l2 – lof

l2tp tunnel hello

要指定 L2TP over IPsec 连接上的 hello 消息之间的间隔，请在全局配置模式下使用 **l2tptunnelhello** 命令。要将间隔重置为默认值，请使用以下命令形 **no**式：

l2tp tunnel hello*interval*
no l2tp tunnel hello*interval*

Syntax Description

间隔	问候消息之间的间隔（以秒为单位）。默认值为 60 秒。范围是 10 到 300 秒。

Command Default

默认值为 60 秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

l2tptunnelhello 命令可使 ASA 检测 L2TP 连接的物理层问题。默认值为 60 秒。在使用默认设置的情况下，L2TP 隧道可能会在 180 秒后断开连接。如果将其配置为较小的值，遇到问题的连接会提前断开。L2TP 的最大重试次数是 3。

CR_Examples

以下示例将 hello 消息之间的间隔配置为 30 秒：

```
ciscoasa(config)# l2tp tunnel hello 30
```

Related Commands

命令	说明
showvpn-sessiondbdetailremotefilterprotocolL2TPOverIPsec	显示 L2TP 连接的详细信息。
vpn-tunnel-protocoll2tp-ipsec	启用 L2TP 作为特定隧道组的隧道协议。

lacp max-bundle

如要指定 EtherChannel 通道组中允许的最大主用接口数，请在接口配置模式下使用**lacpmax-bundle**命令。要将值设置为默认值，请使用此命 **no**令的形式。

注释 仅在 ASA 硬件型号和 ISA 3000 上受支持。

lacp max-bundle编号
no lacp max-bundle

Syntax Description

number 指定通道组中允许的最大主用接口数（介于 1 和 8 之间）；在 9.2(1) 及更高版本中，最大数量提高到 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。

Command Default

（9.1 及更早版本）默认值为 8。

（9.2(1) 和更高版本）默认值为 16。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
8.4(1)	添加了此命令。
9.2(1)	主用接口的数量已从 8 增加到 16。

使用指南

为端口通道接口输入此命令。每个通道组的最大主用接口数量是 8；要减少数量，请使用此命令。

CR_Examples

以下示例将 EtherChannel 中的最大接口数设置为 4：

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# lacp max-bundle 4
```

Related Commands

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacpsystem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载平衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	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。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	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。

lacp port-priority

要在 EtherChannel 中为物理接口设置优先级，请在接口配置模式下使用**lacpport-priority**命令。要将优先级设置为默认值，请使用此命令的 **no**形式。

注释 仅在 ASA 硬件型号和 ISA 3000 上受支持。

lacp port-priority编号
no lacp port-priority

Syntax Description

number 将优先级设置为 1 和 65535 之间。数字越大，优先级越低。

Command Default

默认值为 32768。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
8.4(1)	添加了此命令。

使用指南

为物理接口输入此命令。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。最低接口 ID 具有最高优先级。例如，GigabitEthernet 0/0 的优先级高于 GigabitEthernet 0/1。

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，要使千兆以太网 1/3 在千兆以太网 0/7 之前处于活动状态，则将 1/3 接口上的 **lacpport-priority** 值设为 12345，将 0/7 接口上的值设为默认值 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。查看命令。 **lacpsystem-priority**

链路汇聚控制协议(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。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。

CR_Examples

以下示例为 GigabitEthernet 0/2 设置较低的端口优先级，使其先于 GigabitEthernet 0/0 和 0/1 用作 EtherChannel 的一部分：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode active
```

Related Commands

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacpsystem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载平衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	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。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	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。

lacp rate

要设置接口为 EtherChannel 中的物理接口接收 LACP 数据单元的速率，请在接口配置模式下使用 **lacp rate** 命令。要将速率设置为默认值，请使用此命 **no**令的形式。

注释 仅在 Cisco Secure Firewall 3100/4200 上受支持。

lacp rate {**normal** | **fast**}
no lacp rate

Syntax Description

normal	将接收 LACP 数据单元的速率设置为每 30 秒一次。“正常”也称为“缓慢”。
fast	将 LACP 数据单元接收速率设置为每秒一次。

Command Default

默认是正常的。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.17(1)	添加了此命令。

使用指南

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。

链路汇聚控制协议 (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。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。

CR_Examples

以下示例将 EtherChannel 1 中两个接口上的速率设置为“快速”：

```
ciscoasa(config)# interface Ethernet1/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# lacp rate fast
```

```
ciscoasa(config-if)# interface Ethernet1/2
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# lacp rate fast
```

Related Commands

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。
showlacp	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。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。

lacp system-priority

对于 EtherChannel，要为 ASA 全局设置 LACP 系统优先级，请在全局配置模式下使用 **lacpsystem-priority**命令。要将值设置为默认值，请使用此命 **no**令的形式。

注释 仅在 ASA 硬件型号和 ISA 3000 上受支持。

lacp system-priority编号
no lacp system-priority

Syntax Description

number 设置 LACP 系统优先级，范围为 1 到 65535。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。

Command Default

默认值为 32768。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
8.4(1)	添加了此命令。

使用指南

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。有关以太网通道内的接口优先级，请参阅 **lacpport-priority** 命令。

CR_Examples

以下示例将系统优先级设置为高于默认值（较小的数字）：

```
ciscoasa(config)# lacp system-priority 12345
```

Related Commands

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。

命令	说明
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacpsystem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载平衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	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。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	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。

ldap-attribute-map

要将现有映射配置绑定到LDAP主机，请在aaa-server主机配置模式下使用**ldap-attribute-map**命令。要删除绑定，请使用此**no**命令的形式。

ldap-attribute-map*map-name*
no ldap-attribute-map*map-name*

Syntax Description

map-name	指定LDAP属性映射配置。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
AAA服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

如果思科定义的 LDAP 属性名称不能满足您的易用性或其他要求，您可以创建自己的属性名称，将其映射到思科属性，然后将生成的属性配置绑定到 LDAP 服务器。通常的步骤包括：

1. 在全局配置模式下使用 **ldapattribute-map** 命令来创建未填充的属性映射。此命令进入 ldap 属性映射配置模式。请注意，此命令中的“ldap”后面没有连字符。
2. 在 ldap-attribute-map 配置模式下使用 **map-name** 和 **map-value** 命令填充属性映射配置。
3. 在 aaa-server 主机模式下使用 **ldap-attribute-map** 命令将属性映射配置绑定到 LDAP 服务器。

CR_Examples

在 aaa-server 主机配置模式下输入的以下示例命令将名为 myldapmap 的现有属性映射绑定到名为 ldapsvr1 的 LDAP 服务器：

```
ciscoasa(config)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# ldap-attribute-map myldapmap
ciscoasa(config-aaa-server-host)#
```

Related Commands

命令	说明
ldapattribute-map(globalconfigurationmode)	创建并命名 LDAP 属性映射，以将用户定义的属性名称映射到思科 LDAP 属性名称。
map-name	将用户定义的 LDAP 属性名称与思科 LDAP 属性名称映射。
map-value	将用户定义的属性值映射到思科属性。
show running-config ldap attribute-map	显示特定运行 LDAP 属性映射配置或所有运行属性映射配置。
clearconfigureldapattribute-map	删除所有 LDAP 属性映射。

ldap-base-dn

要指定服务器在收到授权请求时应在LDAP层次结构中开始搜索的位置，请在**ldap-base-dn**aaa-server主机配置模式下使用该命令。可从 aaa-server 协议配置模式访问 aaa-server 主机配置模式。要删除该指定，从而将搜索重置为从列表顶部开始，请使用此命令的 **no** 形式。

ldap-base-dn字符串
no ldap-base-dn

Syntax Description

string 一个区分大小写的字符串，最多 128 个字符，用于指定服务器在收到授权请求时应在 LDAP 层次结构中开始搜索的位置；例如，OU=Cisco。

Command Default

从列表顶部开始搜索。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
AAA服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

该命令仅适用于 LDAP 服务器。

CR_Examples

以下示例在主机 1.2.3.4 上配置名为 srvgrp1 的 LDAP AAA 服务器，设置超时时间为 9 秒，重试间隔为 7 秒，并将 LDAP 基本 DN 配置为 starthere。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server
-host
)# ldap-base-dn starthere
ciscoasa
```

```
(config-aaa-server-host)#
exit
```

Related Commands

命令	说明
aaa-serverhost	进入 AAA 服务器主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
ldap-scope	指定服务器在收到授权请求时应在 LDAP 层次结构中进行的搜索范围。
ldap-naming-attribute	指定唯一标识LDAP服务器上的条目的相对可分辨名称属性（或多个属性）。
ldap-login-dn	指定系统应绑定的目录对象的名称。
ldap-login-password	指定登录 DN 的密码。

ldap-defaults

要定义 LDAP 默认值，请在 crl configure 配置模式下使用 **ldap-defaults**命令。可从加密 ca 信任点配置模式访问 Crl configure 配置模式。这些默认值仅在 LDAP 服务器需要时使用。要指定无 LDAP 默认值，请使用此命 **no**令的形式。

ldap-defaults*server*[*port*]
no ldap-defaults

Syntax Description

port	（可选）指定 LDAP 服务器端口。如果未指定此参数，则 ASA 使用标准 LDAP 端口 (389)。
server	指定LDAP服务器的IP地址或域名。如果 CRL 分发点中存在该证书，则它将覆盖该值。

Command Default

默认设置未设置。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Crl configure 配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

CR_Examples

以下示例定义默认端口 (389) 上的 LDAP 默认值：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# ldap-defaults ldapdomain4 8389
```

Related Commands

命令	说明
crlconfigure	进入 ca-crl 配置模式。
cryptocatrustpoint	进入 trustpoint 配置模式。
protocolldap	指定 LDAP 作为 CRL 的检索方法。

ldap-dn

要传递 X.500 可分辨名称和密码到要求对 CRL 检索进行身份验证的 LDAP 服务器，请在 crl configure 配置模式下使用 **ldap-dn**命令。可从加密 ca 信任点配置模式访问 Crl configure 配置模式。这些参数仅在 LDAP 服务器需要时使用。要指定任何 LDAP DN，请使用此命令的 **no** 形式。

ldap-dn*x.500-namepassword*
no ldap-dn

Syntax Description

password	为此可分辨名称定义密码。最大字段长度为 128 个字符。
x.500 名称	定义用于访问此 CRL 数据库的目录路径，例如：cn=crl,ou=certs,o=CAName,c=US。最大字段长度为 128 个字符。

Command Default

默认设置未开启。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Crl configure 配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

CR_Examples

以下示例为 trustpoint Central 指定 X.500 名称 CN=admin,OU=devtest,O=engineering 和密码 xx 这样的信息：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

Related Commands

命令	说明
crlconfigure	进入 crl configure 配置模式。
cryptocatrustpoint	进入 CA 信任点配置模式。

命令	说明
protocolldap	指定 LDAP 作为 CRL 的检索方法。

ldap-group-base-dn

要在 Active Directory 层次结构中指定用于组搜索的动态访问策略的基本组，请在 aaa-server 主机配置模式下使用 **ldap-group-base-dn** 命令。要从运行配置中删除该命令，请使用该命令的 no 形式：

ldap-group-base-dn [*string*]
no ldap-group-base-dn [*string*]

Syntax Description

string 区分大小写的字符串，最多 128 个字符，用于指定 Active Directory 层次结构中服务器应开始搜索的位置。例如，ou=Employees。该字符串中不允许使用空格，但是允许使用其他特殊字符。

Command Default

无默认行为或值。如果不指定组搜索 DN，则从基本 DN 开始搜索。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
aaa-server主机配置模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(4)	添加了此命令。

使用指南

ldap-group-base-dn 命令仅适用于使用 LDAP 的 Active Directory 服务器，并指定 **showad-groups** 命令用于开始其组搜索的 Active Directory 层次结构级别。动态组策略将从搜索中检索到的组用作特定策略的选择条件。

CR_Examples

以下示例设置组基础 DN，以在组织单位 (ou) 级别 Employees 开始搜索：

```
ciscoasa(config-aaa-server-host)# ldap-group-base-dn ou=Employees
```

Related Commands

命令	说明
group-search-timeout	调整 ASA 等待 Active Directory 服务器响应的时间，以获取组列表。
showad-groups	显示在 Active Directory 服务器上列出的组。

ldap-login-dn

如要指定系统应将其绑定为的目录对象名称，请在 aaa-server 主机配置模式下使用 **ldap-login-dn**命令。可从 aaa-server 协议配置模式访问 aaa-server 主机配置模式。要删除此规范，请使用此 **no**命令的形式。

ldap-login-dn字符串
no ldap-login-dn

Syntax Description

string 一个区分大小写的字符串，最多 128 个字符，用于指定 LDAP 层次结构中的目录对象的名称。该字符串中不允许使用空格，但是允许使用其他特殊字符。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
AAA服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

该命令仅适用于 LDAP 服务器。支持的最大字符串长度为 128 个字符。

某些 LDAP 服务器（包括 Microsoft Active Directory 服务器）要求 ASA 通过经过身份验证的绑定建立握手，然后才能接受对任何其他 LDAP 操作的请求。ASA 通过将 Login DN 字段关联到用户验证请求，为通过身份验证的绑定标识自己。Login DN 字段介绍 ASA 的身份验证特征。这些特征应与具有管理员权限的用户的特征相对应。

对于 字符串 变量，请为 VPN 集中器身份验证绑定输入目录对象的名称，例如：cn=Administrator、cn=users、ou=person、dc=XYZ Corporation、dc=com。对于匿名访问，请将此字段留空。

CR_Examples

以下示例在主机 1.2.3.4 上配置名为 svrgrp1 的 LDAP AAA 服务器，设置超时时间为 9 秒，重试间隔为 7 秒，并将 LDAP 登录 DN 配置为 myobjectname。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
```

```
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server
-host)
# ldap-login-dn myobjectname
ciscoasa(config-aaa-server
-host)
#
```

Related Commands

命令	说明
aaa-serverhost	进入 AAA 服务器主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定当服务器接收授权请求时应开始搜索的位置。
ldap-login-password	指定登录 DN 的密码。该命令仅适用于 LDAP 服务器。
ldap-naming-attribute	指定唯一标识LDAP服务器上的条目的相对可分辨名称属性（或多个属性）。
ldap-scope	指定服务器在收到授权请求时应在 LDAP 层次结构中进行的搜索范围。

ldap-login-password

要指定 LDAP 服务器的登录密码，请在 aaa-server 主机配置模式下使用 **ldap-login-password**命令。可从 aaa-server 协议配置模式访问 aaa-server 主机配置模式。要删除此密码规范，请使用以下命 **no**令的形式：

ldap-login-password字符串
no ldap-login-password

Syntax Description

string 区分大小写的字母数字密码，最长 64 个字符。密码不能包含空格字符。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
AAA服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

该命令仅适用于 LDAP 服务器。密码字符串的最大长度为 64 个字符。

CR_Examples

以下示例在主机 1.2.3.4 上配置名为 srvgrp1 的 LDAP AAA 服务器，设置超时时间为 9 秒，重试间隔为 7 秒，并将 LDAP 登录密码配置为 obscurepassword。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server)# timeout 9
ciscoasa
(config-aaa-server)# retry 7
ciscoasa(config-aaa-server)# ldap-login-password obscurepassword
ciscoasa
(config-aaa-server)#
```

Related Commands

命令	说明
aaa-serverhost	进入 AAA 服务器主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定当服务器接收授权请求时应开始搜索的位置。
ldap-login-dn	指定系统应绑定的目录对象的名称。
ldap-naming-attribute	指定唯一标识LDAP服务器上的条目的相对可分辨名称属性（或多个属性）。
ldap-scope	指定服务器在收到授权请求时应在 LDAP 层次结构中进行的搜索范围。

ldap-naming-attribute

要指定相对可分辨名称属性，请在 aaa-server hostconfiguration [] configuration模式下使用 **ldap-naming-attribute**命令。可从 aaa-server 协议配置模式访问 aaa-server 主机配置模式。要删除此规范，请使用此命 **no**令的形式：

ldap-naming-attribute字符串
no ldap-naming-attribute

Syntax Description

string 区分大小写的字母数字相对可分辨名称属性，最多包含 128 个字符，用于唯一标识 LDAP 服务器上的条目。该字符串中不允许使用空格，但是允许使用其他特殊字符。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
AAA服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

输入唯一标识 LDAP 服务器上条目的相对可分辨名称属性。常见的命名属性有通用名称（cn）和用户ID（uid）。

该命令仅适用于 LDAP 服务器。支持的最大字符串长度为 128 个字符。

CR_Examples

以下示例在主机 1.2.3.4 上配置名为 srvgrp1 的 LDAP AAA 服务器，设置超时时间为 9 秒，重试间隔为 7 秒，并将 LDAP 命名属性配置为 cn。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server
```

```
-host
)# ldap-naming-attribute cn
ciscoasa
(config-aaa-server-host)#
```

Related Commands

命令	说明
aaa-serverhost	进入AAA服务器主机配置模式，以便您可以配置特定于主机的AAA服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定当服务器接收授权请求时应开始搜索的位置。
ldap-login-dn	指定系统应绑定的目录对象的名称。
ldap-login-password	指定登录 DN 的密码。该命令仅适用于 LDAP 服务器。
ldap-scope	指定服务器在收到授权请求时应在 LDAP 层次结构中进行的搜索范围。

ldap-over-ssl

要在 ASA 与 LDAP 服务器之间建立安全 SSL 连接，请在 aaa-server 主机配置模式下使用 **ldap-over-ssl** 命令。要禁用连接的 SSL，请使用此命 **no**令的形式。

ldap-over-ssl [**enable** | **reference-identity**引用 *ID* 名称]

no ldap-over-ssl [**enable** | **reference-identity**引用 *ID* 名称]

Syntax Description

enable	指定使用 SSL 保护与 LDAP 服务器的连接。
reference-identity引用 *ID* 名称	指定引用身份名称来验证LDAP服务器身份。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
AAA服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.1(1)	添加了此命令。
9.18(1)	此命令已得到增强，以验证LDAP服务器身份。

使用指南

使用此命令可指定SSL 保护 ASA 和 LDAP 服务器之间的连接。

注释 如果您使用纯文本身份验证，我们建议启用此功能。请参阅 **sasl-mechanismcommand.**

CR_Examples

在 aaa-server 主机配置模式下输入的以下命令为 ASA 与 IP 地址为 10.10.0.1 的名为 ldapsvr1 的 LDAP 服务器之间的连接启用 SSL。它们还配置明文 SASL 身份验证机制。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
```

```
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)#
```

要通过指定引用身份名称验证LDAP服务器身份，请使用 **reference-identity***ref_id_name*。引用标识对象使用具有匹配条件的 **crypto ca reference-identity refidname** 来创建。在 ldap aaa-server 配置下配置 reference-identity 时，ASA 会尝试查找与 ldap 服务器证书匹配的主机名。如果无法解析主机或未找到匹配项，则连接将终止并显示错误消息。

```
asa(config-aaa-server-host)# ldap-over-ssl ?

aaa-server-host mode commands/options:
  enable              Require an SSL connection to the LDAP server
  reference-identity  Enter reference-identity name to validate LDAP server identity

asa(config-aaa-server-host)# ldap-over-ssl reference-identity ?

aaa-server-host mode commands/options:
  WORD < 65 char  Enter reference-identity name to validate LDAP server identity
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname ?

aaa-server-host mode commands/options:
  <cr>
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname
```

show running-config aaa server 将配置的 reference-identity name 显示为以下选项之一：

```
asa(config-aaa-server-host)# show running-config aaa-server
aaa-server ldaps protocol ldap
aaa-server ldaps (manif) host 10.86.93.107
server-port 636
ldap-base-dn CN=Users,DC=BXBCASERVERS,DC=COM
ldap-scope subtree
ldap-naming-attribute cn
ldap-login-password *****
ldap-login-dn CN=administrator,CN=Users,DC=BXBCASERVERS,DC=com
ldap-over-ssl enable
ldap-over-ssl reference-identity refidname
server-type microsoft
```

Related Commands

命令	说明
sasl-mechanism	指定 LDAP 客户端和服务器之间的 SASL 身份验证。
server-type	将 LDAP 服务器供应商指定为 Microsoft 或 Sun。
ssl-client-certificate	指定使用 LDAPS 时 ASA 应作为客户端证书呈现给 LDAP 服务器的证书。
crypto ca reference-identity refidname	要配置 reference-identity 对象。

ldap-scope

要指定服务器在收到授权请求时应在 LDAP 层次结构中进行的搜索范围，请在 **ldap-scope**aaa-server 主机配置模式下使用该命令。可从 aaa-server 协议配置模式访问 aaa-server 主机配置模式。要删除此规范，请使用此 **no**命令的形式。

ldap-scope*scope*
no ldap-scope

Syntax Description

scope 服务器收到授权请求时要搜索的LDAP层次结构的级别数。有效值为：

- — 仅**onelevel**搜索基本 DN 之下的一级
- **subtree**- 搜索基本 DN 以下的所有级别

Command Default

默认值为 **onelevel**。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
AAA服务器主机配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

将范围指定为 **onelevel** 可使搜索速度加快，因为只会搜索 Base DN 以下的一个级别。指定 **subtree** 的速度较慢，因为系统会搜索 Base DN 以下的所有级别。

该命令仅适用于 LDAP 服务器。

CR_Examples

以下示例在主机 1.2.3.4 上配置名为 svrgrp1 的 LDAP AAA 服务器，设置超时时间为 9 秒，设置重试间隔为 7 秒，并将 LDAP 范围配置为包括子树级别。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
```

```
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa
(config-aaa-server-host)#
```

Related Commands

命令	说明
aaa-serverhost	进入 AAA 服务器主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。
ldap-base-dn	在 LDAP 层次结构中指定当服务器接收授权请求时应开始搜索的位置。
ldap-login-dn	指定系统应绑定的目录对象的名称。
ldap-login-password	指定登录 DN 的密码。该命令仅适用于 LDAP 服务器。
ldap-naming-attribute	指定唯一标识LDAP服务器上的条目的相对可分辨名称属性（或多个属性）。

leap-bypass

要启用 LEAP Bypass，请在 **leap-bypassenable** 策略组配置模式下使用该命令。要禁用 LEAP 绕行，请使用 **leap-bypassdisable**命令。要从运行配置中删除 LEAP Bypass 属性，请使用此命令的 **no**形式。此选项允许从另一个组策略继承 LEAP Bypass 的值。

leap-bypass { **enable** | **disable** }
no leap-bypass

Syntax Description

disable	禁用 LEAP 旁路。
enable	启用 LEAP 旁路。

Command Default

LEAP 旁路已禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
组策略配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

启用后，LEAP Bypass 允许来自 VPN 硬件客户端后面的无线设备的 LEAP 数据包在用户身份验证之前通过 VPN 隧道传输。这样就可让使用思科无线接入点设备的工作站建立 LEAP 身份验证。然后，设备可以按用户身份再次进行身份验证。

如果启用交互式硬件客户端身份验证，则此功能无法按预期工作。

有关更多信息，请参阅 CLI 配置指南。

注释 允许任何未经身份验证的流量穿越隧道可能会存在安全风险。

CR_Examples

以下示例显示如何为名为“FirstGroup”的组策略设置 LEAP Bypass：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# leap-bypass enable
```

Related Commands

命令	说明
secure-unit-authentication	要求 VPN 硬件客户端在每次启动隧道时使用用户名和密码进行身份验证。
user-authentication	要求 VPN 硬件客户端后面的用户在连接之前向 ASA 证明自己的身份。

许可证

要配置 ASA 发送到云网络安全代理服务器的身份验证密钥以指示请求来自哪个组织，请在 **license**scansafe 常规选项配置模式下使用该命令。要删除许可证，请使用此命令的 **no** 形式。

license*hex_key*
nolicense [*hex_key*]

Syntax Description

hex_key 将身份验证密钥指定为 16 字节十六进制数。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

每个 ASA 必须使用您从云网络安全获取的身份验证密钥。身份验证密钥让云网络安全识别与网络请求相关的公司，并确保 ASA 与有效客户相关联。

可以为 ASA 使用两种身份验证密钥类型之一：公司密钥或组密钥。

公司认证密钥

公司身份验证密钥可在同一公司内的多个 ASA 上使用。此密钥仅为您的 ASA 启用云网络安全服务。管理员在 ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp) 中生成此密钥；您可以通过邮件发送密钥以供日后使用。您稍后无法在 ScanCenter 中查找此密钥；则仅在 ScanCenter 中显示最后 4 位数字有关更多信息，请参阅云网络安全文档：
http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html 。

组认证密钥

组身份验证密钥是每个 ASA 独有的特殊密钥，可执行两项功能：

- 为 ASA 启用云网络安全服务。
- 识别 ASA 的所有流量，以便可以为每个 ASA 创建 ScanCenter 策略。

管理员在 ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp) 中生成此密钥；您可以通过邮件发送密钥以供日后使用。您稍后无法在 ScanCenter 中查找此密钥；则仅在 ScanCenter 中显示最后 4 位数字有关更多信息，请参阅云网络安全文档：
http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html 。

CR_Examples

以下示例仅配置主服务器：

```
scansafe general-options server primary ip 180.24.0.62 port 8080 retry-count 5 license
366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

命令	说明
class-maptypeinspectscansafe	为加入白名单的用户和组创建检查类映射。
defaultusergroup	如果 ASA 无法确定进入 ASA 的用户的身份，则指定默认用户名和/或组。
[**https**]（参数）	指定检查策略映射的服务类型：HTTP 或 HTTPS。
inspectscansafe	对类中的流量启用云网络安全检查。
license	配置 ASA 发送到云网络安全代理服务器的身份验证密钥，以指示请求来自哪个组织。
matchusergroup	匹配白名单的用户或组。
policy-maptypeinspectscansafe	创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。
retry-count	输入重试计数器值，即 ASA 在轮询云网络安全代理服务器以检查其可用性之前等待的时间。
scansafe	在多情景模式下，允许基于情景的云网络安全。
scansafegeneral-options	配置常规云网络安全服务器选项。
server{**primary**| **backup**}	配置主或备份云网络安全代理服务器的完全限定域名或 IP 地址。
showconnscansafe	显示所有云网络安全连接，标有大写 Z 标志。
showscansafeserver	显示服务器的状态，表示服务为当前活动服务器、备用服务器还是无法访问。
showscansafestatistics	显示总计和当前 HTTP 连接数。
user-identitymonitor	从 AD 代理下载指定的用户或组信息。
whitelist	对流量类执行白名单操作。

license-server address

要标识供参与者使用的共享许可服务器 IP 地址和共享密钥，请在全局配置模式下使用 **license-serveraddress**命令。要禁用参与共享许可，请使用此命令的 **no** 形式。共享许可证允许您购买大量 SSL VPN 会话，并通过将其中一个 ASA 配置为共享许可服务器，将其余 ASA 配置为共享许可参与者，在一组 ASA 之间根据需要共享会话。

license-server address地址**secret**密钥[**portport**]
no license-server address[地址**secret**密钥[**portport**]]

Syntax Description

地址	标识共享许可服务器 IP 地址。
port端口	（可选）如果您使用该命令更改了服务器配置中的**license-serverport**默认端口，请将备份服务器的端口设置为匹配，介于 1 和 65535 之间。默认端口为 50554。
secret*secret*	标识共享密钥。密钥必须与服务器上使用 **license-serversecret** 命令设置的密钥相匹配。

Command Default

默认端口为 50554。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

共享许可参与者必须拥有共享许可参与者密钥。使用 **showactivation-key**命令检查已安装的许可证。

只能为每个参与者指定一个共享许可证服务器。

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。

1. 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。
2. 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。

1. 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。
2. 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）。
3. 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 如果共享许可服务器的本地会话用完，它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。
3. 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。

参与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。

CR_Examples

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
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverenable	使一个单元成为共享许可服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-serverrefresh-interval	设置提供给参与者的刷新间隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server backup address

要标识供参与者使用的共享许可备用服务器 IP 地址，请在全局配置模式下使用 **license-serverbackupaddress**命令。要禁用备份服务器，请使用此命 **no**令的形式。

license-server backup address*address*
no license-server address [**address**]

Syntax Description

地址	标识共享许可备用服务器 IP 地址。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

共享许可备用服务器必须配置**license-serverbackupenable** 命令。

CR_Examples

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
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。

命令	说明
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverenable	使一个单元成为共享许可服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-serverrefresh-interval	设置提供给参与者的刷新间隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server backup backup-id

要在主共享许可服务器配置中标识共享许可备用服务器，请在全局配置模式下使用 **license-serverbackupbackup-id**命令。要删除备份服务器配置，请使用此命 **no**令的形式。

license-server backup地址**backup-id***serial_number*[**ha-backup-id***ha_serial_number*]
no license-server backup地址[**backup-id***serial_number*[**ha-backup-id***ha_serial_number*]]

Syntax Description

地址	标识共享许可备用服务器 IP 地址。
backup-id *serial_number*	标识共享许可备用服务器序列号。
ha-backup-id*ha_serial_number*	如果对备用服务器使用故障转移，则标识辅助共享许可备用服务器序列号。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

只能确定 1 台备用服务器及其可选的备用设备。

要查看备用服务器序列号，请输入 **showactivation-key**命令。

要使参与者成为备用服务器，请使用 **license-serverbackupenable** 命令。

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。

CR_Examples

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
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverenable	使一个单元成为共享许可服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-serverrefresh-interval	设置提供给参与者的刷新间隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。

命令	说明
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server backup enable

要使此设备成为共享许可备用服务器，请在全局配置模式下使用 **license-serverbackupenable**命令。要禁用备份服务器，请使用此命 **no**令的形式。

license-server backup enable*interface_name*
no license-server enable*interface_name*

Syntax Description

interface_name 指定参与者联系备份服务器的接口。您可以为所需数量的接口重复此命令。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

备用服务器必须具有共享许可参与者密钥。

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。

CR_Examples

以下示例标识许可证服务器和共享密钥，并启用此单元作为内部接口和 dmz 接口上的备份共享许可证服务器。

```
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
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverenable	使一个单元成为共享许可服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-serverrefresh-interval	设置提供给参与者的刷新间隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server enable

要将此设备标识为共享许可服务器，请在全局配置模式下使用 **license-serverenable**命令。要禁用共享许可服务器，请使用此命 **no**令的形式。共享许可证允许您购买大量 SSL VPN 会话，并通过将其中一个 ASA 配置为共享许可服务器，将其余 ASA 配置为共享许可参与者，在一组 ASA 之间根据需要共享会话。

license-server enable*interface_name*
no license-server enable*interface_name*

Syntax Description

interface_name 指定参与者联系服务器的接口。您可以为所需数量的接口重复此命令。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
8.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

共享许可服务器必须具有共享许可服务器密钥。使用 **showactivation-key**命令检查已安装的许可证。

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。

1. 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。
2. 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。

1. 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。
2. 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）。
3. 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 如果共享许可服务器的本地会话用完，它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。
3. 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。

参与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。

CR_Examples

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
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-serverrefresh-interval	设置提供给参与者的刷新间隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server port

要设置共享许可服务器在其上侦听来自参与者的 SSL 连接的端口，请在全局配置模式下使用 **license-serverport**命令。要恢复默认端口，请使用此命 **no**令的形式。

license-server port端口
no license-server port[端口]

Syntax Description

seconds	设置服务器侦听来自参与者的 SSL 连接的端口，介于 1 到 65535 之间。默认值为 TCP 端口 50554。

Command Default

默认端口为 50554。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

如果您更改默认的端口，请务必使用 **license-serveraddress**命令为每个参与者设置相同的端口。

CR_Examples

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
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。

命令	说明
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverenable	使一个单元成为共享许可服务器。
license-serverrefresh-interval	设置提供给参与者的刷新间隔，以设置他们与服务器通信的频率。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server refresh-interval

要设置为参与者提供的刷新间隔，以便设置它们应与共享许可服务器通信的频率，请在全局配置模式下使用 **license-serverrefresh-interval**命令。要恢复默认刷新间隔，请使用此命 **no**令的形式。

license-server refresh-interval秒
no license-server refresh-interval[秒]

Syntax Description

seconds	将刷新间隔设置为 10 到 300 秒。默认值为 30 秒。

Command Default

默认值为 30 秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

每个参与者定期与使用 SSL 的共享许可服务器通信，以便共享许可服务器可以跟踪当前许可证使用情况并接收和响应许可证请求。

CR_Examples

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
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。

命令	说明
clearconfigurelicense-server	清除共享许可服务器配置。
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器IP地址和序列号。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverenable	使一个单元成为共享许可服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-server secret	在共享许可服务器上设置共享密钥。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license-server secret

要在共享许可服务器上设置共享密钥，请在全局配置模式下使用**license-serversecret**命令。要删除秘密，请使用此命 **no**令的形式。

license-server secret*secret*
no license-server secret*secret*

Syntax Description

secret	设置共享密钥，一个介于 4 到 128 个 ASCII 字符之间的字符串。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

任何在命令中识别出此秘密的 **license-serveraddress**参与者都可以使用许可服务器。

CR_Examples

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
```

Related Commands

命令	说明
activation-key	输入许可证激活密钥。
clearconfigurelicense-server	清除共享许可服务器配置。

命令	说明
清除共享许可证	清除共享许可证统计信息。
license-serveraddress	标识参与者的共享许可服务器 IP 地址和共享机密。
license-serverbackupaddress	为参与者确定共享许可备用服务器。
license-serverbackupbackup-id	确定主共享许可服务器的备用服务器 IP 地址和序列号。
license-serverbackupenable	使一个单元成为共享许可备份服务器。
license-serverenable	使一个单元成为共享许可服务器。
license-serverport	设置服务器侦听来自参与者的 SSL 连接的端口。
license-serverrefresh-interval	设置提供给参与者的刷新间隔，以设置他们与服务器通信的频率。
showactivation-key	显示当前安装的许可证。
showrunning-configlicense-server	显示共享许可服务器配置。
showsharedlicense	显示共享许可证统计信息。
showvpn-sessiondb	显示有关 VPN 会话的许可证信息。

license smart

要设置智能许可授权请求，请在**licensesmart**全局配置模式下使用该命令。要删除授权并取消许可您的设备，请使用此命令的 **no**形式。

注释 仅 ASA virtual 和机箱支持此功能。

license smart
no license smart

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.3(2)	添加此命令是为了提供 ASA virtual 支持。
9.4(1.152)	增加了对 Firepower 9300 的支持。
9.6(1)	添加了对 Firepower 4100 系列的支持。
9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南

此命令可进入许可证智能配置模式，在此模式下可以设置功能层和其他许可证授权。对于 ASA virtual，当您第一次请求授权时，您必须退出许可证智能配置模式才能使您的更改生效。

CR_Examples

以下示例将功能级别设置为“标准”，并将吞吐量级别设置为 2G：

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Related Commands

命令	说明
call-home	配置 Smart Call Home。智能许可使用 Smart Call Home 基础设施。
clearconfigurelicense	清除智能许可配置。
featuretier	设置智能许可的功能级别。
http-proxy	为智能许可和 Smart Call Home 设置 HTTP(S) 代理。
licensesmart	让您为智能许可请求许可证授权。
licensesmartderegister	从许可证颁发机构注销设备。
licensesmartregister	向许可证颁发机构注册设备。
licensesmartrenew	续订注册或许可证授权。
servicecall-home	启用 Smart Call Home。
showlicense	显示智能许可状态。
showrunning-configlicense	显示智能许可配置。
throughputlevel	设置智能许可的吞吐量级别。

license smart deregister

要从智能许可的思科许可证颁发机构取消注册设备，请在特权 EXEC 模式下使用**licensesmartderegister**命令。

注释 仅 ASA virtual 和 Firepower 2100 支持此功能。

license smart deregister

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.3(2)	添加此命令是为了提供 ASA virtual 支持。
9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南

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。此命令导致 ASA 重新加载。

CR_Examples

以下示例取消注册设备：

```
ciscoasa# license smart deregister
```

Related Commands

命令	说明
call-home	配置 Smart Call Home。智能许可使用 Smart Call Home 基础设施。
clearconfigurelicense	清除智能许可配置。
featuretier	设置智能许可的功能级别。

命令	说明
http-proxy	为智能许可和 Smart Call Home 设置 HTTP(S) 代理。
licensesmart	让您为智能许可请求许可证授权。
licensesmartderegister	从许可证颁发机构注销设备。
licensesmartregister	向许可证颁发机构注册设备。
licensesmartrenew	续订注册或许可证授权。
servicecall-home	启用 Smart Call Home。
showlicense	显示智能许可状态。
showrunning-configlicense	显示智能许可配置。
throughputlevel	设置智能许可的吞吐量级别。

license smart plr set

要配置与 RAM 和 vCPU 无关的永久许可证预留（灵活的永久许可证预留模式），请在 **license smart plr set**全局配置模式下使用该命令。

要禁用灵活永久许可证预留，请在使用 **no license smart reservation** 命令禁用永久许可证预留模式后，使用此命令的 **no** 形式。

注释 此功能受支持。 ASA virtual

license smart plr set { **ASAV_5_UNIVERSAL** | **ASAV_10_UNIVERSAL** | **ASAV_30_UNIVERSAL** | **ASAV_50_UNIVERSAL** | **ASAV_100_UNIVERSAL** | **ASAV_U_UNIVERSAL** }

Syntax Description

ASAV_5_UNIVERSAL	ASAv5 授权
ASAV_10_UNIVERSAL	ASAv10 授权
ASAV_30_UNIVERSAL	ASAv30 授权
ASAV_50_UNIVERSAL	ASAv50 授权
ASAV_100_UNIVERSAL	ASAv100 授权
ASAV_U_UNIVERSAL	ASAvU 授权

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.23(1)	添加此命令是为了提供 ASA virtual 支持。

使用指南

您可以配置任何型号特定许可证，而不考虑分配给 ASA virtual 的RAM 和 vCPU。此永久许可证预留模式称为灵活永久许可证预留模式。您指定的型号许可证会设置 ASA virtual 的吞吐量水平。您的内

存决 ASA virtual 定了最大安全客户端、TLS 代理会话、最大并发防火墙连接和 VLAN。这些不是由模型许可证决定的。但是，较低的 ASA virtual 内存配置文件将限制实际的会话和功能数量。

例如，如果 ASA virtual 有 8 GB RAM 并注册了 ASAV_50_UNIVERSAL，则分配的最大安全客户端会话数为 750。当会话超过此限制时，系统就会丢弃这些连接。

此永久许可证预留许可证模式的其他优势包括：

- 您可以在永久许可证预留许可证之间切换，而不考虑分配给 ASA virtual 的内存。但是，如果 ASA virtual 的vCPU 超过 16 个，则您只能配置 ASAvU（无限）许可证。
- 您可以更改分配给 ASA virtual 的内存和 vCPU，而无需更改型号许可证。

示例

要配置永久许可证预留的 ASAv30 授权，请执行以下操作：

```
ciscoasa (config)# license smart plr set ASAV_30_UNIVERSAL
ciscoasa (config)# license smart reservation
ciscoasa (config)#license smart reservation request universal
```

Related Commands

命令	说明
license smart reservation	启用永久许可证保留
license smart reservation request universal call-home	请求许可证代码以输入智能软件管理器。

license smart register

要向思科许可证颁发机构注册设备以获取智能许可，请在特权 EXEC 模式下使用**licensesmartregister**命令。

注释 仅 ASA virtual 和 Firepower 2100 支持此功能。

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

Syntax Description

idtoken*id_token*	在智能软件管理器中，请求并复制要添加此ASA的虚拟帐户的注册令牌。
force	注册已注册但可能与许可证颁发机构不同步的 ASA。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.3(2)	添加此命令是为了提供 ASA virtual 支持。
9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南

当您注册 ASA 时，许可证颁发机构会颁发 ID 证书，用于 ASA 和许可证颁发机构之间的通信。它还将 ASA 分配给适当的虚拟账户。通常情况下，此程序是一次性实例。但是，如果 ID 证书由于通信问题等原因过期，您可能需要稍后重新注册 ASA。

CR_Examples

以下示例使用注册令牌进行注册：

```
ciscoasa# license smart register idtoken
YjE3NjctMzYtMGQzMi00OTA4LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzI8NXk2bzV3SDE0ZkgwQkdYRmZlNlNCNG1vRnBHUFpjcm02WlB4TU4w%0Ac2NrMD0%3D%0A
```

Related Commands

命令	说明
call-home	配置 Smart Call Home。智能许可使用 Smart Call Home 基础设施。
clearconfigurelicense	清除智能许可配置。
featuretier	设置智能许可的功能级别。
http-proxy	为智能许可和 Smart Call Home 设置 HTTP(S) 代理。
licensesmart	让您为智能许可请求许可证授权。
licensesmartderegister	从许可证颁发机构注销设备。
licensesmartregister	向许可证颁发机构注册设备。
licensesmartrenew	续订注册或许可证授权。
servicecall-home	启用 Smart Call Home。
showlicense	显示智能许可状态。
showrunning-configlicense	显示智能许可配置。
throughputlevel	设置智能许可的吞吐量级别。

license smart renew

要为智能许可更新注册或许可证授权，请在特权 EXEC 模式下使用**licensesmartrenew**命令。

注释 仅 ASA virtual 和 Firepower 2100 支持此功能。

license smart renew {**id** | **auth**}

Syntax Description

id	续订设备注册。
auth	续订许可证权利。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.3(2)	添加此命令是为了提供 ASA virtual 支持。
9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南

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。

CR_Examples

以下示例更新注册和许可证授权：

```
ciscoasa# license smart renew id
ciscoasa# license smart renew auth
```

Related Commands

命令	说明
call-home	配置 Smart Call Home。智能许可使用 Smart Call Home 基础设施。
clearconfigurelicense	清除智能许可配置。

命令	说明
featuretier	设置智能许可的功能级别。
http-proxy	为智能许可和 Smart Call Home 设置 HTTP(S) 代理。
licensesmart	让您为智能许可请求许可证授权。
licensesmartderegister	从许可证颁发机构注销设备。
licensesmartregister	向许可证颁发机构注册设备。
licensesmartrenew	续订注册或许可证授权。
servicecall-home	启用 Smart Call Home。
showlicense	显示智能许可状态。
showrunning-configlicense	显示智能许可配置。
throughputlevel	设置智能许可的吞吐量级别。

license smart reservation

要启用永久许可证预留，请在全局配置模式下使用 **licensesmartreservation** 命令。要禁用永久许可证预留，请使用此命令的 **no** 形式。

license smart reservation
no license smart reservation

注释 此功能仅适用于 ASA virtual 和 Firepower 2100。

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下会禁用此功能。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.5(2.200)	引入此命令是为了支持 ASA virtual 。
9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南

对于无法访问互联网的 ASA，您可以从智能软件管理器 (https://software.cisco.com/#SmartLicensing-Inventory) 申请永久许可证。永久许可证可启用所有功能的最大级别。

对于 ASA virtual，当您输入 **licensesmartreservation** 命令时，将删除以下命令：

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

要使用常规智能许可，请使用此命令的 **no** 形式，然后重新输入上述命令。其他 Smart Call Home 配置保持不变，但未使用，因此您不需要重新输入这些命令。

对于机箱，您必须为任何非默认许可证输入 **licensesmart/feature** 命令；例如，对于情景许可证。需要使用这些命令，以便 ASA 知道 允许配置该功能。

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。查看 **licensesmartreservationreturn**命令。

CR_Examples

以下示例启用永久许可证预留，请求在智能软件管理器中输入许可证代码，然后安装从智能软件管理器收到的授权代码：

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

Related Commands

命令	说明
licensesmartreservation	启用永久许可证保留。
licensesmartreservationcancel	如果尚未在智能软件管理器中输入代码，则取消永久许可证请求。
licensesmartreservationinstall	输入授权码。
licensesmartreservationrequestuniversal	请求许可证代码以输入智能软件管理器。
licensesmartreservationreturn	将许可证退回给智能软件管理器。

license smart reservation cancel

如果尚未在智能软件管理器中输入代码，则要取消永久许可证预留请求，请在特权 EXEC 模式下使用 **licensesmartreservationcancel**命令。

license smart reservation cancel

注释 此功能仅适用于 ASA virtual 和 Firepower 2100。

Syntax Description 此命令没有任何参数或关键字。

Command Default 无默认行为或值。

Command Modes 下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.5(2.200)	引入此命令是为了支持 ASA virtual 。
9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南 如果您使用 **licensesmartreservationrequestuniversal**命令请求了要在智能软件管理器中输入的许可证代码，并且尚未将此代码输入到智能软件管理器中，则您可以使用**licensesmartreservationcancel**命令取消请求。

如果禁用永久许可证预留（**nolicensesmartreservation**），则所有待处理的请求都将被取消。

如果您已经将代码输入智能软件管理器，那么您必须完成将许可证应用到 ASA，然后才能使用命令返回许可 **licensesmartreservationreturn**证。

CR_Examples 以下示例启用永久许可证预留，请求在智能软件管理器中输入要输入的许可证代码，然后取消请求：

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
```

```
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa(config)# license smart reservation cancel
```

Related Commands

命令	说明
licensesmartreservation	启用永久许可证保留。
licensesmartreservationcancel	如果尚未在智能软件管理器中输入代码，则取消永久许可证请求。
licensesmartreservationinstall	输入授权码。
licensesmartreservationrequestuniversal	请求许可证代码以输入智能软件管理器。
licensesmartreservationreturn	将许可证退回给智能软件管理器。

license smart reservation install

要输入从智能软件管理器收到的永久许可证预留授权码，请在特权 EXEC 模式下使用 **licensesmartreservationinstall** 命令。

license smart reservation install*code*

注释 此功能仅适用于 ASA virtual 和 Firepower 2100。

Syntax Description

code 从智能软件管理器接收的永久许可证预留授权码。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.5(2.200)	引入此命令是为了支持 ASA virtual 。
9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南

对于无法访问互联网的 ASA，您可以从智能软件管理器 (https://software.cisco.com/#SmartLicensing-Inventory) 申请永久许可证。请求使用命令进入智能软件管理器的 **licensesmartreservationrequestuniversal**代码。在将代码输入智能软件管理器时，请复制生成的授权代码，并使用 **licensesmartreservationinstall**命令将其输入到 ASA 中。

CR_Examples

以下示例启用永久许可证预留，请求在智能软件管理器中输入许可证代码，然后安装从智能软件管理器收到的授权代码：

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

Related Commands

命令	说明
licensesmartreservation	启用永久许可证保留。
licensesmartreservationcancel	如果尚未在智能软件管理器中输入代码，则取消永久许可证请求。
licensesmartreservationinstall	输入授权码。
licensesmartreservationrequestuniversal	请求许可证代码以输入智能软件管理器。
licensesmartreservationreturn	将许可证退回给智能软件管理器。

许可证智能预订通用

要请求许可证代码以在智能软件管理器中输入，请在特权 EXEC 模式下使用 **licensesmartreservationuniversal** 命令。

license smart reservation universal

注释 此功能仅适用于 ASA virtual 和 Firepower 2100。

Syntax Description 此命令没有任何参数或关键字。

Command Default 无默认行为或值。

Command Modes 下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.5(2.200)	引入此命令是为了支持 ASA virtual 。
9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南

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。请求使用命令进入智能软件管理器的 **licensesmartreservationrequestuniversal**代码。

ASA virtual 部署确定请求的许可证 (ASAv5/ASAv10/ASAv30)。

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想要取消请求，请输入该 **licensesmartreservationcancel** 命令。

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。查看 **licensesmartreservationreturn**命令。

要请求授权代码，请转到智能软件管理器库存屏幕 (https://software.cisco.com/#SmartLicensing-Inventory)，然后点击 **Licenses** 选项卡。**Licenses**选项卡显示与您的账户相关的所有现有许可证（普通类型和永久类型）。单击 **LicenseReservation**，然后在框中输入 ASA 代码。Click **ReserveLicense**. 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。

如果您没有看到该按**LicenseReservation**钮，则表示您的帐户无权进行永久许可证保留。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。

使用 **licensesmartreservationinstall**命令在 ASA 上输入授权码。

CR_Examples

以下示例启用永久许可证预留，请求在智能软件管理器中输入许可证代码，然后安装从智能软件管理器收到的授权代码：

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

Related Commands

命令	说明
licensesmartreservation	启用永久许可证保留。
licensesmartreservationcancel	如果尚未在智能软件管理器中输入代码，则取消永久许可证请求。
licensesmartreservationinstall	输入授权码。
licensesmartreservationrequestuniversal	请求许可证代码以输入智能软件管理器。
licensesmartreservationreturn	将许可证退回给智能软件管理器。

许可证智能预留返还

要生成用于将许可证退回智能软件管理器的退回代码，请在特权 EXEC 模式下使用 **licensesmartreservationreturn** 命令。

license smart reservation return

注释 此功能仅适用于 ASA virtual 和 Firepower 2100。

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.5(2.200)	引入此命令是为了支持 ASA virtual 。
9.8(2)	添加了对 Firepower 2100 系列的支持。

使用指南

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。如果您不再需要永久许可证（例如，您正在淘汰 ASA 或更改 ASA virtual 模型级别，因此需要新的许可证），则必须正式将许可证退还给智能软件管理器。如果您不归还许可证，则许可证将处于已使用状态，并且不能轻易释放以供其他地方使用。

输入该 **licensesmartreservationreturn** 命令后，ASA 立即变为未许可状态并进入评估状态。如果您需要再次查看此代码，请重新输入此命令。请注意，如果您申请新的永久许可证（**licensesmartreservationrequestuniversal**）或更改模 ASA virtual 型级别（通过关闭电源并更改 vCPU/RAM），则无法重新显示此代码。确保捕获该代码以完成返还。

在智能软件管理器中输入代码之前，请使用命令查看 ASA 通用设备标识符 (UDI)，以便您可以在 **showlicenseudi** 智能软件管理器中找到此 ASA 实例。转至“智能软件管理器库存”屏幕 (https://software.cisco.com/#SmartLicensing-Inventory)，然后单击 **ProductInstances** 选项卡。该 **ProductInstances**选项卡显示所有经 UDI 许可的产品。找到 ASA virtual 您想要取消许可的，选择

Actions>Remove，然后在框中输入 ASA 返回代码。点击 。 **RemoveProductInstance** 永久许可证被返还到可用池。

CR_Examples

以下示例在 ASA virtual上生成返回代码，并查看 ASA virtual UDI：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
```

Related Commands

命令	说明
licensesmartreservation	启用永久许可证保留。
licensesmartreservationcancel	如果尚未在智能软件管理器中输入代码，则取消永久许可证请求。
licensesmartreservationinstall	输入授权码。
licensesmartreservationrequestuniversal	请求许可证代码以输入智能软件管理器。
licensesmartreservationreturn	将许可证退回给智能软件管理器。

lifetime (ca server mode)

如要指定本地证书颁发机构 (CA) 证书、每个颁发的用户证书或证书撤销列表 (CRL) 的有效时间长度，请在 ca 服务器配置模式下使用 **lifetime**命令。要将生存期重置为默认设置，请使用此命令的 **no** 形式。

lifetime {**ca-certificate** | **certificate** | **crl**} *time*
lifetime {**ca-certificate** | **certificate** | **crl**}

Syntax Description

ca-certificate	指定本地 CA 服务器证书的有效期。
certificate	指定 CA 服务器颁发的所有用户证书的有效期。
crl	指定 CRL 的有效期。
time	对于 CA 证书和所有已颁发的证书， 时间 指定证书有效的天数。有效期为5至30年。默认生命周期值为 15 年。 对于所有已颁发的用户证书，有效范围是一天到 4 年。默认生命周期值为 2 年。 对于 CRL， *time* 指定 CRL 有效的小时数。CRL 的有效范围为 1 至 720 小时。

Command Default

默认生命周期为：

- CA 证书 - 15 年
- 颁发证书——两年
- CRL - 六个小时

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
CA 服务器配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。
9.12(1)	ca-certificate 的允许值更改为 5 至 30 年，默认为 15 年。 证书的允许值更改为 1 天/ 4 年，默认值为 2 年。

使用指南

通过指定证书或 CRL 有效的天数或小时数，此命令可以确定证书或 CRL 中包含的到期日期。

该命令在 **lifetimeca-certificate**本地CA服务器证书首次生成时（即首次配置本地CA服务器并发出该 **noshutdown**命令时）生效。当 CA 证书到期时，配置的有效期值用于生成新的 CA 证书。您不能更改现有 CA 证书的有效期值，

CR_Examples

以下示例将 CA 配置为颁发有效期为三个月的证书：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# lifetime certificate 90
ciscoasa
(config-ca-server)
)#
```

以下示例将 CA 配置为颁发有效期为两天的 CRL：

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# lifetime crl 48
ciscoasa
(config-ca-server)
#
```

Related Commands

命令	说明
cdp-url	指定要包括在 CA 颁发的证书中的证书撤销列表分发点 (CDP)。
crypto ca server	提供对 ca 服务器配置模式命令集的访问，允许您配置和管理本地 CA。
cryptocaservercrlissue	强制颁发 CRL。
showcryptocaserver	以 ASCII 文本显示本地 CA 配置详细信息。
showcryptocaservercert-db	显示本地 CA 服务器证书。
showcryptocaservercrl	显示本地 CA 的当前 CRL。

lifetime (ikev2 policy mode)

要在 IKEv2 安全关联 (SA) 中为 AnyConnect IPsec 连接指定加密算法，请在 IKEv2 策略配置模式下使用 encryption 命令。要删除该命令并使用默认设置，请使用以下命令的 **no**形式：

lifetime { { **seconds***seconds* } | **none** }

Syntax Description

seconds	生命周期（以秒为单位），从 120 到 2,147,483,647 秒。默认值为 86,400 秒（24 小时）。

Command Default

默认值为 86,400 秒（24 小时）。

使用指南

IKEv2 SA 是在第 1 阶段使用的密钥，用于使 IKEv2 对等体能够在第 2 阶段安全通信。输入 crypto ikev2 policy 命令后，使用 **lifetime** 命令设置 SA 生命周期。

生命周期设置IKEv2 SA 重新生成密钥的间隔。使用 none 关键字会禁用为 SA 重新生成密钥。但是，Secure Client 仍可以重新生成 SA 密钥。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.4(1)	添加了此命令。

CR_Examples

以下示例进入 IKEv2 策略配置模式并将生命周期设置为 43,200 秒（12 小时）：

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# lifetime 43200
```

Related Commands

命令	说明
encryption	为 AnyConnect IPsec 连接指定 IKEv2 SA 中的加密算法。
group	在 IKEv2 SA 中为 AnyConnect IPsec 连接指定 Diffie-Hellman 群。
integrity	为 AnyConnect IPsec 连接指定 IKEv2 SA 的 ESP 完整性算法。

命令	说明
prf	在 IKEv2 SA 中为 AnyConnect IPsec 连接指定伪随机函数。

limit-resource

要在多情景模式下为类指定资源限制，请在类配置模式下使用**limit-resource** 命令。要将限制恢复为默认值，请使用此命**no**令的形式。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。

limit-resource [**rate**] {**all** | *resource_name*} *number* [**%**] }
no limit-resource [**rate**] {**all** | *resource_name*}

Syntax Description

all	设置所有资源的限制。
number [**%**]	将资源限制指定为一个大于或等于 1 的固定数值，或指定为介于 1 和 100 之间的系统限制的百分比（与百分号 (%) 一起使用时）。将限制设置为 **0** 以指示不受限制的资源，或对于 VPN 资源类型，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。
rate	指定要设置资源的每秒速率。有关可为其设置每秒速率的资源，请参阅 表 7-1 。
resource_name	指定要为其设置限制的资源名称。此限制会覆盖为 **all**设置的限制。

Command Default

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。

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。）
- IPsec 会话 - 5 个会话（每个情景的最大值。）
- MAC 地址 -（因型号而异）。（每个情景的最大值。）
- AnyConnect 对等体 - 0 个会话。（您必须将该类手动配置为允许任何 AnyConnect 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。）

注释 如果您还在 **quotamanagement-session**上下文中设置命令来设置最大管理会话（SSH 等），则将使用较低的值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类配置	• 是	• 支持	—	—	• 是

Command History

版本	修改
7.2(1)	添加了此命令。
9.0(1)	创建了一种新的资源类型 **routes**，用于设置每个上下文中路由表条目的最大数量。 创建了新的资源类型 **vpnother** 和 **vpnburstother**，以设置每个环境中站点到站点 VPN 隧道的最大数量。
9.5(2)	创建了新的资源类型 **vpnanyconnect** 和 **vpnburstanyconnect**，以设置每个环境中 AnyConnect VPN 对等体的最大数量。
9.6(2)	已创建新的资源类型 **storage**，用于设置最大存储。

使用指南

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。

表 7-1 列出了资源类型和限制。另请参阅**showresourcetypes** 命令。

表 *1:* 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[1]	说明
asdm	并发	1（最小值） 5（最大值）	200	ASDM 管理会话。 **注释** 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，200 个 ASDM 会话的系统限制代表 400 个 HTTPS 会话的限制。
conns	并发或速率	不适用	并发连接：有关平台的连接限制，请参阅 CLI 配置指南。 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。

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[1]	说明
hosts	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	应用检查。
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。
routes	并发	不适用	不适用	动态路由数。
ssh	并发	1（最小值） 5（最大值）	100	SSH 会话数。
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)。使用命令指定驱动 **storage-url** 器。
syslogs	Rate	不适用	不适用	系统日志消息。
telnet	并发	1（最小值） 5（最大值）	100	Telnet 会话数。
vpnburstanyconnect	并发	不适用	您型号的 AnyConnect 高级对等体数减去为 vpn anyconnect 向所有情景分配的会话总和。	允许的 AnyConnect 会话数超出了分配给上下文的数量。 **vpnanyconnect** 例如，如果您的模型支持 5000 个对等体，并且您在所有上下文中分配了 4000 个对等体 **vpnanyconnect**，那么剩余的 1000 个会话可用于。 **vpnburstanyconnect** 与 **vpnanyconnect**保证上下文会话的 不同，**vpnburstanyconnect**可以超额认购；突发池按照先到先得的原则提供给所有上下文。
vpnanyconnect	并发	不适用	请参阅 CLI 配置指南中的“每个型号支持的功能许可证”部分，了解适用于您的型号的 AnyConnect VPN 对等体。	AnyConnect 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。

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[1]	说明
vpnburstother	并发	不适用	您的模型的其他 VPN 会话数量减去分配给所有上下文的会话总和。 **vpnother**	允许的站点到站点 VPN 会话数超出了分配给上下文的数量。 **vpnother** 例如，如果您的模型支持 5000 个会话，并且您在所有上下文中分配了 4000 个会话 **vpnother**，则剩余的 1000 个会话可用于。 **vpnburstother** 与 **vpnother**保证上下文会话的 不同，**vpnburstother**可以超额认购；突发池按照先到先得的原则提供给所有上下文。
vpnother	并发	不适用	有关适用于您的型号的其他 VPN 会话的 CLI 配置指南，请参阅“每个型号支持的功能许可证”部分。	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。
xlates	并发	不适用	不适用	地址转换。

[1] 如果此列值为 N/A，则您无法设置资源的百分比，因为该资源没有硬系统限制。

CR_Examples

以下示例将 conn 的默认类限制设置为 10% 而不是不受限制：

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```

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 700
```

Related Commands

命令	说明
class	创建资源类。
context	配置安全上下文。
member	将上下文分配给资源类。

命令	说明
显示资源分配	显示如何跨类分配资源。
show resource types	显示您可以设置限制的资源类型。

lmfactor

要设置重新验证策略以缓存仅具有上次修改时间时间戳的对象，而没有其他服务器设置过期值，请在缓存配置模式下使用 **lmfactor**命令。要设置用于重新验证此类对象的新策略，请再次使用 命令。要将属性重置为默认值 20，请输入此命令的 **no** 版本。

lmfactor值
nolmfactor

Syntax Description

value	0 到 100 范围内的整数。

Command Default

默认值为 20。

Command Modes

下表显示了输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
缓存配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

ASA 使用 流率系数 的值来估计它认为缓存对象未更改的时间长度。这段时间称为到期时间。ASA 通过自上次修改以来经过的时间乘以 lmfactor 来估算到期时间。

将 lmfactor 设置为零相当于强制立即重新验证，而将其设置为 100 则会导致重新验证所需的最长允许时间。

CR_Examples

以下示例显示如何将 流明系数设置为 30：

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# lmfactor 30
ciscoasa(config-webvpn-cache)#
```

Related Commands

命令	说明
cache	进入 WebVPN 缓存模式。
cache-compressed	配置 WebVPN 缓存压缩。
disable	禁用缓存。
expiry-time	配置缓存对象的到期时间而不重新验证它们。
max-object-size	定义要缓存的对象的最大大小。
min-object-size	定义要缓存的最小对象大小。

load-monitor

要配置集群流量负载监控，请在集群配置模式下使用 **load-monitor**命令。要禁用此功能，请使用此 **no**命令的形式。

load-monitor[**frequency**秒][**intervals**间隔]
no load-monitor[**frequency**秒][**intervals**间隔]

Syntax Description

frequency秒	可选）设置监控消息之间的时间（以秒为单位），介于 10 到 360 秒之间。默认值为 20 秒。
intervals间隔	（可选）设置 ASA 维护数据的间隔数，介于 1 到 60 之间。默认值为 30。

Command Default

默认情况下会启用此命令。默认频率为 20 秒。默认间隔为 30。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
集群配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.13(1)	命令已添加。

使用指南

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 **showclusterinfoload-monitor**用命令查看流量负载。

CR_Examples

以下示例将频率设置为 50 秒，将间隔设置为 25：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
```

Related Commands

命令	说明
cluster	进入集群配置模式

local-base-url

（可选）配置用于 VPN 身份验证的 SAML 服务提供商的本地基本 URL。在 DNS 负载平衡集群中，当您在 ASA 上配置 SAML 身份验证时，您可以指定此 URL 来唯一解析应用该配置的设备。

要禁用此功能，请使用此命 **no** 令的形式

local base-url { **url** }
no local base-url

Syntax Description

url	用于 VPN 身份验证的 SAML 服务提供商的本地基本 URL。

Command Default

无。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
参数配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.18(3)	添加了此命令。
9.19(1)5	添加了此命令。

使用指南

您必须将此命令与 **base-url** 命令结合使用。

CR_Examples

以下示例设置了本地 base-url：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# saml idp https://idp.com/<app-specific>
ciscoasa(config-webvpn-saml-idp)# base url https://asa-dns-group.vpn.customer.com
ciscoasa(config-webvpn-saml-idp)# local-base-url https://this-asa.vpn.customer.com
```

Related Commands

命令	说明
signature	在SAML 请求中启用或禁用签名。默认情况下，签名是禁用的。

命令	说明
timeout	配置 SAML IdP 超时。
trustpoint	在 saml-idp 子模式下配置信任点。
url	配置 SAML IdP URL。
base-url	为 VPN 身份验证配置 SAML 服务提供商的基本 URL。

local-domain-bypass

要配置 DNS 请求绕过思科 Umbrella 的本地域，请在 Umbrella 配置模式下使用 **local-domain-bypass** 命令。使用此命 **no**令的形式可以恢复默认设置。

local-domain-bypass { *regular_expression* | **regex class***regex_classmap* }
no local-domain-bypass { *regular_expression* | **regex class***regex_classmap* }

Syntax Description

regular_expression	标识要绕过的本地域的正则表达式。它可以像本地域一样简单，例如 example.com。表达式最多可包含 100 个字符。 如果使用此选项，则可输入 **local-domain-bypass** 命令多次以定义多个本地域。
regexclass*regex_classmap*	定义要绕过的本地域名的正则表达式类的名称。对与该类中的正则表达式相匹配的完全限定域名的任何 DNS 请求都会直接发送到已配置的 DNS 服务器，而不是发送到 Umbrella 服务器。

Command Default

默认情况下，所有域的 DNS 请求都会发送到 Cisco Umbrella。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Umbrella 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.12(1)	添加了此命令。

使用指南

以下是使用此命令的准则：

- 您可以输入此命令多次，以直接定义域名的正则表达式。
- 使用正则表达式类时，只能输入此命令一次。但是，您可以将命令的单个正则表达式类版本与直接使用正则表达式的多个实例结合使用。

CR_Examples

以下示例将 example.com 定义为要绕过的本地域。

```
ciscoasa(config)# umbrella-global
```

```
ciscoasa(config-umbrella)# local-domain-bypass example.com
```

以下示例创建一个正则表达式来匹配example.com，从而匹配*example.com上的任何完全限定域名。然后，该示例创建所需的正则表达式类映射，并将其用作Umbrella的本地域绕行。

```
ciscoasa(config)# regex example-com example.com

ciscoasa(config)# class-map type regex match-any umbrella-bypass

ciscoasa(config-cmap)# match regex example-com

ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# local-domain-bypass regex class umbrella-bypass
```

Related Commands

命令	说明
umbrella-global	配置思科 Umbrella 全局参数。

local-unit

要为此集群成员提供名称，请在**local-unit**集群组配置模式下使用该命令。要删除名称，请使用**no**此命令的形式。

local-unit*unit_name*
no local-unit [*unit_name*]

Syntax Description

unit_name 使用 1 至 38 个字符的唯一 ASCII 字符串命名该集群成员。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
集群组配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

每台设备必须拥有唯一的名称。集群中不允许存在名称重复的设备。

CR_Examples

以下示例将此设备命名为 unit1：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
```

Related Commands

命令	说明
clacpsystem-mac	使用跨网以太网通道时，ASA 使用 cLACP 与邻居交换机协商以太网通道。
cluster group	命名集群并进入集群配置模式。
cluster-interface	指定集群控制链路接口。
clusterinterface-mode	设置集群接口模式。
conn-rebalance	启用连接再均衡。

命令	说明
console-replicate	启用从从属设备到主设备的控制台复制。
enable(clustergroup)	启用集群。
health-check	启用集群健康检查功能，包括单元健康监控和接口健康监控。
key	为集群控制链路上的控制流量设置身份验证密钥。
local-unit	为集群成员命名。
mtucluster-interface	指定集群控制链路接口的最大传输单元。
priority(clustergroup)	设置此单元在主单元选举中的优先级。

location-logging

要让 GTP 检测记录移动站的位置和位置更改，请在 GTP 检测策略映射参数配置模式下使用 **location-logging** 命令。使用此命令的 **no**形式可以禁用位置日志记录。

location-logging [**cell-id**]
no location-logging [**cell-id**]

Syntax Description

cell-id	是否包括用户当前注册的单元 ID。单元 ID 从单元全局标识 (CGI) 或 E-UTRAN 单元全局标识符 (ECGI) 中提取。

Command Default

默认情况下，位置日志记录是禁用的。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
参数配置模式	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.13(1)	引入了此命令。

使用指南

可以使用 GTP 检测跟踪移动站位置更改。跟踪位置更改可能会帮助您识别欺诈漫游费用，例如，如果您看到移动站在不太可能的时间断内从一个位置移至另一个位置，例如在30分钟内从美国的一个小区移至欧洲的一个小区。

启用位置日志记录后，系统会针对每个国际移动用户识别码 (IMSI) 的新位置或更改位置生成系统日志消息：

- 324010 表示创建新的 PDP 上下文，包括移动国家代码 (MCC)、移动网络代码 (MNC)、信息元素，以及可选的用户当前注册的小区 ID。单元 ID 从单元全局标识 (CGI) 或 E-UTRAN 单元全局标识符 (ECGI) 中提取。
- 324011 指示 IMSI 已从 PDP 情景创建过程中存储的位置移开。该消息显示先前和当前的 MCC/MNC 以及可选的小区 ID。

默认情况下，系统日志消息不包含时间戳信息。如果您计划分析这些消息来识别不太可能漫游时，还必须启用时间戳。时间戳日志记录不作为 GTP 检测映射的一部分。使用 **loggingtimestamp** 命令。

CR_Examples

以下示例将时间戳添加到系统日志消息，然后启用具有单元 ID 的位置日志记录。

```
ciscoasa(config)# logging timestamp
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# location-logging cell-id
```

Related Commands

命令	说明
inspectgtp	启用 GTP 应用检查。
policy-maptypeinspectgtp	创建或编辑 GTP 检查策略图。
showservice-policyinspectgtp	显示 GTP 配置和统计信息。

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。