clf - cz

cluster disable

要在设备上禁用集群，请使用 **cluster disable** 命令。

cluster disable

Command History

版本	修改
6.5	引入了此命令。

使用指南

此命令允许您从集群中手动删除集群设备。此命令会保持集群配置不变，以便您稍后可以使用**cluster enable** 命令将其重新添加到集群。

示例

以下示例在设备上禁用集群：

```
> cluster disable
```

Related Commands

命令	Description
cluster enable	启用集群。
cluster master unit	将新的设备设置为集群的主设备。
cluster remove unit	从集群中删除设备。
show cluster info	显示集群信息。
cluster exec	将命令发送到所有集群成员。

cluster enable

要在设备上启用群集技术，请使用 **cluster enable** 命令。

cluster enable

Command History

版本	修改
6.1	引入了此命令。

使用指南

启用第一台设备后，将进行主设备选举。由于第一台设备应是截至目前为止唯一的集群成员，因此它将成为主设备。请勿在此期间执行任何配置更改。

示例

以下示例在设备上启用群集技术：

```
> cluster enable
```

Related Commands

命令	Description
cluster disable	禁用群集技术。
cluster master unit	将新的设备设置为集群的主设备。
cluster remove unit	从集群中删除设备。
show cluster info	显示集群信息。
cluster exec	将命令发送到所有集群成员。

cluster exec

要在集群中的所有设备或特定成员上执行命令，请使用 **cluster exec** 命令。

cluster exec ［**unit** *unit_name*］ *command*

Syntax Description

unit *unit_name*	（可选）对特定设备执行此命令。要查看成员名称，请输入 **cluster exec unit ?**（查看除当前设备以外的所有名称），或输入 **show cluster info** 命令。
command	指定要执行的命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

向所有成员发送 **show** 命令以收集所有输出并将其显示在当前设备的控制台上。也可在整个群集范围内执行其他命令（如 **capture** 和 **copy**）。

示例

要同时将同一捕获文件从群集中的所有设备复制到 TFTP 服务器，请在主设备上输入以下命令：

```
> cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

多个 PCAP 文件（一个文件来自一个设备）将复制到 TFTP 服务器。目标捕获文件名会自动附加设备名称，例如 capture1_device1.pcap, capture1_device2.pcap 等。在本示例中，device1 和 device2 是群集设备名称。

以下是 **cluster exec show port-channel** 汇总命令的输出示例，显示了集群内每个成员的 EtherChannel 信息：

```
> cluster exec show port-channel summary
primary(LOCAL):**********************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 secondary:**********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

Related Commands

命令	Description
cluster enable	在设备上启用群集技术。
cluster master unit	将新的设备设置为集群的主设备。
cluster remove unit	从集群中删除设备。
show cluster info	显示集群信息。
cluster exec	将命令发送到所有集群成员。

cluster exec clear rule hits

要从集群中的所有节点清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息并将其重置为零，请使用 **cluster exec clear rule hits** 命令。

cluster exec clear rule hits ［*ID*］

Syntax Description

ID	（可选）规则的 ID。包含此参数将仅清除指定规则的规则命中信息。 使用 **show access-list** 命令标识规则 ID。但是，此命令的输出中并未列出所有规则。您可以在以下 URL 上触发 REST API GET 操作，以查看所有规则及其 ID： • `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true` • `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`

Command Default

如果不指定规则 ID，则所有规则的规则命中信息都将被清除并重置为零。

注释　使用此命令时请谨慎操作，因为此操作不可逆。

Command History

版本	修改
6.4	引入了此命令。

使用指南

规则命中信息仅涵盖访问控制规则和预过滤器规则。

示例

以下是清除所有规则命中信息的示例：

```
> cluster exec clear rule hits
```

Related Commands

命令	Description
show cluster rule hits	以汇总格式显示来自集群所有节点的访问控制策略和预过滤器策略的所有评估规则命中信息。
cluster exec show rule hits	以隔离的格式显示集群中每个节点的访问控制策略和预过滤器策略的所有评估规则命中信息。

命令	Description
show rule hits	显示访问控制策略和预过滤器策略的所有评估规则的规则命中信息。
clear rule hits	清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。

cluster exec show rule hits

要从集群的每个节点以隔离格式显示访问控制策略和预过滤器策略的所有评估规则的命中信息，请使用 **cluster exec show rule hits** 命令。

cluster exec show rule hits [*id* | **raw** | **gt** *#hit-count* | **lt** *#hit-count* | **range** *#hit-count1 #hit-count2*]

Syntax Description

ID	（可选）规则的 ID。包含此参数会限制向指定规则显示的信息。 使用 **show access-list** 命令标识规则 ID。但是，此命令的输出中并未列出所有规则。您可以在以下 URL 上触发 REST API GET 操作，以查看所有规则及其 ID： • `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true` • `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`
raw	（可选）以 .csv 格式显示规则命中信息。
gt *#hit-count*	（可选）显示命中计数大于 #hit-count 的所有规则。
lt *#hit-count*	（可选）显示命中计数小于 #hit-count 的所有规则。
range *#hit-count1 #hit-count2*	（可选）显示命中计数介于 #hit-count1 和 #hit-count2 之间的所有规则。

Command Default

如果不指定规则 ID，则会显示所有规则的规则命中信息。

Command History

版本	修改
6.4	引入了此命令。

使用指南

规则命中信息仅涵盖访问控制规则和预过滤器规则。

示例

以下示例以隔离格式显示来自集群的每个节点的规则命中信息：

```
> cluster exec show rule hits
unit-1-1(LOCAL):*******************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
-------------------------------------------------------------------------------------
268435260            1                   06:55:17 Mar 8 2019     06:55:17 Mar 8 2019
268435261            1                   06:55:19 Mar 8 2019     06:55:19 Mar 8 2019
```

```
unit-1-3:**********************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
-------------------------------------------------------------------------------------
268435264            1                   06:54:43 Mar 8 2019     06:54:43 Mar 8 2019
268435265            1                   06:54:57 Mar 8 2019     06:54:57 Mar 8 2019


unit-1-2:**********************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
-------------------------------------------------------------------------------------
268435270            1                   06:54:53 Mar 8 2019     06:54:53 Mar 8 2019
268435271            1                   06:55:01 Mar 8 2019     06:55:01 Mar 8 2019
```

Related Commands

命令	Description
cluster exec clear rule hits	从集群中的所有节点清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。
show cluster rule hits	以汇总格式显示来自集群所有节点的访问控制策略和预过滤器策略的所有评估规则命中信息。
show rule hits	显示访问控制策略和预过滤器策略的所有评估规则的规则命中信息。
clear rule hits	清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。

cluster master unit

要将新设备设置为设备集群的主设备，请使用 **cluster master unit** 命令。

cluster master unit *unit_name*

Syntax Description

unit_name	指定要成为新的主设备的本地设备的名称。要查看成员名称，请输入**cluster master unit ?**（查看除当前设备以外的所有名称），或输入 **show cluster info** 命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您需要重新连接到主集群 IP 地址。

示例

以下示例将 **device2** 设置为主设备：

```
> cluster master unit device2
```

Related Commands

命令	Description
cluster enable	在设备上启用群集技术。
cluster exec	将命令发送到所有集群成员。
cluster remove unit	从集群中删除设备。
show cluster info	显示集群信息。

cluster remove unit

要从集群中删除设备，请使用 **cluster remove unit** 命令。

cluster remove unit *unit_name*

Syntax Description

unit_name	指定要从集群中删除的本地设备的名称。要查看成员名称，请输入 **cluster remove unit ?**，或输入 **show cluster info** 命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

引导程序配置保持不变，从主设备同步的最新配置也保持不变，因此您可于稍后重新添加该设备而不会丢失配置。如果在从属设备上输入此命令来删除主设备，将会选举新的主设备。

示例

以下示例检查设备的名称，然后从集群中删除 device2：

```
> cluster remove unit ?
Current active units in the cluster:
device2
> cluster remove unit device2
WARNING: Clustering will be disabled on unit device2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

Related Commands

命令	Description
cluster enable	在设备上启用群集技术。
cluster exec	将命令发送到所有集群成员。
cluster master unit	将新的设备设置为集群的主设备。
show cluster info	显示集群信息。

cluster reset-interface-mode

要在禁用集群后将集群设备转换为独立模式，请使用 **cluster reset-interface-mode** 命令。

cluster reset-interface-mode

Command History

版本	修改
7.0	引入了此命令。

使用指南

必须先使用 **cluster disable** 命令禁用集群。 **cluster reset-interface-mode** 命令会清除 threat defense 配置并重新启动逻辑设备。在 4100 系列的 FXOS 中，逻辑设备也会转换为独立类型的设备。维护引导程序配置和接口分配。

示例

以下示例禁用集群，然后删除集群配置：

```
> cluster disable
> cluster reset-interface-mode

Broadcast message from root@firepower (Tue Apr 27 18:36:12 2021):

The system is going down for reboot NOW!
```

Related Commands

命令	Description
cluster enable	在设备上启用群集技术。
cluster exec	将命令发送到所有集群成员。
cluster master unit	将新的设备设置为集群的主设备。
show cluster info	显示集群信息。

configure cert-update auto-update

要在 threat defense 设备上启用或禁用 CA 证书的自动更新，请使用 **configure cert-update auto-update** 命令。

configure cert-update auto-update { **enable** | **disable** }

Syntax Description

enable	启用 CA 证书的自动更新。
disable	禁用 CA 证书的自动更新。

Command History

版本	修改
7.0.5	引入了此命令。

使用指南

默认情况下，当您安装或升级 threat defense 到版本 7.0.5 时，CA 证书会自动更新。如果要禁用此功能，请使用 **disable** 关键字。要重新启用 CA 捆绑包的自动更新，请使用 **enable** 关键字。当您对 CA 证书启用自动更新时，系统将每天在系统定义的时间执行更新流程。

示例

以下是 **configure cert-update auto-update** 命令的输出示例：

```
> configure cert-update auto-update disable
Autoupdate is disabled
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

Related Commands

命令	Description
show cert-update	显示 CA 证书的自动更新状态。
configure cert-update run-now	立即尝试更新 CA 认证。
configure cert-update test	使用来自思科服务器的最新 CA 证书执行连接检查。

configure cert-update run-now

要立即执行 CA 证书的自动更新，请使用 **configure cert-update run-now** 命令。

configure cert-update run-now [**force**]

Syntax Description

force	即使连接检查失败，也会执行 CA 证书更新。

Command History

版本	修改
7.0.5	引入了此命令。

使用指南

如果要立即更新 CA 证书，请使用 **configure cert-update run-now**。但是，即使其中一台思科服务器的 SSL 连接检查失败，该流程也会终止。要在连接失败的情况下继续更新，请使用 **force** 关键字。例如，本地 CA 捆绑包具有访问多种思科服务（例如智能许可、AMP 注册和 ThreatGrid 服务）的证书，如果与思科智能许可服务的连接失败，则在使用 **configure cert-update run-now force** 命令时仍会执行证书更新过程。

注释 在仅 IPv6 部署中，CA 证书的自动更新可能会失败，因为某些思科服务器不支持 IPv6。在这种情况下，请使用 **configure cert-update run-now force** 命令强制更新 CA 证书。

示例

以下是连接检查失败时 **configure cert-update run-now** 命令的输出示例：

```
> configure cert-update run-now
Certs failed some connection checks.
```

以下是连接检查成功且本地 CA 捆绑包已更新时 **configure cert-update run-now** 命令的输出示例：

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

以下是 **configure cert-update run-now force** 命令的输出示例：

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

Related Commands

命令	Description
configure cert-update auto-update	启用或禁用每天自动更新 CA 证书。

命令	Description
show cert-update	显示 CA 证书的自动更新状态。
configure cert-update test	使用来自思科服务器的最新 CA 证书执行连接检查。

configure cert-update test

要验证本地系统中的 CA 证书是否是最新的（如果它们已过期），要使用新的 CA 捆绑包测试与服务器的 SSL 连接，请使用 **configure cert-update test** 命令。

configure cert-update test

Command History

版本	修改
7.0.5	引入了此命令。

使用指南

configure cert-update test 命令将本地系统上的 CA 捆绑包与最新的 CA 捆绑包（来自思科服务器）进行比较。如果 CA 捆绑包是最新的，则不会执行检查，并且会显示测试结果，如下面的“示例”部分所示。如果 CA 捆绑包已过期，则对下载的 CA 捆绑包执行连接检查，结果如下面的“示例”部分所示。

示例

以下是本地 CA 捆绑包为最新时 **configure cert-update test** 命令的输出示例：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

以下是本地CA 捆绑包过期且对下载的捆绑包进行连接检查失败时 **configure cert-update test** 命令的输出示例：

```
> configure cert-update test
Test failed, not able to fully connect.
```

以下是当本地 CA 捆绑包过期且对已下载捆绑包的连接检查成功或 CA 捆绑包已为最新版本时 **configure cert-update test** 命令的输出示例：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

Related Commands

命令	Description
configure cert-update auto-update	启用或禁用每天自动更新 CA 证书。
show cert-update	显示 CA 证书的自动更新状态。
configure cert-update run-now	立即尝试更新 CA 认证。

configure coredump packet-engine

要启用或禁用数据包引擎核心转储生成，请使用 **configure coredump packet-engine** 命令。

configure coredump packet-engine {**enable** | **disable**}

Syntax Description

disable	禁用数据包引擎核心转储生成。
enable	启用数据包引擎核心转储生成。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

默认情况下，启用数据包引擎核心转储生成。

此命令仅在Firepower 2100 系列上可用。在不受支持的平台上运行此命令时，系统会返回以下消息：

```
This command is not available on this platform.
```

示例

以下示例禁用数据包引擎核心转储生成。

```
> configure coredump packet-engine disable
```

Related Commands

命令	Description
show coredump	显示数据包引擎核心转储生成设置。

configure disable-https-access

要清除 HTTPS 访问列表，将设备配置为拒绝来自所有 IP 地址的 HTTPS 连接尝试，请使用 **configure disable-https-access** 命令。

configure disable-https-access

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可禁用对设备的 HTTPS 访问。使用本地管理器 设备管理器时，需要 HTTPS 访问。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例将设备配置为拒绝来自任何地址的 HTTPS 连接：

```
> configure disable-https-access
```

Related Commands

命令	Description
configure https-access-list	将设备配置为接受来自指定 IP 地址的 HTTPS 连接。
show https-access-list	显示当前的 HTTPS 访问列表。

configure disable-ssh-access

要清除 SSH 访问列表，将设备配置为拒绝来自所有 IP 地址的 SSH 连接尝试，请使用 **configure disable-ssh-access** 命令。

configure disable-ssh-access

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可禁用对设备的 SSH 访问。这可以防止 CLI 访问（通过控制台端口除外）。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例将设备配置为拒绝来自任何地址的 SSH 连接：

```
> configure disable-ssh-access
```

Related Commands

命令	Description
configure ssh-access-list	将设备配置为接受来自指定 IP 地址的 SSH 连接。
show ssh-access-list	显示当前的 SSH 访问列表。

configure firewall

要将防火墙模式设置为透明或路由模式，请使用 **configure firewall** 命令。

configure firewall {**routed** | **transparent**}

Syntax Description

routed	将防火墙模式设置为路由防火墙模式。
transparent	将防火墙设置为透明模式。

Command Default

默认情况下，设备处于路由模式。

Command History

版本	修改
6.1	引入了此命令。

使用指南

透明防火墙是 2 层防火墙，充当“嵌入式防火墙”或“隐藏防火墙”，并且不会被视为所连接设备的路由器跃点。

更改模式时， 设备会清除配置，因为许多命令不会在这两种模式下同时受到支持。如果您已经具有填充的配置，请务必在更改模式之前备份配置；在创建新配置时，可以使用此备份作为参考。

注释 如果使用的是 设备管理器，则无法切换到透明防火墙模式。如果您使用的是本地管理器，并且要转换为透明模式，则必须先使用 **configure manager delete** 删除管理器，然后使用 转换为透明模式，然后使用 **configure manager add** 指向 管理中心。

示例

以下示例将防火墙模式更改为透明：

```
> configure firewall transparent
```

Related Commands

命令	Description
show running-config	显示运行配置。
show firewall	显示防火墙模式。

configure flow-offload

此命令通过在硬件中处理某些流（即流量）来启用或禁用加速。将流处理分流到硬件可提高性能，默认情况下已启用。

Firepower 4100/9300 机箱上 threat defense 支持动态数据流分流。动态流分流使您能够选择要分流到硬件的流量，这意味着它不由 threat defense 设备的软件或 CPU 处理。

configure flow-offload dynamic whitelist {enable | disable}

Syntax Description

dynamic whitelist enable	启用动态分流。
dynamic whitelist disable	禁用动态分流。

Command Default

默认启用。

Command History

版本	修改
6.3	引入了此命令。

使用指南

有关动态数据流分流支持和限制的信息，请参阅 管理中心配置指南 中有关通用规则特征的章节。

示例

以下是禁用动态分流的示例：

```
> configure flow-offload dynamic whitelist disable
```

以下是启用动态分流的示例：

```
> configure flow-offload dynamic whitelist enable
```

Related Commands

命令	Description
show flow-offload	显示动态数据流分流计数器、统计信息和信息。
clear flow-offload	清除动态数据流分流数据流、计数器或统计信息。

configure high-availability

要禁用、暂停或恢复设备之间的高可用性配置（故障转移），请使用 **configure high-availability** 命令。

configure high-availability {**disable** [**clear-interfaces**] | **resume** | **suspend** [**clear-interfaces**]}

Syntax Description

clear-interfaces	（可选）在禁用或暂停高可用性时清除接口配置。
disable	中断此设备与其对等体之间的高可用性关系。 您不能在本地管理的设备上使用此选项；请改为使用 设备管理器 。如果您错误地使用了禁用命令，则必须使用 BreakHAStatus 资源调用 threat defense API 来完成操作。
resume	恢复此设备与其对等体之间的临时暂停的高可用性配置。该设备将与对等设备协商主用/备用状态。您无法恢复已禁用的配置。
suspend	临时暂停此设备与其对等体之间的高可用性配置。您可以稍后恢复配置。 如果您从主用设备暂停高可用性，配置将在主用和备用设备上暂停。如果从备用设备暂停，配置仅在备用设备上暂停，但主用设备不会尝试故障切换至暂停的设备。

Command History

版本	修改
6.1	引入了此命令。

使用指南

可以将两个设备配置成一个高可用性对。这也称为故障转移配置，如果对中的另一台设备发生故障，则一台设备可以接管。

如果由于某种原因无法更新设备管理器中的配置，可以使用 **configure high-availability** 命令来管理高可用性对。例如，如果无法访问高可用性对，可以使用 **configure high-availability disable** 删除两个高可用性对等体的故障转移配置。

您还可以暂时挂起故障转移配置，稍后再将其恢复。在以下情况下，暂停设备上的 HA 非常有用：

- 两台设备都在主用 - 主用情况下，且修复故障转移链路上的通信不能更正问题。
- 希望对主用或备用设备进行故障排除，并且不希望设备在此期间发生故障切换。
- 您想要在备用设备上安装软件升级期间阻止故障转移。

暂停高可用性时，停止将设备对用作故障转移设备。当前主用设备保持活动状态，并处理所有用户连接。但是，不会再监控故障转移条件，并且系统永远不会故障切换到现在的伪备用设备。备用设备将保留其配置，但将保持非活动状态。

暂停 HA 和中断 HA 之间的主要区别是，在暂停的 HA 设备上将保留高可用性配置。如果中断 HA，则会清除配置。因此，您可以选择在暂停系统上恢复高可用性，这样可启用现有配置并再次将两台设备设置为故障转移对。

注释 暂停高可用性是一种临时状态。如果您重新加载一台设备，它会自动恢复高可用性配置，并与对等体协商主用/备用状态。

示例

以下示例显示如何临时暂停然后恢复高可用性配置。

```
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
        This host: Primary - Active
                Active time: 776671 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and
'NO' if you wish to abort: Yes
Successfully suspended high-availability.
> show failover
Failover Off
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
```

```
failover replication http
> configure high-availability resume
Successfully resumed high-availablity.
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Unit Enrollment Hold action is active, timeout in 1792 seconds
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate Unknown
Last Failover at: 20:26:06 UTC Nov 4 2016
        This host: Primary - Active
                Active time: 778071 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - App Sync
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Unknown (Waiting)
                  Interface inside (0.0.0.0): Unknown (Waiting)
                  Interface diagnostic (0.0.0.0): Unknown (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
```

Related Commands

命令	Description
show failover	显示故障转移（高可用性）配置。
show high-availability config	显示故障转移（高可用性）配置。提供 **show failover**相同的输出。

configure https-access-list

要将设备配置为接受来自指定 IP 地址的 HTTPS 连接，请使用 **configure https-access-list** 命令。

configure https-access-list *address_list*

Syntax Description

address_list	主机或网络的 IP 地址的逗号分隔列表，采用 IPv4 无类域间路由 (CIDR) 符号或 IPv6 前缀长度符号。例如，10.100.10.0/24 or 2001:DB8::/96。 要指定所有 IPv4 主机，请输入 0.0.0.0/0。要指定所有 IPv6 主机，请指定 ::/0。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您必须在一个命令中包含所有受支持的主机或网络。此命令中指定的地址将覆盖 HTTPS 访问列表的当前内容。

仅允许 HTTPS 访问不允许用户登录本地管理器。对配置软件的访问由用户名和密码控制。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例将设备配置为接受来自任何 IPv4 或 IPv6 地址的 HTTPS 连接：

```
> configure https-access-list 0.0.0.0/0,::/0
The https access list was changed successfully.
> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:https
```

Related Commands

命令	Description
configure disable-https-access	清除 HTTPS 访问列表。
show https-access-list	显示 HTTPS 访问列表。

configure identity-subnet-filter

要从接收 ISE 的用户到 IP 和安全组标记 (SGT) 到 IP 的映射中排除子网，请使用 **configure identity-subnet-filter** 命令。您通常应对内存较低的受管设备执行此操作，以防止 Snort 身份运行状况监控器内存错误。

configure identity-subnet-filter { **add** | **remove** } *subnet*

Syntax Description

add	将指定的子网添加到排除的子网列表。
remove	从排除的子网列表中删除指定的子网。
子网	指定要添加或排除的子网。

Command History

版本	修改
6.7	引入了此命令。

示例

以下示例为管理接口配置静态 IPv6 地址。

```
> configure identity-subnet-filter 192.0.2.0/24
```

Related Commands

命令	Description
show identity-subnet-filter	显示当前从用户到 IP 和 SGT 到 IP 映射中排除的子网。

configure inspection

要启用或禁用默认应用协议检测引擎，请使用 **configure inspection** 命令。

configure inspection 协议 {**enable** | **disable**}

Syntax Description

disable	禁用检测引擎。
enable	启用检测引擎。
protocol	要启用或禁用的检测协议。有关选项列表，请参阅使用指南部分。

Command History

版本	修改
6.2	引入了此命令。

使用指南

注释 虽然您可以在使用 设备管理器时禁用检测，但每次从 设备管理器部署配置时，都会重新启用默认检测。如果要保持禁用检测，则必须在每次部署后重新输入 命令。从版本 6.2.3 开始，您可以使用 FlexConfig 启用和禁用这些检查，以使更改保持不变。

仅在思科技术支持人员的指示下，或者在确定网络上不会出现关联类型的流量时，才禁用默认检测引擎。例如，如果阻止受检查端口上的所有流量，则可以安全地禁用该端口上的检查。这些检测适用于所有数据接口。

这些检测引擎独立于 Snort 检测。这些引擎提供以下服务：

- 创建小孔 - 一些应用协议在标准端口或协商的端口上打开辅助 TCP 或 UDP 连接。检测会为这些辅助端口打开小孔，使您无需创建访问控制规则予以允许。
- NAT 重写 - 诸如 FTP 等协议会在数据包数据中嵌入用于辅助连接的 IP 地址和端口，作为协议的一部分。如果 NAT 转换涉及到任一终端，则检测引擎会重写数据包数据以反映嵌入式地址和端口的 NAT 转换。在没有 NAT 重写的情况下，辅助连接不起作用。有关 NAT 限制，请参阅您用于配置设备的管理器（管理中心 或 设备管理器）的配置指南中的 NAT 一章。
- 协议实施 - 一些检测会为检测到的协议实施某种程度的 RFC 一致性。

您可以禁用并随后启用以下检测引擎。要查看当前已启用的功能，请使用 **show running-config policy-map** 命令并查找 **inspect** 命令。要查看每个检测的默认参数的详细信息，请使用 **show running-config all policy-map** 命令。

- **dcerpc**-（TCP 端口 135。）分布式计算环境/远程过程调用系统。DCERPC 检测引擎在已知 TCP 端口 135 上检测终端映射程序 (EPM) 与客户端之间的本地 TCP 通信。Microsoft 远程过程调用

(MSRPC) 基于 DCERPC，是 Microsoft 分布式客户端和服务器应用广泛使用的协议，允许软件客户端在服务器上远程执行程序。检测提供针孔创建和 NAT 服务。

- **dns**-（UDP 端口 53。）域名系统。在 UDP 端口 53 上检查 DNS。检测提供 NAT 服务和协议实施。您必须启用此检测引擎，才能在 NAT 规则上使用 NAT 重写选项。在 IPv4 和 IPv6 网络 (NAT64/46) 之间执行 NAT 时，通常需要重写 NAT。
- **esmtp**-（TCP 端口 25。）扩展的简单邮件传输协议。ESMTP 检测可检测垃圾邮件、网络钓鱼、变形邮件等攻击和缓冲流量上溢/下溢攻击。另外，它还支持应用安全和协议符合性（实施 ESMTP 消息合理性检查及冻结发件人/收件人）并可冻结邮件中继。有关检查期间应用的控制的详细信息，请使用 **show running-config all policy-map** 命令并查找“policy-map type inspect esmtp _default_esmtp_map”行和后续参数。

  ESMTP 应用检测可控制和减少用户可使用的命令数以及服务器返回的消息数。它提供 NAT 服务和协议一致性。ESMTP 检测主要执行三种任务：

  - 将 SMTP 请求限制为七个基本 SMTP 命令和八个扩展命令。支持的命令如下：

    扩展 SMTP - AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS 和 VRFY。

    SMTP (RFC 821) - DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET。
  - 监控 SMTP 命令-响应序列。
  - 生成审计追踪。邮件地址中嵌入的无效字符被替换时，会生成系统日志审计记录 108002。有关详细信息，请参阅 RFC 821。
- **ftp**-（TCP 端口 21。）文件传输协议。检测提供针孔和 NAT 服务。
- **h323_h225**-（TCP 端口 1720，UDP 端口 1718。）H.323 检测支持 RAS、H.225 和 H.245，这项检测功能会转换所有嵌入式 IP 地址和端口。它执行状态跟踪和过滤。H.323 检测支持符合 H.323 规范的应用，例如思科 CallManager。H.323 是国际电信联盟制定的一套协议，用于通过 LAN 进行多媒体会议。设备最高支持 H.323 v6，其中包括 H.323 v3“支持在一个呼叫信令信道上进行多个呼叫”的功能。

  H.323 检测具有如下两个主要功能：

  - 对 H.225 和 H.245 消息中必要的嵌入式 IPv4 地址进行 NAT 转换。由于 H.323 消息以 PER 编码格式编码，所以 ASA 使用 ASN.1 解码器来解码 H.323 消息。
  - 动态分配协商的 H.245 和 RTP/RTCP 连接。使用 RAS 时，也可以动态分配 H.225 连接。
- **h323_ras**-（UDP 端口 1718-1719。）请参阅 **h323_h225**的说明。此检查适用于 RAS 信令。
- **icmp**-（仅限 ICMP 流量。）ICMP 检测引擎允许 ICMP 流量具有“会话”，这样可以像对 TCP 和 UDP 流量那样对这种流量进行检测。如果没有 ICMP 检测引擎，我们建议您不要允许 ICMP 通过设备（使用访问控制规则屏蔽）。如果不进行状态检测，ICMP 可能被用于攻击网络。ICMP 检测引擎确保每个请求只有一个响应，并确保序列号是正确的。检测还提供 NAT 服务。

- **icmp_error**-（仅限 ICMP 流量。）如果启用了 ICMP 错误检测，设备会根据 NAT 配置为发送 ICMP 错误消息的中间跃点创建转换会话。设备用转换后的 IP 地址覆盖数据包。这对于在通过设备的跟踪路由中提供有意义的信息是必要的。
- **ip-options**-（仅限 RSVP 流量。）IP 选项检查根据数据包信头中 IP 选项字段的内容控制允许哪些 IP 数据包。允许具有 Router Alert 选项的数据包。丢弃包含任何其他选项的数据包。
- **netbios**—(UDP 源端口137, 138.) NetBIOS Name Server over IP。NetBIOS 应用检测对 NetBIOS 名称服务 (NBNS) 数据包和 NetBIOS 数据报服务数据包中嵌入的 IP 地址执行 NAT。这项检测还会检查各个数量字段和长度字段的一致性，从而强制执行协议符合性。
- **rsh**-（TCP 端口 514。）RSH 协议在 TCP 端口 514 上使用从 RSH 客户端到 TCP RSH 服务器的连接。客户端和服务器协商出 TCP 端口号，客户端会在该端口上侦听 STDERR 输出流。如有必要，RSH 检测打开针孔并支持协商端口号的 NAT。
- **rtsp**-（TCP 端口 554。）实时流传输协议。RTSP 检测引擎使设备可以传递 RTSP 数据包。RealAudio、RealNetworks、Apple QuickTime、RealPlayer 和思科 IP/TV 连接都使用 RTSP。RTSP 应用使用已知 TCP（很少用 UDP）端口 554 作为控制信道。设备仅支持 TCP（这符合 RFC 2326 的要求）。该 TCP 控制信道用于根据客户端配置的传输模式协商用于传输音频/视频流量的数据信道。支持如下 RDT 传输：rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp 和 x-pn-tng/udp。
- **sqlnet**-（TCP 端口 1521。）检测引擎支持 SQL*Net 版本 1 和 2，但仅支持透明网络底层 (TNS) 格式。检测不支持表格数据流 (TDS) 格式。系统会扫描嵌入式地址和端口的 SQL*Net 消息，并在需要时应用 NAT 重写。

  当与 SQL 控制 TCP 端口 1521 相同的端口上发生 SQL 数据传输时，请禁用 SQL*Net 检测。安全设备在启用 SQL*Net 检测之后充当代理，且将客户端窗口大小从 65000 缩小至大约 16000，从而导致数据传输问题。
- **sip**-（TCP/UDP 端口 5060。）会话发起协议。SIP 是一种广泛用于网络会议、电话、展示、事件通知和即时消息的协议。部分原因是 SIP 本质上是文本协议，部分原因是其具有灵活性，因此，SIP 网络面临大量安全威胁。SIP 应用检测会在消息信头和正文中提供地址转换，会动态打开端口，还会执行基本健全性检查。
- **skinny**-（TCP 端口 2000。）瘦客户端控制协议 (SCCP)。SCCP（瘦客户端）应用检测对数据包数据中的嵌入式 IP 地址和端口号执行转换，并会动态打开针孔。它还执行其他协议符合性检查和基本状态跟踪。
- **sunrpc**-（TCP/UDP 端口 111。）Sun RPC 可供 NFS 和 NIS 使用。Sun RPC 服务可在任何端口上运行。当客户端尝试访问服务器上的 Sun RPC 服务时，必须获悉服务运行所在的端口。它通过查询端口映射程序流程执行此操作，通常为 rpcbind，位于公认端口 111。

  客户端将发送服务的 Sun RPC 程序号，而端口映射程序流程将用服务的端口号进行响应。客户端发送其 Sun RPC 查询至服务器，指定端口映射程序流程识别的端口。服务器回复后，设备会截取此数据包，并打开该端口上的初始化 TCP 和 UDP 连接。不支持 Sun RPC 负载信息的 NAT 或 PAT。
- **tftp**-（UDP 端口 69。）简单文件传输协议。检测引擎检测 TFTP 读取请求 (RRQ)、写入请求 (WRQ) 和错误通知 (ERROR)，并且如有必要，还会动态创建连接和转换，从而允许在 TFTP 客户端和服务器之间传输文件。

如有必要，在接收有效的读取 (RRQ) 或写入 (WRQ) 请求时会分配动态辅助信道和 PAT 转换。随后，TFTP 会使用该辅助信道进行文件传输或错误通知。只有 TFTP 服务器可以通过辅助信道发起流量；此外，TFTP 客户端与服务器之间最多只能有一个不完整的辅助信道。服务器发出的错误通知会致使辅助信道关闭。如果使用静态 PAT 重定向 TFTP 流量，则必须启用 TFTP 检测。

- **xdmcp**-（UDP 端口 177。）X 显示管理器控制协议。XDMCP 是使用 UDP 端口 177 来协商 X 会话（建立后使用 TCP）的协议。为了成功协商和启动 XWindows 会话，设备必须允许来自 Xhosted 计算机的 TCP 向后连接。要允许该向后连接，可以使用访问控制来允许 TCP 端口。

  在 XWindows 会话期间，管理器将与已知端口 6000 | n 上的显示器 Xserver 通信。使用以下终端设置，每个显示器都会独立连接到 Xserver：当 *n* 是展示序号时， **setenv DISPLAY Xserver:***n*。

  使用 XDMCP 时，系统将使用 IP 地址协商显示，以便设备可在需要时应用 NAT。XDCMP 检测不支持 PAT。

示例

以下示例显示当前检测配置并禁用 XDMCP 检测。您可以启用或禁用检测引擎，但不能更改其默认行为。例如，此输出显示 DNS/TCP 检测已禁用。不能使用 **configure inspection** 命令将 DNS 检测配置为应用于 TCP 流量。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
!
> configure inspection xdmcp disable
Building configuration...
Cryptochecksum: 46dbea1d 51c2089a fcc3e42f 3dafd2d5
12386 bytes copied in 0.160 secs
[OK]
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
```

```
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
  inspect ftp
!
```

Related Commands

命令	Description
show running-config policy-map	显示服务策略的策略映射，包括检测配置。
show service-policy	显示服务策略统计信息，包括用于检测的统计信息。

configure log-events-to-ramdisk

要启用或禁用将连接事件日志记录到 RAM 磁盘以提高系统性能并减少与将连接事件写入固态驱动器 (SSD) 相关的磁盘磨损，请使用 **configure log-events-to-ramdisk** 命令。

configure log-events-to-ramdisk {**enable** | **disable**}

Syntax Description

enable	启用 RAM 磁盘的连接事件日志记录。
disable	禁用连接事件日志记录到 RAM 磁盘。然后将连接事件记录到 SSD。

Command Default

在支持此功能的平台上会默认启用此功能。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可在使用 RAM 磁盘或物理 SSD 到日志连接事件之间切换。如果启用，连接事件将记录到 RAM 磁盘中。如果禁用，连接事件将记录到 SSD。在断电的情况下，记录到 RAM 磁盘的连接事件将丢失。

此命令并非在所有设备类型上都可用。在不受支持的平台上运行此命令时，系统会返回以下消息：

```
This command is not available on this platform.
```

示例

以下示例禁用 RAM 磁盘日志记录。

```
> configure log-events-to-ramdisk disable
```

Related Commands

命令	Description
show log-events-to-disk	显示日志记录的当前状态。
show disk-manager	显示系统每个部分（包括孤岛、低水位线和高水位线）的磁盘使用情况详细信息。

configure manager add

要将设备配置为接受来自或启动到 管理中心 和/或 CDO 的连接，请使用 **configure manager add** 命令。

⚠

注意 添加远程管理器会将配置重置为出厂默认设置。

configure manager add { *hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*] [*display_name*]

Syntax Description

hostname	指定 管理中心的主机名。
IPv4_address	指定 管理中心的 IPv4 地址。
IPv6_address	指定 管理中心的 IPv6 地址。
display_name	使用 **show managers** 命令提供用于显示此管理器的显示名称。如果您将 CDO 标识为仅用于分析的主用管理器和本地部署 管理中心，则此选项非常有用。如果不指定此参数，防火墙将使用以下方法之一自动生成显示名称： • *hostname* | *IP_address*（如果不使用 **DONTRESOLVE** 关键字） • **manager-***timestamp*
DONTRESOLVE	如果 管理中心无法直接寻址，请使用 **DONTRESOLVE**。如果使用 **DONTRESOLVE**，则需要使用 *nat_id*。当您将此设备添加到 管理中心时，请确保同时指定设备 IP 地址和 *nat_id*；连接的一端需要指定 IP 地址，两端需要指定相同的唯一 NAT ID。
regkey	指定向 管理中心 注册设备所需的唯一字母数字注册密钥。允许使用字母数字和连字符 (-)。
nat_id	当一方未指定 IP 地址时，指定在 管理中心 与设备之间的注册流程中使用的可选字母数字字符串。在 管理中心上指定相同的 NAT ID。如果使用数据接口进行管理，则必须在 threat defense 和 管理中心 上指定注册用的 NAT ID。

Command History

版本	修改
6.1	引入了此命令。
7.2	增加了对多个管理器的支持：主要的云交付 管理中心 (CDO) 和仅用于分析的本地管理器 管理中心 。

使用指南

向 管理中心注册设备始终需要一个唯一的字母数字注册密钥。

通常，需要两个 IP 地址（连同一个注册密钥）： 管理中心 指定设备 IP 地址，设备指定 管理中心 IP 地址。但是，如果您只知道其中一个 IP 地址，您还必须在连接的两端指定唯一的 NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。如果您不知道 管理中心 IP 地址，请使用 **DONTRESOLVE** 关键字而不是 IP 地址或主机名。

注释 如果使用数据接口进行管理，则必须在 threat defense 和d 管理中心 上指定注册用的 NAT ID。

如果注册了 管理中心 和一个使用 IPv4 的设备并要将其转换为 IPv6，则必须在 管理中心删除并重新注册该设备

要从 管理中心 更改为本地 设备管理器，请使用 **configure manager delete** 命令，然后使用 **configure manager local** 命令。

注释 在将设备从一个 管理中心 移动到另一个或更改为本地管理器之前，请将其从当前 管理中心管理器中删除。

示例

```
> configure manager add DONTRESOLVE abc123 efg456
```

Related Commands

命令	Description
configure manager delete	删除管理 管理中心。
configure manager edit	编辑管理 管理中心。
configure manager local	配置本地管理器。
show managers	显示当前的管理器。

configure manager delete

要禁用当前管理器并进入无管理器模式，请使用 **configure manager delete** 命令。

⚠

注意 删除管理器会将 threat defense 配置重置为出厂默认设置。但是，管理引导程序配置会保留。

configure manager delete *identifier*

Syntax Description

identifier	如果定义了多个管理器，则需要指定标识符（也称为 UUID；请参阅 **show managers** 命令）。单独删除每个管理器条目。

Command History

版本	修改
6.1	引入了此命令。
6.3	已添加检查高可用性模式。
7.2	为配置多个管理器时添加了 标识符 变量。

使用指南

使用此命令可删除当前设备管理器(s)。设备处于无管理器模式，然后您可以添加远程管理器(管理中心)或使用本地管理器(设备管理器)。在本地和远程管理之间切换时，或者当远程管理器不再处于活动状态时，可以使用此命令。

如果设备已配置为高可用性，您必须首先使用设备管理器（如果可能）或 **configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

命令行为因当前管理器而异。

- 远程 - 无法访问 管理中心 。如果 管理中心 仍与 threat defense 通信，请先从 管理中心的库存中删除设备。然后，您可以使用此命令。
- 本地 - 无限制。您会立即进入无管理器模式。

示例

以下示例删除当前管理器并进入无管理器模式。

```
> configure manager delete

If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no]:yes

DHCP Server Disabled
>
```

Related Commands

命令	Description
configure manager add	为设备配置管理 管理中心 。
configure manager local	配置本地管理器。
show managers	显示当前的管理器。

configure manager edit

要编辑 threat defense 配置中的 管理中心 IP 地址，请使用 **configure manager edit** 命令。

configure manager edit *identifier* { **hostname** { *ip_address* | *hostname* } | **displayname** *display_name* }

Syntax Description

identifier	指定 管理中心的标识符 (UUID)。使用 **show managers** 命令查看标识符（7.2 或更高版本）或从 管理中心 CLI **show version** 命令获取 UUID。
hostname {*ip_address* | *hostname*}	更改主机名/IP 地址。
displayname *display_name*	更改显示名称。

Command History

版本	修改
6.7	引入了此命令。
7.2	添加了 **hostname** 和 **displayname** 关键字。

使用指南

如果更改 管理中心 IP 地址或主机名，还应在设备 CLI 中更改值，以便配置匹配。虽然在大多数情况下，无需更改设备上的管理中心IP地址或主机名即可重新建立管理连接，但在至少一种情况下，必须执行此任务才能重新建立连接：将设备添加到管理中心 并指定仅NAT ID。即使在其他情况下，我们也建议保持 管理中心 IP 地址或主机名为最新状态，以实现额外的网络恢复能力。

如果 管理中心 最初由 **DONTRESOLVE** 和 NAT ID 标识，则可以使用此命令将该值更改为主机名或 IP 地址。不能将 IP 地址或主机名更改为 **DONTRESOLVE**。

管理连接将关闭，然后重新建立。您可以使用 **sftunnel-status** 命令监控连接状态。

示例

管理中心UUID明确标识管理中心；例如，在 管理中心 高可用性的情况下，您需要在threat defense 设备上指定主用 管理中心 。

输入 **show managers** 命令以查看标识符：

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

获取 UUID 后，即可编辑 threat defense 设备上的 IP 地址。例如：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 10.10.5.1
```

Related Commands

命令	Description
configure manager delete	删除管理 管理中心。
configure manager add	配置 管理中心。
show managers	显示当前的管理器。

configure manager local

要将设备配置为使用本地管理器 设备管理器，请使用 **configure manager local** 命令。

configure manager local

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可启用本地管理器 设备管理器。当您不想使用单独的管理器时，请使用本地管理器管理中心。通过启用本地管理器，您可以使用位于 **http://***management_ip_address* 的浏览器打开 设备管理器 。

注释 完成此命令最多可能需要 4-6 分钟，因为系统必须重新初始化其数据库。Please be patient.

本地管理器适用于从 6.5 开始的大多数平台。如果它不适用于您的平台，请使用 **configure manager add** 命令配置远程管理器。

其他限制

- 设备必须处于无管理器模式，才能切换到本地管理器。使用 **configure manager delete** 命令进入无管理器模式。使用 **show managers** 命令可确定您当前的管理器。
- 设备不能在透明防火墙模式下运行（请参阅 **configure firewall** 命令）。本地管理器仅支持路由模式。

示例

以下示例显示如何配置本地管理器。

```
> configure manager local
```

Related Commands

命令	Description
configure manager add	为设备配置管理 管理中心 。
configure manager delete	删除管理 管理中心。
show managers	显示当前的管理器。

configure mini-coredump

要启用或禁用迷你核心转储生成，请使用 **configure mini-coredump** 命令。

configure mini-coredump { **enable** | **disable** }

Syntax Description

enable	启用迷你核心转储生成。
disable	禁用迷你核心转储生成。

Command History

版本	修改
7.0	引入了此命令。

使用指南

默认情况下，迷你核心转储生成处于启用状态。

由于其多线程性质，Snort 3 流程会转储巨大的核心文件。这些转储需要一段时间才能写入硬盘。在写入核心并启动新流程之前，Snort的流量检查会中断。创建迷你核心转储可避免时间延迟。迷你核心转储具有有助于调试的堆栈和内存值的基本详细信息。

示例

以下示例禁用迷你核心转储生成。

```
> configure mini-coredump disable
```

Related Commands

命令	Description
show mini-coredump status	显示迷你核心转储生成设置。

configure network dns searchdomains

要配置 DNS 搜索域列表，请使用 **configure network dns searchdomains** 命令。

configure network dns searchdomains ［*dnslist*］

Syntax Description

dnslist	指定 DNS 搜索域列表（用逗号隔开）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可将当前的DNS搜索域列表替换为新列表。如果没有在命令中指定完全限定域名，例如 **ping system**，则这些域将添加到主机名中。这些域仅用于管理接口，或通过管理接口的命令。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例配置新的搜索域列表，然后 ping 不完全限定的主机名。

```
> configure network dns searchdomains example.com
> show dns system
search example.com
nameserver 10.163.47.11
> ping system www
PING www.example.com (10.163.4.161) 56(84) bytes of data.
64 bytes from www.example.com (10.163.4.161): icmp_seq=1 ttl=242 time=8.01 ms
64 bytes from www.example.com (10.163.4.161): icmp_seq=2 ttl=242 time=16.7 ms
^C
--- origin-www.cisco.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 7.961/10.216/16.718/3.755 ms
```

Related Commands

命令	Description
configure network dns servers	配置 DNS 服务器。
show dns system	显示管理接口的当前 DNS 配置。

configure network dns servers

要为管理接口配置 DNS 服务器，请使用 **configure network dns servers** 命令。

configure nework dns servers ［*dnslist*］

Syntax Description

dnslist	指定 DNS 服务器列表（用逗号隔开）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可将当前的DNS服务器列表替换为新列表。这些服务器仅通过管理接口使用。它们无法解析通过数据接口的命令的完全限定域名。

从版本 6.3 开始，仅对于本地管理的设备，如果数据和管理接口使用相同的 DNS 组，则在下次部署时从管理器更新该组，这意味着更改也应用于数据接口上使用的DNS组。管理接口的更改会立即生效。我们建议您从本地管理器进行所有 DNS 更改，而不是使用此命令。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例为管理接口配置 DNS 服务器。

```
> configure network dns servers 10.163.47.11,10.124.1.10
> show dns system
search example.com
nameserver 10.163.47.11
nameserver 10.124.1.10
```

Related Commands

命令	Description
configure network dns searchdomains	配置 DNS 搜索域。
show dns system	显示管理接口的当前 DNS 配置。

configure network hostname

要为设备的管理接口配置主机名，请使用 **configure network hostname** 命令。

configure network hostname *name*

Syntax Description

name	指定主机名。

Command History

版本	修改
6.1	引入了此命令。

使用指南

系统主机名在多个位置定义。如果从管理器更新主机名，则系统会在所有进程之间同步主机名。如果在使用 设备管理器 （本地管理器）时使用此命令，则需要从 设备管理器 部署更改以完成更新，以便所有系统进程使用相同的名称。

示例

以下示例将主机名设置为 sfrocks。

```
> configure network hostname sfrocks
```

Related Commands

命令	Description
show network	显示管理接口配置。

configure network http-proxy

要为管理接口配置 HTTP 代理，请使用 **configure network http-proxy** 命令。

configure network http-proxy

Command History

版本	修改
6.1	引入了此命令。
6.6	此命令现在适用于本地管理的系统。

使用指南

使用此命令为设备设置 HTTP 代理地址。发出命令后，系统将提示您 HTTP 代理地址和端口，是否需要进行代理身份验证，如果需要，还会提示代理用户名、代理密码和代理密码确认。

示例

以下示例为管理接口配置 HTTP 代理。在本示例中，配置了身份验证。CLI 不显示您键入的密码。

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

Related Commands

命令	Description
configure network http-proxy-disable	禁用 HTTP 代理设置。
show network	显示管理接口配置。

configure network http-proxy-disable

要删除管理接口的 HTTP 代理，请使用 **configure network http-proxy-disable** 命令。

configure network http-proxy-disable

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例删除管理接口的 HTTP 代理。

```
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                       : Enabled
HTTP Proxy                  : 10.100.10.10
Port                        : 80
Authentication              : Enabled
Username                    : proxyuser
> configure network http-proxy-disable
Are you sure that you wish to delete the current http-proxy configuration? (y/n): y
Configuration successfully deleted.
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                       : Disabled
Authentication              : Disabled
```

Related Commands

命令	Description
configure network http-proxy	配置 HTTP 代理设置。
show network	显示管理接口配置。

configure network ipv4 delete

要禁用设备管理接口的 IPv4 配置，请使用 **configure network ipv4 delete** 命令。

configure network ipv4 delete ［*management_interface*］

Syntax Description

management_ interface	指定管理接口。如果不指定接口，则此命令将配置默认管理接口。仅当使用 **configure management-interface** 命令启用多个管理接口时，才需要此参数。仅在 Firepower 4100 和 9300 系列设备上支持多个管理接口。请勿为其他平台指定此参数。在 Firepower 4100 和 9300 上的管理接口 ID 为 **management0**（对于默认管理接口）和 **management1**（对于可选事件接口）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令以禁用设备管理接口的 IPv4 配置。如果您连接到已删除的 IP 地址，您将失去与该设备的连接。在删除 IPv4 地址之前，请确保已配置 IPv6 地址。

您无需删除配置即可更改 IPv4 地址。如果要保留 IPv4 地址，但只想更改地址，请使用 **configure network ipv4 manual** 或 **configure network ipv4 dhcp** 命令。

示例

以下示例删除 IPv4 地址配置。

```
> configure network ipv4 delete
```

Related Commands

命令	Description
configure network ipv4 dhcp	将 IPv4 配置为从 DHCP 服务器获取地址。
configure network ipv4 manual	使用静态 IP 地址手动配置 IPv4。
show network	显示管理接口配置。

configure network ipv4 dhcp

要将管理接口配置为从 DHCP 服务器获取 IPv4 地址，请使用 **configure network ipv4 dhcp** 命令。

configure network ipv4 dhcp ［*management_interface*］

Syntax Description

management_ interface	指定管理接口。仅在默认管理接口上支持 DHCP，因此您不需要使用此参数。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可指定设备的管理接口从 DHCP 服务器接收其 IPv4 配置。管理接口与 DHCP 服务器通信以获取其配置信息。

注释 如果使用 **configure network management-data-interface** 命令配置数据接口进行 管理中心 访问，则无法将 DHCP 用于管理接口；您必须设置手动 IP 地址，因为默认路由（必须是**数据接口**）可能会被从 DHCP 服务器接收的路由覆盖。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。当流量转发到数据接口时，此 IP 地址将进行 NAT 转换。

示例

以下示例将管理接口配置为使用 DHCP 获取其 IPv4 地址。

```
> configure network ipv4 dhcp
```

Related Commands

命令	Description
configure network ipv4 delete	禁用 IPv4 网络。
configure network ipv4 manual	手动配置 IPv4。
show network	显示管理接口配置。

configure network ipv4 dhcp-dp-route

要恢复管理接口默认 IP 地址、网络掩码和网关，请使用 **configure network ipv4 dhcp-dp-route** 命令。此命令不会更改其他网络设置，例如 DNS 服务器。

注释 Cisco Secure Firewall Threat Defense Virtual (threat defense virtual)、 Firepower 4100/9300或 ISA 3000 不支持此命令。

configure network ipv4 dhcp-dp-route

Command History

版本	修改
6.6	引入了此命令。

使用指南

您必须同时输入此命令的 IPv4 和 IPv6 版本，才能将配置恢复为出厂默认设置，即使您没有识别其中一个版本的 IP 地址。

示例

以下示例恢复管理接口的默认配置。

```
> configure network ipv4 dhcp-dp-route
Creating /etc/sf/sftunnel.conf with header line
Set up management0 as DHCP ipv4 client with the default route through data interfaces.
>
```

Related Commands

命令	Description
configure network ipv4 delete	禁用 IPv4 网络。
configure network ipv4 dhcp	通过 DHCP 配置 IPv4。
configure network ipv4 manual	手动配置 IPv4。
show network	显示管理接口配置。

configure network ipv4 dhcp-server-disable

要在管理接口上禁用 DHCP 服务器，请使用 **configure network ipv4 dhcp-server-disable** 命令。

configure network ipv4 dhcp-server-disable

Command History

版本	修改
6.2	引入了此命令。

使用指南

如果管理接口上有活动的 DHCP 服务器，则可以将其禁用。禁用时，管理网络上的客户端必须配置静态地址，或者您需要在网络上配置其他设备来提供 DHCP 服务器服务。

如果将管理 IP 地址更改为使用 DHCP 获取地址，则会自动禁用 DHCP 服务器（如果已启用）。

示例

以下示例显示如何检查 DHCP 服务器是否已启用，以及如何禁用它。

```
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
> configure network ipv4 dhcp-server-disable
DCHP Server Disabled
> show network-dhcp-server
DHCP Server Disabled
```

Related Commands

命令	Description
configure network ipv4 dhcp-server-enable	启用管理接口上的 DHCP 服务器。
show dhcp-server	显示管理接口上的 DHCP 服务器的状态。

configure network ipv4 dhcp-server-enable

要在管理接口上启用可选的 DHCP 服务器，请使用 **configure network ipv4 dhcp-server-enable** 命令。

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

Syntax Description

start_ip_address *end_ip_address*	指定 DHCP 地址池的起始和结束 IPv4 地址。当管理接口收到 DHCP 客户端请求时，它会提供此池中的地址。该池必须与管理 IPv4 地址位于同一子网上。 请勿在 DHCP 地址池中包含网络地址、管理地址或广播地址。

Command History

版本	修改
6.2	引入了此命令。

使用指南

如果为管理接口配置手动（静态）IPv4 地址，则可以配置 DHCP 服务器为管理网络上的终端提供地址。

在启用服务器之前，请确保管理网络上没有其他 DHCP 服务器。每个网络最多只能有一个 DHCP 服务器，否则结果可能无法预测。

注释 threat defense virtual 设备上不支持此命令。

示例

以下示例显示如何配置 DHCP 服务器并显示其状态。

```
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
```

Related Commands

命令	Description
configure network ipv4 dhcp-server-disable	禁用管理接口上的 DHCP 服务器。
show dhcp-server	显示管理接口上的 DHCP 服务器的状态。

configure network ipv4 manual

要在管理接口上配置静态 IPv4 地址，请使用 **configure network ipv4 manual** 命令。

configure network ipv4 manual *ipaddr netmask gw* ［*management_interface*］

Syntax Description

ipaddr	指定 IP 地址。
netmask	指定子网掩码。
gw	指定默认网关的 IPv4 地址。 您可以选择指定 **data-interfaces**，它将设备上的数据接口用作网关，而不是管理网络上的显式网关。如果不想将管理物理接口连接到单独的管理网络，请使用数据接口。 有关 管理中心 数据接口管理，请参阅 **configure network management-data-interface** 命令。 请注意，此命令中的*gw*用于为设备创建默认路由。如果配置仅事件接口，则必须输入 *gw* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您将 *gw* 设置为与管理接口配合使用，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。
management_ interface	指定管理接口。如果不指定接口，则此命令将配置默认管理接口。仅当使用 **configure management-interface** 命令启用多个管理接口时，才需要此参数。仅在 Firepower 4100 和 9300 系列设备上支持多个管理接口。请勿为其他平台指定此参数。在 Firepower 4100 和 9300 上的管理接口 ID 为 **management0**（对于默认管理接口）和 **management1**（对于可选事件接口）。

Command History

版本	修改
6.1	引入了此命令。
6.2	为网关添加了 **data-interfaces** 关键字。
6.7	**data-interfaces** 关键字现在可用于数据接口上的 管理中心 管理。

使用指南

如果使用 **configure network management-data-interface** 命令为访问 管理中心 配置数据接口，则必须手动设置 IP 地址（IPv4 或 IPv6）。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。当流量转发到数据接口时，此 IP 地址将进行 NAT 转换。您无法使用 DHCP（默认），因为默认路由（必须是 **数据接口**）可能会被从 DHCP 服务器收到的路由覆盖。

示例

以下示例在管理接口上配置静态 IPv4 地址。

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

Related Commands

命令	Description
configure network ipv4 delete	禁用 IPv4 网络。
configure network ipv4 dhcp	通过 DHCP 配置 IPv4。
show network	显示管理接口配置。

configure network ipv6 delete

要禁用设备管理接口的 IPv6 配置，请使用 **configure network ipv4 delete** 命令。

configure network ipv6 delete ［*management_interface*］

Syntax Description

management_ interface	指定管理接口。如果不指定接口，则此命令将配置默认管理接口。仅当使用 **configure management-interface** 命令启用多个管理接口时，才需要此参数。仅在 Firepower 4100 和 9300 系列设备上支持多个管理接口。请勿为其他平台指定此参数。在 Firepower 4100 和 9300 上的管理接口 ID 为 **management0**（对于默认管理接口）和 **management1**（对于可选事件接口）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令以禁用设备管理接口的 IPv6 配置。如果您连接到已删除的 IP 地址，您将失去与该设备的连接。在删除 IPv6 地址之前，请确保已配置 IPv4 地址。

您无需删除配置即可更改 IPv6 地址。如果要保留 IPv6 寻址，但只想更改地址，请使用 **configure network ipv6** {**manual** | **dhcp** | **router**} 命令。

示例

以下示例删除 IPv6 地址配置。

```
> configure network ipv6 delete
```

Related Commands

命令	Description
configure network ipv6 dhcp	通过 DHCP 配置 IPv6。
configure network ipv6 manual	手动配置 IPv6。
configure network ipv6 router	通过路由器配置 IPv6。
show network	显示管理接口配置。

configure network ipv6 destination-unreachable

要在管理接口上使用 IPv6 时启用或禁用 ICMPv6 目标不可达数据包，请使用 **configure network ipv6 destination-unreachable** 命令。

configure network ipv6 destination-unreachable {**enable** | **disable**}

Syntax Description

enable	启用目标不可达数据包。该设置为默认设置。
disable	禁用目标不可达数据包。

Command Default

默认启用。

Command History

版本	修改
6.4.0	命令已添加。

使用指南

您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。

示例

以下示例禁用“目的地不可达”消息。

```
> configure network ipv6 destination-unreachable disable
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 echo-reply	启用或禁用回应应答数据包。
configure network ipv6 manual	手动配置 IPv6 地址。
configure network ipv6 router	通过路由器配置 IPv6。
show network	显示管理接口配置。

configure network ipv6 dhcp

要将管理接口配置为从 DHCP 服务器获取 IPv6 地址，请使用 **configure network ipv6 dhcp** 命令。

configure network ipv6 dhcp ［*management_interface*］

Syntax Description

management_ interface	指定管理接口。仅在默认管理接口上支持DHCP，因此您不需要使用此参数。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可指定设备的管理接口从 DHCP 服务器接收其 IPv6 配置。管理接口与 DHCP 服务器通信以获取其配置信息。

注释 如果使用 **configure network management-data-interface** 命令配置数据接口进行 管理中心 访问，则无法将 DHCP 用于管理接口；您必须设置手动 IP 地址，因为默认路由（必须是**数据接口**）可能会被从 DHCP 服务器接收的路由覆盖。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。当流量转发到数据接口时，此 IP 地址将进行 NAT 转换。

示例

以下示例将管理接口配置为使用 DHCP 获取其 IPv6 地址。

```
> configure network ipv6 dhcp
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 manual	手动配置 IPv6。
configure network ipv6 router	通过路由器配置 IPv6。
show network	显示管理接口配置。

configure network ipv6 dhcp-dp-route

要恢复管理接口默认 IP 地址、网络掩码和网关，请使用 **configure network ipv6 dhcp-dp-route** 命令。此命令不会更改其他网络设置，例如 DNS 服务器。

注释 threat defense virtual、Firepower 4100/9300或 ISA 3000 不支持此命令。

configure network ipv6 dhcp-dp-route

Command History

版本	修改
6.6	引入了此命令。

使用指南

您必须同时输入此命令的 IPv4 和 IPv6 版本，才能将配置恢复为出厂默认设置，即使您没有识别其中一个版本的 IP 地址。

示例

以下示例恢复管理接口的默认配置。

```
> configure network ipv6 dhcp-dp-route
Set up management0 as DHCP ipv6 client with the default route through data interfaces.
>
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 dhcp	通过 DHCP 配置 IPv6。
configure network ipv6 manual	手动配置 IPv6 地址。
show network	显示管理接口配置。

configure network ipv6 echo-reply

要在管理接口上使用 IPv6 时启用或禁用 ICMPv6 回应应答数据包，请使用 **configure network ipv6 echo-reply** 命令。

configure network ipv6 echo-reply {**enable** | **disable**}

Syntax Description

enable	启用回应应答数据包。该设置为默认设置。
disable	禁用回应应答数据包。

Command Default

默认启用。

Command History

版本	修改
6.4.0	命令已添加。

使用指南

您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。禁用回应应答数据包意味着无法使用 IPv6 ping 到设备管理接口，以进行测试。

示例

以下示例禁用回应应答消息。

```
> configure network ipv6 echo-reply disable
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 destination-unreachable	启用或禁用目标不可达数据包。
configure network ipv6 manual	手动配置 IPv6 地址。
configure network ipv6 router	通过路由器配置 IPv6。
show network	显示管理接口配置。

configure network ipv6 manual

要在管理接口上配置静态 IPv6 地址，请使用 **configure network ipv6 manual** 命令。

configure network ipv6 manual *ip6addr ip6prefix* ［*ip6gw*］［*management_interface*］

Syntax Description

ip6addr	指定 IP 地址。
ip6prefix	指定前缀长度。
ip6gw	指定默认网关的 IPv6 地址。 您可以选择指定 **data-interfaces**，它将设备上的数据接口用作网关，而不是管理网络上的显式网关。如果不想将管理物理接口连接到单独的管理网络，请使用数据接口。 有关 管理中心 数据接口管理，请参阅 **configure network management-data-interface** 命令。 请注意，此命令中的 *ip6gw* 用于为设备创建默认路由。如果配置仅事件接口，则必须输入 *ip6gw* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您将 *ip6gw* 设置为与管理接口配合使用，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。
management_ interface	指定管理接口。如果不指定接口，则此命令将配置默认管理接口。仅当使用 **configure management-interface** 命令启用多个管理接口时，才需要此参数。仅在 Firepower 4100 和 9300 系列设备上支持多个管理接口。请勿为其他平台指定此参数。在 Firepower 4100 和 9300 上的管理接口 ID 为 **management0**（对于默认管理接口）和 **management1**（对于可选事件接口）。

Command History

版本	修改
6.1	引入了此命令。
6.2	为网关添加了 **data-interfaces** 关键字。
6.7	**data-interfaces** 关键字现在可用于在数据接口上进行 管理中心 管理。

使用指南

如果使用 **configure network management-data-interface** 命令配置数据接口以访问 管理中心，则必须手动设置 IP 地址（IPv4 或 IPv6）。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。当流量转发到数据接口时，此 IP 地址将进行 NAT 转换。您无法使用 DHCP（默认），因为默认路由（必须是 **数据接口**）可能会被从 DHCP 服务器收到的路由覆盖。

示例

以下示例为管理接口配置静态 IPv6 地址。

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 dhcp	通过 DHCP 配置 IPv6。
configure network ipv6 router	通过路由器配置 IPv6。
show network	显示管理接口配置。

configure network ipv6 router

要将管理接口配置为使用无状态自动配置从路由器获取 IPv6 地址，请使用 **configure network ipv6 router** 命令。

configure network ipv6 router ［*management_interface*］

Syntax Description

management_ interface	指定管理接口。如果不指定接口，则此命令将配置默认管理接口。仅当使用 **configure management-interface** 命令启用多个管理接口时，才需要此参数。仅在 Firepower 4100 和 9300 系列设备上支持多个管理接口。请勿为其他平台指定此参数。在 Firepower 4100 和 9300 上的管理接口 ID 为 **management0**（对于默认管理接口）和 **management1**（对于可选事件接口）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可指定设备的管理接口从路由器接收其 IPv6 配置。管理接口与 IPv6 路由器通信以获取其配置信息。

示例

以下示例使用无状态自动配置将管理接口配置为从路由器接收其 IPv6 地址。

```
> configure network ipv6 router
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 dhcp	通过 DHCP 配置 IPv6。
configure network ipv6 manual	手动配置 IPv6。
show network	显示管理接口配置。

configure network management-data-interface

要配置用于 管理中心 管理的数据接口而不是管理接口，请使用 **configure network management-data-interface** 命令。

configure network managament-data-interface [{ **ipv4** { **dhcp** | [**manual** *ip_address netmask*] [**default-gw** *gateway_ip*] } | **ipv6** { **manual** *ip_address prefix*] [**default-gw** *gateway_ip*] } | **ddns update-url** **https://** *username* **:** *password* **@** *provider-domain* **/** *path* **?hostname=<h>&myip=<a>** | **nameif** *name* | **client** *ip_address mask-or-prefix* | } **interface** *id* | **disable**]

Syntax Description

ipv4	为 IP 地址指定 IPv4。
ipv6	为 IP 地址指定 IPv6。
dhcp	为 IPv4 地址指定 DHCP。
manual *ip_address netmask-or-prefix*	指定手动 IP 地址和网络掩码或前缀。
default-gw *gateway_ip*	指定默认网关的 IP 地址。 如果在 CLI 中编辑辅助接口，您将无法配置网关或以其他方式更改默认路由，因为只能在 管理中心 中编辑此接口的静态路由。
ddns update-url **https://** *username* **:** *password* **@** *provider-domain* **/** *path* **?hostname=<h>&myip=<a>**	指定 DDNS Web 类型更新 URL。在 DDNS 提供商处指定用户名和密码。请向您的 DDNS 提供商咨询正确的路径。 在输入问号 (？) 字符之前，请同时按 Ctrl + V 键。这样，你就可以输入“?”，软件也不会将“?”解释为帮助查询。 虽然这些关键字看起来像参数，但您需要在 URL 末尾逐字输入此文本。这种 threat defense 将自动替换<h>发送 DDNS 更新时包含主机名和 IP 地址的 <a> 字段。
nameif 名称	设置接口的名称。
client *ip_address*	限制在特定网络上通过数据接口访问 管理中心 。请注意，当您输入不带参数的 **configure network managament-data-interface** 命令时，此关键字不是向导的一部分。
interface *ID*	指定要用于 管理中心 管理访问的数据接口 ID。您只能指定一个数据接口进行 管理中心 访问。
disable	禁用数据接口上的 管理中心 管理访问。

Command History

版本	修改
6.7	引入了此命令。

版本	修改
7.3	在 管理中心中添加辅助管理接口后，可以使用此命令在 CLI 中编辑其某些设置。

使用指南

如果首次配置此命令时未指定任何参数，系统将提示您配置数据接口的基本网络设置。

注释 使用此命令时，应使用控制台端口。如果使用 SSH 访问管理接口，连接可能会断开，您必须重新连接到控制台端口。有关 SSH 用法的详细信息，请参阅下文。

如果在管理中心 中配置了辅助管理接口，则可以使用此命令对其进行编辑。您无法在 CLI 中手动添加辅助接口；您必须使用 管理中心。

请参阅以下有关使用此命令的详细信息：

- 如果您要使用数据接口进行管理，则原始管理接口无法使用 DHCP。如果在初始设置期间没有手动设置 IP 地址，则可以使用 **configure network** {**ipv4** | **ipv6**} **manual** 命令立即设置它。如果您尚未将管理接口网关设置为 **data-interfaces**，此命令将立即设置它。
- 从数据接口进行管理中心 访问具有以下限制：
  - 只能在 物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel。 您还可以使用管理中心 在单个辅助接口上启用管理器访问，以实现冗余。
  - 此接口不能是仅管理接口。
  - 仅路由防火墙模式，使用路由接口。
  - 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 威胁防御 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
  - 接口只能位于全局 VRF 中。
  - 默认不对数据接口启用 SSH，因此必须稍后使用 管理中心 来启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。对于 Amazon Web 服务上的 threat defense virtual ，控制台端口不可用，因此您应保持对管理接口的 SSH 访问：在继续配置之前为管理添加静态路由。或者，请确保在配置用于管理器访问的数据接口并断开连接之前完成所有 CLI 配置（包括 **configure manager add** 命令）。
  - 您不能使用单独的管理接口和仅事件接口。
  - 不支持高可用性。在这种情况下，必须使用管理接口。
  - 不支持集群技术。在这种情况下，必须使用管理接口。
- 当您将 threat defense 添加到 管理中心时， 管理中心 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。有关 DNS 服务器配置的详

细信息，请参阅下文。在 管理中心 中，您可以稍后对 管理中心 访问接口配置进行更改，但要确保更改不会阻止 threat defense 或 管理中心 重新建立管理连接。如果管理连接中断， threat defense 将包含 **configure policy rollback** 命令以恢复以前的部署。

- 如果配置 DDNS 服务器更新 URL，则 threat defense 会自动添加来自 Cisco 受信任根 CA 捆绑包的所有主要 CA 证书，以便 threat defense 可以验证用于 HTTPS 连接的 DDNS 服务器证书。 threat defense 支持使用 DynDNS 远程 API 规范 (https://help.dyn.com/remote-access-api/) 的任何 DDNS 服务器。
- 此命令设置数据接口 DNS 服务器。使用设置脚本（或使用 **configure network dns servers** 命令）设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。

  在 管理中心 上，数据接口 DNS 服务器在您分配给此 threat defense 的平台设置策略中配置。当您将 threat defense 添加到 管理中心 时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的 threat defense，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使 管理中心 和 threat defense 同步。

  此外，仅当在初始注册时发现 DNS 服务器，管理中心 才会保留本地 DNS 服务器。例如，如果您使用管理接口注册了设备，但随后使用 **configure network management-data-interface** 命令配置数据接口，则必须在 管理中心中手动配置所有这些设置（包括 DNS 服务器），以便与 threat defense 配置匹配。
- 将 threat defense 注册到 管理中心 后，您可以将该管理接口更改为管理接口或另一数据接口。
- 您在安装向导中设置的 FQDN 将用于此接口。
- 您可以通过命令清除整个设备配置；在恢复场景中可使用此选项，但我们不建议您在初始设置或正常操作中使用它。
- 要禁用数据管理，请输入 **configure network management-data-interface disable** 命令。

示例

以下示例使用 DHCP 将以太网接口 1/1 设置为 管理中心 管理接口。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

以下示例使用手动 IP 地址将以太网接口 1/1 设置为 管理中心 管理接口。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Related Commands

命令	Description
configure network ipv4 manual	使用手动 IPv4 IP 地址配置管理接口。
configure network ipv6 manual	使用手动 IPv6 IP 地址配置管理接口。
configure policy rollback	如果管理连接中断， 将恢复以前的部署。
show network	显示管理接口配置。

configure network management-interface

要在 Firepower 4100 或 9300 系列设备上配置多个管理接口以分隔事件和管理流量，请使用 **configure network management-interface** 命令。对于 threat defense，多个管理接口仅适用于 Firepower 4100 和 9300 系列设备。您还可以使用此命令设置用于 管理中心 通信的 MTU 和 TCP 端口。

configure network management-interface { [**disable** | **disable-event-channel** | **disable-management-channel** | **enable** | **enable-event-channel** | **enable-management-channel**] *interface_id*] | **tcpport** *number* | **mtu-event-channel** [*bytes*] | **mtu-management-channel** [*bytes*] }

Syntax Description

disable	禁用指定的管理接口。
disable-event-channel	在指定的接口上禁用事件信道。
disable-management-channel	在指定的接口上禁用管理信道。
enable	启用指定的管理接口。
enable-event-channel	在指定的接口上启用事件信道。
enable-management-channel	在指定的接口上启用管理信道。
interface_id	指定要启用或禁用的管理接口， **management0** 或 **management1**。management0 和 management1 是这些接口的内部名称，而不考虑物理接口 ID。
tcpport *number*	配置用于与 管理中心通信的 TCP 端口。默认值为 8305。如果更改默认值，请勿指定 SSH (22) 或 HTTPS (443) 端口。保持数字在 1024 以上的高范围内，最高可达 65535。此命令与 **configure network management-port** 命令等效：
mtu-event-channel [*bytes*]	设置事件接口的 MTU，以字节为单位，如果启用 IPv4，该值可以介于 64 和 9000 之间；如果启用 IPv6，该值可以介于 1280 和 9000 之间。如果同时启用 IPv4 和 IPv6，则最小值为 1280。如果不输入字节，系统会提示您输入值。此命令与 **configure network mtu** 命令等效：
mtu-management-channel [*bytes*]	设置管理接口的 MTU，以字节为单位，如果启用 IPv4，该值可以介于 64 和 1500 之间；如果启用 IPv6，该值可以介于 1280 和 1500 之间。如果同时启用 IPv4 和 IPv6，则最小值为 1280。如果不输入字节，系统会提示您输入值。此命令与 **configure network mtu** 命令等效： **注释** 如果设置了 非常 低的 MTU，设备管理器 性能可能会受到影响。

Command Default

management0 接口已启用，并用于事件和管理流量。 management1 已禁用。

默认 UDP 端口为 8305。

管理和事件的默认 MTU 为 1500。

Command History

版本	修改
6.1	引入了此命令。
6.6	我们添加了 **mtu-event-channel** 和 **mtu-management-channel** 关键字。

使用指南

对于设备管理，管理中心管理接口承载两个单独的流量信道：管理流量信道承载所有内部流量（如特定于设备管理的设备间流量），而事件流量通道承载所有事件流量（如 Web 事件）。您可以选择在 管理中心 中配置单独的仅事件接口来处理事件流量（请参阅 管理中心 Web 界面以执行此配置）。只能配置一个仅事件接口。事件流量这能会占用大量带宽，因此将事件流量从管理流量中分离出来可以提高 管理中心的性能。

在 Firepower 4100 和 9300 系列设备上，分配给逻辑设备的管理类型接口被指定为 threat defense 应用中的默认 management0 接口。默认情况下，此接口包括管理信道和事件通道。如果在 管理中心上配置了单独的事件接口，则在 Firepower 4100 或 9300 设备上，可以选择将事件类型接口分配给 threat defense 逻辑设备，以利用这种分离。此接口被指定为 management1 接口。如果可能，在设备事件接口和 管理中心事件接口之间发送事件流量。如果事件网络关闭，则事件流量将恢复到默认管理接口。尽可能使用单独的事件接口，但管理接口始终为备用接口。

管理中心仅事件接口不能接受管理通道流量，因此您应在设备事件接口上禁用管理通道。您可以选择为管理接口禁用事件。不管是哪种情况，设备都会尝试通过事件专属接口发送事件，如果该接口关闭，那么即使您禁用了事件信道，设备也会通过管理接口发送事件。

将事件接口分配给逻辑设备后，此接口不会启用或配置网络设置。您必须访问 threat defense CLI 并使用 **configure network management-interface** 命令启用它。然后使用 **configure network** {**ipv4** | **ipv6**} **manual** 命令来配置接口的地址。

示例

以下示例启用 management1，并禁用管理信道。默认情况下，两个信道均已启用。

```
> configure network management-interface enable management1
> configure network management-interface disable-management-channel management1
>
```

以下示例更改用于与 管理中心通信的端口。

```
> configure network management-interface tcpport 8306
Management port changed to 8306.
```

以下示例将事件接口上的 MTU 设置为 9000。

```
> configure network management-interface mtu-event-channel 9000
```

```
MTU set successfully to 9000 from 1500 for management1
Refreshing Network Config...
Interface management1 speed is set to '10000baseT/Full'
>
```

以下示例使用 CLI 提示符将管理接口上的 MTU 设置为 1400。

```
> configure network management-interface mtu-management-channel
Do you want to change the MTU [1500] for management0 interface?(Yes/No): Yes
Enter the new value for MTU [1500]> 1400
MTU set successfully to 1400 from 1500 for management0
Refreshing Network Config...
Interface management0 speed is set to '10000baseT/Full'
>
```

Related Commands

命令	Description
configure network mtu	设置管理或事件接口 MTU。
configure network static-routes ipv4/ipv6	为管理接口配置静态路由。
show network	显示管理接口配置。

configure network management-port

要配置用于与 管理中心通信的 TCP 端口，请使用 **configure network management-port** 命令。

configure network management-port 编号

Syntax Description

number	配置用于与 管理中心通信的 TCP 端口。默认值为 8305。如果更改默认值，请勿指定 SSH (22) 或 HTTPS (443) 端口。保持数字在 1024 以上的高范围内，最高可达 65535。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可将用于管理连接的端口更改为管理中心。此命令不会更改用于本地管理器设备管理器的端口。此命令等同于**configure network management-interface tcpport** 命令；您不需要同时使用这两个命令。

示例

以下示例更改用于与 管理中心通信的端口。

```
> configure network management-port 8306
Management port changed to 8306.
```

Related Commands

命令	Description
configure network ipv4	为管理接口配置 IPv4 寻址。
configure network ipv6	为管理接口配置 IPv6 寻址。
show network	显示管理接口配置。

configure network mtu

要为管理或事件接口配置 MTU，请使用 **configure network mtu** 命令。

configure network mtu ［ *interface_id* ］ ［ *bytes* ］

Syntax Description

bytes	（可选）以字节为单位设置 MTU。对于管理接口，如果启用 IPv4，则值可以介于 64 和 1500 之间；如果启用 IPv6，则值可以介于 1280 和 1500 之间。 对于事件接口，如果启用 IPv4，该值可以介于 64 和 9000 之间；如果启用 IPv6，该值可以介于 1280 和 9000 之间。 如果同时启用 IPv4 和 IPv6，则最小值为 1280。如果不输入 字节，系统会提示您输入值。 **注释** 如果设置了 非常 低的 MTU，设备管理器 性能可能会受到影响。
interface_id	（可选）- 指定要设置 MTU 的接口 ID。使用 **show network** 命令查看可用的接口 ID，例如 management0、management1、br1 和 eth0，具体取决于平台。如果未指定接口，则使用管理接口。

Command Default

管理和事件的默认 MTU 为 1500。

Command History

版本	修改
6.6	引入了此命令。

使用指南

此命令等同于 和 命令；您不需要同时使用 **configure network management-interface mtu-event-channel** 和 **configure network management-interface mtu-management-channel** 命令。

示例

以下示例将事件接口 management1 上的 MTU 设置为 8192。

```
> configure network mtu 8192 management1
MTU set successfully to 8192 from 1500 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

以下示例使用 CLI 提示符将管理接口上的 MTU 设置为 1400。

```
> configure network mtu
Do you want to change the MTU [1500] for management0 interface?(Yes/No): Yes
Enter the new value for MTU [1500]> 1400
MTU set successfully to 1400 from 1500 for management0
Refreshing Network Config...
Interface management0 speed is set to '10000baseT/Full'
>
```

Related Commands

命令	Description
configure network ipv4	为管理接口配置 IPv4 寻址。
configure network ipv6	为管理接口配置 IPv6 寻址。
configure network management-interface	设置管理或事件接口 MTU。
show network	显示管理接口配置。

configure network speed

要设置管理接口或数据接口的速度，请使用 **configure network speed** 命令。

注释 仅在 Secure Firewall 3100 上支持此命令。

configure network speed { *speed* | **sfp-detect** [*interface_id*]

Syntax Description

interface_id	（可选）指定要设置速度的接口 ID。默认值为 management0。
sfp-detect	检测已安装的SFP模块的速度并使用适当的速度。该设置为默认设置。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。
速度	将速度设置为特定速度。可用速度因接口而异。

Command Default

默认速度为 **sfp-detect**。

Command History

版本	修改
7.1	此命令是为安全防火墙 3100 引入的。

使用指南

我们建议使用默认 **sfp-detect**，除非您想将速度设置为特定速度，而不考虑 SFP 功能。

示例

以下示例将管理接口 management0 上的速度设置为 1gbps。

```
> configure network speed 1gbps
```

Related Commands

命令	Description
configure network ipv4	为管理接口配置 IPv4 寻址。
configure network ipv6	为管理接口配置 IPv6 寻址。
configure network management-interface	设置管理或事件接口 MTU。
show network	显示管理接口配置。

configure network static-routes

要添加或删除静态路由，请使用此命令的 **configure network static-routes** 形式。

configure network static-routes {**ipv4** | **ipv6**} {**add** *interface destination netmask_or_prefix gateway* | **delete**}

Syntax Description

add	为管理接口添加静态路由。
delete	为管理接口删除静态路由。系统会提示您选择要删除的路由。
interface	管理接口的 ID。使用 **show network** 命令查看您的型号的管理接口 ID。
ipv4	添加或删除 IPv4 管理地址的静态路由。
ipv6	添加或删除 IPv6 管理地址的静态路由。
destination	要添加或删除的目标 IP 地址，采用 IPv4 或 IPv6 格式（视情况而定）。例如，10.100.10.10 或 2001:db8::201。
netmask_or_prefix	IPv4 的网络地址掩码或 IPv6 的前缀。IPv4 网络掩码必须采用点分十进制格式，例如 255.255.255.0。IPv6 前缀是标准前缀编号，例如 96。
gateway	要添加或删除的网关地址，采用 IPv4 或 IPv6 格式（视情况而定）。

Command History

版本	修改
6.0.1	引入了此命令。

使用指南

如果使用 **configure network management-interface** 命令配置仅事件接口，并且此接口与管理接口位于不同的网络，则需要配置静态路由。静态路由不会影响通过设备的流量，即数据接口上的流量。如果没有静态路由，所有管理流量都使用指定为默认管理接口网关的默认路由。使用单个管理接口或事件专用接口位于同一网络时，通常不需要静态路由。

注释 对于默认路由，请勿使用此命令；当您将 **configure network ipv4** 或 **ipv6** 命令用于默认管理接口时，只能更改默认路由网关 IP 地址。

示例

以下示例使用目的地址、网络地址掩码和网关地址为管理接口添加 IPv4 静态路由：
management110.115.24.0255.255.255.010.115.9.2

```
> configure network static-routes ipv4 add management1 10.115.24.0 255.255.255.0 10.115.9.2
```

以下示例使用 的目的地址、IPv6 前缀长度和网关地址为管理接口添加 IPv6 静态路由。
management12001:db8::201642001:db8::3657

```
> configure network static-routes ipv6 add management1 2001:db8::201 64 2001:db8::3657
```

以下示例显示如何删除静态路由。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 10.1.1.0
Gateway                   : 192.168.0.254
Netmask                   : 255.255.255.0
> configure network static-routes ipv4 delete
Please select which IPv4 Static Route to delete:
1) management1:   dest 10.1.1.0          nmask 255.255.255.0     gw 192.168.0.254
Please enter number of route to delete: 1
Interface:    management1
Destination:  10.1.1.0
Netmask:      255.255.255.0
Gateway:      192.168.0.254
Are you sure that you want to delete this route?  (y/n) [n]: y
Configuration updated successfully
> show network-static-routes
No static routes currently configured.
```

Related Commands

命令	Description
configure network management-interface	配置多个管理接口。
configure network static-routes ipv4	为管理接口添加或删除 IPv4 静态路由。
show network-static-routes	显示为管理接口配置的静态路由。

configure password

要更改当前登录的用户账号的密码，请使用 **configure password** 命令。

configure password

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令，当前用户可以在 CLI 中更改其密码。发出命令后，CLI 会提示用户其当前（或旧）密码，然后提示用户输入新密码两次。

示例

以下示例更改当前用户账号的密码。

```
> configure password
Enter current password: oldpassword
Enter new password: newpassword
Confirm new password: newpassword
```

Related Commands

命令	Description
configure user add	添加用于 CLI 访问的用户账号。

configure policy rollback

要将 threat defense 上的配置回滚到上次部署的配置，请使用 **configure policy rollback** 命令。

configure policy rollback

Command History

版本	修改
6.7	引入了此命令。
7.2	支持回滚以实现高可用性。

使用指南

如果将 threat defense 上的数据接口用于 管理中心 管理（请参见 **configure network management-data-interface** 命令），并从 管理中心 部署影响网络连接的配置更改，则可以将 threat defense 上的配置回滚到上次部署的配置，以便恢复管理连接。然后，您可以调整 管理中心 中的配置设置，以便保持网络连接并重新部署。即使没有丢失连接，也可以使用回滚功能；它不仅限于此故障排除情况。

请参阅以下准则：

- 只有以前的部署可以在 threat defense 上本地提供；您无法回滚到任何较早的部署。
- 从 管理中心 7.2 开始，支持回滚以实现高可用性。
- 群集技术部署不支持回滚。
- 回滚只会影响您可以在 管理中心中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在 threat defense CLI 中进行配置。请注意，如果您在上次 管理中心 部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的 管理中心 设置。
- UCAPL/CC 模式无法回滚。
- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

回滚后，threat defense 会通知 管理中心 已成功完成回滚。在 管理中心中，部署屏幕将显示一条横幅，说明配置已回滚。

如果回滚失败，请参阅 https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html 以了解常见的部署问题。在某些情况下，恢复 管理中心 管理访问权限后回滚可能会失败；在这种情况下，您可以解决 管理中心 配置问题，并从 管理中心重新部署。

示例

以下示例回滚上次部署的配置。

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Related Commands

命令	Description
configure network management-data-interface	为 管理中心 管理配置数据接口。

configure raid

要管理 RAID 中的 SSD，请使用 **configure raid** 命令。

注释 仅在 Secure Firewall 3100 上支持此命令。

configure raid { **add** | **remove** | **remove-secure** } **local-disk** { **1** | **2** } [*psid*]

Syntax Description

add	将 SSD 添加到 RAID。将新 SSD 同步到 RAID 可能需要几个小时，在此期间防火墙完全正常运行。您甚至可以重新启动，同步将在启动后继续。
psid	如果您添加的 SSD 以前在另一个系统上使用过，并且仍处于锁定状态，请输入 *psid*。*Psid* 印在 SSD 背面的标签上。或者，您可以重新启动系统，SSD 将被重新格式化并添加到 RAID。
remove	从 RAID 中删除 SSD 并保持数据不变。
remove-secure	从 RAID 中删除 SSD，禁用自加密磁盘功能，并对 SSD 执行安全清除。
local-disk {**1** | **2**}	指定 SSD、disk1 或 disk2。

Command Default

如果您有两个 SSD，它们会在您启动时形成 RAID。

Command History

版本	修改
7.1	此命令是为安全防火墙 3100 引入的。

使用指南

防火墙启动时，您可以在 CLI 上执行以下任务： 威胁防御

- 热插拔其中一个 SSD - 如果 SSD 出现故障，您可以更换它。请注意，如果您只有一个 SSD，则无法在防火墙开启时将其删除。
- 删除一个 SSD - 如果您有两个 SSD，可以删除一个。
- 添加第二个 SSD - 如果您有一个 SSD，可以添加第二个 SSD 并形成 RAID。

注意 请勿在未使用此程序从 RAID 中移除 SSD 的情况下将其移除。可能会导致数据丢失。

示例

以下示例从 RAID 中删除 disk2 并执行安全清除。

```
> configure raid remove-secure local-disk 2
```

Related Commands

命令	Description
show raid	显示 RAID 状态。
show ssd	显示 SSD 状态。

configure snort

要配置 Snort 检测引擎的高级行为，请使用 **configure snort** 命令。

configure snort preserve-connection {**enable** | **disable**}

Syntax Description

preserve-connection {**enable** | **disable**}	是否在Snort流程关闭时保留路由和透明接口上的现有TCP/UDP连接。默认情况下该选项处于启用状态，但可以禁用它。启用后，已被允许的连接仍保持建立状态，但在Snort再次可用之前，无法建立新连接。当禁用时，所有新的或现有连接会在 Snort 关闭时被丢弃。 非 TCP/UDP 连接（例如 ICMP ping）不会保留。 要查看当前设置，请使用 **show running-config snort** 命令。查看整个运行配置时， **snort preserve-connection** 命令的 **no** 形式表示该功能已禁用。

Command History

版本	修改
6.2.0.2、 6.2.3	引入了此命令。但是， **preserve-connection disable** 不支持 设备管理器 与 （本地管理）一起使用，每次部署配置时都会重新启用保留连接。 此命令在 threat defense 或 管理中心 运行版本 6.2.1、6.2.2、6.2.2.x 或早于 6.2.0.2 的版本时不可用，这种情况下，设备行为就像已禁用该命令一样，因此，当Snort关闭时，所有新的或现有的连接都会被丢弃。

使用指南

启用 **preserve-connection** 后，如果 Snort 关闭，任何现有连接仍会保持建立。当 Snort 可用时，这些已建立的连接会继续绕过 Snort 检查。任何需要 Snort 检查的新连接都将被丢弃，直到 Snort 再次可用。

示例

以下示例禁用 **preserve-connection**。

```
> configure snort preserve-connection disable
```

Related Commands

命令	Description
show conn	显示连接。
show conn detail	在连接详细信息中包括 snort 检测信息。
show conn detail long	在长格式连接详细信息中包括 snort 检测信息。

configure ssh-access-list

要将设备配置为接受来自指定 IP 地址的 SSH 连接，请使用 **configure ssh-access-list** 命令。

configure ssh-access-list *address_list*

Syntax Description

address_list	主机或网络的 IP 地址的逗号分隔列表，采用 IPv4 无类域间路由 (CIDR) 符号或 IPv6 前缀长度符号。例如，10.100.10.0/24 or 2001:DB8::/96。 要指定所有 IPv4 主机，请输入 0.0.0.0/0。要指定所有 IPv6 主机，请指定 ::/0。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您必须在一个命令中包含所有受支持的主机或网络。此命令中指定的地址将覆盖 SSH 访问列表的当前内容。

仅允许 SSH 访问不允许用户登录本地管理器。对配置软件的访问由用户名和密码控制。

如果排除当前登录 CLI 的 IP 地址，连接将中断。您需要更改 IP 地址才能重新进入 CLI。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例将设备配置为接受来自任何 IPv4 或 IPv6 地址的 SSH 连接：

```
> configure ssh-access-list 0.0.0.0/0,::/0
The ssh access list was changed successfully.
> show ssh-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:ssh
```

Related Commands

命令	Description
configure disable-ssh-access	清除 SSH 访问列表。
show ssh-access-list	显示 SSH 访问列表。

configure ssl-protocol

要配置客户端可在与设备的 HTTPS 连接中使用的 SSL 协议，请在使用本地管理器时使用 **configure ssl-protocol** 命令。

configure ssl-protocol {*protocol_list* | **default**}

Syntax Description

default	启用默认 SSL 协议列表： **TLSv1.1**、 **TLSv1.2**。
protocol_list	指定以下任何协议的逗号分隔列表： **TLSv1**、 **TLSv1.1**、 **TLSv1.2**、 **SSLv3**。

Command Default

默认设置为 **TLSv1.1**、 **TLSv1.2**。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令设置客户端可用于对设备进行 HTTPS Web 访问的协议。这与本地管理器 设备管理器配合使用。它不与远程管理器一起使用。

注释 如果使用此命令禁用当前用于与设备通信的协议，则会断开连接。

示例

以下示例将设备配置为接受 HTTPS 连接的所有 SSL 协议。

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
> configure ssl-protocol TLSv1,TLSv1.1,TLSv1.2,SSLv3
The following ssl protocols are now enabled:  TLSv1 TLSv1.1 TLSv1.2 SSLv3
> show ssl-protocol
The supported ssl protocols are  TLSv1 TLSv1.1 TLSv1.2 SSLv3
```

Related Commands

命令	Description
show ssl-protocol	显示当前配置的 SSL 协议。

configure tcp-randomization

要禁用 TCP 序列号随机化，请使用 **configure tcp-randomization** 命令。

configure tcp-randomization {**enable** | **disable**}

Syntax Description

enable	随机更改传入和传出数据包中的 TCP 序列号，以防止攻击者预测下一个数据包的序列号。
disable	请勿更改传入和传出数据包中的 TCP 序列号。

Command Default

默认启用 TCP 序列号随机化。

Command History

版本	修改
6.2	引入了此命令。

使用指南

每个 TCP 连接都有两个初始序列号 (ISN)：一个由客户端生成，一个由服务器生成。threat defense设备会为通过入站和出站两个方向的 TCP SYN 随机生成 ISN。

随机化受保护主机的 ISN 可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。

可以根据需要禁用 TCP 初始序列号随机化，例如，由于数据混乱。例如，您可能正在使用依赖于具有顺序编号的TCP数据包的软件测试工具、软件产品或硬件设备。更改TCP随机化设置会影响设备上的所有接口和所有流量；不能更改特定接口或流量类。

仅当因随机化而遇到特定问题时，才应禁用 TCP 序列号随机化。

注释 虽然您可以在使用 设备管理器 时禁用 TCP 序列号随机化，但每次从 设备管理器 部署配置时，此功能都会重新启用。如果要保持禁用 TCP 序列号随机化，则必须在每次部署后重新输入命令。

示例

以下示例禁用 TCP 序列号随机化。

```
> configure tcp-randomization disable
```

要确定 TCP 序列号随机化当前是启用还是禁用，请查看 **set connection random-sequence-number disable** 命令的运行配置。此命令将位于 global_policy 策略映射中，因此您可以使用 **show running-config policy-map** 命令限制配置视图。如果 **set connection random-sequence-number** 命令未出现在配置中，则 TCP 序列号随机化已启用。

例如，以下内容显示 TCP 序列号随机化已禁用（相关命令已突出显示）。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
 class tcp
  set connection random-sequence-number disable
!
```

以下示例显示已启用 TCP 序列号随机化，因为 **set connection random-sequence-number** 命令不在 global_policy 策略映射中。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
```

configure unlock_time

要设置用户账户在超过最大失败登录次数后自动解锁的时间长度，请使用 **configure unlock_time** 命令。此命令仅在 CC/UCAPL 合规性模式下有效。

configure unlock_time 编号

Syntax Description

number	指定解锁时间（以分钟为单位），范围为 1 到 9999。

Command Default

在 CC/UCAPL 模式下运行时，默认解锁时间为 30 分钟。

当不在 CC/UCAPL 模式下运行时，用户账户将保持锁定状态，直到您使用 **configure user unlock** 命令将其解锁。您无法设置自动解锁时间。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

如果您在CC/UCAPL合规性模式下运行，则可以为锁定的用户设置全局解锁时间。在超过用户账户最大失败登录尝试次数的给定用户的时间到期后，账户将被解锁，用户可以重试。使用 **configure user maxfailedlogins** 命令设置允许的最大失败登录尝试次数。

即使设置了解锁时间，您也可以随时使用 **configure user unlock** 命令解锁用户账户。用户无需等待解锁时间到期。

示例

以下示例将解锁时间配置为 60 分钟。

```
> configure unlock_time 60
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user maxfailedlogins	为用户设置最多允许的登录失败次数。
configure user unlock	解锁指定用户的账户。
show user	显示用户账号。

configure user access

要更改现有用户的访问授权级别，请使用 **configure user access** 命令。

configure user access *username* {**basic** | **config**}

Syntax Description

username	指定现有用户的名称。
basic	提供用户基本访问权限。此级别不允许用户输入配置命令。
config	提供用户配置访问权限。此级别将赋予用户完整管理员权限，让其可以输入所有配置命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

创建用户账号时，需要指定用户的访问权限。使用 **configure user access** 命令以修改指定用户的访问级别。命令在指定用户下次登录时生效。

示例

以下示例将用户 jdoe 的访问权限更改为 Basic。

```
> configure user access jdoe basic
```

Related Commands

命令	Description
configure user add	添加新用户。
show user	显示用户账号和访问权限。

configure user add

要创建用于 CLI 访问的新用户账号，请使用 **configure user add** 命令。

configure user add 用户名 {**basic** | **config**}

Syntax Description

username	指定现有用户的名称。
basic	提供用户基本访问权限。此级别不允许用户输入配置命令。
config	提供用户配置访问权限。此级别将赋予用户完整管理员权限，让其可以输入所有配置命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可创建具有指定名称、访问级别和密码的新用户。此命令提示输入密码。所有其他账户属性均使用默认属性进行配置。

示例

以下示例将添加一个名为 joecool 且具有配置访问权限的用户账号。在您键入密码时，密码不会显示。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

Related Commands

命令	Description
configure user access	设置用户访问级别。
configure user aging	设置用户密码时效。
configure user delete	删除指定用户。
configure user disable	禁用指定用户。
configure user enable	启用指定用户。
configure user forcereset	强制重置指定用户的密码。

命令	Description
configure user maxfailedlogins	为指定用户设置最多登录失败次数。
configure user password	为指定用户设置密码。
configure user strengthcheck	为指定用户设置密码强度检查要求。
configure user unlock	为指定用户解锁账户。
show user	显示用户账号。

configure user aging

要设置用户密码的到期日期，请使用 **configure user aging** 命令。

configure user aging *username max_days warn_days* [*grace_period*]

Syntax Description

username	指定用户的名称。您无法更改 **管理员** 用户老化设置。
max_days	指定密码的最大有效天数。值范围为 1 到 9999。
warning_days	指定在密码到期前允许用户更改密码的天数。值范围为 1 到 9999，但必须小于最大天数。
grace_period	（可选，仅限 FXOS 平台。）指定在密码到期后用户仍可更改密码的天数。在非 FXOS 平台上，该参数被接受，但 **show user** 输出显示宽限期已禁用。

Command History

版本	修改
6.1	引入了此命令。
7.0	添加了 *grace_period* 参数。

示例

以下示例将用户的密码设置为在 100 天后到期，并在密码到期前 30 天开始警告用户。在 show user 输出中，请注意 Exp 和 Warn 列中的数字。

```
> configure user aging jdoe 100 30
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

以下示例将密码设置为在 180 天后到期，在到期前 7 天开始警告用户，并包括 7 天的宽限期。

```
> configure user aging joeuser 180 7 7
> show user
Login          UID   Auth Access  Enabled Reset   Exp   Warn    Grace  MinL Str Lock Max
admin          100  Local Config  Enabled    No  10000     7  Disabled    8 Ena   No N/A
extuser        501 Remote Config Disabled   N/A  99999     7  Disabled    1 Dis   No N/A
joeuser       1000  Local Config  Enabled   Yes    180     7         7    8 Dis   No   5
```

Related Commands

命令	Description
configure user add	添加新用户。

命令	Description
configure user forcereset	强制重置指定用户的密码。
configure user password	为指定用户设置密码。
show user	显示用户账号。

configure user delete

要删除用户账号，请使用 **configure user delete** 命令。

configure user delete 用户名

Syntax Description

username	指定用户的名称。您无法删除 管理员 用户。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例删除用户账号。

```
> configure user delete jdoe
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user disable	禁用用户账号，而不将其删除。
show user	显示用户账号。

configure user disable

要禁用用户账号而不将其删除，请使用 **configure user disable** 命令。

configure user disable 用户名

Syntax Description

username	指定用户的名称。您无法禁用 管理员 用户。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可禁用用户账号而不将其删除。被禁用的用户将无法登录。使用 **configure user enable** 命令重新启用已禁用的用户账号。

示例

以下示例禁用用户账号。

```
> configure user disable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user delete	删除指定用户。
configure user enable	启用指定用户。
configure user unlock	为指定用户解锁账户。
show user	显示用户账号。

configure user enable

要启用以前禁用的用户，请使用 **configure user enable** 命令。

configure user enable 用户名

Syntax Description

username	指定用户的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可启用用户并允许登录。

示例

以下示例启用已禁用的用户账户。请注意 **show user** “已启用”列中的更改。

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
> configure user enable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user disable	禁用指定用户。
configure user forcereset	强制重置指定用户的密码。
configure user unlock	为指定用户解锁账户。
show user	显示用户账号。

configure user forcereset

要强制用户在下次登录时更改密码，请使用 **configure user forcereset** 命令。

configure user forcereset 用户名

Syntax Description

username	指定用户的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令以强制用户在下次登录时更改密码。当用户登录并更改密码时，会自动启用强度检查。

示例

以下示例强制用户在下次登录时重置密码。

```
> configure user forcereset jdoe
```

Related Commands

命令	Description
configure user password	为指定用户设置密码。
configure user strengthcheck	为指定用户设置密码强度检查要求。
show user	显示用户账号。

configure user maxfailedlogins

要设置用户的最大连续登录失败次数，请使用 **configure user maxfailedlogins** 命令。

configure user maxfailedlogins *username number*

Syntax Description

username	指定用户的名称。
number	指定最大连续失败登录次数，范围为 1 到 9999。

Command Default

没有默认行为或值。但是，当您创建新账户时，默认的最大连续登录失败次数为 5。

Command History

版本	修改
6.1	引入了此命令。
6.2.2	在 CC/UCAPL 合规性模式下运行时，还可以配置 **admin** 用户的最大失败登录尝试次数。

使用指南

使用此命令可设置指定用户在其账户被锁定之前的最大连续登录失败次数。如果用户账号被锁定，请使用 **configure user unlock** 命令将其解锁。

示例

以下示例将最大连续失败登录次数设置为 3。

```
> configure user maxfailedlogins jdoe 3
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user password	为指定用户设置密码。
configure user unlock	解锁指定用户的账户。
show user	显示用户账号。

configure user minpasswdlen

要设置用户密码的最小长度，请使用 **configure user minpasswdlen** 命令。

configure user minpasswdlen *username number*

Syntax Description

username	指定用户的名称。
number	指定密码的最小长度，从 1 到 127。

Command Default

无最小密码长度。

Command History

版本	修改
6.1	引入了此命令。
6.2.2	您现在可以为 **admin** 用户配置最小密码长度。

使用指南

使用此命令可设置指定用户的最小密码长度。系统将提示您输入用户账号的当前密码。如果最小长度大于当前密码长度，系统还会提示您设置新密码。

示例

以下示例将最小密码长度设置为 8 个字符。在本示例中，当前密码小于新的最小值，因此您需要设置新密码。

```
> configure user minpasswdlen jdoe 8
Setting minimum password length to 8
Enter current password: <enter old password>
Enter new password for user jdoe: <enter new password>
Confirm new password for user jdoe: <enter new password>

Setting Minimum password length succeeded
```

Related Commands

命令	Description
configure user add	添加新用户。
show user	显示用户账号。

configure user password

要设置其他用户账户的密码，请使用 **configure user password** 命令。

configure user password 用户名

Syntax Description

username	指定用户的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可设置指定用户的密码。此命令提示输入用户密码。要更改您自己的密码，请使用 **configure password** 命令而不是此命令。

示例

以下示例设置另一个用户账户的密码。在您键入密码时，密码不会显示。

```
> configure user password jdoe
Enter new password for user jdoe: newpassword
Confirm new password for user jdoe: newpassword
```

Related Commands

命令	Description
configure password	更改当前登录用户的密码。
configure user add	添加新用户。
configure user aging	设置用户密码时效。
configure user forcereset	强制重置指定用户的密码。
configure user maxfailedlogins	为指定用户设置最多登录失败次数。
configure user strengthcheck	为指定用户设置密码强度检查要求。
show user	显示用户账号。

configure user strengthcheck

要启用或禁用针对用户密码的强度要求，请使用 **configure user strengthcheck** 命令。

configure user strengthcheck 用户名 {**enable** | **disable**}

Syntax Description

username	指定用户的名称。
enable	设置指定用户密码的要求。
disable	删除对指定用户密码的要求。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令启用或禁用强度检查，用户修改密码时需要满足特定的密码条件。如果用户密码到期或使用了 **configure user forcereset** 命令，则此要求会在用户下次登录时自动启用。

示例

以下示例对用户账号启用强度检查。

```
> configure user strengthcheck jdoe enable
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user forcereset	强制重置指定用户的密码。
configure user maxfailedlogins	为指定用户设置最多登录失败次数。
configure user password	为指定用户设置密码。
configure user unlock	为指定用户解锁账户。
show user	显示用户账号。

configure user unlock

要解锁登录失败次数超过最大数量的用户账号，请使用 **configure user unlock** 命令。

configure user unlock 用户名

Syntax Description

username	指定用户的名称。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例解锁用户账号。

```
> configure user unlock jdoe
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user maxfailedlogins	为指定用户设置最多登录失败次数。
show user	显示用户账号。

conn data-rate

要查看传输大量数据的设备上的连接，请使用 **conn data-rate** 命令。此命令展示每个流的数据速率与现有的连接信息。要禁用按数据速率收集连接，请使用命令的 **no** 形式。

conn data-rate

no conn data-rate

Command History

版本	修改
6.6	引入了此命令。

使用指南

conn data-rate 命令对于确定哪些连接和用户可能对设备的整体负载贡献最大。

启用后， **conn data-rate** 功能会跟踪所有连接的两项统计信息：

- 连接的正向和反向的当前（1 秒）数据速率。
- 连接的前向和反向最大 1 秒数据速率。

示例

以下示例显示如何启用连接数据速率收集，验证该功能是否已启用，以及如何查看数据速率：

```
> conn data-rate
> show conn data-rate
Connection data rate tracking is currently enabled.
Use 'show conn detail' to see the data rates of active connections.

> show conn detail

TCP outside: 198.51.100.1/46994 NP Identity Ifc: 203.0.113.1/22,
flags UOB , idle 0s, uptime 9m24s, timeout 1h0m, bytes 68627
Initiator: 198.51.100.1, Responder: 203.0.113.1
data-rate forward/reverse
current rate: 1194/0 bytes/sec <----------------current data rate for forward/reverse flows
max rate: 2520/0 bytes/sec <----------------max data rate for forward/reverse flows
time since last max 0:08:54/NA <----------------time since last max data rate for
forward/reverse flows
```

Related Commands

命令	Description
show conn data-rate	显示连接数据速率跟踪的当前状态。
show conn detail	按数据速率值显示已过滤的连接。
clear conn data-rate	清除当前最大数据速率值。

connect fxos

要进入 FXOS 服务管理器 CLI 模式，请使用 **connect fxos** 命令。

connect fxos

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

FXOS 是 Firepower 2100、4100 和 9300 系列设备上的基础软件。

示例

以下示例显示在 threat defense CLI 中启动时如何进入 FXOS CLI。输入 ? 查看 FXOS 中的可用命令。

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2015, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

(...remaining copyrights omitted...)

kp-fpr2100-2#
```

以下示例显示如果您最初从 FXOS CLI 进入 threat defense CLI（使用 **connect ftd** FXOS 命令），会发生什么情况。

```
> connect fxos
You came from FXOS Service Manager. Please enter 'exit' to go back.
```

copy

要将文件复制到闪存或从闪存中复制，请使用 **copy** 命令。

copy [**/noconfirm** | **/noverify**] [*interface_name*] { **/pcap capture:/** [*buffer_name*] | *src_url* | **running-config** | **startup-config** } *dest_url*

Syntax Description

/noverify	（可选）复制开发密钥签名映像时跳过签名验证。
/noconfirm	（可选）复制文件而不提示确认。
interface_name	（可选）指定将通过其复制文件的接口名称。如果不指定接口，threat defense 将检查 数据路由表。要使用不属于数据路由表的 **管理** 接口或任何其他管理专用接口，必须使用此选项进行指定。
/pcap capture:/ [*buffer_name*]	从指定缓冲区复制 **capture** 命令的原始数据包捕获转储。
running-config	指定存储在系统内存中的运行配置。
startup-config	指定存储在闪存中的启动配置。闪存中启动配置是隐藏文件。

src-url *dest-url*	指定源文件（您要复制的文件）和目标文件（您通过复制创建的文件）。您无法在两个远程位置之间复制，因此如果源文件是本地文件，则目标文件可以是本地文件或远程文件。如果源文件是远程文件，则目标文件必须是本地文件。对文件位置使用以下URL 语法： • **disk0:/**[[*path/*]*filename*] 或 **flash:/**[[*path/*]*filename*] - **flash** 和 **disk0** 均指示内部闪存。可以使用任一选项。 • **disk***n***:/**[[*path/*]*filename*]- 表示可选的外部闪存驱动器，其中 *n* 指定驱动器编号。 • **smb:/**[[*path/*]*filename*] - 指示服务器消息阻止（一种 UNIX 服务器本地文件系统）。 • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]—The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode). • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]—Indicates an SCP server. **;int=***interface* 选项会绕过路由查找，并始终使用指定接口来访问安全复制 (SCP) 服务器。 • **system:/**[[*path/*]*filename*]- 表示系统内存。 • **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]] - 指示 TFTP 服务器。路径名不能包含空格。**;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问 TFTP 服务器。 • **cluster_trace:** - 表示 cluster_trace 文件系统。

Command History

版本	修改
7.1	如果不指定接口， threat defense将检查数据路由表。没有回退到管理路由表。以前，默认查找是回退到数据路由表的管理路由表。由于管理和诊断接口合并，管理路由表不再自动使用；如果要使用管理接口，则必须指定该接口。
6.1	引入了此命令。

使用指南

执行一个整个集群范围内的捕获后，您可以通过在主设备上输入以下命令，将同一个捕获文件同时从集群中的所有设备复制到 TFTP 服务器：

cluster exec copy /noconfirm /pcap capture:*cap_name* **tftp://***location*/*path*/*filename***.pcap**

多个 PCAP 文件（一个文件来自一个设备）将复制到 TFTP 服务器。目标捕获文件名自动附有设备名称，如 filename_A.pcap、filename_B.pcap，其中 A 和 B 是集群设备名称。

注释 如果在文件名末尾添加设备名称，将生成不同的目标名称。

示例

以下示例复制安装日志。

```
> copy /noconfirm flash:/install.log flash:/install.save.log
Copy in progress...CC
INFO: No digital signature found
150498 bytes copied in 0.20 secs
```

以下示例展示如何将文件从磁盘复制到系统执行空间中的 TFTP 服务器：

```
> copy /noconfirm disk0:/install.log
tftp://10.7.0.80/install.log
```

以下示例展示如何将运行配置复制到 TFTP 服务器：

```
> copy /noconfirm running-config tftp://10.7.0.80/firepower/device1.cfg
```

以下示例展示如在不对开发密钥签名的映像不进行验证的情况下对其进行复制：

```
> copy /noverify /noconfirm lfbff.SSA exa_lfbff.SSA
Source filename [lfbff.SSA]?
Destination filename [exa_lfbff.SSA]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Writing file disk0:/exa_lfbff.SSA...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Digital Signature was not verified
124125968 bytes copied in 61.740 secs (2034851 bytes/sec)
```

Related Commands

命令	Description
write net	将运行配置复制到 TFTP 服务器。

cpu hog granular-detection

要在短时间内提供实时占用检测并设置 CPU 占用阈值，请使用 **cpu hog granular-detection** 命令。

cpu hog granular-detection ［**count** *number*］［**threshold** *value*］

Syntax Description

count *number*	指定已执行的代码执行中断的数量。值为 1 到 10000000。默认值和建议值均为 1000。
threshold *value*	范围为 1 至 100。如果未设置，则使用默认值，平台之间有所不同。

Command Default

count 默认值为 1000。 **threshold** 默认设置因平台而异。

Command History

版本	修改
6.1	引入了此命令。

使用指南

cpu hog granular-detection 命令每隔 10 毫秒中断当前代码执行并总计中断数。CPU 占用的中断检查。如果存在，则登录。此命令可缩短数据路径中 CPU 占用检测的时间间隔。

每个基于安排的占用最多与 5 个基于中断的占用条目关联；每个条目可最多有 3 个回溯。无法覆盖基于中断的占用；如果没有空间，将丢弃新的。根据LRU策略仍可重用基于安排的占用，且当时会清除其关联的基于中断的占用。

示例

以下示例展示如何触发 CPU 占用检测：

```
> cpu hog granular-detection count 1000 threshold 10
Average time spent on 1000 detections is 10 seconds, and it may take longer
under heavy traffic.
Please leave time for it to finish and use show process cpu-hog to check results.
```

Related Commands

命令	Description
show processes cpu-hog	显示占用 CPU 的进程。
clear process cpu-hog	清除占用 CPU 的进程。

cpu profile activate

要启动 CPU 分析，请使用 **cpu profile activate** 命令。

cpu profile activate ［*n_samples* ［**sample-process** *process_name*］［**trigger cpu-usage** *cpu%* ［*process_name*］］］

Syntax Description

n_samples	分配用于存储 *n* 采样号的内存。有效值为从 1 到 100,000。
sample-process *process_name*	仅对特定流程采样。
trigger cpu-usage *cpu%* [*process_name*]	在全局 CPU 百分比大于 5 秒之前防止分析器启动，并且在 CPU 百分比低于此值时，停止分析器。 如果指定流程名称，它将使用该流程的 5 秒 CPU 百分比作为触发器。

Command Default

n_samples 默认值为 1000。

cpu% 默认值为 0。

Command History

版本	修改
6.1	引入了此命令。

使用指南

CPU 分析器可帮助您确定哪个流程正在使用 CPU。在计时器中断时，分析 CPU 可捕获已在 CPU 上运行的流程地址。无论 CPU 负载如何，每隔 10 毫秒进行此分析。例如，如果需要 5000 份采样，分析确切的需要 50 秒完成。如果 CPU 分析器使用的 CPU 时间数量相对较低，则收集采样的时间会更长。CPU 配置文件记录在单独的缓冲区进行采样。

将 **show cpu profile** 命令与 **cpu profile activate** 命令配合使用可显示可收集的信息，以及 TAC 可用于排除 CPU 问题的故障的信息。 **show cpu profile dump** 命令输出为十六进制格式。

如果 CPU 分析器等待启动条件发生， **show cpu profile** 命令会显示以下输出：

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

示例

默认情况下，以下示例激活分析器并指示其存储 1000 份采样。接下来， **show cpu profile** 命令显示正在进行分析。等待一段时间后，下一个 **show cpu profile** 命令显示分析已完成。最

后，我们使用**show cpu profile dump**命令获取结果。复制输出并将其提供给思科技术支持。您可能需要记录 SSH 会话以获取完整输出。

```
> cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU profiling currently in progress:
    Core 0: 501 out of 1000 samples collected.
    CP: 586 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU Profiling has stopped.
    Core 0 done with 1000 samples
    CP done with 1000 samples
Use "show cpu profile dump" to see the results.
> show cpu profile dump
(...output omitted...)
```

Related Commands

命令	Description
show cpu profile	显示 CPU 分析进程。
show cpu profile dump	显示不完整的或已完成的分析结果。

cpu profile dump

要将 CPU 分析的结果保存到文本文件，请使用 **cpu profile dump** 命令。

cpu profile dump *dest_url*

Syntax Description

dest_url	• **disk0:**/[[*path/*]*filename*] 或 **flash:**/[[*path/*]*filename*] - **flash** 和 **disk0** 均指示内部闪存。可使用任一选项。 • **disk***n***:**/[[*path/*]*filename*]- 表示可选的外部闪存驱动器，其中 *n* 指定驱动器编号。 • **smb:**/[[*path/*]*filename*] - 指示 UNIX 服务器本地文件系统。使用 LAN 管理器及类似的网络系统中的 Server Message Block（服务器消息块）文件系统协议包装数据并与其他系统交换信息。 • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]—The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode). • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*password*]@] *server*[/*path*]/*filename*[*;int=***;int=***interface_name*]] **-;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问安全复制 (SCP) 服务器。 • **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]—路径名不能包含空格。**;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问 TFTP 服务器。 • **cluster:**- 表示集群文件系统。

Command History

版本	修改
6.1	引入了此命令。

使用指南

CPU profile dump 命令以十六进制格式将 CPU 分析器输出写入指定的文本文件。

示例

以下示例将最新的 CPU 配置文件转储存储到名为 cpudump.txt 的文件：

```
> cpu profile dump disk0:/cpudump.txt
```

Related Commands

命令	Description
show cpu profile dump	显示不完整的或已完成的分析结果。

crashinfo force

要强制设备崩溃，请使用 **crashinfo force** 命令。

crashinfo force /noconfirm {**page-fault** | **watchdog** | **process** *process_ID*}

Syntax Description

page-fault	由于页面错误而强制崩溃。
watchdog	由于监视而强制崩溃。
process *process_ID*	强制 process_ID 指定的流程崩溃。使用 **show kernel process** 命令查看流程 ID。

Command Default

默认情况下，设备将崩溃信息文件保存到闪存。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您可以使用 **crashinfo force** 命令测试崩溃输出生成。在崩溃输出中，没有什么可以区分实际崩溃与由 **crashinfo force page-fault** 或 **crashinfo force watchdog** 命令导致的崩溃（因为这些都是真正的崩溃）。设备将在故障转储完成后重新加载。

注意事项 请勿在生产环境中使用 **crashinfo force** 命令。 **crashinfo force** 命令会使设备崩溃并强制其重新加载。

示例

以下示例因页面错误而强制崩溃。

```
> crashinfo force /noconfirm page-fault
```

Related Commands

命令	Description
clear crashinfo	清除崩溃信息文件的内容。
crashinfo test	测试设备将故障信息保存到闪存中文件的能力。
show crashinfo	显示崩溃信息文件的内容。

crashinfo test

要测试设备将崩溃信息保存到闪存中的文件的能力，请使用 **crashinfo test** 命令。

crashinfo test

Command History

版本	修改
6.1	引入了此命令。

使用指南

输入 **crashinfo test** 命令不会使设备崩溃。如果以前的崩溃信息文件已存在于闪存中，则覆盖该文件。

示例

以下示例展示崩溃信息文件测试的输出。

```
> crashinfo test
```

Related Commands

命令	Description
clear crashinfo	清除崩溃信息文件的内容。
crashinfo force	强制设备崩溃。
show crashinfo	显示崩溃信息文件的内容。

crypto ca trustpool export

要导出构成 PKI 信任池的证书，请使用 **crypto ca trustpool export** 命令。

crypto ca trustpool export *filename*

Syntax Description

filename	要在其中存储已导出信任池证书的文件。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令将活动信任池的全部内容复制到 PEM 编码格式的指定文件路径。

示例

```
> crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
>
> more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE
<More>
```

Related Commands

命令	Description
crypto ca trustpool import	导入构成 PKI 信任池的证书。
crypto ca trustpool remove	从 PKI 信任池中删除单个证书。
show crypto ca trustpool	显示 PKI 信任池。

crypto ca trustpool import

要导入构成 PKI 信任池的证书，请使用 **crypto ca trustpool import** 命令。

crypto ca trustpool import ［**clean**］ **url** *URL* **noconfirm** ［**signature-required**］
crypto ca trustpool import ［**clean**］ **default noconfirm**

Syntax Description

clean	在导入之前删除所有下载的信任池证书。
default	恢复设备的默认受信任 CA 列表。
noconfirm	抑制所有交互式提示。
signature-required	指示仅接受经过签署的文件。如果包括 **signature-required** 关键字，但签名不存在或无法验证，则导入失败。
url *url*	指定要导入的信任池文件的位置。 • [[*path/*]disk0:/filename] - 指示内部闪存。 • **disk***n***:/**[[*path/*]*filename*]- 表示可选的外部闪存驱动器，其中 *n* 指定驱动器编号。 • **smb:/**[[*path/*]*filename*] - 指示 UNIX 服务器本地文件系统。使用 LAN 管理器及类似的网络系统中的 Server Message Block（服务器消息块）文件系统协议包装数据并与其他系统交换信息。 • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]—The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode). • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*password*]@] *server*[/*path*]/*filename*[*;int=***;int=***interface_name*]] **-;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问安全复制 (SCP) 服务器。 • **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]—路径名不能包含空格。**;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问 TFTP 服务器。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令可在从 cisco.com 下载信任池捆绑包时验证文件上的签名。当从其他源下载捆绑包或其格式不支持签名时，有效签名不是必填项。用户获悉签名状态并且可以选择是否接受捆绑包。

可能出现的交互警告如下：

- 具有无效签名的思科捆绑包格式
- 非思科捆绑包格式
- 具有有效签名的思科捆绑包格式

注释 除非您通过其他方法验证了文件的合法性，否则在文件签名无法验证时请勿安装证书。

示例

以下示例恢复默认信任池。

```
> crypto ca trustpool import clean default noconfirm
```

Related Commands

命令	Description
crypto ca trustpool export	导出构成 PKI 信任池的证书。
crypto ca trustpool remove	从 PKI 信任池中删除单个证书。
show crypto ca trustpool	显示 PKI 信任池。

crypto ca trustpool remove

要从 PKI 信任池中删除单个指定证书，请使用 **crypto ca trustpool remove** 命令。

crypto ca trustpool remove *cert_fingerprint* ［**noconfirm**］

Syntax Description

cert_fingerprint	十六进制的证书指纹。
noconfirm	指定此关键字以抑制所有交互式提示。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例删除证书。

```
> crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0
```

Related Commands

命令	Description
clear crypto ca trustpool	从信任池删除所有证书。
crypto ca trustpool export	导出构成 PKI 信任池的证书。
crypto ca trustpool import	导入构成 PKI 信任池的证书。
show crypto ca trustpool	显示 PKI 信任池。

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。