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 1 页
- 查看调试消息， 第 5 页
- 数据包捕获， 第 5 页
- 查看崩溃转储， 第 11 页
- 查看核心转储， 第 11 页
- CPU 使用情况和报告， 第 11 页
- 测试配置， 第 16 页
- 监控连接， 第 28 页
- 测试和故障排除的历史记录 ， 第 28 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）。

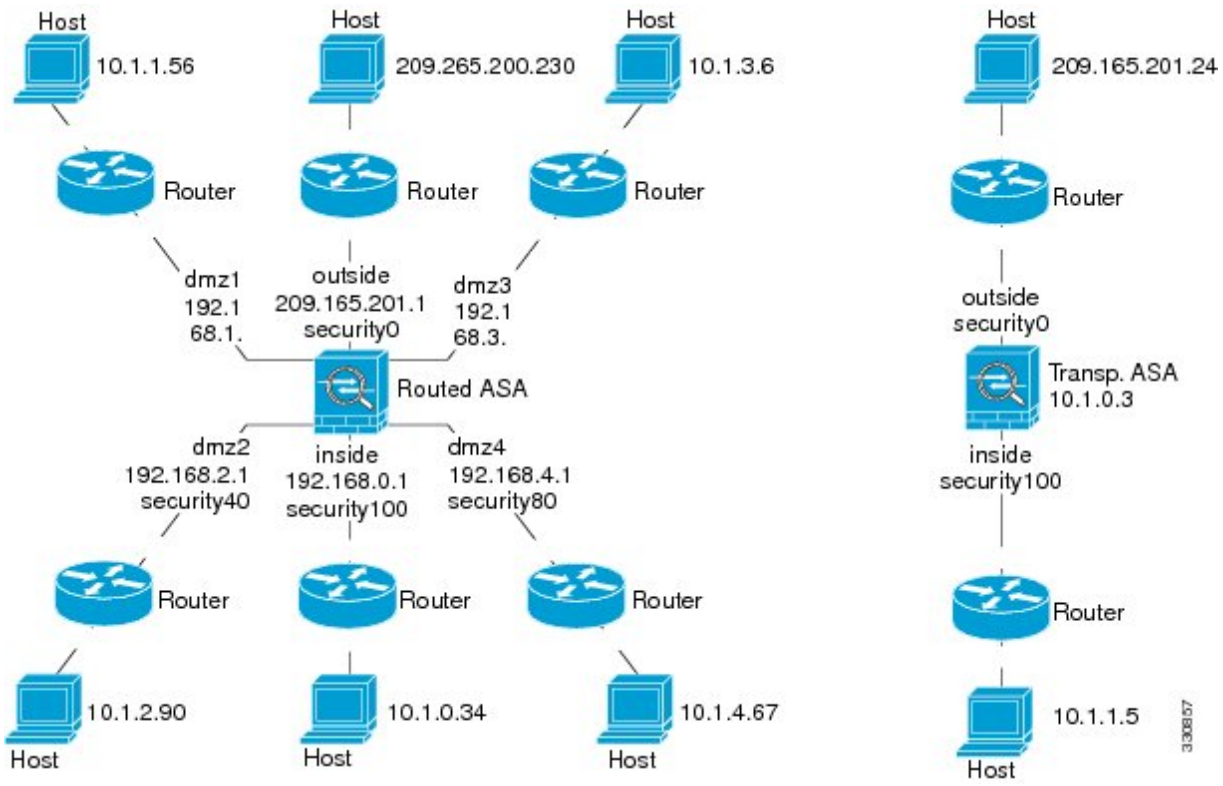
完成测试后，请禁用调试。保留此配置可能构成性能和安全风险。如果仅为了测试而启用日志记录，还可以禁用日志记录。

```
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 *1:* 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 *2: ASA* 接口的 *ping* 故障

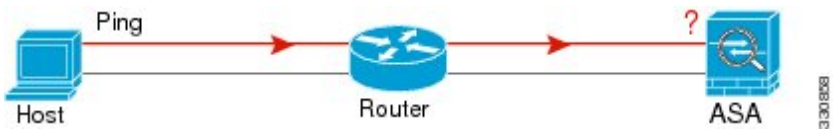
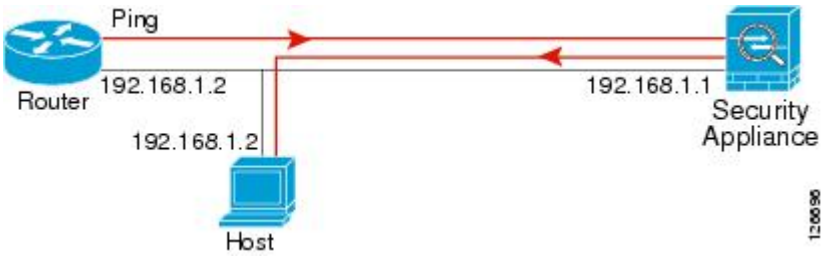


图 *3: IP* 寻址问题引发的 *Ping* 故障



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 *4: 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 *5: 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 23 页。
步骤 2 确定数据包路由，第 24 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 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 新增/修改的命令： **capture** *capture_name* **switch interface** *interface_* **direction** { **both** | **egress** | **ingress** }]

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。