 地址和目标 IP 地址。
增强型日志记录和连接阻止	8.3(2)	当您将系统日志服务器配置为使用 TCP 且系统日志服务器不可用时，ASA 将阻止生成系统日志消息的新连接，直到该服务器重新变为可用状态（例如 VPN、防火墙和直接转发代理连接）。此外，此功能已增强，也能在 ASA 上的日志记录队列已满时阻止新连接；连接将在日志记录队列被清除后恢复。 为符合通用标准 EAL4+ 而添加了此功能。除非要求，否则建议在无法发送或接收系统日志消息时允许连接。要允许连接，请继续使用 **logging permit-hostdown**命令。 引入了以下系统日志消息：414005、414006、414007 和 414008。 修改了以下命令：**show logging**。
系统日志消息过滤和排序	8.4(1)	已为下列各项添加了支持： • 根据与各列对应的多个文本字符串过滤系统日志消息 • 创建自定义过滤器 • 对消息进行列排序。有关详细信息，请参阅 ASDM 配置指南。 此功能与所有 ASA 版本互操作。
集群	9.0(1)	添加了对集群环境下在 ASA 5580 和 5585-X 上生成系统日志消息的支持。 修改了以下命令：**logging device-id**。
在备用设备上阻止系统日志	9.4(1)	添加了对于在故障转移配置中的备用设备上阻止生成特定系统日志消息的支持。 引入了以下命令：**logging message** *syslog-id* **standby**。

功能名称	平台版本	说明
安全系统日志服务器连接的参考身份	9.6(2)	TLS 客户端处理现在支持针对 RFC 6125 第 6 节中定义的服务器身份验证的规则。身份验证将在对到系统日志服务器的 TLS 连接进行 PKI 验证期间进行。如果提供的标识无法与配置的引用标识相匹配，则不会建立连接。 添加或修改了以下命令：**[no] crypto ca reference-identity**、**logging host**。
系统日志服务器支持 IPv6 地址	9.7(1)	现在，您可以使用 IPv6 地址来配置系统日志服务器，从而通过 TCP 和 UDP 记录、发送和接收系统日志。 修改了以下命令：**logging host**
日志记录类	9.12(1)	添加了对 BFD、BGP、接口、IPv6、组播、对象组搜索、PBR、路由、SLA 类日志记录消息的支持。 修改了以下命令：**logging class**。
系统日志的环回接口支持	9.18(2)	您现在可以添加环回接口并用于系统日志： 新增/修改的命令： **interface loopback**、**logging host**
SNMP 系统日志的速率限制	9.20(1)	如果未设置系统范围的速率限制，那么您现在可以为发送到 SNMP 服务器的系统日志单独配置速率限制。 新增/修改的命令：**logging history rate-limit**

第 47 章

SNMP

本章介绍如何配置简单网络管理协议 (SNMP) 来监控 ASA。

- 关于 SNMP，第 1403 页
- SNMP 准则，第 1419 页
- 配置 SNMP，第 1422 页
- 监控 SNMP，第 1431 页
- SNMP 示例，第 1433 页
- SNMP 的历史记录，第 1433 页

关于 SNMP

SNMP 是促进网络设备之间的管理信息交换的应用层协议，并且是 TCP/IP 协议套件的一部分。ASA 使用 SNMP 第 1、2c 和 3 版为网络监控提供支持，并且支持同时使用所有三个版本。利用在 ASA 接口上运行的 SNMP 代理，您可以通过诸如 HP OpenView 之类的网络管理系统 (NMS) 监控网络设备。ASA 通过发出 GET 请求来支持 SNMP 只读访问。不允许 SNMP 写访问，因此您无法对 SNMP 进行更改。此外，不支持 SNMP SET 请求。

您可以将 ASA 配置为向 NMS 发送陷阱，即针对特定事件从托管设备发送到管理站的未经请求的消息（事件通知），也可以使用 NMS 浏览安全设备上的管理信息库 (MIB)。MIB 是定义的集合，而 ASA 维护由每个定义的值组成的数据库。浏览 MIB 意味着从 NMS 发出 MIB 树的一系列 GET-NEXT 或 GET-BULKGET 请求以确定值。

注释 对于密集型工作负载，部署超过 10 个 NMS 可能会影响设备的性能。为确保设备的稳定性和响应速度，我们建议您谨慎使用 NMS 进行 SNMP 漫游轮询和管理陷阱流量。

ASA 具有 SNMP 代理，用于在发生预定义为需要通知（例如，当网络中的链路开启或关闭时）的事件的情况下通知指定的管理站。它发送的通知包括用于向管理站表明其自身身份 SNMP OID。ASA 代理还会在管理站请求信息时进行回复。

SNMP 术语

下表列出在使用 SNMP 时常用的术语。

表 *62: SNMP* 术语

术语	说明
代理	在 ASA 上运行的 SNMP 服务器。SNMP 代理具有以下功能： • 对来自网络管理站的信息和操作请求作出响应。 • 控制对其管理信息库（即 SNMP 可以查看或更改的对象的集合）的访问。 • 不允许 SET 操作。
浏览	通过从设备上的 SNMP 代理轮询所需信息来从网络管理站监控该设备的运行状况。此活动可能包括从网络管理站发出 MIB 树的一系列 GET-NEXT 或 GET-BULK 请求以确定值。
管理信息库 (MIB)	用于收集有关数据包、连接、缓冲区、故障转移等的信息的标准化数据结构。MIB 由大多数网络设备使用的产品、协议和硬件标准来定义。SNMP 网络管理站可以浏览 MIB，并请求在出现特定数据或事件时将其发送。
网络管理站 (NMS)	设置 PC 或工作站是为了监控 SNMP 事件和管理设备，例如 ASA。
对象标识符 (OID)	用于向设备的 NMS 表明该设备的身份并向用户指示监控和显示的信息源的系统。
陷阱	用于生成从 SNMP 代理到 NMS 的消息的预定义事件。事件包括警报条件，例如链路开启、链路关闭、冷启动、热启动、身份验证或系统日志消息。

MIB 和陷阱

MIB 特定于标准或特定于企业。标准 MIB 由 IETF 创建并记录在各种 RFC 中。陷阱报告发生在网络设备上的重大事件，大多数情况下是错误或故障。SNMP 陷阱在特定于标准或特定于企业的 MIB 中进行定义。标准陷阱由 IETF 创建并记录在各种 RFC 中。SNMP 陷阱会编译成 ASA 软件。

如果需要，您还可以从以下位置下载 RFC、标准 MIB 和标准陷阱：

http://www.ietf.org/

从以下位置浏览思科 MIB、陷阱和 OID 的完整列表：

https://github.com/cisco/cisco-mibs/blob/main/supportlists/asa/asa-supportlist.html

此外，从以下位置通过 FTP 下载思科 OID：

https://github.com/cisco/cisco-mibs/tree/main/oid

注释 在软件 7.2(1) 版、8.0(2) 版及更高版本中，通过 SNMP 访问的接口信息大约每 5 秒刷新一次。因此，我们建议在连续的轮询之间等待至少 5 秒。

在 MIB 中，并非所有 OID 都受支持。要获取特定 ASA 的受支持 SNMP MIB 和 OID 的列表，请输入以下命令：

```
ciscoasa(config)# show snmp-server oidlist
```

注释 尽管 **oidlist** 关键字没有显示在 **show snmp-server** 命令的选项列表中，但它是可用的。但是，此命令仅供思科 TAC 使用。使用此命令之前，请联系思科 TAC。

以下是 **show snmp-server oidlist** 命令的输出示例：

```
ciscoasa(config)# show snmp-server oidlist
[0]     1.3.6.1.2.1.1.1.        sysDescr
[1]     1.3.6.1.2.1.1.2.        sysObjectID
[2]     1.3.6.1.2.1.1.3.        sysUpTime
[3]     1.3.6.1.2.1.1.4.        sysContact
[4]     1.3.6.1.2.1.1.5.        sysName
[5]     1.3.6.1.2.1.1.6.        sysLocation
[6]     1.3.6.1.2.1.1.7.        sysServices
[7]     1.3.6.1.2.1.2.1.        ifNumber
[8]     1.3.6.1.2.1.2.2.1.1.    ifIndex
[9]     1.3.6.1.2.1.2.2.1.2.    ifDescr
[10]    1.3.6.1.2.1.2.2.1.3.    ifType
[11]    1.3.6.1.2.1.2.2.1.4.    ifMtu
[12]    1.3.6.1.2.1.2.2.1.5.    ifSpeed
[13]    1.3.6.1.2.1.2.2.1.6.    ifPhysAddress
[14]    1.3.6.1.2.1.2.2.1.7.    ifAdminStatus
[15]    1.3.6.1.2.1.2.2.1.8.    ifOperStatus
[16]    1.3.6.1.2.1.2.2.1.9.    ifLastChange
[17]    1.3.6.1.2.1.2.2.1.10.   ifInOctets
[18]    1.3.6.1.2.1.2.2.1.11.   ifInUcastPkts
[19]    1.3.6.1.2.1.2.2.1.12.   ifInNUcastPkts
[20]    1.3.6.1.2.1.2.2.1.13.   ifInDiscards
[21]    1.3.6.1.2.1.2.2.1.14.   ifInErrors
[22]    1.3.6.1.2.1.2.2.1.16.   ifOutOctets
[23]    1.3.6.1.2.1.2.2.1.17.   ifOutUcastPkts
[24]    1.3.6.1.2.1.2.2.1.18.   ifOutNUcastPkts
[25]    1.3.6.1.2.1.2.2.1.19.   ifOutDiscards
[26]    1.3.6.1.2.1.2.2.1.20.   ifOutErrors
[27]    1.3.6.1.2.1.2.2.1.21.   ifOutQLen
[28]    1.3.6.1.2.1.2.2.1.22.   ifSpecific
[29]    1.3.6.1.2.1.4.1.        ipForwarding
[30]    1.3.6.1.2.1.4.20.1.1.   ipAdEntAddr
[31]    1.3.6.1.2.1.4.20.1.2.   ipAdEntIfIndex
[32]    1.3.6.1.2.1.4.20.1.3.   ipAdEntNetMask
[33]    1.3.6.1.2.1.4.20.1.4.   ipAdEntBcastAddr
[34]    1.3.6.1.2.1.4.20.1.5.   ipAdEntReasmMaxSize
[35]    1.3.6.1.2.1.11.1.       snmpInPkts
[36]    1.3.6.1.2.1.11.2.       snmpOutPkts
[37]    1.3.6.1.2.1.11.3.       snmpInBadVersions
[38]    1.3.6.1.2.1.11.4.       snmpInBadCommunityNames
```

```
[39]    1.3.6.1.2.1.11.5.       snmpInBadCommunityUses
[40]    1.3.6.1.2.1.11.6.       snmpInASNParseErrs
[41]    1.3.6.1.2.1.11.8.       snmpInTooBigs
[42]    1.3.6.1.2.1.11.9.       snmpInNoSuchNames
[43]    1.3.6.1.2.1.11.10.      snmpInBadValues
[44]    1.3.6.1.2.1.11.11.      snmpInReadOnlys
[45]    1.3.6.1.2.1.11.12.      snmpInGenErrs
[46]    1.3.6.1.2.1.11.13.      snmpInTotalReqVars
[47]    1.3.6.1.2.1.11.14.      snmpInTotalSetVars
[48]    1.3.6.1.2.1.11.15.      snmpInGetRequests
[49]    1.3.6.1.2.1.11.16.      snmpInGetNexts
[50]    1.3.6.1.2.1.11.17.      snmpInSetRequests
[51]    1.3.6.1.2.1.11.18.      snmpInGetResponses
[52]    1.3.6.1.2.1.11.19.      snmpInTraps
[53]    1.3.6.1.2.1.11.20.      snmpOutTooBigs
[54]    1.3.6.1.2.1.11.21.      snmpOutNoSuchNames
[55]    1.3.6.1.2.1.11.22.      snmpOutBadValues
[56]    1.3.6.1.2.1.11.24.      snmpOutGenErrs
[57]    1.3.6.1.2.1.11.25.      snmpOutGetRequests
[58]    1.3.6.1.2.1.11.26.      snmpOutGetNexts
[59]    1.3.6.1.2.1.11.27.      snmpOutSetRequests
[60]    1.3.6.1.2.1.11.28.      snmpOutGetResponses
[61]    1.3.6.1.2.1.11.29.      snmpOutTraps
[62]    1.3.6.1.2.1.11.30.      snmpEnableAuthenTraps
[63]    1.3.6.1.2.1.11.31.      snmpSilentDrops
[64]    1.3.6.1.2.1.11.32.      snmpProxyDrops
[65]    1.3.6.1.2.1.31.1.1.1.1. ifName
[66]    1.3.6.1.2.1.31.1.1.1.2. ifInMulticastPkts
[67]    1.3.6.1.2.1.31.1.1.1.3. ifInBroadcastPkts
[68]    1.3.6.1.2.1.31.1.1.1.4. ifOutMulticastPkts
[69]    1.3.6.1.2.1.31.1.1.1.5. ifOutBroadcastPkts
[70]    1.3.6.1.2.1.31.1.1.1.6. ifHCInOctets
--More--
```

SNMP 对象标识符

每个思科系统级产品都具有供用作 MIB-II sysObjectID 的 SNMP 对象标识符 (OID)。CISCO-PRODUCTS-MIB 和 CISCO-ENTITY-VENDORTYPE-OID-MIB 包括可在 SNMPv2-MIB、Entity Sensor MIB 和 Entity Sensor Threshold Ext MIB 内的 sysObjectID 对象中报告的 OID。您可以使用此值标识型号。下表列出了不同型号 ASA 和 ISA 的 sysObjectID OID。

表 *63: SNMP* 对象标识符

产品标识符	**sysObjectID**	型号编号
ASA Virtual	ciscoASAv (ciscoProducts 1902)	思科自适应安全虚拟设备 (ASA virtual)
ASA Virtual 系统情景	ciscoASAvsy (ciscoProducts 1903)	思科自适应安全虚拟设备 (ASA virtual) 系统情景
ASA Virtual 安全情境	ciscoASAvsc (ciscoProducts 1904)	思科自适应安全虚拟设备 (ASA virtual) 安全情景.

产品标识符	sysObjectID	型号编号
Cisco Secure Firewall 1200	ciscoCsf1210ce (ciscoProducts 3303) ciscoCsf1210cp (ciscoProducts 3304) ciscoCsf1220cx (ciscoProducts 3305)	CSF1210CE, CSF1210CP, CSF1220CX
Cisco Secure Firewall 4200	ciscoFpr4215td (ciscoProducts 3043) ciscoFpr4225td (ciscoProducts 3042) ciscoFpr4245td (ciscoProducts 3041)	FPR4215, FPR4225, FPR4245
ISA 30004C 工业安全设备	ciscoProducts 2268	ciscoISA30004C
带有 4 GE 铜缆安全情景的思科 ISA30004C	ciscoProducts 2139	ciscoISA30004Csc
带有 4 GE 铜缆系统情景的思科 ISA30004C	ciscoProducts 2140	ciscoISA30004Csy
ISA 30002C2F 工业安全设备	ciscoProducts 2267	ciscoISA30002C2F
带有 2 GE 铜缆端口 + 2 GE 光纤安全情景的思科 ISA30002C2F	ciscoProducts 2142	ciscoISA30002C2Fsc
带有 2 GE 铜缆端口 + 2 GE 光纤系统情景的思科 ISA30002C2F	ciscoProducts 2143	ciscoISA30002C2Fsy
思科工业安全设备 (ISA) 30004C 机箱	cevChassis 1677	cevChassisISA30004C
思科工业安全设备 (ISA) 30002C2F 机箱	cevChassis 1678	cevChassisISA30002C2F
适用于 ISA30004C 铜缆 SKU 的中央处理单元温度传感器	cevSensor 187	cevSensorISA30004CCpuTempSensor
适用于 ISA30002C2F 光纤的中央处理单元温度传感器	cevSensor 189	cevSensorISA30002C2FCpuTempSensor
适用于 ISA30004C 铜缆 SKU 的处理器卡温度传感器	cevSensor 192	cevSensorISA30004CPTS
适用于 ISA30002C2F 光纤 SKU 的处理器卡温度传感器	cevSensor 193	cevSensorISA30002C2FPTS
适用于 ISA30004C 铜缆 SKU 的电源卡温度传感器	cevSensor 197	cevSensorISA30004CPowercardTS
适用于 ISA30002C2F 光纤 SKU 的电源卡温度传感器	cevSensor 198	cevSensorISA30002C2FPowercardTS
适用于 ISA30004C 的端口卡温度传感器	cevSensor 199	cevSensorISA30004CPortcardTS

产品标识符	sysObjectID	型号编号
适用于 ISA30002C2F 的端口卡温度传感器	cevSensor 200	cevSensorISA30002C2FPortcardTS
适用于 ISA30004C 铜缆 SKU 的中央处理单元	cevModuleCpuType 329	cevCpuISA30004C
适用于 ISA30002C2F 光纤 SKU 的中央处理单元	cevModuleCpuType 330	cevCpuISA30002C2F
模块 ISA30004C、ISA30002C2F	cevModule 111	cevModuleISA3000Type
30004C 工业安全设备固态硬盘	cevModuleISA3000Type 1	cevModuleISA30004CSSD64
30002C2F 工业安全设备固态硬盘	cevModuleISA3000Type 2	cevModuleISA30002C2FSSD64
思科 ISA30004C/ISA30002C2F 硬件旁路	cevModuleISA3000Type 5	cevModuleISA3000HardwareBypass
Cisco Secure Firewall 1210CE 机箱	cevChassis 2580	cevChassisCsf1210ce
Cisco Secure Firewall 1210CP 机箱	cevChassis 2581	cevChassisCsf1210cp
Cisco Secure Firewall 1220CX 机箱	cevChassis 2582	cevChassisCsf1220cx
Cisco Secure Firewall 1200 系列风扇	cevFan 468	cevFanCsf1200
Cisco Secure Firewall 1220CX 的中央处理器	cevModuleCpuType 380	cevCpuCsf1220cx
Cisco Secure Firewall 1210CP 的中央处理器	cevModuleCpuType 381	cevCpuCsf1210cp
Cisco Secure Firewall 1210CE 的中央处理器	cevModuleCpuType 382	`cevCpuCsf1210ce`
FirePOWER 4140 安全设备，1U，带有内置安全模块 36	ciscoFpr4140K9 (ciscoProducts 2293)	FirePOWER 4140
FirePOWER 4120 安全设备，1U，带有内置安全模块 24	ciscoFpr4120K9 (ciscoProducts 2294)	FirePOWER 4120
FirePOWER 4K 风扇槽位	cevContainer 363	cevContainerFPR4KFanBay
FirePOWER 4K 电源槽位	cevContainer 364	cevContainerFPR4KPowerSupplyBay
Cisco Cisco Secure Firewall Threat Defense Virtual、VMware	cevChassis 1795	cevChassisCiscoFTDVVMW
Cisco Threat Defense Virtual、 AWS	cevChassis 1796	cevChassisCiscoFTDVAWS

物理供应商类型值

每个思科机箱或独立系统都具有供 SNMP 使用的唯一类型编号。entPhysicalVendorType OID 在 CISCO-ENTITY-VENDORTYPE-OID-MIB 中进行定义。此值在 ASA、 ASA virtual或 ASASM SNMP 代理的 entPhysicalVendorType 对象中返回。您可以使用此值标识组件的类型（模块、电源、风扇、传感器、CPU 等）。下表列出用于各型号 ASA 的物理供应商类型值。

表 *64:* 物理供应商类型值

项目	**entPhysicalVendorType OID** 说明
千兆以太网端口	cevPortGe (cevPort 109)
思科自适应安全虚拟设备	cevChassisASAv (cevChassis 1451)
Cisco Secure Firewall 4200-X (FPR4215/FPR4225/FPR4245)	cevFPRNM4X200Gng 和 cevFPRNM2X100Gng（为插槽 2 和插槽 3 添加的双 EPM 2X100G 和 4X200G）

MIB 中支持的表格和对象

下表列出对指定 MIB 支持的表和对象。

在多情景模式下，这些表和对象提供单个情景的信息。如果需要跨情景的数据，则需要对它们求和。例如，要获取整体内存使用率，请对每个情景的cempMemPoolHCUsed值求和。

表 *65: MIB* 中支持的表格和对象

MIB 名称和 **OID**	支持的表和对象
ENTITY-MIB; OID:1.3.6.1.2.1.47	entPhysicalTable, entPhysicalDescr, entPhysicalVendorType, entPhysicalName

MIB 名称和 OID	支持的表和对象
CISCO-ENHANCED-MEMPOOL-MIB; OID:1.3.6.1.4.1.9.9.221	cempMemPoolTable、cempMemPoolIndex、cempMemPoolType、cempMemPoolName、cempMemPoolAlternate、cempMemPoolValid。 对于 32 位内存系统，使用 32 位内存计数器进行轮询—cempMemPoolUsed、 cempMemPoolFree、cempMemPoolUsedOvrflw、 cempMemPoolFreeOvrflw、cempMemPoolLargestFree、 cempMemPoolLowestFree、cempMemPoolUsedLowWaterMark、 cempMemPoolAllocHit、cempMemPoolAllocMiss、 cempMemPoolFreeHit、cempMemPoolFreeMiss、 cempMemPoolLargestFreeOvrflw、cempMemPoolLowestFreeOvrflw、cempMemPoolUsedLowWaterMarkOvrflw、cempMemPoolSharedOvrflw。 对于 64 位内存系统，使用 64 位内存计数器进行轮询 - cempMemPoolHCUsed、cempMemPoolHCFree、cempMemPoolHCLargestFree、cempMemPoolHCLowestFree、cempMemPoolHCUsedLowWaterMark、cempMemPoolHCShared
CISCO-REMOTE-ACCESS-MONITOR-MIB; OID:1.3.6.1.4.1.9.9.392 注释 这三个MIB OID可用于跟踪远程访问连接失败的原因。	crasNumTotalFailures，crasNumSetupFailInsufResources，crasNumAbortedSessions
CISCO-ENTITY-SENSOR-EXT-MIB; OID:1.3.6.1.4.1.9.9.745	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB; OID:1.3.6.1.4.1.9.9.480	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB; OID:1.3.6.1.4.1.9.9.720 注释 ASA virtual上不支持。	ctsxSxpGlobalObjects、ctsxSxpConnectionObjects、ctsxSxpSgtObjects
DISMAN-EVENT-MIB; OID:1.3.6.1.2.1.88	mteTriggerTable、mteTriggerThresholdTable、mteObjectsTable、mteEventTable、mteEventNotificationTable
DISMAN-EXPRESSION-MIB; OID:1.3.6.1.2.1.90	expExpressionTable、expObjectTable、expValueTable

MIB 名称和 OID	支持的表和对象
ENTITY-SENSOR-MIB; OID: 1.3.6.1.2.1.99 注释 提供与物理传感器相关的信息，例如机箱温度，风扇RPM，电源电压等。 ASA virtual 平台不支持。	entPhySensorTable
NAT-MIB; OID:1.3.6.1.2.1.123	natAddrMapTable、natAddrMapIndex、natAddrMapName、natAddrMapGlobalAddrType、natAddrMapGlobalAddrFrom、natAddrMapGlobalAddrTo、natAddrMapGlobalPortFrom、natAddrMapGlobalPortTo、natAddrMapProtocol、natAddrMapAddrUsed、natAddrMapRowStatus
CISCO-PTP-MIB; OID:1.3.6.1.4.1.9.9.760 注释 只有与 E2E 透明时钟模式对应的 MIB 受支持。	ciscoPtpMIBSystemInfo、cPtpClockDefaultDSTable、cPtpClockTransDefaultDSTable、cPtpClockPortTransDSTable
CISCO-PROCESS-MIB; 1.3.6.1.4.1.9.9.109.1.1.1.1.7.1 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 至 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	cpmCPUTotal1minRev cpmCPUTotal1minRev 的关联参数和值 示例： • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2) - 聚合系统 CPU 使用率百分比（此值与单情景模式下 .3.6.1.4.1.9.9.109.1.1.1.1.7.1 中的系统 CPU 使用率相同）。 • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3) - Snort 平均 CPU 使用率百分比（所有 snort 实例的总值） • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4) - 系统进程平均百分比（“Sysproc”核心的平均值）

支持的陷阱（通知）

下表列出支持的陷阱（通知）及其关联 MIB。

表 *66:* 支持的陷阱（通知）

陷阱和 **MIB** 名称	**Varbind** 列表	说明
authenticationFailure (SNMPv2-MIB)	-	对于 SNMP 第 1 版或第 2 版，SNMP 请求中提供的社区字符串不正确。对于 SNMP 第 3 版，如果 auth 或 priv 关键字或用户名不正确，则会生成报告 PDU 而不是陷阱。 **snmp-server enable traps snmp authentication** 命令用于启用和禁用这些陷阱的传输。
bgpBackwardTransition	bgpPeerLastError、bgpPeerState	**snmp-server enable traps peer-flap** 命令用于启用此陷阱的传输。
ccmCLIRunningConfigChanged (CISCO-CONFIG-MAN-MIB)	ccmHistoryRunningLastChanged、ccmHistoryEventTerminalType	**snmp-server enable traps config** 命令用于启用此陷阱的传输。
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	**snmp-server enable traps entity fru-insert** 命令用于启用此通知。
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	**snmp-server enable traps entity fru-remove** 命令用于启用此通知。

陷阱和 **MIB** 名称	**Varbind** 列表	说明
ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)	entPhysicalName、 entPhysicalDescr、 entPhySensorValue、 entPhySensorType、 ceSensorExtThresholdValue	**snmp-server enable traps entity** [**power-supply-failure** | **fan-failure** | **cpu-temperature**] 命令用于启用实体阈值通知的传输。系统会针对电源故障发送此通知。所发送的对象会识别风扇和 CPU 温度。 **snmp-server enable traps entity fan-failure** 命令用于启用风扇故障陷阱的传输。此陷阱不适用于 Firepower 2100 系列。 **snmp-server enable traps entity power-supply-failure** 命令用于启用电源故障陷阱的传输。 **snmp-server enable traps entity chassis-fan-failure** 命令用于启用机箱风扇故障陷阱的传输。 **snmp-server enable traps entity cpu-temperature** 命令用于启用高 CPU 温度陷阱的传输。 **snmp-server enable traps entity power-supply-presence** 命令用于启用电源状态故障陷阱的传输。 **snmp-server enable traps entity power-supply-temperature** 命令用于启用电源温度阈值陷阱的传输。 **snmp-server enable traps entity chassis-temperature** 命令用于启用机箱环境温度陷阱的传输。 **snmp-server enable traps entity accelerator-temperature** 命令用于启用机箱加速器温度陷阱的传输。
cikeTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr、 cikePeerRemoteAddr、 cikeTunLifeTime	**snmp-server enable traps ikev2 start** 命令用于启用此陷阱的传输。
cikeTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr、 cikePeerRemoteAddr、 cikeTunActiveTime	**snmp-server enable traps ikev2 stop** 命令用于启用此陷阱的传输。
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunLifeTime, cipSecTunLifeSize	**snmp-server enable traps ipsec start** 命令用于启用此陷阱的传输。

陷阱和 **MIB** 名称	**Varbind** 列表	说明
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunActiveTime	**snmp-server enable traps ipsec stop** 命令用于启用此陷阱的传输。
ciscoConfigManEvent (CISCO-CONFIG-MAN-MIB)	ccmHistoryEventCommandSource, ccmHistoryEventConfigSource, ccmHistoryEventConfigDestination	**snmp-server enable traps config** 命令用于启用此陷阱的传输。
ciscoRasTooManySessions (CISCO-REMOTE-ACCESS-MONITOR-MIB)	crasNumSessions、 crasNumUsers、 crasMaxSessionsSupportable、 crasMaxUsersSupportable、 crasThrMaxSessions	**snmp-server enable traps remote-access session-threshold-exceeded** 命令用于启用这些陷阱的传输。
ciscoUFwFailoverStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	gid, FOStatus	**snmp-server enable traps failover-state** 命令用于启用此陷阱的传输。
clogMessageGenerated (CISCO-SYSLOG-MIB)	clogHistFacility、 clogHistSeverity、 clogHistMsgName、 clogHistMsgText、 clogHistTimestamp	系统将生成系统日志消息。 clogMaxSeverity 对象的值用于决定哪些系统日志消息作为陷阱发送。 **snmp-server enable traps syslog** 命令用于启用和禁用这些陷阱的传输。
clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB)	crlResourceLimitValueType、 crlResourceLimitMax、 clogOriginIDType、clogOriginID	**snmp-server enable traps connection-limit-reached** 命令用于启用 connection-limit-reached 通知的传输。clogOriginID 对象包括陷阱源于的情景名称。
coldStart (SNMPv2-MIB)	-	配置 SNMP 后，SNMP 代理启动时发生的 coldStart 陷阱。当代理在系统重启后启动时，也会出现此陷阱。 **注释** 对于集群和HA节点，重载后，如果接口重启时间超过5分钟（预设阈值），陷阱就会被丢弃。当集群和HA节点重启成功后，所有其他陷阱都会按预期发送。 **snmp-server enable traps snmp coldstart** 命令用于启用和禁用这些陷阱的传输。

陷阱和 **MIB** 名称	**Varbind** 列表	说明
cpmCPURisingThreshold (CISCO-PROCESS-MIB)	cpmCPURisingThresholdValue、cpmCPUTotalMonIntervalValue、cpmCPUInterruptMonIntervalValue、cpmCPURisingThresholdPeriod、cpmProcessTimeCreated、cpmProcExtUtil5SecRev	**snmp-server enable traps cpu threshold rising** 命令用于启用 CPU threshold rising 通知的传输。cpmCPURisingThresholdPeriod 对象与其他对象一起发送。
cufwClusterStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	status	**snmp-server enable traps cluster-state** 命令用于启用此陷阱的传输。
entConfigChange (ENTITY-MIB)	-	**snmp-server enable traps entity config-change fru-insert fru-remove** 命令用于启用此通知。 注释 仅当创建或删除了安全情景时，才会以多模方式发送此通知。
linkDown (IF-MIB)	ifIndex、ifAdminStatus、ifOperStatus	接口的链路关闭陷阱。 **snmp-server enable traps snmp linkdown** 命令用于启用和禁用这些陷阱的传输。
linkUp (IF-MIB)	ifIndex、ifAdminStatus、ifOperStatus	接口的链路开启陷阱。 **snmp-server enable traps snmp linkup** 命令用于启用和禁用这些陷阱的传输。
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、mteHotValue、cempMemPoolName、cempMemPoolHCUsed	**snmp-server enable traps memory-threshold** 命令用于启用内存阈值通知。mteHotOID 设置为 cempMemPoolHCUsed。cempMemPoolName 和 cempMemPoolHCUsed 对象与其他对象一起发送。
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、mteHotValue、ifHCInOctets、ifHCOutOctets、ifHighSpeed、entPhysicalName	**snmp-server enable traps interface-threshold** 命令用于启用接口阈值通知。entPhysicalName 对象将与其他对象一起发送。
natPacketDiscard (NAT-MIB)	ifIndex	**snmp-server enable traps nat packet-discard** 命令用于启用 NAT 数据包丢弃通知。此通知会受到时长为 5 分钟的速率限制，并且是在 IP 数据包因映射空间不可用而被 NAT 丢弃的情况下生成。ifIndex 提供映射接口的 ID。

陷阱和 **MIB** 名称	**Varbind** 列表	说明
ospfNbrStateChange	ospfRouterId, ospfNbrIpAddr, ospfNbrAddressLessIndex, ospfNbrRtrId, ospfNbrState	**snmp-server enable traps peer-flap** 命令用于启用此陷阱的传输。 注释 对于 ASA5585 型号，SNMP 引擎已更改为使用 netsnmp 5.8 版库，库中不提供以下 OID： • ospfIfStateChange 1.3.6.1.2.1.14.16.2.16 • ospfVirtIfStateChange 1.3.6.1.2.1.14.16.2.1 • ospfVirtNbrStateChange 1.3.6.1.2.1.14.16.2.3
warmStart (SNMPv2-MIB)	-	SNMP 代理首次重启时发出的 warmStart 陷阱。当代理在 SNMP 配置更改后重新启动时，所有 SNMP 主机配置都会被移除，并重新进行 SNMP 配置，这时也会出现此陷阱。 **snmp-server enable traps snmp warmstart** 命令用于启用和禁用这些陷阱的传输。

接口类型和示例

产生 SNMP 流量统计信息的接口类型包括：

- 逻辑 - 由软件驱动程序收集的统计信息，它是物理统计信息的子集。
- 物理 - 由硬件驱动程序收集的统计信息。每个物理指定接口具有一组与其关联的逻辑和物理统计信息。每个物理接口可能具有多个与其关联的 VLAN 接口。VLAN 接口仅具有逻辑统计信息。

注释 对于具有多个与其关联的 VLAN 接口的物理接口，请注意，ifInOctets OID 和 ifOutoctets OID 的 SNMP 计数器会与该物理接口的汇聚流量计数器相匹配。

- VLAN 专用 - SNMP 使用 ifInOctets 和 ifOutOctets 的逻辑统计信息。

下表中的示例显示 SNMP 流量统计信息中的差异。示例 1 显示对于 **show interface** 命令和 **show traffic** 命令而言物理与逻辑输出统计信息中的差异。示例 2 显示对于 **show interface** 命令和 **show traffic** 命令而言 VLAN 专用接口的输出统计信息。示例表明统计信息接近于为 **show traffic** 命令显示的输出。

表 *67:* 物理接口和 ***VLAN*** 接口的 ***SNMP*** 流量统计信息

示例 1	示例 2
ciscoasa# **show interface GigabitEthernet3/2** interface GigabitEthernet3/2 description fullt-mgmt nameif mgmt security-level 10 ip address 10.7.14.201 255.255.255.0 management-only ciscoasa# **show traffic** (Condensed output) Physical Statistics GigabitEthernet3/2: received (in 121.760 secs) **36 packets 3428 bytes** 0 pkts/sec 28 bytes/sec Logical Statistics mgmt: received (in 117.780 secs) **36 packets 2780 bytes** 0 pkts/sec 23 bytes/sec 以下示例显示管理接口和物理接口的SNMP输出统计信息。ifInOctets值接近于**show traffic** 命令输出中显示的物理统计信息输出，但不接近于逻辑统计信息输出。 管理接口的 ifIndex： IF_MIB::ifDescr.6 = Adaptive Security Appliance ‘mgmt’ interface 对应于物理接口 统计信息的 ifInOctets： **IF-MIB::ifInOctets.6 = Counter32:3246**	ciscoasa# **show interface GigabitEthernet** interface GigabitEthernet0/0.100 vlan 100 nameif inside security-level 100 ip address 10.7.1.101 255.255.255.0 stan ciscoasa# **show traffic** inside received (in 9921.450 secs) **1977 packets 126528 bytes** 0 pkts/sec 12 bytes/sec transmitted (in 9921.450 secs) **1978 packets 126556 bytes** 0 pkts/sec 12 bytes/sec VLAN 内部的 ifIndex： IF-MIB::ifDescr.9 = Adaptive Security Ap **IF-MIB::ifInOctets.9 = Counter32: 126318**

SNMP 第 3 版概述

SNMP 第 3 版提供第 1 版或第 2c 版中没有的安全增强功能。SNMP 第 1 版和第 2c 版以明文形式在 SNMP 服务器和 SNMP 代理之间传输数据。SNMP 第 3 版向安全协议操作中添加了身份验证和隐私选项。此外，此版本通过基于用户的安全模式 (USM) 和基于视图的访问控制模式 (VACM) 控制对 SNMP 代理和 MIB 对象的访问。ASA 还支持创建 SNMP 组和用户，以及为安全 SNMP 通信启用传输身份验证和加密所需的主机。

安全模型

为进行配置，身份验证和隐私选项会共同组成安全模式。安全模式应用于用户和组，它们分为以下三种类型：

- NoAuthPriv - 无身份验证且无隐私，意味着未对消息应用安全设置。
- AuthNoPriv - 有身份验证但无隐私，意味着消息会进行身份验证。
- AuthPriv - 有身份验证并有隐私，意味着消息会进行身份验证并加密。

SNMP 组

SNMP 组是可以将用户添加到的访问控制策略。每个 SNMP 组配置有安全模式，并与 SNMP 视图关联。SNMP 组内的用户必须与 SNMP 组的安全模式匹配。这些参数指定 SNMP 组内的用户使用的身份验证和隐私类型。每个 SNMP 组名称/安全模式对必须唯一。

SNMP 用户

SNMP 用户具有指定的用户名、用户所属的组、身份验证密码、加密密码，以及要使用的身份验证和加密算法。身份验证算法选项包括 SHA-1、SHA-224、SHA-256 HMAC 和 SHA-384。加密算法选项为 3DES 和 AES（在 128、192 和 256 版中可用）。创建用户时，必须将其与 SNMP 组相关联。然后，用户将继承该组的安全模式。

注释 配置 SNMP v3 用户账户时，请确保身份验证算法的长度等于或大于加密算法的长度。

SNMP 主机

SNMP 主机是 SNMP 通知和陷阱所发送到的 IP 地址。要配置 SNMP 第 3 版主机及目标 IP 地址，必须配置用户名，因为陷阱仅发送到已配置的用户。SNMP 目标 IP 地址和目标参数名称在 ASA 上必须唯一。每个 SNMP 主机只能具有一个与其关联的用户名。要接收 SNMP 陷阱，请在添加 **snmp-server host** 命令后，确保将 NMS 上的用户凭证配置为与 ASA 的凭证相匹配。

注释 最多可以添加 8192 台主机。但是，其中仅 128 台可用于陷阱。

ASA 和思科 IOS 软件之间的实施差异

ASA 中的 SNMP 第 3 版实施在以下方面不同于思科 IOS 软件中的 SNMP 第 3 版实施：

- 本地引擎和远程引擎 ID 为不可配置。本地引擎 ID 是在 ASA 启动时或者创建了情景时生成。
- 不支持基于视图的访问控制，导致 MIB 浏览不受限制。
- 支持限于以下 MIB：USM、VACM、FRAMEWORK 和 TARGET。
- 您必须使用正确的安全模式创建用户和组。
- 您必须按正确的顺序删除用户、组和主机。
- 使用 snmp - server host 命令创建 ASA 规则以允许传入 SNMP 流量。

SNMP 系统日志消息传递

SNMP 生成编号为 212*nnn* 的详细系统日志消息。系统日志消息向指定接口上的指定主机表明 SNMP 请求、SNMP 陷阱、SNMP 信道和来自 ASA 或 ASASM 的 SNMP 响应的状态。

有关系统日志消息的详细信息，请参阅系统日志消息指南。

注释 如果 SNMP 系统日志消息超过较高的速率（约 4000 条/秒），则 SNMP 轮询将失败。

应用服务和第三方工具

有关 SNMP 支持的信息，请参阅以下 URL：

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

有关使用第三方工具处理 SNMP 第 3 版 MIB 的信息，请参阅以下 URL：

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP 准则

本节介绍您在配置 SNMP 之前应查看的准则和限制。

故障转移和集群准则

- 将 SNMPv3 用于集群或故障转移时，如果在初始集群形成后添加新的集群设备或更换故障转移设备，则 SNMPv3 用户不会复制到新设备。您必须将 SNMPv3 用户重新添加到控制/主用设备，以强制用户复制到新设备；或者，也可以直接在新设备上添加用户（SNMPv3 用户和组是无法在集群数据设备上输入配置命令的规则的例外）。重新配置每个用户，方法是在控制/主用设备上输入 **snmp-server user***username group-name***v3** 命令，或者直接使用未加密形式的 *priv-password* 选项和 *auth-password* 选项连接到数据/备用设备。

IPv6 准则（所有 ASA 型号）

可以通过 IPv6 传输来配置 SNMP，以便 IPv6 主机能够执行 SNMP 查询，并从运行 IPv6 软件的设备接收 SNMP 通知。SNMP 代理和相关的 MIB 已进行增强，以支持 IPv6 寻址。

其他准则

- 在设备模式下运行的系统不会发出电源陷阱。
- 您必须具有 Cisco Works for Windows 或其他符合 SNMP MIB-II 标准的浏览器才能接收 SNMP 陷阱或浏览 MIB。

- SNMP 不支持通过 VPN 隧道进行管理访问（**management-access** 命令）。 对于基于 VPN 的 SNMP，我们建议在环回接口上启用 SNMP。您无需启用管理访问功能即可在环回接口上使用 SNMP。环回接口也适用于 SSH。
- 不支持基于视图的访问控制，但是 VACM MIB 可供浏览以确定默认视图设置。
- ENTITY-MIB 在非管理情景中不可用。在非管理情景中改用 IF-MIB 执行查询。
- ENTITY-MIB 对 Firepower 9300不可用。相反，请使用 CISCO-FIREPOWER-EQUIPMENT-MIB 和 CISCO-FIREPOWER-SM-MIB。
- 在某些设备上，观察到 **snmpwalk** 输出中的接口 (ifDescr) 顺序在重新启动后发生变化。ASA 使用一种算法来确定 SNMP 查询的 ifIndex 表。当 ASA 启动时，接口将按 ASA 读取配置时加载的顺序添加到 ifIndex 表中。添加到 ASA 的新接口会附加到 ifIndex 表中的接口列表。随着接口的添加，删除或重命名，可能会影响重新启动时接口的顺序。
- 在 **snmpwalk** 命令中提供 OID 时，snmpwalk 工具会查询子树中指定 OID 下的所有变量并显示其值。因此，要查看设备上对象的全面输出，请确保在 **snmpwalk** 命令中提供 OID。
- 对于 AIP SSM 或 AIP SSC 不支持 SNMP 第 3 版。
- 不支持 SNMP 调试。
- 不支持 ARP 信息检索。
- 不支持 SNMP SET 命令。
- 使用 NET-SNMP 第 5.4.2.1 版时，仅支持 AES128 加密算法版本。不支持 AES256 或 AES192 加密算法版本。
- 如果结果导致 SNMP 处于不一致状态，则会对现有配置进行更改。
- 对于 SNMP 第 3 版，必须按以下顺序进行配置：组、用户、主机。
- 对于 Cisco Secure Firewall 模型， **snmpwalk** 命令仅从管理情景轮询 FXOS mib。
- 在删除组之前，您必须确保删除与该组关联的所有用户。
- 在删除用户之前，您必须确保未配置与该用户名关联的主机。
- 如果已使用特定安全模式将用户配置为属于特定组，并且如果该组的安全级别进行了更改，则必须按此顺序执行以下操作：
  - 从该组中删除用户。
  - 更改组安全级别。
  - 添加属于新组的用户。
- 不支持创建自定义视图来限制对 MIB 对象子集的用户访问。
- 所有的请求和陷阱只能在默认的 Read/Notify View 中获取。
- 在管理情景中生成 connection-limit-reached 陷阱。要生成此陷阱，您必须在已达到连接限制的用户情景中配置至少一个 SNMP 服务器主机。

- 您最多可以添加 4000 台主机。但是，其中仅 128 台可用于陷阱。
- 支持的活动轮询目标总数为 128。
- 您可以指定网络对象以指示要添加为主机组的个别主机。
- 您可以将多个用户与一台主机关联。
- 您可以在不同的 **host-group** 命令中指定重叠网络对象。为最后一个主机组指定的值会对不同网络对象中的公用主机集合生效。
- 如果删除主机组或与其他主机组重叠的主机，则系统会使用所配置的主机组中已指定的值再次设置主机。
- 主机获取的值取决于用于运行命令的指定序列。
- SNMP 发送的消息大小的限制为 1472 字节。
- ASA 支持每个情景的 SNMP 服务器陷阱主机数不受限制。**show snmp-server host** 命令输出仅显示正在轮询 ASA 的活动主机，以及静态配置的主机。

故障排除提示

- 要确保接收来自 NMS 的传入数据包的 SNMP 进程，请输入以下命令：

```
ciscoasa(config)# show process | grep snmp
```

- 要捕获来自 SNMP 的系统日志消息并将其显示在 ASA 控制台上，请输入以下命令：

```
ciscoasa(config)# logging list snmp message 212001-212015
ciscoasa(config)# logging console snmp
```

- 要确保 SNMP 进程正在发送和接收数据包，请输入以下命令：

```
ciscoasa(config)# clear snmp-server statistics
ciscoasa(config)# show snmp-server statistics
```

  输出基于 SNMPv2-MIB 的 SNMP 组。

- 要确保 SNMP 数据包通过 ASA 并指向 SNMP 进程，请输入以下命令：

```
ciscoasa(config)# clear asp drop
ciscoasa(config)# show asp drop
```

- 如果 NMS 无法成功请求对象或者未正确处理来自 ASA 的传入陷阱，请使用数据包捕获确定问题，方法是输入以下命令：

```
ciscoasa (config)# access-list snmp permit udp any eq snmptrap any
ciscoasa (config)# access-list snmp permit udp any any eq snmp
ciscoasa (config)# capture snmp type raw-data access-list snmp interface mgmt
```

```
ciscoasa (config)# copy /pcap capture:snmp tftp://192.0.2.5/exampledir/snmp.pcap
```

- 如果 ASA 不按预期执行，请通过执行以下操作来获取有关网络拓扑和流量的信息：
  - 对于 NMS 配置，请获取以下信息：

    超时次数

    重试计数

    引擎 ID 缓存

    使用的用户名和密码
  - 发出以下命令：

    show block

    show interface

    show process

    show cpu

    show vm
- 如果发生严重错误，如要帮助重现错误，请将回溯文件和 **show tech-support** 命令的输出发送到思科 TAC。
- 如果不允许 SNMP 流量通过 ASA 接口，您可能还需要使用 **icmp permit** 命令允许来自远程 SNMP 服务器的 ICMP 流量。
- 如果您使用 **snmp-server enable oid** 配置了设备，在执行 SNMP 漫游操作时，ASA 将查询 MEMPOOL_DMA 和 MEMPOOL_Global_SHARED 池中的内存信息。这可能会导致与SNMP相关的CPU消耗导致丢包。要缓解此问题，请避免使用 **no snmp-server enable oid** 命令轮询与全局共享池相关的 OID。禁用时，内存池 OID 将返回 0 字节。
- 当您在一个请求中使用 SNMPGET 对大量 OID 进行轮询 ASP 丢弃计数器时，需要重复轮询 ASP 丢弃计数器，而这会导致更高的 CPU 占用率。因此，我们建议您确定要监控的重要计数器，并在每个计数器上使用 SNMPGET 来获取这些值，以减少对 CPU 的影响。
- 有关更多故障排除信息，请参阅以下 URL：
  http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116423-troubleshoot-asa-snmp.html

配置 SNMP

本节介绍如何配置 SNMP。

过程

步骤 1 启用 SNMP 代理和 SNMP 服务器。

步骤 2 配置 SNMP 陷阱。

步骤 3 配置 SNMP 第 1 版和第 2c 版参数或 SNMP 第 3 版参数。

启用 SNMP 代理和 SNMP 服务器

要启用 SNMP 代理和 SNMP 服务器，请执行以下步骤：

过程

在 ASA 上启用 SNMP 代理和 SNMP 服务器。默认情况下，SNMP 服务器已启用。

snmp-server enable

示例：

```
ciscoasa(config)# snmp-server enable
```

配置 SNMP 陷阱

要指定 SNMP 代理生成哪些陷阱以及如何将其收集并发送到 NMS，请执行以下步骤：

注释 启用所有 SNMP 或系统日志陷阱时，SNMP 进程可能会消耗代理和网络中的过多资源，导致系统挂起。如果您发现系统延迟、未完成的请求或超，可以选择性地启用 SNMP 和系统日志陷阱。例如，您可以跳过信息系统日志陷阱严重性级别。

过程

将单个陷阱、陷阱集合或所有陷阱发送到 NMS。

snmp-server enable traps [**all** | **syslog** | **snmp** [**authentication** | **linkup** | **linkdown** | **coldstart** | **warmstart**] | **config** | **entity** [**config-change** | **fru-insert** | **fru-remove** | **fan-failure** | **cpu-temperature** | **chassis-fan-failure** | **power-supply**] | **chassis-temperature** | **power-supply-presence** | **power-supply-temperature** **l1-bypass-status**] | **ikev2** [**start** | **stop**] | **cluster-state** | **failover-state** | **peer-flap** | **ipsec** [**start** | **stop**] | **remote-access** [**session-threshold-exceeded**] | **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [**packet-discard**]

示例：

```
ciscoasa(config)# snmp-server enable traps snmp authentication
```

```
linkup linkdown coldstart warmstart
```

通过此命令可以将系统日志消息作为陷阱发送到NMS。默认配置已启用所有SNMP标准陷阱，如示例所示。要禁用这些陷阱，请使用 **no snmp-server enable traps snmp** 命令。

如果输入此命令而不指定陷阱类型，则默认为 **syslog** 陷阱。默认情况下，会启用 **syslog** 陷阱。默认 SNMP 陷阱随**系统日志**陷阱继续启用。

您需要同时配置 **logging history** 命令和 the **snmp-server enable traps syslog** 命令才能从系统日志 MIB 生成陷阱。

要恢复 SNMP 陷阱的默认启用，请使用 **clear configure snmp-server** 命令。默认情况下会禁用所有其他陷阱。

仅在管理情景中可用的陷阱：

- **connection-limit-reached**
- **entity**
- **memory-threshold**

仅通过管理情景为系统情景中物理连接的接口生成的陷阱：

- **interface-threshold**

在单一模式下，所有其他陷阱在管理情景和用户环境中都可用。

config 陷阱启用 ciscoConfigManEvent 通知和 ccmCLIRunningConfigChanged 通知，在退出配置模式后会生成这些通知。

如果 CPU 使用率大于所配置监控期的所配置阈值，则系统会生成 **cpu threshold rising** 陷阱。

当已用系统情景内存达到总系统内存的80%时，系统会从管理情景中生成**memory-threshold**陷阱。对于所有其他用户情景，当在该特定情景中已用内存达到总系统内存的 80% 时会生成此陷阱。

某些陷阱不适用于某些硬件型号。使用 ? 代替陷阱关键字来确定哪些陷阱可用于您的设备。例如：

- Firepower 1000 系列 仅支持以下实体陷阱：**chassis-temperature**、**config-change** 和 **cpu-temperature**。

注释
SNMP 不监控电压传感器。

配置 CPU 使用率阈值

要配置 CPU 使用率阈值，请执行以下步骤：

过程

为高 CPU 阈值和阈值监控期配置阈值。

snmp cpu threshold rising *threshold_value monitoring_period*

示例：

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

要清除阈值和 CPU 使用率的监控期间，请使用此命令的 **no** 形式。如果未配置 **snmp cpu threshold rising** 命令，则高阈值级别的默认值为超过 70%，临界阈值级别的默认值为超过 95%。默认监控期设置为 1 分钟。

临界 CPU 阈值级别始终保持在 95%，无法配置。高 CPU 阈值的有效阈值范围为 10% 到 94%。监控期的有效值范围为 1 到 60 分钟。

配置物理接口阀值

要配置物理接口阈值，请执行以下步骤：

过程

配置 SNMP 物理接口的阀值。

snmp interface threshold *threshold_value*

示例：

```
ciscoasa(config)# snmp interface threshold 75%
```

要清除 SNMP 物理接口的阈值，请使用此命令的 **no** 形式。阈值定义为接口带宽利用率的百分比。有效阈值范围为 30% 到 99%。默认值为 70%。

snmp interface threshold 命令仅在管理情景中可用。

物理接口使用情况在单模和多模下受到监控，系统情景中物理接口的陷阱通过管理情景发送。仅物理接口用于计算阈值使用情况。

配置 SNMP 版本 1 或版本 2c 的参数

要配置 SNMP 第 1 版或第 2c 版的参数，请执行以下步骤：

过程

步骤 1 指定 SNMP 通知的接收者，指示从其发送陷阱的接口，并识别可以连接至 ASA 的 NMS 或 SNMP 管理器的名称和 IP 地址。

{interface hostname | ip_address} [|] [community-string] [{|用户名}] [端口] **snmp-server host trappollcommunity version1 2cudp-port**

示例：

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2c
ciscoasa(config)# snmp-server host corp 172.18.154.159 community public

ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 2c
```

trap 关键字可将 NMS 限制为仅接收陷阱。**poll** 关键字可将 NMS 限制为仅发送请求（轮询）。默认情况下，SNMP 陷阱已启用。默认情况下，UDP 端口为 162。社区字符串是 ASA 与 NMS 之间的共享密钥。密钥是一个区分大小写的值，长度最多为32个字母数字字符。不允许使用空格。默认社区字符串为 public。ASA 使用此密钥确定传入的 SNMP 请求是否有效。例如，您可以使用某社区字符串来指定站点，然后使用同一字符串配置 ASA 和管理站。ASA 使用指定的字符串，并且不会对包含无效社区字符串的请求作出响应。但是，如果 SNMP 监控是通过管理接口而不是诊断接口，则无需 ASA 验证社区字符串即可进行轮询。在使用加密的社区字符串后，对所有系统（例如 CLI、ASDM、CSM 等）仅显示加密的形式。明文密码不可见。加密的社区字符串始终由 ASA 生成；您输入的一般是明文形式。

关键字指定用于陷阱和请求（轮询）的SNMP版本。**version** 仅允许使用所选版本与服务器通信。

要在添加 **snmp-server host** 命令后接收陷阱，请确保使用 ASA 上配置的凭证相同的凭证来配置 NMS 上的用户。

步骤 2 设置仅供与 SNMP 第 1 版或第 2c 版配合使用的社区字符串。

snmp-server community *community-string*

示例：

```
ciscoasa(config)# snmp-server community onceuponatime
```

注释
您应避免使用特殊字符（！，@, #, $, %, ^, &, *, \) 在社区字符串。通常，使用为操作系统使用的功能保留的任何特殊字符可能会导致意外结果。例如，反斜线（\）被解释为转义字符，不应在社区字符串中使用。

步骤 3 设置 SNMP 服务器位置或联系人信息。

snmp-server [**contact** | **location**] *text*

示例：

```
ciscoasa(config)# snmp-server location building 42
```

```
ciscoasa(config)# snmp-server contact EmployeeA
```

text 参数指定联系人或 ASA 系统管理员的名称。名称区分大小写，最多可包含 127 个字符。可包含空格，但多个空格将缩为一个空格。

步骤 4 设置 SNMP 请求的侦听端口。

snmp-server listen-port *lport*

示例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 参数是接受传入请求的端口。默认侦听端口为 161。**snmp-server listen-port** 命令仅在管理情景中可用，在系统情景中不可用。如果在当前使用中的端口上配置 **snmp-server listen-port** 命令，系统将显示以下消息：

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different port.
```

现有 SNMP 线程会持续轮询（每 60 秒一次），直到端口可用，如果端口仍在使用中，则会发出系统日志 %ASA-1-212001。

配置 SNMP 第 3 版的参数

要配置 SNMP 第 3 版的参数，请执行以下步骤：

过程

步骤 1 指定仅供与 SNMP 第 3 版配合使用的新 SNMP 组。

snmp-server group *group-name* **v3** [**auth** | **noauth** | **priv**]

示例：

```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

配置社区字符串后，系统会自动生成具有与社区字符串相匹配的名称的另外两个组：一个表示第 1 版的安全模式，一个表示第 2 版的安全模式。**auth** 关键字可启用数据包身份验证。**noauth** 关键字表示未在使用数据包身份验证或加密。**priv** 关键字可启用数据包加密和身份验证。**auth** 或 **priv** 关键字不存在默认值。

步骤 2 为仅供与 SNMP 第 3 版配合使用的 SNMP 组配置新用户。

snmp-server user *username group_name* **v3** [**engineID** *engineID*] [**encrypted**] [**auth** {**sha** | **sha224** | **sha256** | **sha384**} *auth_password* [**priv** {**3des** | **aes** {**128** | **192** | **256**}} *priv_password*]]

示例：

```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword
aes 128 mypassword
ciscoasa(config)# snmp-server user testuser1 public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

username 参数是属于 SNMP 代理的主机上用户的名称。用户名最多输入 32 个字符。名称必须以字母开头。有效字符包括字母、数字、_（下划线）、.（句点）、@（邮箱符号）和 -（连字符）。

group-name 参数是用户所属的组的名称。**v3** 关键字指定应使用 SNMP 第 3 版安全模式并允许使用 **encrypted**、 **priv**和 **auth** 关键字。**engineID** 关键字是可选的，可指定用于本地化用户的身份验证和加密信息的 ASA 的 engineID。engineID 参数必须指定有效的 ASA engineID。

encrypted 关键字指定加密格式的密码。加密密码必须满足以下要求。

- 必须是十六进制格式。
- 必须包含最少 8 个字符，最多 80 个字符。
- 必须仅包含字母、数字和以下字符：~`!@#%^&*()_-+{}[]|\:;"'<,>./
- 不得包含以下符号：$（美元符号）、?（问号）或 =（等号）。
- 必须包含至少 5 个不同的字符。
- 不得包含过多连续递增或递减数字或字母。例如，字符串“12345”包含四个此类字符，字符串“ZYXW”包含三个此类字符。如果此类字符的总数超过某个限值（通常约大于 4 至 6 个字符），则简单性检查将会失败。

  注释
  在使用的非递增或递减字符数介于两者之间时，系统不会重置连续递增或递减字符计数。例如，abcd&!21 将致使密码检查失败，但 abcd&!25 不会。

auth 关键字指定应使用的身份验证级别（（**sha**、**sha224**、**sha256** 或 **sha384**）。**priv** 关键字指定加密级别。不存在 **auth** 或 **priv** 关键字或默认关键字的默认值。

对于加密算法，可以指定 **3des** 或 **aes** 关键字。您还可以指定要使用的 AES 加密算法版本：**128**、**192** 或 **256**。auth-password 参数指定身份验证用户密码。priv-password 参数指定加密用户密码。

如果忘记密码，则无法将其恢复，必须重新配置用户。您可以指定纯文本密码或本地化摘要。本地化摘要必须与为用户选择的身份验证算法（SHA、SHA-224、SHA-256 或 SHA-384）相匹配。当用户配置显示在控制台上或写入到文件（例如，启动配置文件）时，始终显示本地化身份验证和隐私摘要而非纯文本密码（参阅第二个示例）。密码的最小长度为 1 个字母数字字符；但是，出于安全原因，我们建议使用至少 8 个字母数字字符。

将 SNMPv3 用于集群或故障转移时，如果在初始集群形成后添加新的集群设备或更换故障转移设备，则 SNMPv3 用户不会复制到新设备。您必须将 SNMPv3 用户重新添加到控制/主用设备，以强制用户复制到新设备；或者，也可以直接在新设备上添加用户（SNMPv3 用户和组是无法在集群数据设备上输入配置命令的规则的例外）。重新配置每个用户，方法是在控制/主用设备上输入username group-name命令，或者直接在数据/备用设备上输入priv-password选项和auth-password选项（未加密形式）。**snmp-server user v3**

如果在控制/主用设备上使用 **encrypted** 关键字输入用户，系统将显示一条错误消息，通知您 SNMPv3 用户命令不会被复制。此行为还意味着在复制期间不会清除现有 SNMPv3 用户和组命令。

例如，使用通过加密密钥输入的命令的控制/主动设备：

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a
priv aes 256 cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:
f6:86:cf:18:c0:f0:47:d6:94:e5:da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

例如，在集群复制期间的数据设备上（仅在配置中存在 **snmp-server user** 命令的情况下才会显示）：

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

步骤 3 指定 SNMP 通知的接收方。指示从其发送陷阱的接口。确定可以连接到 ASA 的 NMS 或 SNMP 管理器的名称和 IP 地址。

snmp-server host *interface* {*hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

示例：

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1
ciscoasa(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2
ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 3 testuser3
```

trap 关键字可将 NMS 限制为仅接收陷阱。**poll** 关键字可将 NMS 限制为仅发送请求（轮询）。默认情况下，SNMP 陷阱已启用。默认情况下，UDP 端口为 162。社区字符串是 ASA 与 NMS 之间的共享密钥。密钥是一个区分大小写的值，最多为 32 个字母数字字符。不允许使用空格。默认社区字符串为 public。ASA 使用此密钥确定传入的 SNMP 请求是否有效。例如，您可以使用某社区字符串来指定站点，然后使用同一字符串配置 ASA 和 NMS。ASA 使用指定的字符串，并且不会对包含无效社区字符串的请求作出响应。在使用加密的社区字符串后，对所有系统（例如 CLI、ASDM、CSM 等）仅显示加密的形式。明文密码不可见。加密的社区字符串始终由 ASA 生成；您输入的一般是明文形式。

关键字指定用于陷阱和请求（轮询）的SNMP版本。**version** 仅允许使用所选版本与服务器通信。

在 ASA 上配置 SNMP 第 3 版主机时，用户必须与该主机关联。

要在添加 **snmp-server host** 命令后接收陷阱，请确保使用 ASA 上配置的凭证相同的凭证来配置 NMS 上的用户。

步骤 4 设置 SNMP 服务器位置或联系人信息。

snmp-server [**contact** | **location**] *text*

示例：

```
ciscoasa(config)# snmp-server location building 42
```

```
ciscoasa(config)# snmp-server contact EmployeeA
```

text 参数指定联系人或 ASA 系统管理员的名称。名称区分大小写，最多可包含 127 个字符。可包含空格，但多个空格将缩为一个空格。

步骤 5 设置 SNMP 请求的侦听端口。

snmp-server listen-port *lport*

示例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 参数是接受传入请求的端口。默认侦听端口为 161。**snmp-server listen-port** 命令仅在管理情景中可用，在系统情景中不可用。如果在当前使用中的端口上配置 **snmp-server listen-port** 命令，系统将显示以下消息：

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different port.
```

现有 SNMP 线程会持续轮询（每 60 秒一次），直到端口可用，如果端口仍在使用中，则会发出系统日志 %ASA-1-212001。

配置用户组

要配置其中含有一组指定用户的 SNMP 用户列表，请执行以下步骤：

过程

配置 SNMP 用户列表。

snmp-server user-list *list_name* **username** *user_name*

示例：

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

listname 参数指定用户列表的名称，长度可以为最多 33 个字符。**username***user_name* 关键字/参数对指定在用户列表中可以配置的用户。使用 **snmp-server user***username* 命令配置用户列表中的用户，仅在使用的是 SNMP 第 3 版的情况下该命令才可用。用户列表必须具有多个用户，并且能与主机名或 IP 地址范围关联。

将用户与网络对象关联

要将用户列表中的单个用户或用户组与网络对象相关联，请执行以下步骤：

过程

将用户列表中的单个用户或用户组与网络对象相关联。

snmp-server host-group *net_obj_name* [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}] [**udp-port** *port*]

示例：

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

net_obj_name 参数指定用户或用户组与之关联的接口网络对象名称。

trap 关键字指定只能发送陷阱，并且不允许浏览此主机（轮询）。默认情况下，SNMP 陷阱处于启用状态。

poll 关键字指定允许浏览主机（轮询），但不能发送陷阱。

community 关键字指定来自 NMS 的请求需要非默认字符串，或是当生成发送至 NMS 的陷阱时需要非默认字符串。您只能将此关键字用于 SNMP 第 1 版或第 2c 版。*community-string* 参数指定类似密码的字符串，该字符串随通知一起发送或者在 NMS 发出的请求中发送。社区字符串最多可以包含 32 个字符。

version 关键字将 SNMP 通知版本设置为版本 1、2c 或 3 以用于发送陷阱和接受请求（投票）。默认版本为 1。

username 参数指定您在使用 SNMP 版本 3 时用户的名称。

user-list *list_name* 关键字/参数对指定用户列表的名称。

udp-port *port* 关键字/参数对指定必须将 SNMP 陷阱发送到非默认端口上的 NMS 主机并设置该 NMS 主机的 UDP 端口号。默认 UDP 端口为 162。

监控 SNMP

请参阅以下用于监控 SNMP 的命令。

- **show running-config snmp-server** [**default**]

  此命令可显示所有 SNMP 服务器配置信息。

- **show running-config snmp-server group**

此命令可显示 SNMP 组配置设置。

- **show running-config snmp-server host**

  此命令可显示供 SNMP 用于控制发送到远程主机的消息和通知的配置设置。

- **show running-config snmp-server host-group**

  此命令可显示 SNMP 主机组配置。

- **show running-config snmp-server user**

  此命令可显示 SNMP 基于用户的配置设置。

- **show running-config snmp-server user-list**

  此命令可显示 SNMP 用户列表配置。

- **show snmp-server engineid**

  此命令可显示所配置的 SNMP 引擎的 ID。

- **show snmp-server group**

  此命令可显示已配置的 SNMP 组的名称。如果已经配置社区字符串，则默认情况下在输出中会显示两个额外的组。此行为是正常的。

- **show snmp-server statistics**

  此命令可显示已配置的 SNMP 服务器特征。要将所有 SNMP 计数器重置为零，请使用 **clear snmp-server statistics** 命令。

- **show snmp-server user**

  此命令可显示已配置的用户特征。

示例

以下示例说明如何显示 SNMP 服务器统计信息：

```
ciscoasa(config)# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
```

```
    0 Trap PDUs
```

以下示例说明如何显示 SNMP 服务器运行配置：

```
ciscoasa(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

SNMP 示例

下节提供了可用作所有 SNMP 版本的参考的示例。

SNMP 第 1 版和第 2c 版

下例显示了 ASA 如何从内部接口上的主机 192.0.2.5 接收 SNMP 请求，但又不向任何主机发送任何 SNMP 系统日志请求：

```
ciscoasa(config)# snmp-server host 192.0.2.5
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
ciscoasa(config)# snmp-server community ohwhatakeyisthee
```

SNMP 第 3 版

下例显示了 ASA 如何使用 SNMP 版本 3 安全模型接收 SNMP 请求，这要求配置遵循如下特定的顺序：组、用户、主机：

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

SNMP 的历史记录

表 *68: SNMP* 的历史记录

功能名称	版本	说明
SNMP 第 1 版和第 2c 版	7.0(1)	通过明文社区字符串在 SNMP 服务器与 SNMP 代理之间传输数据来提供 ASA 网络监控及事件信息。

功能名称	版本	说明
SNMP 第 3 版	8.2(1)	为最安全形式的受支持安全模式 SNMP 第 3 版提供 3DES 或 AES 加密和支持。通过使用USM，此版本允许配置用户、组和主机以及身份验证特征。此外，此版本还允许对代理和MIB对象进行访问控制，并且包含其他 MIB 支持。 引入或修改了以下命令：**show snmp-server engineid**、**show snmp-server group**、**show snmp-server user**、**snmp-server group**、**snmp-server user**、**snmp-server host**。
密码加密	8.3(1)	支持密码加密。 修改了以下命令：**snmp-server community** 和 **snmp-server host**。
SNMP 陷阱和 MIB	8.4(1)	支持以下其他关键字：**connection-limit-reached**、**cpu threshold rising**、**entity cpu-temperature**、**entity fan-failure**、**entity power-supply**、**ikev2 stop | start**、**interface-threshold**、**memory-threshold**、**nat packet-discard**、**warmstart**。 entPhysicalTable 报告传感器、风扇、电源和相关组件的条目。 支持以下其他 MIB：CISCO-ENTITY-SENSOR-EXT-MIB、CISCO-ENTITY-FRU-CONTROL-MIB、CISCO-PROCESS-MIB、CISCO-ENHANCED-MEMPOOL-MIB、CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、DISMAN-EVENT-MIB、DISMAN-EXPRESSION-MIB、ENTITY-SENSOR-MIB、NAT-MIB。 支持以下其他陷阱：ceSensorExtThresholdNotification、clrResourceLimitReached、cpmCPURisingThreshold、mteTriggerFired、natPacketDiscard、warmStart。 引入或修改了以下命令：**snmp cpu threshold rising**、**snmp interface threshold**、**snmp-server enable traps**。
IF-MIB ifAlias OID 支持	8.2(5) / 8.4(2)	ASA 现在支持 ifAlias OID。浏览 IF-MIB 时，ifAlias OID 将设置为已为接口说明设置的值。

功能名称	版本	说明
ASA 服务模块 (ASASM)	8.5(1)	ASASM 支持 8.4(1) 中提供的所有 MIB 和陷阱，但以下项目除外： 8.5(1) 中不受支持的 MIB： • CISCO-ENTITY-SENSOR-EXT-MIB（仅支持 entPhySensorTable 组下的对象）。 • ENTITY-SENSOR-MIB（仅支持 entPhySensorTable 组中的对象）。 • DISMAN-EXPRESSION-MIB（仅支持 expExpressionTable、expObjectTable 和 expValueTable 组中的对象）。 8.5(1) 中不受支持的陷阱： • ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)。此陷阱仅用于电源故障、风扇故障和高 CPU 温度事件。 • InterfacesBandwidthUtilization。
SNMP 陷阱	8.6(1)	支持 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X 的以下其他关键字：**entity power-supply-presence**、**entity power-supply-failure**、**entity chassis-temperature**、**entity chassis-fan-failure**、**entity power-supply-temperature**。 修改了以下命令：**snmp-server enable traps**。
VPN 相关 MIB	9.0(1)	已实施更新版本的 CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB 来支持下一代加密功能。 已为 ASASM 启用以下 MIB： • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	添加了对以下 MIB 的支持：CISCO-TRUSTSEC-SXP-MIB。
SNMP OID	9.1(1)	已添加五个新的 SNMP 物理供应商类型 OID 来支持 ASA 5512-X、5515-X、5525-X、5545-X 和 5555-X。

功能名称	版本	说明
NAT MIB	9.1(2)	添加了 cnatAddrBindNumberOfEntries 和 cnatAddrBindSessionCount OID 来支持 xlate_count 和 max_xlate_count 条目，相当于允许使用 **show xlate count** 命令进行轮询。
SNMP 主机、主机组和用户列表	9.1(5)	最多可以添加 4000 台主机。支持的活动轮询目标数量为 128。您可以指定网络对象以指示要添加为主机组的个别主机。您可以将多个用户与一台主机关联。 引入或修改了以下命令：**snmp-server host-group**、**snmp-server user-list**、**show running-config snmp-server**、**clear configure snmp-server**。
SNMP 消息大小	9.2(1)	SNMP 发送的消息大小限制已增大为 1472 字节。
SNMP OID 和 MIB	9.2(1)	ASA 现在支持 cpmCPUTotal5minRev OID。 ASA virtual 已作为新产品添加到 SNMP sysObjectID OID 和 entPhysicalVendorType OID 中。 CISCO-PRODUCTS-MIB 和 CISCO-ENTITY-VENDORTYPE-OID-MIB 已更新为支持新的 ASA virtual 平台。 已添加用于监控 VPN 共享许可证使用情况的新 SNMP MIB。
SNMP OID 和 MIB	9.3(1)	已为 ASASM 添加 CISCO-REMOTE-ACCESS-MONITOR-MIB (OID 1.3.6.1.4.1.9.9.392) 支持。
SNMP MIB 和陷阱	9.3(2)	CISCO-PRODUCTS-MIB 和 CISCO-ENTITY-VENDORTYPE-OID-MIB 均已更新，以支持 ASA 5506-X。 ASA 5506-X 已作为新产品添加到 SNMP sysObjectID OID 和 entPhysicalVendorType OID 表中。 ASA 现在支持 CISCO-CONFIG-MAN-MIB，它使您能够执行以下操作： • 了解已为特定配置输入的命令。 • 在运行配置发生更改后通知 NMS。 • 跟踪与上一次更改或保存运行配置相关的时间戳。 • 跟踪命令的其他更改，例如，终端详细信息和命令源。 修改了以下命令：**snmp-server enable traps**。
SNMP MIB 和陷阱	9.4(1)	ASA 5506W-X、ASA 5506H-X、ASA 5508-X 和 ASA 5516-X 已作为新产品添加到 SNMP sysObjectID OID 与 entPhysicalVendorType OID 表中。

功能名称	版本	说明
每个情景的SNMP服务器陷阱主机数没有限制	9.4(1)	ASA 对于每个情景支持无限制的 SNMP 服务器陷阱主机数。**show snmp-server host** 命令输出仅显示正在轮询 ASA 的活动主机，以及静态配置的主机。 修改了以下命令：**show snmp-server host**。
添加了对 ISA 3000 的支持	9.4(1.225)	现在，SNMP 支持 ISA 3000 产品系列。我们为此平台添加了新的 OID。**snmp-server enable traps entity** 命令已修改为包括新变量 *l1-bypass-status*。这样将支持硬件旁路状态更改。 修改了以下命令：**snmp-server enable traps entity**。
在 CISCO-ENHANCED-MEMPOOL-MIB 中支持 cempMemPoolTable	9.6(1)	现在支持 CISCO-ENHANCED-MEMPOOL-MIB 的 cempMemPoolTable。这是一个内存池表，监控受管系统上所有物理实体的条目。 **注释** CISCO-ENHANCED-MEMPOOL-MIB 使用 64 位计数器，并且支持报告 RAM 超过 4GB 的平台上的内存。
对于精确时间协议 (PTP) 支持 E2E 透明时钟模式 MIB	9.7(1)	现在支持与 E2E 透明时钟模式对应的 MIB。 **注释** 仅支持 SNMP get、bulkget、getnext 和 walk 操作。
基于 IPv6 的 SNMP	9.9(2)	ASA 现在支持基于 IPv6 的 SNMP，包括通过 IPv6 与 SNMP 服务器通信，允许通过 IPv6 执行查询和陷阱，以及支持现有 MIB 使用 IPv6 地址。我们添加了以下新的 SNMP IPv6 MIB 对象，如 RFC 8096 中所述。 • ipv6InterfaceTable (OID: 1.3.6.1.2.1.4.30) - 包含每个接口 IPv6 特定的信息。 • ipAddressPrefixTable (OID:1.3.6.1.2.1.4.32) - 包含由此实体获知的所有前缀。 • ipAddressTable (OID: 1.3.6.1.2.1.4.34) - 包含与实体接口相关的寻址信息。 • ipNetToPhysicalTable (OID: 1.3.6.1.2.1.4.35) - 包含从 IP 地址到物理地址的映射。 新增或修改的命令：**snmp-server host** **注释** **snmp-server host-group** 命令不支持 IPv6。
支持在SNMP审核操作期间启用和禁用可用内存和已用内存统计信息的结果	9.10(1)	为避免 CPU 资源的过度占用，您可以启用和禁用通过 SNMP 审核操作收集的可用内存和已用内存统计数据的查询。 新增/修改的命令：**snmp-server enable oid**

功能名称	版本	说明
支持在SNMP审核操作期间启用和禁用可用内存和已用内存统计信息的结果	9.12(1)	为避免 CPU 资源的过度占用，您可以启用和禁用通过 SNMP 审核操作收集的可用内存和已用内存统计数据的查询。 未修改任何命令。
SNMPv3 身份验证	9.14(1)	现在，您可以使用 SHA-256 HMAC 验证用户身份。 新增/修改的命令：**snmp-server user**
对于9.14（1）+中的故障转移对等体，ASA不再与其对等体共享SNMP客户端引擎数据。	9.14(1)	ASA 再与其对等体共享 SNMP 客户端引擎数据。
通过站点间 VPN 进行 SNMP 轮询	9.14(2)	对于通过站点间 VPN 进行安全 SNMP 轮询，请将外部接口的 IP 地址包含在加密映射访问列表中作为 VPN 配置的一部分。
已弃用对于 CISCO-MEMORY-POOL-MIB OID 的支持	9.15(1)	对于使用 64 位计数器的系统，已弃用 CISCO-MEMORY-POOL-MIB OID（ciscoMemoryPoolUsed、ciscoMemoryPoolFree）。 CISCO-ENHANCED-MEMPOOL-MIB 的 cempMemPoolTable 为使用 64 位计数器的系统提供内存池监控条目。
SNMPv3 身份验证	9.16（1）	您现在可以使用 SHA-224 和 SHA-384 进行用户身份验证。您不能再使用 MD5 进行用户身份验证。 您不能再使用 DES 进行加密。 新增/修改的命令：**snmp-server user**
基于 IPv6 的 SNMP	9.17(1)	**snmp-server host-group** 命令现在支持 IPv6 主机、范围和子网对象。
环回接口支持 SNMP	9.18(2)	您现在可以添加环回接口并用于 SNMP： 新增/修改的命令： **interface loopback**、**snmp-server host**
SNMP MIB 和陷阱	9.20(1)	Cisco Secure Firewall 4200 型号设备（FPR4215、FPR4225 和 FPR4245）已作为新产品添加到 SNMP sysObjectID OID 和 entPhysicalVendorType OID 表中。添加了对这些 Cisco Secure Firewall 4200 系列设备的两个 EPM 卡（4X200G 和 2X100G）的 SNMP 支持。

第 48 章

思科成功网络和遥测数据

本章介绍思科成功网络以及如何在 ASA 上启用它。它还列出了发送到安全服务引擎 (SSE) 云的遥测数据点。

- 关于思科成功网络 ， 第 1439 页
- 启用或禁用思科成功网络 ， 第 1440 页
- 查看 ASA 遥测数据 ， 第 1441 页
- 思科成功网络 - 遥测数据， 第 1441 页
- 调试遥测数据， 第 1447 页

关于思科成功网络

思科成功网络是用户启用的云服务，可与安全服务交换 (SSE) 云建立安全连接，以流式传输ASA使用信息和统计信息。数据流遥测提供一种机制，能以结构化的格式 (JSON) 将 ASA 使用情况和其他详细信息传输至远程管理站，从而获得以下优势：

- 通知您适用于您产品的更多技术支持服务和监控。
- 帮助思科改善产品。

默认情况下，在托管 ASA 设备的 Firepower 4100/9300 平台上启用思科成功网络（在刀片级别）。但是，要传输遥测数据，必须在机箱级别启用 FXOS 上的配置（请参阅《思科 Firepower 4100/9300 FXOS CLI 配置指南》）或在机箱管理器上启用思科成功网络（请参阅思科 Firepower 4100/9300 FXOS）Firepower 机箱管理器配置指南）ASA 允许您在任何时间点禁用遥测服务。

在 ASA 设备上收集的遥测数据包括 CPU、内存、磁盘或带宽，以及许可证使用情况、已配置的功能列表、集群/故障转移信息等。请参见 思科成功网络 - 遥测数据， 第 1441 页。

支持的平台和所需的配置

- 运行 ASA 版本 9.13.1或更高版本的 FP9300/4100平台支持。
- 需要 FXOS 2.7.1 或更高版本才能与云连接。
- FXOS 上的 SSE 连接器必须连接到 SSE 云。通过在智能许可后端启用和注册智能许可证来建立此连接。FXOS 上的 SSE 连接器通过注册智能许可证自动注册到 SSE 云。

- 必须在机箱管理器上启用思科成功网络配置。
- 必须在 ASA 上启用遥测配置。

ASA 遥测数据如何到达 SSE 云

默认情况下， ASA 9.13(1)中的 Firepower 4100/9300 平台支持思科成功网络。FXOS 服务管理器每天会向在平台上运行的ASA应用程序发送遥测请求。ASA引擎根据配置和连接状态，以独立模式或集群模式将遥测数据发送到FXOS。也就是说，如果在 ASA 中启用了遥测支持，并且连接了 SSE 连接器状态，则遥测线程会从各种来源（例如，系统或平台或设备 API、许可证 API、CPU AP、内存 API、磁盘 API、Smart Call Home API）获取所需信息 Call Home 功能 API 等。但是，如果在 ASA 中禁用遥测支持或 SSE 连接器状态断开，ASA 会向 FXOS (appAgent) 发送指示遥测配置状态的回复，并且不发送任何遥测数据。

FXOS 上仅运行一个 SSE 连接器实例。当它向 SSE 云注册时，它被视为一台设备，SSE 基础设施会为 FXOS 分配一个设备 ID。通过 SSE 连接器发送的任何遥测报告都归入同一设备 ID 下。因此，FXOS 将来自每个 ASA 的遥测报告汇聚为一个报告。其他内容（例如智能许可证帐户信息）会添加到报告中。然后，FXOS 将最终报告发送到 SSE 云。遥测数据保存在 SSE 数据交换 (DEX) 中，可供思科 IT 团队使用。

启用或禁用思科成功网络

开始之前

- 在 FXOS 上启用并注册智能许可证。
- 在机箱级别启用 FXOS 上的遥测支持（请参阅《思科 Firepower 4100/9300 FXOS CLI 配置指南》）或在机箱管理器上启用思科成功网络（请参阅《思科 Firepower 4100/9300 FXOS Firepower 机箱管理器配置指南》）。

过程

要在 ASA 上启用遥测服务，请在全局配置模式下输入以下命令。使用命令的否定形式禁用遥测服务：

[no] service telemetry

示例：

```
ciscoasa(config)# service telemetry
ciscoasa(config)# no service telemetry
```

下一步做什么

- 您可以查看遥测配置和活动日志或遥测数据。请参阅 查看 ASA 遥测数据 ， 第 1441 页
- 要查看遥测数据和数据字段的示例，请参阅 思科成功网络 - 遥测数据 ， 第 1441 页

查看 ASA 遥测数据

开始之前

- 在 ASA 上启用遥测服务。请参阅 启用或禁用思科成功网络 ， 第 1440 页

过程

要在网络的 ASA 设备上查看遥测数据，请在特权 EXEC 模式下输入以下命令：

show telemetry [**history | last-report | sample**]

示例：

```
ciscoasa# show telemetry history
17:38:24 PDT Apr 30 2019: Telemetry support on the blade: enabled
17:38:03 PDT Apr 30 2019: Telemetry support on the blade: disabled
11:49:47 PDT Apr 29 2019: msgId 3. Telemetry support on the chassis: disabled
11:48:47 PDT Apr 29 2019: msgId 2. Telemetry request from the chassis received. SSE connector
 status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent
11:47:47 PDT Apr 29 2019: msgId 1. Telemetry request from the chassis received. SSE connector
 status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent.
```

使用 **history** 查看与遥测配置和活动相关的过去 100 个事件；**last-report** 来查看以 JSON 格式发送到 FXOS 的最新遥测数据，和 **sample** 来查看以 JSON 格式即时生成的遥测数据。

思科成功网络 - 遥测数据

默认情况下， Firepower 4100/9300 平台支持思科成功网络。FXOS 服务管理器每天会向在平台上运行的ASA引擎发送遥测请求。ASA引擎在收到请求时，根据连接状态，以独立模式或集群模式将遥测数据发送到FXOS。下表提供有关遥测数据点、其说明和样本值的信息。

表 *69:* 设备信息

数据点	描述	示例值
设备型号	设备型号	思科自适应安全设备
序列号	设备序列号	FCH183771EZ

数据点	描述	示例值
系统时间	系统运行时间	11658000
平台	硬件	FPR9K-SM-24
部署模式	部署类型	原生
安全情景模式	单一/多个	单模式

表 *70:* 版本信息

数据点	描述	示例值
版本全局变量	ASA 版本	9.13.1.5
设备管理器版本	设备管理器版本	7.10.1

表 *71:* 许可证信息

数据点	描述	示例值
智能许可证全局变量	激活的许可证	regid.2015-06.com.cisco.ASA-SSP-STRONG-ENCRYPTION,1.0_555507e9-85f8-4e41-96de-860b59f10bbe

表 *72:* 平台信息

数据点	描述	示例值
CPU	过去 5 分钟的 CPU 使用率	fiveSecondsPercentage: 0.2000000, oneMinutePercentage: 0, fiveMinutesPercentage: 0
内存	内存使用率	freeMemoryInBytes: 225854966384, usedMemoryInBytes：17798281616， totalMemoryInBytes：243653248000
磁盘	磁盘使用率	freeGB：21.237285， usedGB：0.238805， totalGB：21.476090

数据点	描述	示例值
带宽	带宽使用情况	receivedPktsPerSec：3， receivedBytesPerSec：212， sentPktsPerSec：3， sentBytesPerSec：399

表 *73:* 功能信息

数据点	描述	示例值
功能列表	已启用功能列表	名称：集群 状态：已启用

表 *74:* 集群信息

数据点	描述	示例值
集群信息	集群信息	clusterGroupName：ssp-cluster interfaceMode：spanned unitName：unit-3-3 unitState：从属 otherMembers： 项目： memberName：unit-2-1 memberState：MASTER memberSerialNum：FCH183771BA

表 *75:* 故障转移信息

数据点	描述	示例值
故障转移	故障转移信息	myRole：Primary， peerRole：Secondary， myState：active， peerState：standby， peerSerialNum：FCH183770EZ

表 *76:* 登录信息

数据点	描述	示例值
登录	登录历史记录	loginTimes：2 times in last 2 days， lastSuccessfulLogin：12:25:36 PDT Mar 11 2019

ASA 遥测数据样本

以下是从 ASA 以 JSON 格式发送的遥测数据示例。当服务管理器收到此输入时，它会聚合来自所有 ASA 的数据，并在发送到 SSE 连接器之前添加必要的报头/字段。信头/字段包括“version”、“metadata”、“payload”、“recordedAt”、“recordType”、“ recordVersion”和 ASA 遥测数据，“smartLicenseProductInstanceIdentifier”、“smartLicenseVirtualAccountName”等。

```
{
  "version": "1.0",
  "metadata": {
    "topic": "ASA.telemetry",
    "contentType": "application/json"
  },
  "payload": {
    "recordType": "CST_ASA",
    "recordVersion": "1.0",
    "recordedAt": 1557363423705,
    "SSP": {
      "SSPdeviceInfo": {
        "deviceModel": "Cisco Firepower FP9300 Security Appliance",
        "serialNumber": "JMX2235L01J",
        "smartLicenseProductInstanceIdentifier": "f85a5bb0-xxxx-xxxx-xxxx-xxxxxxxxx",
        "smartLicenseVirtualAccountName": "SSP-general",
        "systemUptime": 198599,
        "udiProductIdentifier": "FPR-C9300-AC"
      },
      "versions": {
        "items": [
          {
            "type": "package_version",
            "version": "92.7(1.342g)"
          }
        ]
      }
    },
    "asaDevices": {
      "items": [
        {
    "deviceInfo": {
        "deviceModel": "Cisco Adaptive Security Appliance",
        "serialNumber": "AANNNXXX",
        "systemUptime": 285,
        "udiProductIdentifier": "FPR9K-SM-36",
        "deploymentType": "Native",
        "securityContextMode": "Single"
    },
    "versions": {
        "items": [
            {
                "type": "asa_version",
```

```
                "version": "201.4(1)82"
            },
            {
                "type": "device_mgr_version",
                "version": "7.12(1)44"
            }
        ]
    },
    "licenseActivated": {
        "items": [
            {
                "type": "Strong encryption",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-STRONG-ENCRYPTION,1.0_xxxxxxx-xxxx-xxxx-96de-860b59f10bbe",

                "count": 1
            },
            {
                "type": "Carrier",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-MOBILE-SP,1.0_xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
                "count": 1
            }
        ]
    },
    "CPUUsage": {
        "fiveSecondsPercentage": 0,
        "oneMinutePercentage": 0,
        "fiveMinutesPercentage": 0
    },
    "memoryUsage": {
        "freeMemoryInBytes": 99545662064,
        "usedMemoryInBytes": 20545378704,
        "totalMemoryInBytes": 120091040768
    },
    "diskUsage": {
        "freeGB": 21.237027,
        "usedGB": 0.239063,
        "totalGB": 21.476090
    },
    "bandwidthUsage": {
        "receivedPktsPerSec": 3,
        "receivedBytesPerSec": 268,
        "transmittedPktsPerSec": 4,
        "transmittedBytesPerSec": 461
    },
    "featureStatus": {
        "items": [
            {
                "name": "call-home",
                "status": "enabled"
            },
            {
                "name": "cluster",
                "status": "enabled"
            },
            {
                "name": "firewall_user_authentication",
                "status": "enabled"
            },
            {
                "name": "inspection-dns",
                "status": "enabled"
            },
```

```
{
    "name": "inspection-esmtp",
    "status": "enabled"
},
{
    "name": "inspection-ftp",
    "status": "enabled"
},
{
    "name": "inspection-netbios",
    "status": "enabled"
},
{
    "name": "inspection-rsh",
    "status": "enabled"
},
{
    "name": "inspection-sip",
    "status": "enabled"
},
{
    "name": "inspection-sqlnet",
    "status": "enabled"
},
{
    "name": "inspection-sunrpc",
    "status": "enabled"
},
{
    "name": "inspection-tftp",
    "status": "enabled"
},
{
    "name": "inspection-xdmcp",
    "status": "enabled"
},
{
    "name": "logging-console",
    "status": "informational"
},
{
    "name": "management-mode",
    "status": "normal"
},
{
    "name": "sctp-engine",
    "status": "enabled"
},
{
    "name": "threat_detection_basic_threat",
    "status": "enabled"
},
{
    "name": "threat_detection_stat_access_list",
    "status": "enabled"
},
{
    "name": "webvpn-activex-relay",
    "status": "enabled"
},
{
    "name": "webvpn-dtls",
    "status": "enabled"
}
```

```
        ]
    },
    "clusterInfo": {
        "clusterGroupName": "ssp-cluster",
        "interfaceMode": "spanned",
        "unitName": "unit-3-3",
        "unitState": "SLAVE",
        "otherMembers": {
            "items": [
                {
                    "memberName": "unit-2-1",
                    "memberState": "MASTER",
                    "memberSerialNum": "FCH183771BA"
                },
                {
                    "memberName": "unit-2-3",
                    "memberState": "SLAVE",
                    "memberSerialNum": "FLM1949C6JR"
                },
                {
                    "memberName": "unit-2-2",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                },
                {
                    "memberName": "unit-3-2",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                },
                {
                    "memberName": "unit-3-1",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                }
            ]
        }
    },
    "loginHistory": {
        "loginTimes": "1 times in last 1 days",
        "lastSuccessfulLogin": "12:25:36 PDT Mar 11 2019"
    }
}
```


调试遥测数据

开始之前

- 在 ASA 上启用遥测服务。请参阅 启用或禁用思科成功网络 ， 第 1440 页

过程

步骤 1 要查看与遥测相关的调试消息，请在特权 EXEC 模式下使用以下命令启用调试遥测服务：

debug telemetry<*1-255*>

示例：

```
asa# debug telemetry ?
   <1-255>  Specify an optional debug level (default is 1)
```

使用命令的 **no** 形式可禁用调试遥测服务。

步骤 2 要查看所选调试级别的调试遥测消息，请使用以下命令：

show debug telemetry

示例：

```
asa# show debug telemetry
debug telemetry  enabled at level 1

[telemetry_collect_device_info]: telemetry successfully collected device info
[telemetry_collect_versions]: telemetry successfully collected version info
[telemetry_collect_licenses]: no smart-lic entitlement in use
[telemetry_collect_cpu]: telemetry successfully collected cpu info
[telemetry_collect_memory]: telemetry successfully collected mem info
[telemetry_collect_disk_usage]: telemetry successfully collected disk info
[telemetry_collect_bandwidth_usage]: telemetry successfully collected bandwidth usage info
[telemetry_collect_enabled_feature_status]: telemetry successfully collected enabled feature
 info
[telemetry_collect_cluster_info]: telemetry successfully collected cluster info
[telemetry_collect_failover_info]: ha is not configured
[telemetry_get_user_login_hist]: telemetry successfully collected login history
[telemetry_collect_blocks]: telemetry successfully collected block info
[telemetry_collect_perfmon]: telemetry successfully collected perfmon stats
[telemetry_collect_resource_usage]: telemetry successfully collected res usage
[telemetry_collect_process_cpu_usage]: telemetry successfully collected res usage
[telemetry_collect_crashinfo]: telemetry successfully collected crashinfo
[telemetry_collect]: the serialized string is generated
[telemetry_collect]: successfully allocated mem for serialized string
[telemetry_history_add_record]: telemetry has a new history record: 16:23:29 PDT Oct 22
2019: Telemetry support on the blade: enabled
[telemetry_history_add_record]: telemetry has a new history record: 16:24:01 PDT Oct 22
2019: Telemetry support on the blade: disabled
```

第 49 章

Anonymous Reporting 和 Smart Call Home

本章介绍如何配置 Anonymous Reporting 和 Smart Call Home 服务。

- 关于 Anonymous Reporting，第 1449 页
- 关于 Smart Call Home，第 1450 页
- Anonymous Reporting 和 Smart Call Home 准则，第 1456 页
- 配置 Anonymous Reporting 和 Smart Call Home，第 1457 页
- 监控 Anonymous Reporting 和 Smart Call Home，第 1468 页
- Smart Call Home 示例，第 1469 页
- Anonymous Reporting 和 Smart Call Home 的历史记录，第 1470 页

关于 Anonymous Reporting

可以通过启用 Anonymous Reporting 服务来帮助改进 ASA 平台，此服务使思科能够安全地接收来自设备的最少量错误和运行状况信息。启用此功能后，客户身份将保持匿名，并且不会发送任何识别信息。

启用 Anonymous Reporting 将会创建信任点并安装证书。ASA 需要 CA 证书以验证 Smart Call Home Web 服务器上存在的服务器证书并建立 HTTPS 会话，以使 ASA 能够安全地发送消息。思科将导入软件中预定义的证书。如果决定启用 Anonymous Reporting，则 ASA 上将会安装一个证书，其硬编码的信任点名称为 _SmartCallHome_ServerCA。当启用 Anonymous Reporting 时，系统将会创建此信任点，安装相应的证书，并且您将接收到有关此操作的消息。然后，该证书将出现在配置中。

如果启用 Anonymous Reporting 时相应的证书已存在于配置中，则不会创建信任点，并且不会安装任何证书。

注释 启用 Anonymous Reporting 即表示您同意将指定的数据传输至思科或代表思科运营的供应商（包括美国以外的国家/地区）。思科将保护所有客户的隐私。有关思科对个人信息处理方式的信息，请参阅思科隐私权生命，网址如下： http://www.cisco.com/web/siteassets/legal/privacy.html

ASA 在后台配置 Smart Call Home 匿名报告时，ASA 会自动创建一个包含颁发 Call Home 服务器证书的 CA 的证书的信任点。现在，如果服务器的颁发层次结构发生变化，ASA 支持对证书进行验证，而无需客户来进行证书层次结构更改。您也可以自动导入信任池证书，以便 ASA 可以在不进行任何人工干预的情况下更新证书层次结构。

升级 ASA 9.14(2.14) 时，信任点配置会自动从 CallHome_ServerCA 更改为 CallHome_ServerCA2。

DNS 要求

必须正确配置 DNS 服务器，ASA 才能访问 Cisco Smart Call Home 服务器并向思科发送消息。由于 ASA 可能位于专用网络中，而未接入公用网络，因此思科将验证 DNS 配置，并在必要时通过执行以下任务来配置 DNS：

1. 为所有已配置的 DNS 服务器执行 DNS 查找。
2. 通过在最高安全级别的接口上发送 DHCPINFORM 消息，从 DHCP 服务器获取 DNS 服务器。
3. 使用思科 DNS 服务器进行查找。
4. 将静态 IP 地址随机用于 tools.cisco.com。

执行这些任务并不会更改当前配置。（例如，从 DHCP 获取的 DNS 服务器不会添加到配置中。）

如果未配置任何 DNS 服务器，并且 ASA 无法访问 Cisco Smart Call Home 服务器，则对于发送的每条 Smart Call Home 消息，思科都将生成一条严重性级别为“警告”的系统日志消息，以提醒您正确配置 DNS。

有关系统日志消息的信息，请参阅系统日志消息指南。

关于 Smart Call Home

对 Smart Call Home 服务进行全面配置后，此服务可以检测到站点中的问题，并且通常在您知道这些问题存在之前，向思科报告这些问题或者通过用户定义的其他渠道进行报告（例如通过邮件报告或者直接向您报告）。根据这些问题的严重性，思科将通过提供以下服务，对系统配置问题、产品寿命终止声明以及安全公告问题等等作出回应：

- 通过持续进行监控、发出实时的主动警报以及进行详细诊断，迅速确定问题。
- 通过 Smart Call Home 通知使您知晓潜在的问题，在这些通知中，已提交服务请求，并随附了所有诊断数据。
- 自动直接联系思科 TAC 专家，更迅速地解决紧急问题。
- 缩短故障排除时间，从而更高效地利用员工资源。

- 自动生成发往思科 TAC 的服务请求（如果签订了服务合同），这些请求将发送给适当的支持团队，该支持团队将提供可以加快解决问题的详细诊断信息。

可以通过 Smart Call Home 门户快速访问使您能够执行下列活动的必需信息：

- 在一个位置查看所有 Smart Call Home 消息、诊断信息和建议。
- 检查服务请求状态。
- 查看所有支持 Smart Call Home 的设备的最新清单和配置信息。

订用警报组

警报组是 ASA 上支持的 Smart Call Home 警报的预定义子集。各种类型的 Smart Call Home 警报根据其类型分组到不同的警报组中。每个警报组都报告特定 CLI 的输出。受支持的 Smart Call Home 警报组如下所示：

- syslog
- 诊断
- 环境
- 清单
- 配置
- 威胁
- 快照
- 遥测
- 测试

警报组的属性

警报组具有下列属性：

- 事件首先向一个警报组注册。
- 一个组可以与多个事件相关联。
- 可以订用特定警报组。
- 可以启用和禁用特定警报组。对所有警报组都启用了默认设置。
- 诊断和环境警报组支持订用周期性消息。
- 系统日志警报组支持基于消息 ID 的订用。
- 对于环境警报组，可以配置 CPU 和内存使用率阈值。当某个参数超过预定义的阈值时，将发送消息。大部分阈值依赖于平台，并且不可更改。

- 可以配置快照警报组，以便发送所指定的 CLI 的输出。

通过警报组发送给思科的消息

消息定期发送到思科，每当 ASA 重新加载时，也会发送这些消息。这些消息按警报组进行分类。

清单警报包含下列命令的输出：

- **show version** - 显示设备的 ASA 软件版本、硬件配置、许可密钥和相关运行时间数据。
- **show inventory**—检索并显示网络设备中安装的每款思科产品的相关清单信息。每款产品都由唯一的设备信息（称为 UDI）进行标识，UDI 是以下三个不同数据元素的组合：产品标识符 (PID)、版本标识符 (VID) 和序列号 (SN)。
- **show failover state** - 显示故障转移对中的两个装置的故障转移状态。显示的信息包括设备的主要或辅助状态、设备的主用/备用状态以及最新报告的故障转移原因。
- **show environment** - 显示 ASA 系统组件的系统环境信息，例如机箱、驱动器、风扇和电源的硬件运行状态以及温度状态、电压和 CPU 利用率。

配置警报包含下列命令的输出：

- **show context**- 显示已分配的接口、配置文件 URL 以及配置的情景数目，如果在系统执行空间中启用了匿名报告，则显示所有情景的列表。
- **show call-home registered-module status**- 显示已注册的模块状态。如果使用系统配置模式，则此命令将根据整台设备（而不是每个情景）显示系统模块状态。
- **show running-config** - 显示 ASA 上当前正在运行的配置。
- **show startup-config** - 显示启动配置。
- **show access-list | include elements** - 显示命中计数器和访问列表的时间戳值。

诊断警报包含下列命令的输出：

- **show failover** - 显示有关装置的故障转移状态的信息。
- **show interface - 显示接口统计信息**。
- **show cluster info - 显示集群信息**。
- **show cluster history - 显示集群历史记录**。
- **show crashinfo**（截断） - 发生意外的软件重新加载之后，设备将发送修改后的崩溃信息文件（仅包括该文件的回溯部分），以便仅向思科报告函数调用、注册表值和堆栈转储。
- **show tech-support no-config - 显示由技术支持分析师用于诊断的信息**。

环境警报包含下列命令的输出：

- **show environment** - 显示 ASA 系统组件的系统环境信息，例如机箱、驱动器、风扇和电源的硬件运行状态以及温度状态、电压和 CPU 利用率。

- **show cpu usage** - 显示 CPU 利用率信息。
- **show memory detail** - 显示有关可用系统内存和已分配系统内存的详细信息。

威胁警报包含下列命令的输出：

- **show threat-detection rate** - 显示威胁检测统计信息。
- **show threat-detection shun** - 显示当前绕过的主机。
- **show shun** - 显示绕过信息。
- **show dynamic-filter reports top** - 生成按僵尸网络流量过滤器分类的前 10 个恶意软件站点、端口和受感染主机的报告。

快照警报可能包含下列命令的输出：

- **show conn count** - 显示处于活动状态的连接的数目。
- **show asp drop** - 显示加速安全路径丢弃的数据包或连接数。

遥测警报包含下列命令的输出：

- **show perfmon detail** - 显示 **ASA** 性能详细信息。
- **show traffic** - 显示接口发送和接收活动。
- **show conn count** - 显示处于活动状态的连接的数目。
- **show vpn-sessiondb summary** - 显示 **VPN** 会话摘要信息。
- **show vpn load-balancing** - 显示 **VPN** 负载均衡虚拟集群配置的运行时统计信息。
- **show local-host | include interface** - 显示本地主机的网络状态。
- **show memory** - 显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要。
- **show context**- 显示已分配的接口、配置文件 URL 以及配置的情景数目，如果在系统执行空间中启用了匿名报告，则显示所有情景的列表。
- **show access-list | include elements** - 显示命中计数器和访问列表的时间戳值。
- **show interface** - 显示接口统计信息。
- **show threat-detection statistics protocol** - 显示 **IP** 协议统计信息。
- **show phone-proxy media-sessions count** - 显示 **Phone Proxy** 所存储的相应介质会话数。
- **show phone-proxy secure-phones count** - 显示数据库中存储的支持安全模式的电话数。
- **show route** - 显示路由表。
- **show xlate count** - 显示 **NAT** 会话 **(xlate)** 的数目。

消息严重性阈值

使目标配置文件订用某些警报组时，可以设置阈值，以便根据消息严重性级别发送警报组消息。值小于目标配置文件的指定阈值的所有消息都不会发送到目标。

下表显示消息严重性级别与系统日志严重性级别之间的对应关系。

表 *77*: 消息严重性级别与系统日志级别对应关系

Level	消息 严重性级别	系统日志 严重性级别	说明
9	巨大灾难	不适用	全网范围的灾难性故障。
8	灾难	不适用	重大网络影响。
7	由指定的 CLI 关键字确定： **subscribe-to-alert-group** 警报组名称 **severity** 严重性级别	0	紧急。系统不可用。
6	由指定的 CLI 关键字确定： **subscribe-to-alert-group** 警报组名称 **severity** 严重性级别	1	警报。严重情况；需要立即引起注意。
5	由指定的 CLI 关键字确定： **subscribe-to-alert-group** 警报组名称 **severity** 严重性级别	2	严重。严重情况。
4	由指定的 CLI 关键字确定： **subscribe-to-alert-group** 警报组名称 **severity** 严重性级别	3	错误。轻微情况。
3	警告	4	警告情况。
2	通知	5	基本通知和信息消息。可能是独立的无关紧要情况。
1	正常状态	6	信息。正常事件，表示恢复正常状态。
0	调试	7	调试消息（默认设置）。

订用配置文件

订用配置文件使您能够将目标收件人与感兴趣的组相关联。在配置文件中向订用的组注册的事件被触发时，与该事件相关联的消息将发送到配置的收件人。订用配置文件具有下列属性：

- 可以创建并配置多个配置文件。
- 一个配置文件可以配置多个邮件或 HTTPS 收件人。
- 一个配置文件可以使多个组订用指定的严重性级别。
- 配置文件支持三种消息格式：短文本、长文本和 XML。
- 可以启用和禁用特定配置文件。默认情况下，配置文件处于禁用状态。
- 可以指定最大消息大小。默认为 3 MB。

已提供一个默认配置文件“Cisco TAC”。默认配置文件包含一组要监控的预定义组（诊断、环境、清单、配置和遥测）以及预定义的目标邮件地址和 HTTPS URL。最初配置 Smart Call Home 时，系统将自动创建默认配置文件。目标邮件地址为 callhome@cisco.com，目标 URL 为 https://tools.cisco.com/its/service/oddce/services/DDCEService。

注释 无法更改默认配置文件的目标邮件地址或目标 URL。

在使目标配置文件订用配置、清单、遥测或快照警报组时，可以选择以异步方式接收或者在指定时间定期接收警报组消息。

下表将默认警报组映射到其严重性级别订用和周期（如果适用）：

表 *78:* 警报组到严重性级别订用的映射

警报组	严重性级别	周期
配置	信息	每月
诊断	信息及更高级别	不适用
环境	通知及更高级别	不适用
清单	信息	每月
快照	信息	不适用
系统日志	等效系统日志	不适用
遥测	信息	每天
测试	不适用	不适用
威胁	通知	不适用

Anonymous Reporting 和 Smart Call Home 准则

本节介绍在配置 Anonymous Reporting 和 Smart Call Home 之前应查看的准则和限制。

Anonymous Reporting 准则

- 必须配置 DNS。
- 如果首次尝试无法发送 Anonymous Reporting 消息，则 ASA 将再重试两次，然后才丢弃该消息。
- Anonymous Reporting 可以与其他 Smart Call Home 配置共存，而不会更改现有配置。例如，如果启用 Anonymous Reporting 之前 Smart Call Home 处于禁用状态，那么 Smart Call Home 将保持禁用状态，即使在 Anonymous Reporting 启用后也是如此。
- 如果 Anonymous Reporting 处于启用状态，将无法删除信任点，并且禁用 Anonymous Reporting 时，信任点仍保留。如果 Anonymous Reporting 处于禁用状态，则可以删除信任点，但禁用 Anonymous Reporting 不会导致删除信任点。
- 如果使用的是多情景模式配置，则 **dns**、**interface** 和 **trustpoint** 命令处于管理情景中，而 **call-home** 命令处于系统情景中。
- 您可以按照定期间隔自动进行 trustpool 捆绑包的更新，以便在 CA 服务器的自签名证书更改时，Smart Call Home 可以保持活动状态 。此 trustpool 自动续订功能在多情景部署下不受支持。

Smart Call Home 准则

- 在多情景模式下，subscribe-to-alert-group snapshot periodic 命令划分成两条命令：一条命令用于从系统配置中获取信息，另一条命令用于从用户情景中获取信息。
- Smart Call Home 后台服务器只能接受 XML 格式的消息。
- 如果已启用集群功能，并且已将 Smart Call Home 配置为订用严重性级别为“严重”的诊断警报组，那么将向思科发送 Smart Call Home 消息以报告重要的集群事件。仅对于下列事件，才会发送 Smart Call Home 集群消息：
  - 当装置加入集群时
  - 当装置离开集群时
  - 当集群装置变成集群控制设备时
  - 当集群中的辅助装置发生故障时

  发送的每条消息都包含以下信息：
  - 处于活动状态的集群成员的计数
  - 对集群控制设备运行的 **show cluster info** 命令和 **show cluster history** 命令的输出

配置 Anonymous Reporting 和 Smart Call Home

虽然 Anonymous Reporting 是 Smart Call Home 服务的组成部分，并且使思科能够以匿名方式接收来自设备的最少量错误和运行状况信息，但是 Smart Call Home 服务提供了对系统运行状况的自定义支持，从而使思科 TAC 能够监控设备，并且在存在问题时（通常在知道问题已发生之前）提交个案。

可以在系统上同时配置这两个服务，尽管配置 Smart Call Home 服务将会提供与 Anonymous Reporting 相同的功能以及自定义服务。

进入配置模式时，系统将会显示提示符，要求您根据下列准则启用 Anonymous Reporting 和 Smart Call Home 服务：

- 在提示符处，可以选择 [Y]（是）、[N]（否）或 [A]（稍后询问）。如果选择 [A]（稍后询问），则系统将在 7 天后或者在 ASA 重新加载时再次提醒您。如果继续选择 [A]（稍后询问），则 ASA 将以 7 天作为时间间隔再次提示 2 次，然后采用 [N]（否）响应并且不再询问。
- 如果未收到提示符，可通过执行配置 Anonymous Reporting，第 1457 页或配置 Smart Call Home，第 1458 页中的步骤启用 Anonymous Reporting 或 Smart Call Home。

配置 Anonymous Reporting

要配置 Anonymous Reporting，请执行以下步骤：

过程

步骤 1 启用 Anonymous Reporting 功能并创建新的匿名配置文件。

call-home reporting anonymous

示例：

```
ciscoasa(config)# call-home reporting anonymous
```

输入此命令将会创建信任点，并安装用来验证思科 Web 服务器身份的证书。

步骤 2 （可选）确保已连接到服务器并且系统能够发送消息。

call-home test reporting anonymous

示例：

```
ciscoasa(config)# call-home test reporting anonymous

INFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...

INFO: Succeeded
```

系统将通过一条成功或错误消息返回测试结果。

配置 Smart Call Home

在 ASA 上配置 Smart Call Home 服务包括下列任务：

过程

步骤 1 启用 Smart Call Home 服务。请参阅启用 Smart Call Home，第 1458 页。

步骤 2 配置用于将 Smart Call Home 消息传递给用户的邮件服务器。请参阅配置邮件服务器，第 1463 页。

步骤 3 为 Smart Call Home 消息设置联系人信息。请参阅配置客户联系信息，第 1462 页。

步骤 4 定义警报处理参数，例如可以处理的最大事件率。请参阅配置警报组订用，第 1460 页。

步骤 5 设置警报订用配置文件。请参阅配置目标配置文件，第 1465 页。

每个警报订用配置文件都标识了以下信息：

- Smart Call Home 消息所发送到的用户，例如思科的 Smart Call Home 服务器或一系列邮件收件人。
- 要针对其接收警报的信息类别，例如配置或清单信息。

启用 Smart Call Home

要启用 Smart Call Home 并激活报障配置文件，请执行以下步骤：

过程

步骤 1 启用 Smart Call Home 服务。

service call-home

示例：

```
ciscoasa(config)# service call-home
```

步骤 2 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call home
```

声明和验证证书颁发机构信任点

如果 Smart Call Home 配置为通过 HTTPS 向网络服务器发送消息，则需要将 ASA 配置为信任该 Web 服务器的证书或签发该证书的证书颁发机构 (CA) 的证书。Cisco Smart Call Home Production 服务器证书由 Verisign 签发。Cisco Smart Call Home Staging 服务器证书由 Digital Signature Trust Company 签发。

注释 不应该为客户端类型或验证用途设置信任点，以避免将信任点用于 VPN 验证。

要声明思科服务器安全认证并对其进行身份验证，然后与 Smart Call Home 服务的思科 HTTPS 服务器进行通信，请执行以下步骤：

过程

步骤 1 （仅限多情景模式）在管理情景中安装证书。

changeto context *admincontext*

示例：

```
ciscoasa(config)# changeto context contextA
```

步骤 2 配置信任点并为认证登记作准备。

crypto ca trustpoint *trustpoint-name*

示例：

```
ciscoasa(config)# crypto ca trustpoint cisco
```

注释
如果使用 HTTP 作为传输方法，则必须通过信任点安装 HTTPS 所需的安全认证。请在以下 URL 处查找要安装的特定证书：

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380

步骤 3 指定以手动剪切并粘贴的方法进行认证登记。

enroll terminal

示例：

```
ciscoasa(ca-trustpoint)# enroll terminal
```

步骤 4 对指定的 CA 进行身份验证。CA 名称应与 **crypto ca trustpoint** 命令中指定的信任点名称匹配。在提示符处，粘贴安全认证文本。

crypto ca authenticate trustpoint

示例：

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

步骤 5 指定安全认证文本结束，并确认接受所输入的安全证书。

quit

示例：

```
ciscoasa(ca-trustpoint)# quit
%Do you accept this certificate [yes/no]:
yes
```

配置环境和快照警报组

要配置环境警报组和快照警报组，请执行以下步骤：

过程

进入警报组配置模式。

alert-group-config {**environment** | **snapshot**}

示例：

```
ciscoasa(config)# alert-group-config environment
```

配置警报组订用

要使目标配置文件订用警报组，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 启用指定的 Smart Call Home 警报组。

alert-group {**all** | **configuration** | **diagnostic** | **environment** | **inventory** | **syslog**}

示例：

```
ciscoasa(cfg-call-home)# alert-group syslog
```

使用 **all** 关键字启用所有警报组。默认情况下，所有警报组都处于启用状态。

步骤 3 进入指定目标配置文件的配置文件配置模式。

profile *profile-name*

示例：

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

步骤 4 订用所有的可用警报组。

subscribe-to-alert-group all

示例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

步骤 5 使此目标配置文件订用配置警报组。

subscribe-to-alert-group configuration periodic {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

示例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
```

periodic 关键字可为配置警报组配置定期通知。默认周期为每日。

daily 关键字以 *hh:mm* 格式指定每天的发送时间（采用 24 小时制，例如 14:30）。

weekly 关键字以 *day hh:mm* 格式指定一周内的哪几天和一天内的时间，其中星期几将拼写出来（例如 Monday）。

monthly 关键字以 *date hh:mm* 格式指定数字日期（1 到 31）和一天内的时间。

配置客户联系信息

要配置客户联系信息，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 指定客户电话号码。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

phone-number *phone-number-string*

示例：

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

步骤 3 指定客户地址，地址是长度最多为 255 个字符的自由格式字符串。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

street-address *street-address*

示例：

```
ciscoasa(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
```

步骤 4 指定客户姓名，姓名长度可达 128 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

contact-name *contact-name*

示例：

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

步骤 5 指定思科客户 ID，此 ID 的长度最多为 64 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

customer-id *customer-id-string*

示例：

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

步骤 6 指定思科客户 ID，此 ID 的长度最多为 64 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

site-id *site-id-string*

示例：

```
ciscoasa(cfg-call-home)# site-id site1234
```

步骤 7 指定客户合同 ID，此 ID 的长度最多为 128 个字符。允许使用空格，但在字符串包含空格时，必须使用引号将其括起来。

contract-id *contract-id-string*

示例：

```
ciscoasa(cfg-call-home)# contract-id contract1234
```

示例

以下示例显示如何配置联系信息：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
ciscoasa(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234
```

配置邮件服务器

建议您使用 HTTPS 进行消息传输，因为此协议最安全。但是，您可以为 Smart Call Home 配置邮件目标，然后将邮件服务器配置为使用邮件消息传输。

要配置邮件服务器，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 指定 SMTP 邮件服务器。

mail-server*ip-address* **name priority** [**1-100**] [**all**]

示例：

```
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1
```

可以使用 5 个单独的命令指定多达 5 个邮件服务器。必须至少将一个邮件服务器配置为使用邮件传输方法来传输 Smart Call Home 消息。

数字越小，邮件服务器的优先级越高。

ip-address 参数可以是 IPv4 或 IPv6 邮件服务器地址。

示例

以下示例显示如何配置主邮件服务器（名为“smtp.example.com”）和辅助邮件服务器（IP 地址为 10.10.1.1）：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
ciscoasa(cfg-call-home)# exit
ciscoasa(config)#
```

配置流量速率限制

要配置流量速率限制，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 指定 Smart Call Home 每分钟可以发送的消息数。默认值为 10 条消息/分钟。

rate-limit *msg-count*

示例：

```
ciscoasa(cfg-call-home)# rate-limit 5
```

发送 Smart Call Home 通信

要发送特定 Smart Call Home 通信，请执行以下步骤：

过程

选择以下其中一个选项：

- 选项 1 - 使用配置文件配置来手动发送测试消息。

  call-home test [*test-message*] **profile** *profile-name*

  示例：

  ```
  ciscoasa# call-home test [testing123] profile CiscoTAC-1
  ```

- 选项2 - 向一个目标配置文件（如果已指定）发送警报组消息。如果未指定配置文件，则向订用了清单、配置、快照或遥测警报组的所有配置文件发送消息。

  call-home send alert-group inventory { | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

  示例：

  ```
  ciscoasa# call-home send alert-group inventory
  ```

- 选项3 - 将命令输出发送到邮件地址。指定的CLI命令可以是任何命令，包括用于所有已注册的模块的命令。

  call-home send*cli command* [**email** *email*]

  示例：

  ```
  ciscoasa# call-home send cli destination email username@example.com
  ```

  如果已指定邮件地址， 命令输出将被发送到该地址。如果未指定邮件地址，则输出将发送到思科 TAC。邮件将以日志文本格式发送，服务编号（如果已指定）将包括在主题行中。

  仅在未指定邮件地址或已指定思科 TAC 邮件地址时， 才需要服务编号。

配置目标配置文件

要配置目标配置文件以进行邮件或 HTTP 传输，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 进入指定目标配置文件的配置文件配置模式。如果指定的目标配置文件不存在，将会创建该文件。

profile *profile-name*

示例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

最多可以创建 10 个处于活动状态的配置文件。默认配置文件将向思科 TAC 报告。如果要将报障信息发送到其他位置（例如您自己的服务器），则可以配置一个单独的配置文件。

步骤 3 配置 Smart Call Home 消息接收方的目标、消息大小、消息格式和传输方法。默认消息格式为 XML，默认启用的传输方法为邮件。

destination address {**email** *address* | **http** *url*[**reference-identity** *ref-id-name*]} | **message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

示例：

```
ciscoasa(cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService reference-identity
ExampleService

ciscoasa(cfg-call-home-profile)# destination address email username@example.com
ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

reference-identity 选项可启用对收到的服务器证书的 RFC 6125 参考身份检查。这些检查仅适用于配置了 http 地址的目标。ID 检查根据以前配置的参考身份对象执行。有关参考身份对象的详细信息，请参阅配置引用标识，第 889 页。

邮件地址是 Smart Call Home 消息接收方的邮件地址，此地址的长度可达 100 个字符。默认情况下，最大 URL 大小为 5 MB。

在移动设备上，使用短文本格式来发送和读取消息；在计算机上，使用长文本格式来发送和读取消息。

如果消息接收方是 Smart Call Home 后台服务器，请确保 **preferred-msg-format** 值是 XML，这是因为后端服务器只能接受 XML 格式的消息。

使用此命令可以将传输方法重新更改为邮件。

复制目标配置文件

要通过复制现有的目标配置文件来创建新的目标配置文件，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 指定要复制的配置文件。

profile *profile-name*

示例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

步骤 3 将现有配置文件的内容复制到新配置文件。

copy profile *src-profile-name dest-profile-name*

示例：

```
ciscoasa(cfg-call-home)# copy profile newprofile profile1
```

现有配置文件 (*src-profile-name*) 和新配置文件 (*dest-profile-name*) 的长度可达 23 个字符。

示例

以下示例显示如何复制现有配置文件：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1
```

重命名目标配置文件

要更改现有配置文件的名称，请执行以下步骤：

过程

步骤 1 进入报障配置模式。

call-home

示例：

```
ciscoasa(config)# call-home
```

步骤 2 指定要重命名的配置文件。

profile *profilename*

示例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

步骤 3 更改现有配置文件的名称。

rename profile *src-profile-name dest-profile-name*

示例：

```
ciscoasa(cfg-call-home)# rename profile newprofile profile1
```

现有配置文件 (*src-profile-name*) 和新配置文件 (*dest-profile-name*) 的长度可达 23 个字符。

示例

以下示例显示如何重命名现有配置文件：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

监控 Anonymous Reporting 和 Smart Call Home

请参阅以下命令来监控 Anonymous Reporting 和 Smart Call Home 服务。

- **show call-home detail**

  此命令显示当前 Smart Call Home 详细配置。

- **show call-home mail-server status**

此命令显示当前邮件服务器状态。

- **show call-home profile** {profile name | **all**}

  此命令显示 Smart Call Home 配置文件的配置。

- **show call-home registered-module status** [**all**]

  此命令显示已注册的模块状态。

- **show call-home statistics**

  此命令显示报障详细状态。

- **show call-home**

  此命令显示当前 Smart Call Home 配置。

- **show running-config call-home**

  此命令显示当前 Smart Call Home 运行配置。

- **show smart-call-home alert-group**

  此命令显示 Smart Call Home 警报组的当前状态。

- **show running-config all**

  此命令显示有关 Anonymous Reporting 用户配置文件的详细信息。

Smart Call Home 示例

以下示例显示如何配置 Smart Call Home 服务：

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group telemetry periodic weekly Monday
 23:30
```

Anonymous Reporting 和 Smart Call Home 的历史记录

表 *79: Anonymous Reporting* 和 *Smart Call Home* 的历史记录

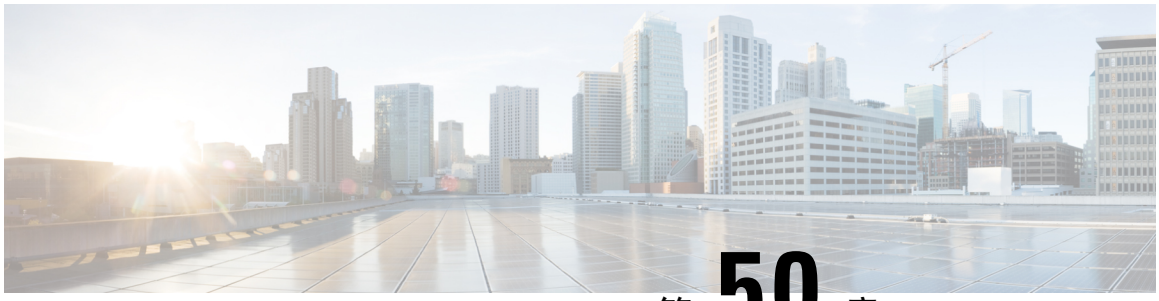
功能名称	平台版本	说明
Smart Call Home	8.2(2)	Smart Call Home 服务用于在 ASA 上提供主动诊断和实时警报，并提供更高的网络可用性和运行效率。 引入或修改了下列命令： **active (call home)**、**call-home**、**call-home send alert-group**、**call-home test**、**contact-email-addr**、**customer-id (call home)**、**destination (call home)**、**profile**、**rename profile**、**service call-home**、**show call-home**、**show call-home detail**、**show smart-call-home alert-group**、**show call-home profile**、**show call-home statistics**、**show call-home mail-server status**、**show running-config call-home**、**show call-home registered-module status all**、**site-id**、**street-address**、**subscribe-to-alert-group all**、**alert-group-config**、**subscribe-to-alert-group configuration**、**subscribe-to-alert-group diagnostic**、**subscribe-to-alert-group environment**、**subscribe-to-alert-group inventory periodic**、**subscribe-to-alert-group snapshot periodic**、**subscribe-to-alert-group syslog** 和 **subscribe-to-alert-group telemetry periodic**。
Anonymous Reporting	9.0(1)	可以通过启用 Anonymous Reporting 服务来帮助改进 ASA 平台，此服务使思科能够安全地接收来自设备的最少量错误和运行状况信息。 引入了以下命令：**call-home reporting anonymous** 和 **call-home test reporting anonymous**。
Smart Call Home	9.1(2)	**show local-host** 命令已更改为 **show local-host | include interface** 命令，以进行遥测警报组报告。

功能名称	平台版本	说明
Smart Call Home	9.1(3)	如果已启用集群功能，并且已将 Smart Call Home 配置为订用严重性级别为“严重”的诊断警报组，那么将向思科发送 Smart Call Home 消息以报告重要的集群事件。仅对于以下三个事件，才会发送 Smart Call Home 集群消息： • 当装置加入集群时 • 当装置离开集群时 • 当集群装置变成集群控制设备时 发送的每条消息都包含以下信息： • 处于活动状态的集群成员的计数 • 对集群控制设备运行的 **show cluster info** 命令和 **show cluster history** 命令的输出
安全 Smart Call Home 服务器连接的引用标识	9.6(2)	TLS 客户端处理现在支持针对 RFC 6125 第 6 节中定义的服务器身份验证的规则。标识验证将在对通向 Smart Call Home 服务器的 TLS 连接进行 PKI 验证时完成。如果提供的标识无法与配置的引用标识相匹配，则不会建立连接。 添加或修改了以下命令：**[no] crypto ca reference-identity**、**call home profile destination address http**。

第 IX 部分

参考

- 使用命令行界面， 第 1475 页
- 地址、协议和端口， 第 1485 页



第 50 章

使用命令行界面

本章介绍如何在 ASA 上使用 CLI。

注释 CLI 与思科 IOS CLI 使用类似的语法和其他约定，但 ASA 操作系统不是思科 IOS 软件的版本。请勿假定思科 IOS CLI 命令可与 ASA 一起使用或与之具有相同的功能。

- 防火墙模式和安全情景模式，第 1475 页
- 命令模式和提示符，第 1476 页
- 语法格式，第 1477 页
- 缩写命令，第 1478 页
- 命令行编辑，第 1478 页
- 命令补全，第 1478 页
- 命令帮助，第 1478 页
- 查看运行配置，第 1479 页
- 过滤 show 和 more 命令输出，第 1479 页
- 重定向和待处理 show 命令输出，第 1480 页
- 获取 show 命令输出的行计数，第 1480 页
- 命令输出分页，第 1481 页
- 添加注释，第 1482 页
- 文本配置文件，第 1482 页
- 支持的字符集，第 1483 页

防火墙模式和安全情景模式

ASA 在以下模式组合下运行：

- 透明防火墙或路由防火墙模式

  该防火墙模式确定 ASA 作为第 2 层还是第 3 层防火墙运行。

- 多情景模式或单情景模式

此安全情景模式确定ASA作为单台设备运行还是作为多个安全情景（类似于虚拟设备的作用）运行。

有些命令仅在特定模式下可用。

命令模式和提示符

ASA CLI 包括命令模式。有些命令只能在特定模式下输入。例如，要输入显示敏感信息的命令，您需要输入密码并进入具有更多特权的模式。然后，为确保不会意外输入配置更改，必须进入配置模式。所有较低的命令均可在较高模式下输入。例如，可以在全局配置模式下输入特权 EXEC 命令。

注释 各种类型的提示全部是默认提示，并且配置后可能会不同。

- 当处于系统配置模式或单情景模式时，提示以主机名开头：

  ```
  ciscoasa
  ```

- 在打印提示字符串时，系统会解析提示配置并按您设置的提示命令的顺序打印配置的关键字值。关键字参数可以是以下任意项并且可采用任意顺序：主机、域、情景、优先级、状态。

  prompt hostname context priority state

- 如果您在某一情景中，则提示符以主机名开头，后跟情景名称：

  ```
  ciscoasa/context
  ```

提示根据访问模式而异：

- 用户执行模式

  用户 EXEC 模式允许您查看最低 ASA 设置。当您首次访问 ASA 时，用户 EXEC 模式提示按以下方式显示：

  ```
  ciscoasa>
  ```

  ```
  ciscoasa/context>
  ```

- 特权执行模式

  通过特权EXEC模式可查看特权级别内的所有当前设置。任何用户EXEC模式命令在特权EXEC模式下都将适用。在用户 EXEC 模式下输入 **enable** 命令（需要密码），以启动特权 EXEC 模式。提示包含数字符号 (#)：

  ```
  ciscoasa#
  ```

```
ciscoasa/context#
```

- 全局配置模式

  全局配置模式允许您更改 ASA 配置。所有用户 EXEC、特权 EXEC 和全局配置命令在此模式下均可用。在特权 EXEC 模式下输入 **configure terminal** 命令，以启动全局配置模式。提示将更改为以下形式：

```
ciscoasa(config)#

ciscoasa/context(config)#
```

- 命令特定配置模式

  从全局配置模式下，某些命令可进入命令特定配置模式。所有用户 EXEC、特权 EXEC、全局配置和命令特定配置命令在此模式下均可用。例如，使用 **interface** 命令会进入接口配置模式。提示将更改为以下形式：

```
ciscoasa(config-if)#

ciscoasa/context(config-if)#
```

语法格式

命令语法说明采用下表所列的约定。

表 *80:* 语法约定

约定	说明
粗体	粗体文本指示按字面显示输入的命令和关键字。
斜体	斜体文本指示由您提供值的参数。
[x]	方括号中包含可选元素（关键字或参数）。
|	竖线指示可选或必需的关键字或参数集中的选项。
[x | y]	将以竖线分隔的关键字或参数括起来的方括号指示可选选项。
{x | y}	将以竖线分隔的关键字或参数括起来的大括号指示必需选项。
[x {y | z}]	方括号或大括号的嵌套集合指示可选或必需元素中的可选或必需选项。方括号中的大括号和竖线指示可选元素中的必需选项。

缩写命令

您可以将大多数命令缩写为最少的命令独有字符；例如，您可以输入 **wr t**（而不是输入完整命令 **write terminal**）查看配置，也可以输入 **en** 启动特权模式和输入 **conf t** 启动配置模式。此外，还可以输入 **0** 以表示 **0.0.0.0**。

命令行编辑

ASA 使用的命令行编辑规则与思科 IOS 软件相同。使用 **show history** 命令可查看以前输入的所有命令；使用向上箭头或 **^p** 命令可逐个查看以前输入的所有命令。在检查以前输入的命令后，可使用向下箭头或 **^n** 命令在列表中向前移动。到达想要重新使用的命令后，您可以编辑该命令或按 **Enter** 键启动该命令。此外，还可以使用 **^w** 删除光标左侧的词语，或使用 **^u** 擦除整行。

ASA 在命令中最多允许 512 个字符，额外的字符将被忽略。

命令补全

要在输入部分字符串后补全命令或关键字，请按 **Tab** 键。仅当部分字符串仅与一个命令或关键字匹配时，ASA 才会补全命令或关键字。例如，如果输入 **s** 并按 **Tab** 键，则 ASA 不会补全命令，因为它与多个命令匹配。但是，如果输入 **dis**，则 **Tab** 键会补全 **disable** 命令。

命令帮助

通过输入以下命令，可从命令行获取帮助信息：

- **help** *command_name*

  显示特定命令的帮助。

- *command_name* **?**

  显示可用参数列表。

- *string***?**（无空格）

  列出以字符串开头的可能命令。

- ？和 **+?**

  列出所有可用命令。如果输入 **?**，ASA 仅显示当前模式可用的命令。要显示所有可用命令，包括可用于较低模式的命令，请输入 **+?**。

注释 如果要在命令字符串中包含问号 (?)，则在键入问号之前必须按 **Ctrl-V**，以便不会无意中调用 CLI 帮助。

查看运行配置

要查看运行配置，请使用以下其中一个选项：

- **show running-config** [**all**] [*command*]

  如果指定 **all**，则还会显示所有默认设置。如果指定 *command*，则输出仅包含相关命令。

注释 许多关键字都显示为 *****。要以明文或以加密形式（如果已启用主密码）查看密码，请使用 **more** 命令。

- **more system:running-config**

过滤 **show** 和 **more** 命令输出

您可以将竖线 (|) 与任何 **show** 命令配合使用，并包含过滤器选项和筛选表达式。与思科 IOS 软件类似，通过将各输出行与正则表达式匹配来执行筛选。通过选择不同过滤器选项，可以包含或排除与表达式匹配的所有输出。您还可以显示以与表达式匹配的行开头的所有输出。

将筛选选项与 **show** 命令配合使用的语法如下：

show *command* | {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

或

more system:running-config| {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

注释 输入 **more** 命令允许您查看任何文件的内容，而不只是运行配置；有关详细信息，请参阅命令参考。

在此命令字符串中，第一根竖线 (|) 是运算符，并且必须包含在命令中。此运算符会将 **show** 命令的输出指引到过滤器。在语法图中，其他竖线 (|) 指示备用选项，并且不是命令的一部分。

include 选项包括匹配正则表达式的所有输出行。不带 **-v** 的 **grep** 选项具有同样的效果。**exclude** 选项不包括匹配正则表达式的所有输出行。不带 **-v** 的 **grep** 选项不具有同样的效果。**begin** 选项显示以匹配正则表达式的行开头的所有输出行。

将 *regexp* 更换为任何思科 IOS 正则表达式。正则表达式未括在引号或双引号中，所以请注意后面的空格，它们也会被视为正则表达式的一部分。

创建正则表达式时，可以使用要与之匹配的任何字母或数字。此外，某些关键字字符（称为元字符）在正则表达式中使用时具有特殊含义。

使用 **Ctrl+V** 可转义 CLI 中的所有特殊字符，如问号 (?) 或制表符。例如，键入 **d[Ctrl+V]?g** 以在配置中输入 **d?g**。

重定向和待处理 show 命令输出

如果要显示大量输出，则命令补全可能需要很长时间。例如，如果您尝试显示一百万个访问控制条目或一个非常大的 ASP 表，您可能会认为系统会卡住。

您可以将 **show** 命令的输出重定向到设备上或远程位置中的文件，而不是将其显示在屏幕上。当重定向到设备上的文件时，也可以将该命令输出附加到文件。

show *command* | {**append | redirect**} *url*

- **append** *url* 将输出添加到现有文件。使用以下方法之一指定文件：
  - **disk0:/**[[*path/*]*filename*] 或 **flash:/**[[*path/*]*filename*] - **flash** 和 **disk0** 均指示内部闪存。可以使用任一选项。
  - **disk1:/**[[*path/*]*filename*] - 指示外部存储器。
- **redirect** *url* 创建指定的文件，或者将其覆盖（如果该文件已存在）。
  - **disk0:/**[[*path/*]*filename*] 或 **flash:/**[[*path/*]*filename*] - **flash** 和 **disk0** 均指示内部闪存。可以使用任一选项。
  - **disk1:/**[[*path/*]*filename*] - 指示外部存储器。
  - **smb:/**[[*path/*]*filename*] - 指示服务器消息阻止（一种 UNIX 服务器本地文件系统）。
  - **ftp://**[[*user*[**:***password*]@] *server*[*:port*]/[*path/*] *filename*[**;type=***xx*]] - 指示 SCP 服务器。**type** 可以是以下关键字之一：**ap**（ASCII 被动模式）、**an**（ASCII 普通模式）、**ip**（默认 - 二进制被动模式）、**in**（二进制普通模式）。
  - **scp://**[[*password*]@] *server*[*/path*]/*filename*[*;int=***;int=***interface_name*]] **-;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问安全复制 (SCP) 服务器。
  - **tftp://**[[*user*[**:***password*]@] *server*[*:port*] /[*path/*]*filename*[**;int=***interface_name*]] - 指示 TFTP 服务器。路径名不能包含空格。**;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问 TFTP 服务器。

获取 show 命令输出的行计数

您可能只需输出中的行数计数或与正则表达式匹配的行数，而不是查看实际 **show** 命令输出。然后，您可以轻松将此行数与您上次输入命令时的行数进行比较。当执行配置更改时，可以快速对此进行检查。可以使用 **count** 关键字，也可以向 grep 关键字添加 **-c**。

show *command* | **count** [*regular_expression*]

show *command* | **grep -c** [*regular_expression*]

将 *regular_expression* 替换为任何思科 IOS 正则表达式。正则表达式未括在引号或双引号中，所以请注意后面的空格，它们也会被视为正则表达式的一部分。正则表达式是可选的；如果未包含正则表达式，则计数会在未过滤的输出中返回总行数。

创建正则表达式时，可以使用要与之匹配的任何字母或数字。此外，某些关键字字符（称为元字符）在正则表达式中使用时具有特殊含义。使用 Ctrl+V 可转义 CLI 中的所有特殊字符，如问号 (?) 或制表符。例如，键入 **d[Ctrl+V]?g** 以在配置中输入 **d?g**。

例如，要在 **show running-config** 输出中显示所有行的总数：

```
ciscoasa# show running-config | count
Number of lines which match regexp = 271
```

以下示例显示了如何快速检查有多少个接口在工作。第一个示例显示如何将 **grep** 关键字与正则表达式配合使用以仅对显示启动状态的行进行过滤。下一个示例添加 **-c** 选项以仅显示计数而不是实际输出行。

```
ciscoasa# show interface | grep is up
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
Interface GigabitEthernet0/1 "inside", is up, line protocol is up

ciscoasa# show interface | grep -c is up
Number of lines which match regexp = 2
```

命令输出分页

对于如 **help** 或 **?**、**show**、**show xlate** 之类的命令或者提供长列表的其他命令，您可以决定是让信息显示一屏后暂停，还是让命令运行到完成为止。通过 **pager** 命令，您可以选择在 More 提示出现之前要显示的行数。

启用分页后，会出现以下提示：

```
<--- More --->
```

More 提示符使用与 UNIX **more** 命令类似的语法：

- 按**空格**键可查看其他屏幕。
- 按 **Enter** 键可查看下一行。
- 按 q 键可返回到命令行。

添加注释

您可以在某一行之前前置冒号(:)来创建注释。但是，该注释仅出现在命令历史记录缓冲区中，而不出现在配置中。因此，您可以使用 **show history** 命令或通过按箭头键检索以前的命令来查看注释，但是由于注释不在配置中，**write terminal** 命令不会显示注释。

文本配置文件

本节介绍如何设置可下载到 ASA 的文本配置文件的格式。

命令如何与文本文件中的行相对应

文本配置文件包含与本指南中所述命令对应的行。

在示例中，命令之前前置有 CLI 提示。以下示例中的提示为“ciscoasa(config)#”：

```
ciscoasa(config)# context a
```

在系统未提示输出命令的文本配置文件中，会因此省略提示：

```
context a
```

命令特定配置模式命令

命令特定配置模式命令在命令行中输入时缩进显示在主命令下。只要这些命令紧跟在主命令后显示，便无需缩进文本行。例如，以下未缩进文本的读取与缩进文本相同：

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

自动文本条目

将配置下载至 ASA 时，ASA 会自动插入一些行。例如，ASA 会为默认设置或修改配置的时间插入行。创建文本文件时，无需输入这些自动条目。

行顺序

大致上，命令可以依照文件中的任何顺序。但是，某些行（例如 ACE）按其显示顺序进行处理，并且顺序可影响访问列表的功能。其他命令也可能具有顺序要求。例如，必须首先为接口输入 **nameif**

命令，因为许多后续命令都使用该接口的名称。此外，命令特定配置模式下的命令必须紧跟在主命令之后。

文本配置中不包括的命令

有些命令不会在配置中插入行。例如，运行时命令（**show running-config**）不会在文本文件中有对应的行。

密码

登录、启用和用户密码存储在配置中之前会自动加密。例如，密码“cisco”的加密形式可能类似于jMorNbK0514fadBh。您可以将配置密码以其加密形式复制到另一个ASA，但是无法自行解密密码。

如果您在文本文件中输入了未加密的密码，则 ASA 不会在您将配置复制到 ASA 时将其自动加密。仅当使用 **copy running-config startup-config** 或 **write memory** 命令从命令行保存运行 配置时，ASA 才会将其加密。

多个安全情景文件

对于多个安全情景，整个配置由以下多个部分组成：

- 安全情景配置
- 系统配置，用于确定 ASA 的基本设置，包括情景列表
- 管理情景，用于为系统配置提供网络接口

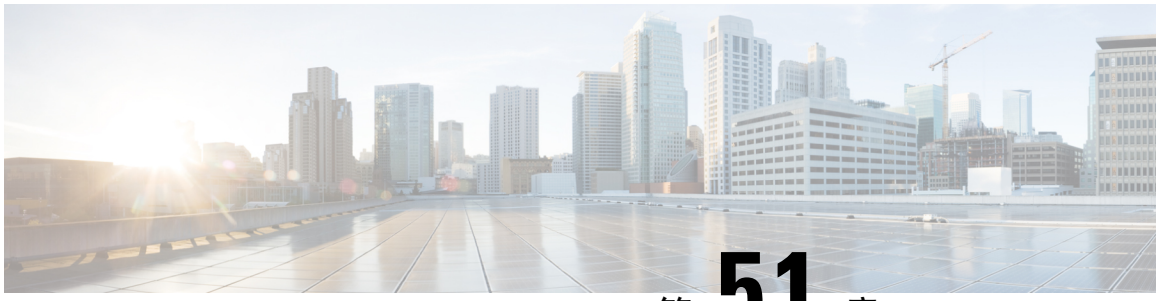
  系统配置不包含其自己的任何接口或网络设置。相反，当系统需要访问网络资源（例如从服务器下载情景）时，它会使用指定为管理情景的情景。

每个情景都类似于一个单情景模式配置。系统配置与情景配置的不同之处在于，系统配置仅包含系统命令（例如所有情景的列表），而其他典型命令不存在（例如许多接口参数）。

支持的字符集

ASA CLI 当前仅支持 UTF-8 编码。UTF-8 是 Unicode 符号的特定编码方案，并已设计为与符号的 ASCII 子集兼容。ASCII 字符在 UTF-8 中表示为单字节字符。所有其他字符在 UTF-8 中均表示为多字节符号。

完全支持 ASCII 可打印字符（0x20 到 0x7e）。可打印的 ASCII 字符与 ISO 8859-1 相同。UTF-8 是 ISO 8859-1 的超集，因此前 256 个字符 (0-255) 与 ISO 8859-1 相同。ASA CLI 最多支持 255 个 ISO 8859-1 字符（多字节字符）。



第 51 章

地址、协议和端口

本章提供有关 IP 地址、协议和应用的快速参考。

- IPv4 地址和子网掩码， 第 1485 页
- IPv6 地址， 第 1489 页
- 协议和应用， 第 1494 页
- TCP 和 UDP 端口， 第 1495 页
- 本地端口和协议， 第 1499 页
- ICMP 类型， 第 1500 页

IPv4 地址和子网掩码

本部分描述如何在 ASA 中使用 IPv4 地址。IPv4 地址是采用点分十进制记法的 32 位数字：从二进制转换为十进制数字的四个 8 位字段（八位组），字段之间用点分隔。IP 地址的第一个部分标识主机所在的网络，而第二个部分标识给定网络上的特定主机。网络号字段称为网络前缀。给定网络上的所有主机都共享同一网络前缀，但必须有唯一的主机号。对于有类 IP，地址类确定网络前缀与主机号之间的边界。

类

IP 主机地址划分为三个不同的地址类：A 类、B 类和 C 类。每个类在 32 位地址内的不同点固定网络前缀与主机号之间的边界。D 类地址保留用于组播 IP。

- A 类地址（1.xxx.xxx.xxx 至 126.xxx.xxx.xxx）仅将第一个八位组用作网络前缀。
- B 类地址（128.0.xxx.xxx 至 191.255.xxx.xxx）将前两个八位组用作网络前缀。
- C 类地址（192.0.0.xxx 至 223.255.255.xxx）将前三个八位组用作网络前缀。

由于 A 类地址具有 16,777,214 个主机地址，B 类地址具有 65,534 个主机，因此您可以使用子网掩码将这些庞大的网络分为较小的子网。

专用网络

如果在网络上需要大量地址，但不需要在互联网上路由这些地址，则可以使用互联网编号分配机构 (IANA) 推荐的专用 IP 地址（请参阅 RFC 1918）。以下地址范围指定为不应通告的专用网络：

- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 至 172.31.255.255
- 192.168.0.0 到 192.168.255.255

子网掩码

通过子网掩码，您可以将单个 A 类、B 类或 C 类网络转换为多个网络。利用子网掩码，可以创建扩展网络前缀，从而将主机号中的位添加到网络前缀中。例如，C 类网络前缀始终包含 IP 地址的前三个八位组。但是，C 类扩展网络前缀还使用第四个八位组的一部分。

如果使用二进制表示法而不是点分十进制表示法，则有助于理解子网掩码。子网掩码中的位与互联网地址一一对应：

- 如果 IP 地址中的对应位是扩展网络前缀的一部分，则该位会设置为 1。
- 如果该位是主机号的一部分，则会设置为 0。

示例 1：如果您有 B 类地址 129.10.0.0，并要将第三个八位组全部用作扩展网络前缀而不是主机号的一部分，则必须将子网掩码指定为 11111111.11111111.11111111.00000000。该子网掩码将此 B 类地址转换为等效的 C 类地址，其中的主机号仅包含最后一个八位组。

示例 2：如果您只想将第三个八位组的一部分用于扩展网络前缀，则必须将子网掩码指定为类似 11111111.11111111.11111000.00000000 的形式，这种形式的子网掩码仅将第三个八位组中的 5 位用于扩展网络前缀。

您可以将子网掩码编写为点分十进制掩码或/位数（“斜杠位数”）掩码。在示例 1 中，对于点分十进制掩码，您可以将每个二进制八位组转换为十进制数：255.255.255.0。对于 /位数掩码，可以添加数字 1s: /24。在示例 2 中，十进制数为 255.255.248.0，/位数为 /21。

您还可以将第三个八位组的一部分用于扩展网络前缀，从而将多个C类网络构建成一个更大的超网。例如，192.168.0.0/20。

确定子网掩码

请参阅下表以根据所需的主机数来确定子网掩码。

注释 子网的第一个和最后一个数字已保留，但 /32 除外，该数字用于标识单个主机。

表 *81:* 主机数、位掩码和点分十进制掩码

主机数	/位掩码	点分十进制掩码
16,777,216	/8	255.0.0.0 A 类网络
65,536	/16	255.255.0.0 B 类网络
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 C 类网络
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
不使用	/31	255.255.255.254
1	/32	255.255.255.255 单个主机地址

确定要与子网掩码配合使用的地址

以下各节介绍如何确定要与 C 类规模和 B 类规模网络的子网掩码配合使用的网络地址。

C 类规模网络地址

对于主机数介于 2 和 254 之间的网络，第四个八位组是主机地址数量的倍数，从 0 开始。例如，下表显示 192.168.0.x 的 8 主机子网 (/29)。

注释 子网的第一个和最后一个地址已保留。在第一个子网示例中，不能使用 192.168.0.0 或 192.168.0.7。

表 *82: C* 类规模网络地址

掩码为 /29 的子网 (255.255.255.248)	地址范围
192.168.0.0	192.168.0.0 到 192.168.0.7
192.168.0.8	192.168.0.8 到 192.168.0.15
192.168.0.16	192.168.0.16 到 192.168.0.31
-	—
192.168.0.248	192.168.0.248 到 192.168.0.255

B 类规模网络地址

要确定将与主机数在 254 和 65,534 之间的网络的子网掩码配合使用的网络地址，您需要确定每个可能的扩展网络前缀的第三个八位组的值。例如，您可能想要为类似于 10.1.*x*.0 的地址构建子网，在该地址中，前两个八位组是固定的，因为它们用于扩展网络前缀中，第四个八位组是 0，因为所有位都用于主机号。

要确定第三个八位组的值，请按照以下步骤操作：

1. 通过用 65,536（使用第三个和第四个八位组的地址的总数）除以所需的主机地址数，计算出可从网络构建的子网数量。

   例如，65,536 除以 4096 个主机等于 16。因此，4096 个地址有 16 个子网，每个都位于 B 类规模网络上。

2. 通过用 256（第三个八位组值的数量）除以子网数量，确定第三个八位组值的倍数：

   在本示例中，256/16 = 16。

   第三个八位组是 16 的倍数，从 0 开始。

下表显示网络 10.1 的 16 个子网。

注释 子网的第一个和最后一个地址已保留。在第一个子网示例中，不能使用 10.1.0.0 或 10.1.15.255。

表 *83:* 网络的子网

掩码为 /20 的子网 (255.255.240.0)	地址范围
10.1.0.0	10.1.0.0 到 10.1.15.255
10.1.16.0	10.1.16.0 到 10.1.31.255
10.1.32.0	10.1.32.0 到 10.1.47.255
-	—

掩码为 /20 的子网 (255.255.240.0)	地址范围
10.1.240.0	10.1.240.0 到 10.1.255.255

IPv6 地址

IPv6 是继 IPv4 之后的下一代互联网协议。它提供经过扩展的地址空间、简化的报头格式、经过改进的扩展和选项支持、流标签功能以及身份验证和隐私功能。有关 IPv6 的介绍，请参阅 RFC 2460。有关 IPv6 寻址架构的介绍，请参阅 RFC 3513。

本节介绍 IPv6 地址的格式和架构。

IPv6 地址格式

IPv6 地址以一系列八个 16 位十六进制字段表示，字段之间用冒号 (:) 分隔，格式为：x:x:x:x:x:x:x:x。下面是 IPv6 地址的两个示例：

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

注释 IPv6 地址中的十六进制字母不区分大小写。

不需要将前导零包含在地址的各个字段中，但每个字段必须至少包含一位数。因此，示例地址 2001:0DB8:0000:0000:0008:0800:200C:417A 可以通过删除从左侧数第三到第六个字段中的前导零来缩短为 2001:0DB8:0:0:8:800:200C:417A。其中的数字全部为零的字段（从左侧数起的第三和第四个字段）缩减为一个零。从左侧数起的第五个字段删除了三个前导零，仅留下了一个 8，从左侧数起的第六个字段删除了一个前导零，留下了 800。

对 IPv6 地址来说，包含几个连续的十六进制零字段很常见。可以使用两个冒号 (::) 压缩 IPv6 地址开头、中间或结尾位置的连续零字段（冒号表示连续的十六进制零字段）。下表显示若干不同类型的 IPv6 地址的地址压缩示例。

表 *84: IPv6* 地址压缩示例

地址类型	标准形式	压缩形式
单播	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
组播	FF01:0:0:0:0:0:0:101	FF01::101
环回	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

注释 两个冒号 (::) 在 IPv6 地址中只能使用一次，用以表示连续的零字段。

在处理同时包含 IPv4 和 IPv6 地址的环境时，通常使用 IPv6 的替代格式。此替代格式为 x:x:x:x:x:x:y.y.y.y，其中，x 表示 IPv6 地址六个高位部分的十六进制值，y 表示该地址 32 位 IPv4 部分的十进制值（该部分代替 IPv6 地址的剩余两个 16 位部分）。例如，IPv4 地址 192.168.1.1 可表示为 IPv6 地址 0:0:0:0:0:0:FFFF:192.168.1.1 或 ::FFFF:192.168.1.1。

IPv6 地址类型

以下是 IPv6 地址的三种主要类型：

- **Unicast** - 单播地址是单个接口的标识符。发送到单播地址的数据包将会传输到通过该地址标识的接口。一个接口可能分配有多个单播地址。
- **Multicast** - 组播地址是一组接口的标识符。发送到某个组播地址的数据包将会传输到通过该地址标识的所有地址。
- **Anycast** - 任播地址是一组接口的标识符。与组播地址不同的是，发送到任播地址的数据包仅传输到“最近”的接口（以路由协议的距离为测量标准）。

注释 IPv6 中没有广播地址。组播地址提供广播功能。

单播地址

本节介绍 IPv6 单播地址。单播地址用于标识网络节点上的接口。

全局地址

IPv6 全局单播地址的通用格式是全局路由前缀后跟子网 ID，然后是接口 ID。全局路由前缀可以是未被其他 IPv6 地址类型保留的任何前缀。

所有全局单播地址（以二进制 000 开头的除外）都具有改良 EUI-64 格式的 64 位接口 ID。

以二进制 000 作为开头的全局单播地址在地址的接口 ID 部分的大小或结构上没有任何限制。例如，具有嵌入式 IPv4 地址的 IPv6 地址即是此类型的地址。

站点本地地址

站点本地地址用于在站点内寻址。此类地址可在不使用全局唯一前缀的情况下用于对整个站点进行寻址。站点本地地址具有前缀 FEC0::/10，后跟 54 位子网 ID，并以改良 EUI-64 格式的 64 位接口 ID 结尾。

站点本地路由器不将具有源或目标站点本地地址的任何数据包转发到站点外。因此，可将站点本地地址视为专用地址。

本地链路地址

所有接口都需要有至少一个链路本地地址。您可以为每个接口配置多个IPv6地址，但只能配置一个链路本地地址。

链路本地地址是一个IPv6单播地址，通过使用链路本地前缀FE80::/10和改良EUI-64格式接口标识符，可在任意接口上自动配置此类地址。链路本地地址用于邻居发现协议和无状态自动配置过程。使用链路本地地址的节点可进行通信；它们不需要站点本地地址或全局唯一地址即可进行通信。

路由器不会转发具有源或目标链路本地地址的任何数据包。因此，可将链路本地地址视为专用地址。

兼容 IPv4 的 IPv6 地址

有两种类型的IPv6地址可包含IPv4地址。

第一种类型是与IPv4兼容的IPv6地址。IPv6过渡机制包括主机和路由器通过IPv4路由基础设施用隧道动态传输IPv6数据包的技术。使用此技术的IPv6节点分配有特殊的IPv6单播地址，从而可传送低位32位的全局IPv4地址。此类地址称为与IPv4兼容的IPv6地址，其格式为::y.y.y.y，其中，y.y.y.y是IPv4单播地址。

注释 在与IPv4兼容的IPv6地址中使用的IPv4地址必须为全局唯一的IPv4单播地址。

第二种类型的IPv6地址具有嵌入式IPv4地址，称为IPv4映射IPv6地址。此类地址用于将IPv4节点的地址表示为IPv6地址。此类地址的格式为::FFFF:y.y.y.y，其中，y.y.y.y是IPv4单播地址。

不特定地址

未指定地址0:0:0:0:0:0:0:0表示没有IPv6地址。例如，IPv6网络上新初始化的节点可能将未指定地址用作其数据包的源地址，直至它接收到IPv6地址。

注释 不能将未指定IPv6地址分配给接口。未指定IPv6地址不得用作IPv6数据包或IPv6路由报头中的目标地址。

环回地址

环回地址0:0:0:0:0:0:0:1可由节点用于向其自身发送IPv6数据包。IPv6中的环回地址与IPv4(127.0.0.1)中的环回地址功能相同。

注释 不能将IPv6环回地址分配给物理接口。将IPv6环回地址用作其源地址或目标地址的数据包必须保留在创建该数据包的节点内。IPv6路由器不转发将IPv6环回地址用作其源地址或目标地址的数据包。

接口标识符

IPv6 单播地址中的接口标识符用于标识链路上的接口。接口标识符在子网前缀内必须是唯一的。在许多情况下，接口标识符派生自接口链路层地址。同一接口标识符可用于一个节点的多个接口上，只要这些接口连接到不同子网即可。

对于所有单播地址，除了以二进制 000 开头的之外，接口标识符的长度需要是 64 位，且以改良 EUI-64 格式构造。改良 EUI-64 格式以 48 位 MAC 地址为基础，通过颠倒 MAC 地址中的通用/本地位并在 MAC 地址的上三个字节与下三个字节之间插入十六进制数 FFFE 创建而成。

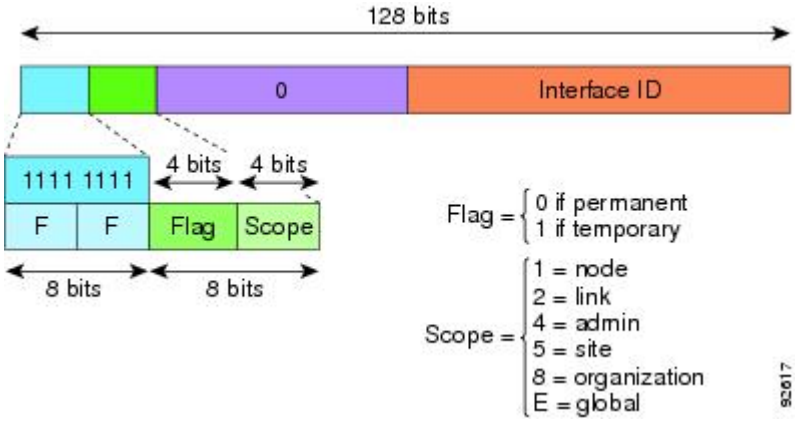
例如，具有 MAC 地址 00E0.b601.3B7A 的接口将会有一个 64 位接口 ID 02E0:B6FF:FE01:3B7A。

组播地址

IPv6 组播地址是一组通常位于不同节点的接口的标识符。发送到某个组播地址的数据包将会传输到通过该组播地址标识的所有接口。一个接口可属于任意数量的组播组。

IPv6 组播地址具有前缀 FF00::/8 (1111 1111)。紧跟前缀的八位组定义组播地址的类型和范围。永久分配（公认）的组播地址具有一个等于 0 的标志参数；临时（瞬时）组播地址具有一个等于 1 的标志参数。有节点范围、链路范围、站点范围、组织范围或全局范围的组播地址分别具有范围参数 1、2、5、8 或 E。例如，前缀为 FF02::/16 的组播地址是具有链路范围的永久组播地址。下图显示 IPv6 组播地址的格式。

图 *91: IPv6* 组播地址格式



IPv6 节点（主机和路由器）需要加入以下组播组：

- 全节点组播地址：
  - FF01::（接口本地）
  - FF02::（链路本地）
- 节点上每个 IPv6 单播地址和任播地址的请求节点地址：FF02:0:0:0:0:1:FFXX:XXXX/104，其中，XX:XXXX 是单播地址或任播地址的低位 24 位。

注释 请求节点地址用于邻居请求消息中。

IPv6 路由器需要加入以下组播组：

- FF01::2（接口本地）
- FF02::2（链路本地）
- FF05::2（站点本地）

组播地址不应用作 IPv6 数据包中的源地址。

注释 IPv6 中没有广播地址。系统使用 IPv6 组播地址而非广播地址。

任播地址

IPv6 任播地址是分配给多个接口的单播地址（通常属于不同的节点）。路由至一个任播地址的数据包会路由至具有该地址的最近接口，接近度由所用的路由协议确定。

任播地址从单播地址空间中进行分配。任播地址是分配给多个接口的单播地址，这些接口必须配置为将该地址标识为任播地址。

以下限制适用于任播地址：

- 任播地址不能用作 IPv6 数据包的源地址。
- 任播地址不能分配给 IPv6 主机，而只能分配给 IPv6 路由器。

注释 ASA 上不支持任播地址。

必需地址

IPv6 主机必须至少配置有以下地址（自动或手动）：

- 每个接口的链路本地地址
- 环回地址
- 全节点组播地址
- 每个单播或任播地址的请求节点组播地址

IPv6 路由器必须至少配置有以下地址（自动或手动）：

- 必需主机地址

- 用于配置为用作路由器的所有接口的子网路由器任播地址
- 全路由器组播地址

IPv6 地址前缀

IPv6 地址前缀（格式为 ipv6 前缀/前缀长度）可用于表示整个地址空间的连续比特块。IPv6 前缀必须采用 RFC 2373 规定的格式，其中地址以十六进制的 16 位值指定，各个值之间用冒号分隔。前缀长度是十进制值，表示组成前缀（地址的网络部分）的地址高位连续位的数量。例如，2001:0DB8:8086:6502::/32 是有效的 IPv6 前缀。

IPv6 前缀标识 IPv6 地址的类型。下表显示每个 IPv6 地址类型的前缀。

表 *85: IPv6* 地址类型前缀

地址类型	二进制前缀	IPv6 表示法
未指定	000...0（128 位）	::/128
环回	000...1（128 位）	::1/128
组播	11.111.111	FF00::/8
链路本地（单播）	1.111.111.010	FE80::/10
站点本地（单播）	1.111.111.111	FEC0::/10
全局（单播）	所有其他地址。	
任播	取自单播地址空间。	

协议和应用

下表列出了协议文字值和端口号；两者均可使用 ASA 命令输入。

表 *86:* 协议文字值

文字	值	说明
ah	51	IPv6 的身份验证报头，RFC 1826。
eigrp	88	增强型内部网关路由协议。
esp	50	IPv6 的封装安全负载，RFC 1827。
gre	47	通用路由封装。
icmp	1	互联网控制消息协议，RFC 792。

文字	值	说明
icmp6	58	IPv6 的互联网控制消息协议，RFC 2463。
igmp	2	互联网组管理协议，RFC 1112。
igrp	9	内部网关路由协议。
ip	0	互联网协议。
ipinip	4	IP 嵌套封装。
ipsec	50	IP 安全。输入 ipsec 协议文字相当于输入 esp 协议文字。
nos	94	网络操作系统（Novell 的 NetWare）。
ospf	89	开放式最短路径优先路由协议，RFC 1247。
pcp	108	负载压缩协议。
pim	103	协议无关组播。
pptp	47	点对点隧道协议。输入 ppp 协议文字相当于输入 gre 协议文字。
snp	109	Sitara 网络协议。
tcp	6	传输控制协议，RFC 793。
udp	17	用户数据报协议，RFC 768。

您可以在 IANA 网站上在线查看协议号：

http://www.iana.org/assignments/protocol-numbers

TCP 和 UDP 端口

下表列出了文字值和端口号；两者均可在 ASA 命令中输入。请参阅以下说明：

- ASA 将端口 1521 用于 SQL*Net。这是 Oracle for SQL*Net 所用的默认端口。但是，此值与 IANA 端口分配不一致。
- ASA 在端口 1645 和 1646 上侦听 RADIUS。如果 RADIUS 服务器使用标准端口 1812 和 1813，则您可以将 ASA 配置为使用 **authentication-port** 和 **accounting-port** 命令来侦听这些端口。
- 要分配用于 DNS 访问的端口，请使用 **domain** 文字值而不是 **dns**。如果使用 **dns**，则 ASA 会假定您是要使用 **dnsix** 文字值。

您可以在 IANA 网站上在线查看端口号：

http://www.iana.org/assignments/port-numbers

表 87: 端口文字值

文字	TCP 或 UDP？	值	说明
aol	TCP	5190	美国在线
bgp	TCP	179	边界网关协议，RFC 1163
biff	UDP	512	供邮件系统用于通知用户收到新邮件
bootpc	UDP	68	Bootstrap 协议客户端
bootps	UDP	67	Bootstrap 协议服务器
chargen	TCP	19	字符生成器
cifs	TCP、UDP	3020	通用互联网文件系统
citrix-ica	TCP	1494	Citrix 独立计算架构 (ICA) 协议
cmd	TCP	514	与 exec 类似，但 cmd 还具有自动身份验证功能
ctiqbe	TCP	2748	计算机电话接口快速缓冲区编码
daytime	TCP	13	日间，RFC 867
discard	TCP、UDP	9	丢弃
dnsix	UDP	195	DNSIX 会话管理模块审核重定向器
domain	TCP、UDP	53	DNS
echo	TCP、UDP	7	回应
EXEC	TCP	512	远程进程执行
finger	TCP	79	Finger
ftp	TCP	21	文件传输协议（控制端口）
ftp-data	TCP	20	文件传输协议（数据端口）
gopher	TCP	70	Gopher
h323	TCP	1720	H.323 呼叫信令
hostname	TCP	101	NIC 主机名服务器
http	TCP、UDP	80	万维网 HTTP
https	TCP	443	HTTP over SSL
ident	TCP	113	身份验证服务

文字	TCP 或 UDP？	值	说明
imap4	TCP	143	互联网消息访问协议，版本 4
irc	TCP	194	互联网中继聊天协议
isakmp	UDP	500	互联网安全关联和密钥管理协议
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn Shell
ldap	TCP	389	轻量级目录访问协议
ldaps	TCP	636	轻量级目录访问协议 (SSL)
login	TCP	513	远程登录
lotusnotes	TCP	1352	IBM Lotus Notes
lpd	TCP	515	行式打印机后台守护程序 - 打印后台处理程序
mobile-ip	UDP	434	移动 IP 代理
nameserver	UDP	42	主机名服务器
netbios-dgm	UDP	138	NetBIOS 数据报服务
netbios-ns	UDP	137	NetBIOS 名称服务
netbios-ssn	TCP	139	NetBIOS 会话服务
nfs	TCP、UDP	2049	网络文件系统 - Sun Microsystems
nntp	TCP	119	网络新闻传输协议
ntp	UDP	123	网络时间协议
pcanywhere-data	TCP	5631	pcAnywhere data
pcanywhere-status	UDP	5632	pcAnywhere status
pim-auto-rp	TCP、UDP	496	协议无关组播，反向路径泛洪，密集模式
pop2	TCP	109	邮局协议 - 版本 2
pop3	TCP	110	邮局协议 - 版本 3
pptp	TCP	1723	点对点隧道协议
radius	UDP	1645	远程身份验证拨入用户服务
radius-acct	UDP	1646	远程身份验证拨入用户服务（记帐）

文字	TCP 或 UDP?	值	说明
rip	UDP	520	路由信息协议
rsh	TCP	514	远程外壳
rtsp	TCP	554	实时流协议
secureid-udp	UDP	5510	SecureID over UDP
SIP	TCP、UDP	5060	会话发起协议
smtp	TCP	25	简单邮件传输协议
snmp	UDP	161	简单网络管理协议
snmptrap	UDP	162	简单网络管理协议 - 陷阱
sqlnet	TCP	1521	结构化查询语言网络
ssh	TCP	22	安全外壳
sunrpc	TCP、UDP	111	Sun 远程过程调用
syslog	UDP	514	系统日志
tacacs	TCP、UDP	49	增强型终端访问控制器访问控制系统
talk	TCP、UDP	517	通话
telnet	TCP	23	RFC 854 Telnet
tftp	UDP	69	简单文件传输协议
time	UDP	37	时间
uucp	TCP	540	UNIX 对 UNIX 复制程序
vxlan	UDP	4789	虚拟可扩展局域网 (VXLAN)
who	UDP	513	身份
whois	TCP	43	主体
www	TCP、UDP	80	万维网
xdmcp	UDP	177	X 显示管理器控制协议

本地端口和协议

下表列出 ASA 可能会为处理流向 ASA 的流量而打开的协议、TCP 端口和 UDP 端口。除非您已启用此表中列出的功能和服务，否则 ASA 不会打开任何本地协议或任何 TCP 或 UDP 端口。您必须为 ASA 配置功能或服务，才能打开默认侦听协议或端口。在许多情况下，启用功能或服务后，可以配置除默认端口以外的端口。

表 ***88:*** 根据功能和服务打开的协议与端口

功能或服务	协议	端口号	备注
DHCP	UDP	67、68	-
故障转移控制	105	不适用	—
HTTP	TCP	80	—
HTTPS	TCP	443	-
ICMP	1	不适用	—
IGMP	2	不适用	仅在目标 IP 地址 224.0.0.1 上开放协议
ISAKMP/IKE	UDP	500	可配置。
IPsec (ESP)	50	不适用	—
IPsec over UDP (NAT-T)	UDP	4500	-
IPsec over TCP (CTCP)	TCP	-	未使用默认端口。配置 IPsec over TCP 时，必须指定端口号。
NTP	UDP	123	—
OSPF	89	不适用	仅在目标 IP 地址 224.0.0.5 和 224.0.0.6 上开放协议
PIM	103	不适用	仅在目标 IP 地址 224.0.0.13 上开放协议
RIP	UDP	520	-
RIPv2	UDP	520	仅在目标 IP 地址 224.0.0.9 上开放端口
SNMP	UDP	161	可配置。
SSH	TCP	22	-
状态更新	8（非安全）9（安全）	不适用	—

功能或服务	协议	端口号	备注
Telnet	TCP	23	-
VPN 负载均衡	UDP	9023	可配置。
VPN 个人用户身份验证代理	UDP	1645、1646	只能通过 VPN 隧道访问端口。

ICMP 类型

下表列出了可在 ASA 命令中输入的 ICMP 类型编号和名称。

表 *89: ICMP* 类型

ICMP 编号	ICMP 名称
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error

ICMP 编号	ICMP 名称
32	mobile-redirect

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。