d - r

debug

要显示给定功能的调试消息，请使用 **debug** 命令。要禁用调试消息的显示，请使用此命令的 **no** 形式。使用 **no debug all** 关闭所有调试命令。

debug *feature* [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

Syntax Description

feature	指定要为其启用调试的功能。若要查看可用功能，请使用 **debug ?** 命令获取 CLI 帮助。
subfeature	（可选）根据功能，您可以为一项或多项子功能启用调试消息。使用 ? 查看可用的子功能。
level	（可选）指定调试级别。级别可能并非对所有功能都适用。使用 ? 可查看可用的级别。

Command Default

默认调试级别为 1。

Command History

版本	修改
6.1	引入了此命令。
7.2	此命令已修改为包括用于路径监控的调试。

使用指南

由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以使用 **show console-output** 命令在常规 threat defense CLI 中查看输出。

示例

以下示例启用 DNS 调试并执行在诊断 CLI 中生成消息的操作。调试消息在“ERROR: % Invalid Hostname”消息之后开始。Press enter to get to the prompt. 然后，该示例将显示这些调试消息在 **show console-output** 显示屏中的外观。

```
> debug dns
debug dns enabled at level 1.

> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
firepower# ping www.example.com
                ^
ERROR: % Invalid Hostname
firepower# DNS: get global group DefaultDNS handle 1fa0b047
DNS: Resolve request for 'www.example.com' group DefaultDNS
DNS: No interfaces enabled
DNS: get global group DefaultDNS handle 1fa0b047
DNS: Resolve request for 'www.example.com' group DefaultDNS
DNS: No interfaces enabled

firepower# (press Ctrl+a, then d, to return to the regular CLI.)

Console connection detached.
> show console-output
... (output redacted)...
Message #75 : DNS: get global group DefaultDNS handle 1fa0b047
Message #76 : DNS: Resolve request for 'www.cisco.com' group DefaultDNS
Message #77 : DNS: No interfaces enabled
Message #78 : DNS: get global group DefaultDNS handle 1fa0b047
Message #79 : DNS: Resolve request for 'www.cisco.com' group DefaultDNS
Message #80 : DNS: No interfaces enabled
```

Related Commands

命令	Description
show debug	显示当前活动的调试设置。
undebug	禁用功能调试。此命令与 **no debug** 的效果相同。

debug packet-condition

要对必须调试的流应用过滤器，请使用 **debug packet-condition** 命令。要删除流上的过滤器，可使用此命令的 **no** 形式。使用 **no debug packet-condition** 以关闭流上的所有过滤器。

debug packet-condition [**position** *<line>*] **match** *<proto> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}* [*<src_operator> <ports> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}*] [*<dest_operator> <ports>*] [*<icmp_type>* | *<icmp6_type>*] [*connection <connection-id>*] [*unidirectional*]

Syntax Description

position *<line>*	指定过滤器应放置在现有过滤器列表中的位置。 *<line>* 表示数字。
match*<proto> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>| <ipv6>/<prefixlen>}*	指定过滤器的匹配条件。 *<proto>* 表示协议。 *{any|any4|any6|host<ip> |<ipv4> |<ipv4_mask> |<ipv6> /<prefixlen> }* 表示 IP 地址选项。
<src_operator><port> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>| <ipv6>/<prefixlen>}	（可选）指定源的端口或 IP 地址详细信息。
<dest_operator><port> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>| <ipv6>/<prefixlen>}	（可选）指定目标的端口或 IP 地址详细信息。
<icmp_type>|<icmp6_type>	（可选）指定连接的 ICMP 类型。
connection <connection-id>	（可选）指定正在进行的连接的连接 ID。
unidirectional	（可选）指定应仅对指定方向的数据包执行调试。如果未提供该变量，则默认行为是双向的，其中流量将与连接的正向和反向流量匹配。

Command Default

Command History

版本	修改
6.4	引入了此命令。
6.5	**debug packet condition** 命令已更改为 **debug packet-condition**。
6.6	**debug packet-condition** 命令已得到增强，以提供对持续连接的支持。

使用指南

由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以使用 **show console-output** 命令在常规 threat defense CLI 中查看输出。

示例

以下示例显示如何为必须调试的流设置过滤器。

```
> debug packet-condition position 7 match tcp 1.2.3.0 255.255.255.0 any4
> debug packet-condition match tcp 1.2.3.0 255.255.255.0 eq www any4 unidirectional
> debug packet-condition match connection 70856531
> no debug packet-condition match tcp 1.2.3.0 255.255.255 eq www unidirectional
```

Related Commands

命令	Description
debug packet-start	打开与调试日志数据库的连接，并开始将调试日志写入数据库。
debug packet-stop	关闭与调试日志数据库的连接，并停止将调试日志写入数据库。

debug packet-module

要为每个模块设置发送调试消息的级别，请使用 **debug packet-module** 命令。级别可以设置为介于 0（应急）到 7（调试）之间。设置级别后，系统将记录具有相同或更高严重性的所有消息。目前，仅支持 DAQ、PDTS、ACL 和 Snort 模块。

debug packet-module [**acl** | **all** | **daq** | **pdts** | **snort-engine** | **snort-fileprocessor** | **snort-firewall**] < *0-7* >

Syntax Description

acl	选择数据包处理路径中的访问控制策略。
all	选择数据包处理路径中的所有模块。
daq	选择数据包处理路径中的 DAQ 信息。
pdts	选择数据包处理路径中的 PDTS（数据平面传输/接收队列到 snort）通信。
snort-engine	选择数据包处理路径中的 Snort 信息。
snort-fileprocessor	选择数据包处理路径中的 Snort 文件处理器信息。
snort-firewall	选择数据包处理路径中的 Snort 防火墙信息。

Command History

版本	修改
6.4	引入了此命令。
6.5	**debug packet** 命令已更改为 **debug packet-module**。

使用指南

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以使用 **show console-output** 命令在常规 threat defense CLI 中查看输出。

示例

以下示例显示如何在数据包处理路径中设置 DAQ 信息的级别。

```
> debug packet daq 6
```

Related Commands

命令	Description
debug packet-start	打开与调试日志数据库的连接，并开始将调试日志写入数据库。

命令	Description
debug packet-stop	关闭与调试日志数据库的连接，并停止将调试日志写入数据库。

debug packet-module trace

要启用模块级数据包跟踪，请使用 **debug packet-module trace** 命令。

debug packet-module trace

Command History

版本	修改
6.6	引入了此命令。

使用指南

由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以使用 **show console-output** 命令在常规 threat defense CLI 中查看输出。

示例

以下示例显示如何启用模块级数据包跟踪。

```
> debug packet-module trace
```

以下是 **debug packet-module trace** 命令的输出示例：

```
ID         | Details                                                                 | Time (ns)

---------- -------------------------------------------------------------------------
------------------------------
6525759    | TCP        74.125.24.156      : 443   -> 192.168.0.31      : 58280 | 19-02-2020
 06:48:43.050675868
```

此外，可以使用以下命令获取数据包的详细信息。

```
> show packet debugs module trace packet-id 6525759

Module: tcp-normalizer
Entry Time: 19-02-2020 06:48:43.050675868(ns)
****************************************
Module: translate
Entry Time: 19-02-2020 06:48:43.050684452(ns)
****************************************
Module: inspect_snort
Entry Time: 19-02-2020 06:48:43.050688028(ns)
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.050691843(ns)
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.051417112(ns)
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.051421642(ns)
```

```
*****************************************
Module: tcp-normalizer
Entry Time: 19-02-2020 06:48:43.051424980(ns)
*****************************************
Module: adjacency
Entry Time: 19-02-2020 06:48:43.051438331(ns)
*****************************************
Module: fragment
Entry Time: 19-02-2020 06:48:43.051442861(ns)
*****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750763893(ns)
*****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750815391(ns)
*****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750831365(ns)
*****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750843286(ns)
*****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750889778(ns)
*****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750911474(ns)
*****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750942230(ns)
*****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.750986576(ns)
*****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.750999689(ns)
*****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751020193(ns)
*****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751051425(ns)
*****************************************
Module: snort_firewall
Entry Time: 19-02-2020 06:48:43.751075029(ns)
*****************************************
Module: snort_firewall
Entry Time: 19-02-2020 06:48:43.751084804(ns)
*****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751099348(ns)
*****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751118421(ns)
*****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751137018(ns)
*****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751152753(ns)
*****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751164197(ns)
*****************************************
```

```
Module: daq
Entry Time: 19-02-2020 06:48:43.751177072(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751186609(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751203775(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751224517(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751236677(ns)
****************************************
```

Related Commands

命令	Description
show packet debugs module trace	显示从每个模块收集的所有调试跟踪的列表。
debug packet-start	打开与调试日志数据库的连接，并开始将调试日志写入数据库。
debug packet-stop	关闭与调试日志数据库的连接，并停止将调试日志写入数据库。

debug packet-start

要开始调试数据包并将调试日志写入调试日志数据库，请使用 **debug packet-start** 命令。

debug packet-start

Command History

版本	修改
6.4	引入了此命令。
6.5	**debug packet start** 命令已更改为 **debug packet-start**。

使用指南

debug packet-start 打开与调试日志数据库的连接。除非调用此命令，否则不会将调试日志写入数据库。

示例

以下示例显示如何开始调试数据包：

```
> debug packet-start
```

Related Commands

命令	Description
debug packet-stop	关闭与调试日志数据库的连接，并停止将调试日志写入数据库。

debug packet-stop

要停止数据包调试并停止将调试日志写入调试日志数据库，请使用 **debug packet-stop** 命令。

debug packet-stop

Command History

版本	修改
6.4	引入了此命令。
6.5	**debug packet stop** 命令已更改为 **debug packet-stop**。

使用指南

debug packet-stop 关闭与调试日志数据库的连接。

示例

以下示例显示如何停止调试数据包：

```
> debug packet-stop
```

Related Commands

命令	Description
debug packet-start	打开与调试日志数据库的连接，并开始将调试日志写入数据库。

delete

要从闪存中删除文件，请使用 **delete** 命令。

delete /noconfirm ［**/recursive**］［**/replicate**］［**disk0:** | **disk***n***:** | **flash:**］［*path/*］*filename*

Syntax Description

/noconfirm	不提示确认。
/recursive	（可选）循环删除所有子目录中指定的文件。
/replicate	（可选）删除备用设备上指定的文件。
disk0:	（可选）指定内部闪存。
disk*n***:**	（可选）表示可选的外部闪存驱动器，其中 n 指定驱动器编号。这通常是 disk1：
filename	指定要删除的文件的名称。
flash:	（可选）指定内部闪存。此关键字与 **disk0** 相同。
path/	（可选）指定文件的路径。

Command Default

如果不指定目录，则默认为当前工作目录。

Command History

版本	修改
6.1	引入了此命令。

使用指南

如果未指定路径，将从当前工作目录删除文件。删除文件时支持通配符。

示例

以下示例展示如何从当前工作目录中删除名为 test.cfg 的文件：

```
> delete /noconfirm test.cfg
```

Related Commands

命令	Description
cd	将当前工作目录更改为指定的目录。
dir	列出当前目录中的文件。
rmdir	删除文件或目录。

dig

要查找完全限定域名 (FQDN) 的 IP 地址，请使用 **dig** 命令。

dig *hostname*

Syntax Description

hostname	要查找其 IP 地址的主机的完全限定域名。例如，www.example.com。

Command History

版本	修改
7.1	引入了此命令。它取代了 **nslookup** 命令。

使用指南

某些允许完全限定域名的命令无法使用为管理接口配置的 DNS 服务器来查找名称的 IP 地址。如果没有为通过数据接口的命令配置 DNS 服务器，请使用 命令确定 IP 地址，然后在 **dig** 命令中使用 IP 地址。

dig 命令仅通过管理接口工作，并从为管理接口配置的 DNS 服务器返回信息。如果为数据接口配置不同的服务器，则在通过数据接口的命令上使用 FQDN 可能会返回不同的 IP 地址，或者如果这些 DNS 服务器无法解析名称，则根本不会返回 IP 地址。

示例

以下示例查找 FQDN www.example.com 的 IP 地址。地址在输出的 ANSWER 部分突出显示。输出末尾附近的 SERVER 指示显示返回解析的 DNS 服务器的 IP 地址（本示例中的 IP 地址已清理）。

信头中的 NOERROR 状态表示请求成功；任何其他值均表示错误。例如，NXDOMAIN 表示响应的 DNS 服务器中不存在域名。您可以在互联网上搜索有关读取 Linux dig 命令输出的更多详细信息。

```
> dig www.example.com
; <<>> DiG 9.11.4 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14008
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 88335c9f3dc2ca124e36b5eb60db9067b6cae4de2ea5bffb (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        0       IN      A       93.184.216.34
;; AUTHORITY SECTION:
example.com.            58911   IN      NS      a.iana-servers.net.
example.com.            58911   IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
```

```
a.iana-servers.net.     0       IN      A       199.43.135.53

;; Query time: 12 msec
;; SERVER: 10.163.47.11#53(10.163.47.11)
;; WHEN: Tue Jun 29 21:28:07 UTC 2021
;; MSG SIZE  rcvd: 152
```

dir

使用 dir 命令显示目录中的内容。

dir ［**/all**］［**all-filesystems**］［**/recursive**］［ **disk0:** | **disk***n***:** | **flash:** | **system:**］［*path*］［*filename*］

Syntax Description

/all	（可选）显示所有文件。
/recursive	（可选）递归显示目录内容。
all-filesystems	（可选）显示所有文件系统的文件。
disk0:	（可选）指定内部闪存，后跟冒号。
disk*n***:**	（可选）表示可选的外部闪存驱动器，其中 *n* 指定驱动器编号。这通常是 disk1：
flash:	（可选）显示默认闪存分区的目录内容。
path	（可选）指定特定路径。
filename	（可选）指定文件的名称。
system:	（可选）显示文件系统的目录内容。

Command Default

如果不指定目录，则默认为当前工作目录。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何显示目录内容：

```
> dir
Directory of disk0:/
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

Related Commands

命令	Description
cd	将当前工作目录更改为指定的目录。

命令	Description
pwd	系统随即会显示当前工作目录。
mkdir	Creates a directory.
rmdir	删除目录。

dns update

要不等待 DNS 轮询计时器到期即启动 DNS 查找以解析指定的主机名，请在特权 EXEC 模式下使用 **dns update** 命令。

dns update ［**host** *fqdn_name*］［**timeout seconds** *number*］

Syntax Description

host *fqdn_name*	指定要运行 DNS 更新的主机的完全限定域名。
timeout seconds *number*	指定查找操作的超时时间（以秒为单位），范围为 3-30。默认值为 30。

Command History

版本	修改
6.3	引入了此命令。

使用指南

此命令立即启动 DNS 查找以解析指定的主机名，而不等待 DNS 轮询计时器到期。在不指定主机名的情况下运行DNS更新时，访问控制规则中使用的所有名称（称为“已激活”）都将被解析。该命令完成运行后，系统将在命令提示符下显示[已完成]，然后生成系统日志消息。

示例

以下示例对访问控制规则中使用的所有 FQDN 执行 DNS 更新。

```
> dns update
INFO: update dns process started
> [Done]
```

Related Commands

命令	Description
clear dns	删除 FQDN 网络对象 DNS 解析。
show dns	显示 FQDN 网络对象 DNS 解析。

eotool commands

只能在思科技术支持中心的指导下使用 **eotool** 命令。

exit

要退出 CLI，请使用 **exit** 命令。

exit

Command History

版本	修改
6.1	引入了此命令。

使用指南

在常规 CLI 中， **exit** 和 **logout** 命令执行相同的操作，即关闭与设备的 SSH 会话。

当您处于专家模式时， **exit** 会离开专家模式并返回到常规 CLI。

当您处于诊断 CLI (**system support diagnostic-cli**) 中时， **exit** 命令还会将您从特权 EXEC 模式移回用户 EXEC 模式。

示例

以下示例显示如何使用 **exit** 命令关闭与 CLI 的 SSH 连接。

```
> exit
```

以下示例显示如何使用 **exit** 命令 go 从诊断 CLI 中的特权 EXEC 模式（在提示符中以 # 符号表示）返回到用户 EXEC 模式。您可以忽略注销消息，您的 CLI 会话保持活动状态。

```
firepower# exit
Logoff
Type help or '?' for a list of available commands.
firepower>
```

Related Commands

命令	Description
logout	从 CLI 会话注销。

expert

要进入某些程序所需的专家模式，请使用 **expert** 命令。

expert

Command History

版本	修改
6.1	引入了此命令。

使用指南

仅当书面程序指出必须使用或思科技术支持中心告知使用专家模式时，才使用专家模式。

⚠

注意 您可能能够在专家模式下执行其结果未反映在 设备管理器中的命令。仅在专家模式下使用记录的命令，或按照思科技术支持的指示使用命令，以避免出现意外结果。

示例

以下示例显示如何进入和退出专家模式。专家模式提示符显示 username@hostname 信息。

```
> expert
admin@firepower:~$
admin@firepower:~$ exit
logout
>
```

Related Commands

命令	Description
exit	从专家模式退出。

failover active

要将备用设备 切换到主用状态，请使用 **failover active** 命令。要将主用设备 切换到备用状态，请使用此命令的 **no** 形式。

failover active
no failover active

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **failover active** 命令从备用设备发起故障转移，或使用 **no failover active** 命令从主用设备发起故障转移。您可以使用此功能使故障设备恢复服务，或强制主用设备离线以进行维护。如果不使用“状态故障转移”，所有活动连接都将被丢弃，并且在进行故障切换之后必须由客户端重新建立。

示例

以下示例将备用设备切换为主用设备：

```
> failover active
```

Related Commands

命令	Description
failover reset	使设备从故障状态变为备用状态。

failover exec

要在故障转移对中的特定设备上执行命令，请使用 **failover exec** 命令。

failover exec {**active** | **standby** | **mate**} *cmd_string*

Syntax Description

active	指定在故障转移对中的主用设备 上执行命令。
cmd_string	要执行的命令。有关支持的命令，请参阅 CLI 帮助。
mate	指定在故障转移对等设备上执行命令。
standby	指定在故障转移对中的备用设备 上执行命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您可以使用 **failover exec** 命令向故障转移对中的特定设备发送命令。

命令的输出显示在当前终端会话中，所以您可以使用 **failover exec** 命令在对等设备上发出 **show** 命令并在当前终端中查看结果。

您必须拥有足够在本地设备上执行命令的权限才能在对等设备上执行命令。

限制

- 命令完成和情景帮助对于 *cmd_string* 参数中的命令不可用。
- 不能将 **debug** (**undebug**) 命令与 **failover exec** 命令配合使用。
- 备用设备处于故障状态时，如果这种故障是因服务卡故障引起，则该设备仍可以从 **failover exec** 命令接收命令；否则远程命令执行失败。
- 不能输入递归 **failover exec** 命令，例如 **failover exec mate failover exec mate** 命令。
- 需要用户输入或确认的命令必须使用 **/nonconfirm** 选项。

示例

以下示例使用 **failover exec** 命令显示故障转移对等设备的故障转移配置。命令在主要设备（主用设备）上执行，因此所显示的信息来自辅助设备（备用设备）。

```
> failover exec mate show running-config failover
failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
```

```
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
```

以下示例使用 **failover exec** 命令将 **show interface** 命令发送到备用设备：

```
> failover exec standby show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
...
```

以下示例展示当向对等设备发出非法命令时返回的错误消息：

```
> failover exec mate bad command
bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

以下示例展示在禁用故障转移的情况下使用 **failover exec** 命令时返回的错误消息：

```
> failover exec mate show failover
ERROR: Cannot execute command on mate because failover is disabled
```

Related Commands

命令	Description
debug fover	显示故障转移相关的调试消息。
debug xml	显示 **failover exec** 命令使用的 XML 解析器的调试消息。
show failover exec	显示 **failover exec** 命令模式。

failover reload-standby

要强制备用设备重新启动，请使用 **failover reload-standby** 命令。

failover reload-standby

Command History

版本	修改
6.1	引入了此命令。

使用指南

当故障切换设备不同步时，请使用此命令。备用设备会重新启动并在完成启动后与主用设备重新同步。

示例

以下示例展示如何在主用设备上使用 **failover reload-standby** 命令强制备用设备重新启动：

```
> failover reload-standby
```

failover reset

要将故障设备恢复为正常状态，请使用 **failover reset** 命令。

failover reset

Command History

版本	修改
6.1	引入了此命令。

使用指南

failover reset 命令允许您将故障设备 切换为无故障状态。 **failover reset** 命令可在任一设备上输入，但我们建议您始终在主用设备上输入该命令。在主用设备输入 **failover reset** 命令将使备用设备“无故障”。

可以使用 **show failover** 命令显示设备的故障转移状态。

示例

以下示例展示将故障设备切换为无故障状态：

```
> failover reset
```

Related Commands

命令	Description
show failover	显示有关设备的故障转移状态的信息。

file copy

要通过 FTP 将文件从公共目录传输到远程主机，请使用 **file copy** 命令。

file copy *host_name user_id path filename_1* [*filename_2 . . . filename_n*]

Syntax Description

host_name	指定目标远程主机的名称或 IP 地址。
user_id	指定远程主机上的用户。
path	指定远程主机上的目的路径。
filename_1 through *filename_n*	指定要从公共目录传输的文件的名称。如果指定了多个文件名，则必须以空格分隔它们。此参数支持通配符。

Command Default

此命令仅从系统写入故障排除文件的通用目录传输文件。

Command History

版本	修改
6.0.1	引入了此命令。

示例

此示例将公共目录中的所有文件传输到 **/pub** 通过用户 **jdoe**访问的远程主机 **sentinel** 上的目录：

```
> file copy sentinel jdoe /pub *
```

Related Commands

命令	Description
file list	列出公共目录中的文件。
file delete	从公共目录中删除文件。
file secure-copy	通过 SCP 传输公共目录中的文件。

file delete

要清除公共目录中的文件，请使用 **file delete** 命令。

file delete *filename_1* [*filename_2 ... filename_n*]

Syntax Description

filename_1 through *filename_n*	指定要从公用目录中删除的文件的名称。如果指定了多个文件名，则必须以空格分隔它们。此参数支持通配符。

Command Default

此命令仅对系统写入故障排除文件的通用目录中的文件起作用。

Command History

版本	修改
6.0.1	引入了此命令。

示例

此示例删除单个文件：

```
> file delete 10.83.170.31-43235986-2363-11e6-b278-aff0a43948fe-troubleshoot.tar.gz
```

Related Commands

命令	Description
file list	列出公共目录中的文件。
file copy	通过 FTP 传输公共目录中的文件。
file secure-copy	通过 SCP 传输公共目录中的文件。

file list

要列出公共目录中的文件，请使用 **file list** 命令。

file list ［*filename_1 . . . filename_n*］

Syntax Description

filename_1 through *filename_n*	指定要从公共目录列出的文件的名称。如果指定了多个文件名，则必须以空格分隔它们。此参数支持通配符。

Command History

版本	修改
6.0.1	引入了此命令。

使用指南

此命令仅列出系统写入故障排除文件的通用目录中的文件。如果未指定文件名，则列出公共目录中的所有文件。

示例

此示例列出了通用目录的内容：

```
> file list
May 26 17:46        137474048 /core_1464284811_rackham-sfr.cisco.com_diskmanager_11.21145
Jun 27 20:36       1464696832 /core_1467059810_rackham-sfr.cisco.com_lina_6.21293
```

Related Commands

命令	Description
file copy	通过 FTP 传输公共目录中的文件。
file delete	从公共目录中删除文件。
file secure-copy	通过 SCP 传输公共目录中的文件。

file secure-copy

要通过 SCP 将文件从通用目录传输到远程主机，请使用 **file secure-copy** 命令。

file secure-copy *host_name user_id path filename_1* [*filename_2 . . . filename_n*]

Syntax Description

host_name	指定目标远程主机的名称或 IP 地址。
user_id	指定远程主机上的用户。
path	指定远程主机上的目的路径。
filename_1 through *filename_n*	指定要从公共目录传输的文件的名称。如果指定了多个文件名，则必须以空格分隔它们。此参数支持通配符。

Command Default

此命令仅从系统写入故障排除文件的通用目录传输文件。

Command History

版本	修改
6.0.1	引入了此命令。

示例

此示例将公共目录中的所有文件传输到 **/tmp** 通过用户 **jdoe**访问的远程主机 **101.123.31.1** 上的目录：

```
> file secure-copy 101.123.31.1 jdoe /tmp *
```

Related Commands

命令	Description
file copy	通过 FTP 传输公共目录中的文件。
file delete	从公共目录中删除文件。
file list	列出公共目录中的文件。

fsck

要执行文件系统检查并修复损坏，请使用 **fsck** 命令。

fsck /noconfirm disk*n*:

Syntax Description

disk*n*:	指定闪存驱动器，其中 *n* 是驱动器编号。
/noconfirm	指定命令在不提示的情况下运行。此关键字是必需的。

Command History

版本	修改
6.1	引入了此命令。

使用指南

fsck 命令检查并尝试修复损坏的文件系统。请在尝试更永久性的修复过程之前使用此命令。

如果 FSCK 实用程序修复磁盘损坏实例（例如由于电源故障或异常关闭导致的损坏），则会创建名为 FSCKxxx.REC 的恢复文件。这些文件可以包含 FSCK 在运行时恢复的文件的一小部分或整个文件。在极少数情况下，您可能需要检查这些文件以恢复数据；通常不需要这些文件，可以将其安全删除。

注释 FSCK 实用程序在启动时自动运行，因此，即使没有手动输入 **fsck** 命令，您也可能看到这些恢复文件。

示例

以下示例展示如何检查闪存的文件系统：

```
> fsck /noconfirm disk0:
```

Related Commands

命令	Description
delete	删除用户可见的所有文件。
erase	删除所有文件并格式化闪存。
format	格式化文件系统。

help

要显示指定命令的帮助信息，请使用 **help** 命令。

help { 命令 | **?**}

Syntax Description

?	显示所有可获得帮助的命令。
command	指定为其显示 CLI 帮助的命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

help 命令显示有关某些命令的帮助信息。您可以输入 **help** 命令后跟命令名，以获取某个命令的帮助。如果不指定命令名称并输入 **?**，则列出所有具有帮助的命令。

您还可以通过输入？输入部分命令后。这将显示命令字符串中该位置的有效参数。

示例

以下示例展示如何显示 **traceroute** 命令的帮助：

```
> help traceroute
USAGE:
        traceroute <destination> [source <src_address|src_intf>]
                   [numeric] [timeout <time>] [ttl <min-ttl> <max-ttl>]
                   [probe <probes>] [port <port-value>] [use-icmp]
DESCRIPTION:
traceroute      Print the route packets take to a network host
SYNTAX:
destination     Address or hostname of destination
src_address     Source address used in the outgoing probe packets
src_intf        Interface through which the destination is accessible
numeric         Do not resolve addresses to hostnames
time            The time in seconds to wait for a response to a probe
min-ttl         Minimum time-to-live value used in probe packets
max-ttl         Maximum time-to-live value used in probe packets
probes          The number of probes to send for each TTL value
port-value      Base UDP destination port used in probes
use-icmp        Use ICMP probes instead of UDP probes
```

history

要显示当前会话的命令行历史记录，请使用 **history** 命令。

history *limit*

Syntax Description

limit	历史记录列表的大小（以条目数表示）。要将大小设置为无限制，即查看完整历史记录，请输入 0。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您还可以使用向上箭头滚动浏览过去的命令。

历史记录视图包括命令输入顺序的序列号。

示例

以下示例显示命令历史记录。

```
> history 0
   48  show environment
   49  show network-static-routes
   50  show network
   51  show running-config
   52  show service-policy
   53  show ntp
   54  show cpu
   55  show memory
   56  history 0
>
```

logging savelog

要将日志缓冲区保存到闪存，请使用 **logging savelog** 命令。

logging savelog ［*savefile*］

Syntax Description

savefile	（可选）已保存日志的文件名。如果您未指定文件名，则系统将使用如下所示的默认时间戳格式保存日志文件： `LOG-YYYY-MM-DD-HHMMSS.TXT` 其中 *YYYY* 是年，*MM* 是月，*DD* 是月日期，*HHMMSS* 是时间（以小时、分钟和秒为单位）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

在您将日志缓冲区保存到闪存之前，您必须启用日志记录到缓冲区；否则日志缓冲区始终不会将数据保存到闪存。但是，如果配置的日志记录缓冲区大小超过 2 MB，则内部日志缓冲区不会写入闪存。使用 管理中心 （远程）或 设备管理器 （本地）配置缓冲区日志记录。

注释 **logging savelog** 命令不会清除缓冲区。要清除缓冲区，请使用 **clear logging buffer** 命令。

示例

以下示例使用文件名 latest-logfile.txt 将日志缓冲区保存到闪存：

```
> logging savelog latest-logfile.txt
>
```

Related Commands

命令	Description
clear logging buffer	清除包含的所有系统日志消息的日志缓冲区。
copy	将文件从一个位置复制到另一个位置，包括复制到 TFTP 或 FTP 服务器。
delete	从磁盘分区删除文件（如已保存的日志文件）。

logout

要退出 CLI，请使用 **logout** 命令。

logout

Command History

版本	修改
6.1	引入了此命令。

使用指南

logout 命令允许您注销设备并结束 CLI 会话。您也可以使用 **exit** 命令。

示例

以下示例显示如何注销设备：

```
> logout
```

memory caller-address

要为呼叫跟踪或主叫方 PC 配置特定范围的程序内存，以帮助隔离内存问题，请使用 **memory caller-address** 命令。调用方 PC 是调用内存分配基元的程序的地址。要删除地址范围，请使用此命令的 no 形式。

memory caller-address *startPC endPC*
no memory caller-address

Syntax Description

endPC	指定内存块的结束地址范围。
startPC	指定内存块的开始地址范围。

Command Default

实际调用方 PC 会被记录以用于内存跟踪。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **memory caller-address** 命令将内存问题隔离到特定的内存块。

在某些情况下，内存分配基元的实际调用方 PC 是程序中许多位置使用的已知库功能。要隔离程序中的个别位置，请配置库功能的开始和结束程序地址，从而记录库功能调用方的程序地址。

注释 启用调用方地址跟踪时，设备的性能可能会临时下降。

示例

以下示例显示了使用 **memory caller-address** 命令配置的地址范围，以及 **show memory caller-address** 命令的结果显示：

```
> memory caller-address 0x00109d5c 0x00109e08
> memory caller-address 0x009b0ef0 0x009b0f14
> memory caller-address 0x00cf211c 0x00cf4464
> show memory caller-address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

Related Commands

命令	Description
memory profile enable	启用对内存使用（内存分析）的监控。

命令	Description
memory profile text	配置要分析的内存的文本范围。
show memory	显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要。
show memory binsize	显示为特定存储空间分配的数据块的摘要信息。
show memory profile	显示设备内存使用情况（分析）的信息。
show memory caller-address	显示设备上配置的地址范围。

memory delayed-free-poisoner

使用 **memory delayed-free-poisoner** 命令设置延迟可用内存毒化工具的参数。要启用延迟的可用内存毒化工具，请使用 **memory delayed-free-poisoner enable** 命令。要禁用 delayed free-memory poisoner 工具，请使用此命令的 **no** 形式。delayed free-memory poisoner 工具可用于监视可用的内存在被应用释放后有何变化。

memory delayed-free-poisoner {**enable** | **desired-fragment-count** *frag_count* | **desired-fragment-size** *frag-size* | **threshold** *heap_use_percent* | **validate** | **watchdog-percent** *watchdog_limit*}
no memory delayed-free-poisoner enable

Syntax Description

enable	启动延迟的可用内存毒化工具。
desired-fragment-count *frag_count*	设置要在毒化器队列中保留的内存分段数。合法值范围为 0 到 8192；默认值为 16
desired-fragment-size *Frag-size*	设置要保留在毒化器队列中的连续可用内存分段的大小（以字节为单位）。合法值范围为 0 到 268435456；默认值为 102400。
threshold *heap_use_percent*	设置系统将从毒化器队列中释放内存的系统内存使用百分比阈值，范围为 0 到 100。默认值为 100。
validate	强制验证 delay-free-poisoner 队列中的所有元素。
watchdog-percent *watchdog_limit*	将监视器限制设置为监视器阈值的百分比，即 15 秒。值范围为 10 到 100。默认值为 50。

Command Default

memory delayed-free-poisoner enable 命令默认禁用。

desired-fragment-count 默认值为 16。

desire-fragment-size 默认值为 102400。

watchdog-percent 默认值为 50。

Command History

版本	修改
6.1	引入了此命令。

使用指南

启用 delayed free-memory poisoner 工具对内存使用和系统性能有重大影响。此命令只能在思科技术支持中心的监督下使用。在大量使用系统的生产环境下不应该运行此工具。

启用此工具时，要求释放设备上运行的应用可用内存的请求将写入 FIFO 队列。当每个请求写入毒化器队列时，低层内存管理不需要的每个关联内存字节会写入值 0xcc 而“中毒”。

释放的内存请求会一直保留在队列中，直到应用要求的内存超过系统可用内存。当需要更多内存时，毒化器至少会在其队列中查找 **desired-fragment-count** 内存缓冲区，从 **desired-fragment-size** 队列字

节中提取该内存，并对其进行验证。您可以通过更改 **desired-fragment-size** 和 **desired-fragment-count** 的值来调整毒化器满足大内存请求所需的时间。

如果内存未经修改，将返回到系统可用内存池，然后该毒化器从发出初始请求的应用重新发出内存请求。此流程会重复到为请求的应用释放足够的内存为止。

如果中毒的内存已修改，则系统发生故障并产生诊断输出来确定故障的原因。

延迟释放毒化器包括一种监视机制，可防止流程过度使用资源。监视器阈值是15秒，当流程在这段时间内持续执行而不放弃 CPU 时，中毒者会强制系统崩溃。

您可以通过设置监视器限制（表示15秒看门狗阈值的百分比）来调整监视器行为；默认值为50%。因此，当延迟释放毒化器处于活动状态时，如果流程在不放弃 CPU 的情况下连续执行 7.5 秒，则该流程的进一步内存分配请求将失败，直到重新安排该进程。您可以通过更改监视程序限制的值来调整此行为。

为防止内存碎片过多并减少系统 CPU 负载，可以设置毒化器自动将内存从其队列释放到 **threshold** 系统内存池的可用内存使用率百分比。（默认情况下，在系统内存耗尽之前，投毒器不会从其队列中释放内存。）

delayed free-memory poisoner 工具自动定期验证队列的所有元素。您还可以使用 **memory delayed-free-poisoner validate** 命令手动启动验证。如果有元素包含非预期的值，则系统发生故障并产生诊断输出来确定故障的原因。如果没有出现非预期的值，这些元素将保留在队列中被工具正常处理； **memory delayed-free-poisoner validate** 命令不会使队列中的内存返回到系统内存池。

若使用此命令的**no**形式，则队列中请求引用的所有内存不经过验证即返回到可用内存池，同时清除所有统计数据计数器。

示例

以下示例启用 delayed free-memory poisoner 工具：

```
> memory delayed-free-poisoner enable
```

下面是 delayed free-memory poisoner 工具检测到非法内存重用时的示例输出：

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.
    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15
Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........
An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.
```

```
assertion "0" failed: file "delayfree.c", line 191
```

下表描述了输出的主要部分。

表 *1:* 非法内存使用输出说明

字段	Description
heap region	可供请求的应用使用的地址区域以及内存区域大小。这与请求的大小不同，根据发出内存请求时系统分配内存的方式，它可能小于请求的大小。
memory address	内存中检测到故障的位置。
byte offset	字节偏移与堆区域的开头有关，可在结果用于保存以此地址开头的数据结构时用于查找修改的字段。0 或大于堆区域字节计数的值可能表示问题是低层堆数据包中的值异常。
allocated by/freed by	指示最近发出的、涉及此特定内存区域的 malloc/calloc/realloc 和释放调用的地址。
Dumping...	一个或两个内存区域的转储，具体取决于检测到的故障相距堆内存区域开头的距离。任何系统堆信头后的八个字节是此工具用来保存各系统报头散列值以及队列链路的内存。区域中在遇到任何系统堆尾部之前的所有其他字节应设置为 0xcc。

Related Commands

命令	Description
clear memory delayed-free-poisoner	清除 delayed free-memory poisoner 工具队列和统计信息。
show memory delayed-free-poisoner	显示 delayed free-memory poisoner 工具队列使用摘要。

memory logging

要启用内存日志记录，请使用**memory logging**命令。要禁用内存日志记录功能，请使用此命令的**no**形式。

memory logging 1024-4194304 ［**wrap** ［**size** ［**1-2147483647**］ | **process** *process-name*］
no memory logging

Syntax Description

1024-4194304	指定内存日志记录缓冲区中的日志记录条目数。这是唯一需要指定的参数。
process *process-name*	指定要监控的进程。 注释 Checkheaps 进程被当作一个进程完全忽略，因为它以非标准方式使用内存分配器。
size 1-2147483647	指定要监控的条目的大小和数量。
wrap	回绕时保存缓冲区。缓冲区只能保存一次。如果它wrap多次，会被覆写。当缓冲区wrap时，系统会将触发器发送到事件管理器，以启用数据保存。

Command History

版本	修改
6.1	引入了此命令。

使用指南

要更改内存日志记录参数，必须将其禁用，然后重新启用。使用 **show memory logging** 命令查看日志。

示例

以下示例启用内存日志记录：

```
> memory logging 202980
```

Related Commands

命令	Description
show memory logging	显示内存日志记录结果。

memory profile enable

要启用内存使用情况监控（内存分析），请使用 **memory profile enable** 命令。要禁用内存分析功能，请使用此命令的 **no** 形式。

memory profile enable ［**peak** *peak_value*］
no memory profile enable ［**peak** *peak_value*］

Syntax Description

peak *peak_value*	指定内存使用阈值，达到此阈值就会在峰值使用缓冲区中保存内存使用率快照。此缓冲区的内容以后可用来分析以确定系统的峰值内存需求。

Command Default

内存分析默认禁用。

Command History

版本	修改
6.1	引入了此命令。

使用指南

在启用内存分析之前，必须先使用 **memory profile text** 命令配置要分析的内存文本范围。

部分内存由分析系统保留，直到您输入 **clear memory profile** 命令。请参阅 **show memory profile status** 命令的输出。

注释 启用内存分析时，设备的性能可能会临时下降。

示例

以下示例启用内存分析：

```
> memory profile enable
```

Related Commands

命令	Description
memory profile text	配置要分析的内存的文本范围。
show memory profile	显示设备内存使用情况（分析）的信息。

memory profile text

要配置内存的程序文本范围，请使用 **memory profile text** 命令。要禁用，请使用此命令的 no 形式。

memory profile text {*startPC endPC* | **all**} *resolution*
no memory profile text {*startPC endPC* | **all**} *resolution*

Syntax Description

all	指定内存块的整个文本范围。
endPC	指定内存块的整个文本范围。
resolution	您必须为源文本区域设置跟踪分辨率，范围为 1-44582263。
startPC	指定内存块的开始文本范围。

Command History

版本	修改
6.1	引入了此命令。

使用指南

如果文本范围小，分辨率“4”通常便可跟踪对指令的调用。如果文本范围较大，低分辨率对第一遍可能够了，但在下一遍时范围可能需要缩小到一组更小的区域。

使用 **memory profile text** 命令输入文本范围后，必须输入 **memory profile enable** 命令以开始内存分析。内存分析默认禁用。

注释 启用内存分析时，设备的性能可能会临时下降。

示例

以下示例显示如何在分辨率为 100 的条件下配置要分析的内存文本范围。

```
> memory profile text all 100
```

以下示例显示文本范围的配置和内存分析的状态 (OFF)：

```
> show memory profile status
InUse profiling: OFF
Peak profiling: OFF
Memory used by profile buffers: 0 bytes
Profile:
0x00007efc3e0227a8-0x00007efc40aa1f8e(00000100)
```

注释 要开始内存分析，必须输入 **memory profile enable** 命令。内存分析默认禁用。

Related Commands

命令	Description
clear memory profile	清除内存分析功能保留的缓冲区。
memory profile enable	启用对内存使用（内存分析）的监控。
show memory profile	显示设备内存使用情况（分析）的信息。

memory tracking

要启用堆内存请求跟踪，请使用 **memory tracking** 命令。要禁用内存日志跟踪功能，请使用此命令的 **no** 形式。

memory tracking {**enable** | **allocates-by-threshold** *min_allocates* | **bytes-threshold** *min_bytes* | **filter-from-address-pool** *address*}
no memory tracking enable

Syntax Description

enable	启用内存跟踪。
allocates-by-threshold *min_allocates*	调用方的地址池条目必须至少进行此数量的分配调用，范围为 0-4294967295。
bytes-threshold *min_bytes*	调用方的地址池条目必须至少消耗这么多字节的内存才能包含在内，范围为 0-4294967295。
filter-from-address-pool *address*	排除此地址的地址池条目。要确定地址，请先启用跟踪，然后使用 show memory tracking address。在“内存跟踪地址池”列表中查找“分配者”地址。例如，如果您看到以下内容： ...allocated by 0x00007efc3f80e508 您可以使用以下命令将其排除： **filter-from-address-pool 0x00007efc3f80e508**

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例启用跟踪堆内存请求：

```
> memory tracking enable
```

Related Commands

命令	Description
clear memory tracking	清除所有当前收集的信息。
show memory tracking	显示内存跟踪结果。

more

要显示文件的内容，请使用 **more** 命令。

more [**/ascii** | **/binary** | **/ebcdic** | **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **tftp:**] *filename*

Syntax Description

/ascii	（可选）在二进制模式下显示二进制文件和 ASCII 文件。
/binary	（可选）在二进制模式下显示任何文件。
/ebcdic	（可选）以 EBCDIC 显示二进制文件。
disk0:	（可选）显示内部闪存上的文件。
disk1:	（可选）显示外部闪存卡上的文件。
filename	指定要显示的文件的名称。
flash:	（可选）指定内部闪存，后跟冒号。在ASA 5500 系列自适应安全设备中，**flash** 关键字是 **disk0**的别名。
ftp:	（可选）显示 FTP 服务器上的文件。
http:	（可选）显示网站上的文件。
https:	（可选）显示安全网站上的文件。
tftp:	（可选）显示 FTP 服务器上的文件。

Command Default

ASCII 模式。

Command History

版本	修改
6.1	引入了此命令。

使用指南

system support view-files 命令是查找和查看日志文件的更好选择。

示例

以下示例显示如何显示名为“test.cfg”的本地文件的内容：

```
> more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
```

```
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

Related Commands

命令	Description
cd	更改为指定的目录。
pwd	系统随即会显示当前工作目录。
system support view-files	查找并查看日志文件的内容。

nslookup (deprecated)

要查找完全限定域名 (FQDN) 的 IP 地址或 reverse，请使用 **nslookup** 命令。

nslookup {*hostname* | *ip_address*}

Syntax Description

hostname	要查找其 IP 地址的主机的完全限定域名。例如，www.example.com。
ip_address	要查找其完全限定域名的主机的 IP 地址。

Command History

版本	修改
6.1	引入了此命令。
6.6	此命令不再有效，已弃用。
7.1	此命令已被删除并替换为 **dig**。

使用指南

某些允许完全限定域名的命令无法使用为管理接口配置的 DNS 服务器来查找名称的 IP 地址。如果没有为通过数据接口的命令配置 DNS 服务器，请使用 命令确定 IP 地址，然后在 **nslookup** 命令中使用 IP 地址。

nslookup 命令还可用于确定给定 IP 地址的完全限定域名。

示例

以下示例查找 www.cisco.com 的 IP 地址。初始服务器和地址信息显示 DNS 服务器（可以是完全限定域名）、IP 地址和端口。（此示例中的地址是伪造的。）以下信息显示您输入的名称的规范（实际）主机名和 IP 地址。

```
> nslookup www.cisco.com
Server:         10.102.6.247
Address:        10.102.6.247#53

www.cisco.com   canonical name = origin-www.cisco.com.
Name:   origin-www.cisco.com
Address: 173.37.145.84
```

以下示例显示如何执行反向查找并确定 IP 地址的主机名。初始信息适用于所使用的 DNS 服务器。映射的主机名由 **name =** 字段指示。

```
> nslookup 173.37.145.84
Server:         10.102.6.247
Address:        10.102.6.247#53

84.145.37.173.in-addr.arpa      name = www2.cisco.com.
```

packet-tracer

要通过指定 5 元组测试防火墙规则来启用数据包跟踪功能以进行故障排除，请使用 **packet-tracer** 命令。为清楚起见，下面分开展示了 ICMP、TCP/UDP 和 IP 数据包建模的语法。您可以使用 **pcap** 关键字重放多个数据包并跟踪完整的工作流程。

packet-tracer input *ifc_name* **icmp** {*sip* | **user** *username*} *type code* [*ident*] {*dip* | **fqdn** *fqdn-string*} [**detailed**] [**xml**]
packet-tracer input *ifc_name* {**tcp** | **udp**} {*sip* | **user** *username*} *sport* {*dip* | **fqdn** *fqdn-string*} *dport* [**detailed**] [**xml**]
packet-tracer input *ifc_name* **rawip** {*sip* | **user** *username*} *protocol* {*dip* | **fqdn** *fqdn-string*} [**detailed**] [**xml**]
packet-tracer input *ifc_name* **pcap** *pcap_filename* [**bypass-checks** | **decrypted** | **detailed** | **persist** | **transmit** | **xml** | **json** | **force**]

Syntax Description

bypass-checks	（可选）绕过针对模拟数据包的安全检查。
decrypted	（可选）将模拟数据包视为 IPsec/SSL VPN 解密。
code	指定 ICMP 数据包跟踪的 ICMP 代码。
detailed	（可选）提供详细的跟踪结果信息。
dip	指定数据包跟踪的目标 IPv4 或 IPv6 地址。
dport	指定 TCP/UDP/SCTP 数据包跟踪的目标端口。
fqdn *fqdn-string*	指定主机的完全限定域名。仅支持 IPv4 的 FQDN。
force	删除现有的 pcap 跟踪并执行新的 pcap 文件。
icmp	指定要使用的协议为 ICMP。
ident	（可选。）指定 ICMP 数据包跟踪的 ICMP 标识符。
inline-tag *tag*	指定要嵌入第 2 层 CMD 信头中的安全组标记值。有效值范围为 0 到 65533。
input *ifc_name*	指定在其上跟踪数据包的源接口的名称。
json	（可选）以 JSON 格式显示跟踪结果。
pcap	指定 pcap 作为输入。
pcap_filename	包含要跟踪的数据包的 pcap 文件名。
protocol	指定原始 IP 数据包跟踪的协议编号，从 0 到 255。
persist	（可选）启用长期跟踪，并在集群中进行跟踪。

rawip	指定要使用的协议为原始 IP。
sip	指定数据包跟踪的源 IPv4 或 IPv6 地址。
sport	指定 TCP/UDP/SCTP 数据包跟踪的源端口。
tcp	指定要使用的协议为 TCP。
transmit	（可选）允许从设备传输模拟数据包
type	指定 ICMP 数据包跟踪的 ICMP 代码。
udp	指定要使用的协议为 UDP。
user *username*	如果您要指定用户为源 IP 地址，请以域\用户格式指定用户身份。跟踪中使用最近为用户映射的地址（如有）。
xml	（可选）以 XML 格式显示跟踪结果。

Command History

版本	修改
6.1	引入了此命令。
6.6	增强了输出，以提供在路由数据包时允许/丢弃数据包的具体原因。
7.1	增强了 packet-tracer 命令，以允许 pcap 文件作为跟踪的输入。

使用指南

除捕获数据包外，还可以通过 threat defense 设备跟踪数据包的寿命，查看它的行为是否与预期一致。**packet-tracer** 命令使您能够执行以下操作：

- 调试生产网络中的所有数据包丢弃。
- 验证配置是否达到预期。
- 显示适用于数据包和导致规则添加的 CLI 行的所有规则。
- 显示数据路径中数据包更改的时间线。
- 向数据路径中注入跟踪数据包。

packet-tracer 命令可提供有关数据包的详细信息，以及 threat defense 设备对数据包的处理方式。如果配置的命令没有导致数据包丢弃，则 **packet-tracer** 命令以易读格式提供有关原因的信息。例如，如果因无效信头验证丢弃了数据包，将显示以下消息：“数据包因错误的 IP 报头 [原因] 而丢弃。”

packet-tracer 注入和跟踪单个数据包时，使用 **pcap** 关键字可使数据包跟踪器重放多个数据包（最多 100 个数据包）并跟踪整个数据流。您可以提供 pcap 文件作为输入，并以 XML 或 JSON 格式获取结果以进行进一步分析。要清除跟踪输出，请使用 **clear packet-tracer** 的 **pcap trace** 子命令。在跟踪过程中，您无法使用跟踪输出。

示例

以下示例显示如何使用 pcap 文件作为输入运行 packet-tracer：

```
> packet-tracer input inside pcap http_get.pcap detailed xml
```

以下示例显示如何通过清除现有的 pcap 跟踪缓冲区并提供 pcap 文件作为输入来运行 packet-tracer：

```
> packet-tracer input inside pcap http_get.pcap force
```

以下示例跟踪从 10.100.10.10 到 10.100.11.11 的 HTTP 端口的 TCP 数据包。结果表明隐式拒绝访问规则将丢弃该数据包。

```
> packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11 80
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

以下示例跟踪具有下一跳 ARP 条目的直连主机中的 TCP 数据包。

```
firepower(config)# packet-tracer input inside tcp 192.168.100.100 12345 192.168.102.102 80
 detailed
Phase: 1
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
```

```
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=17, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=34, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8488800, priority=0, domain=inspect-ip-options, deny=true
hits=22, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside(vrfid:0), output_ifc=any

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=36, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=10, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 7
Type: FLOW-CREATION
Subtype:
```

```
Result: ALLOW
Config:
Additional Information:
New flow created with id 21, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 8
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 9
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

以下示例跟踪由于缺少有效的下一跳 ARP 条目而被丢弃的 TCP 数据包。请注意，丢弃原因提供了检查 ARP 表的提示。

```
<Displays same phases as in the previous example till Phase 8>

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-v4-adjacency) No valid V4 adjacency. Check ARP table (show arp) has entry
 for nexthop., Drop-location: frame snp_fp_adj_process_cb:200 flow (NA)/NA
```

以下示例描述了使用 NAT 和可访问的下一跳进行次优路由的数据包跟踪器。

```
firepower(config)# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1
route outside 0.0.0.0 0.0.0.0 192.168.102.102 10

firepower(config)# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24
firepower(config)# packet-tracer input dmz tcp 192.168.104.104 12345 10.10.10.10 80 detailed


Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
NAT divert to egress interface outside(vrfid:0)
Untranslate 10.10.10.10/80 to 9.9.9.10/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=20, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
Static translate 192.168.104.104/12345 to 192.168.104.104/12345
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa4ff0, priority=6, domain=nat, deny=false
hits=4, user_data=0x2ae2a8a9d690, cs_id=0x0, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
```

```
hits=40, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a89de1b0, priority=0, domain=inspect-ip-options, deny=true
hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=any

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
Forward Flow based lookup yields rule:
out id=0x2ae2a8aa53d0, priority=6, domain=nat-reverse, deny=false
hits=5, user_data=0x2ae2a8a9d580, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=9.9.9.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=42, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=13, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
New flow created with id 24, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 10
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.100.100 using egress ifc  inside(vrfid:0)

Phase: 11
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Config:
Additional Information:
Input route lookup returned ifc  inside is not same as existing ifc  outside
Doing adjacency lookup lookup on existing ifc outside

Phase: 12
Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Lookup Nexthop on interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 13
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

以下示例描述了使用 NAT 进行次优路由的数据包跟踪器，其中，由于下一跳不可达而丢弃数据包。

```
firepower(config)# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1

firepower(config)# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24


<Displays same phases as in the previous example till Phase 11>

Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame
snp_fp_adjacency_internal:5890 flow (NA)/NA
```

Related Commands

命令	Description
capture	捕获数据包信息，包括跟踪数据包。
show capture	在未指定选项时显示捕获配置。
show packet-tracer	显示最近在 PCAP 文件上运行的数据包跟踪器的跟踪缓冲区输出。

perfmon

要在控制台显示性能信息，请使用 **perfmon** 命令。

perfmon {**verbose** | **interval**几秒 | **settings**}

Syntax Description

verbose	在控制台上显示性能监控信息。默认为不显示信息，在 perfmon 设置中显示为“quiet”。 您必须在诊断 CLI 中才能关闭 **perfmon verbose**。
interval *seconds*	指定控制台上刷新性能显示前的秒数。
settings	显示间隔，以及 perfmon 是安静模式还是详细模式。

Command Default

间隔默认值为 120 秒。

Command History

版本	修改
6.1	引入了此命令。

使用指南

perfmon 命令允许您监控设备的性能。使用 **show perfmon** 命令以立即显示这些信息。

使用 **perfmon verbose** 命令在每个时间间隔的控制台上显示信息。

仅当您在控制台端口上实际连接到 CLI 或在诊断 CLI 中（**system support diagnostic-cli**）时，才会自动显示该信息。如果您位于不同端口（包括管理接口）的 CLI 中，请使用 **show console-output** 命令查看自动生成的信息。或者，不要使用此命令，而直接使用 **show perfmon** 命令。

我们建议您仅在诊断 CLI 中使用此命令。

注释 您无法从常规 CLI 关闭 **verbose** 。相反，您必须在诊断 CLI 中从特权 EXEC 模式下将其关闭。请参阅示例部分。

示例

以下示例显示如何在控制台上每隔 120 秒显示性能监控统计信息：在输出中，“Fixup”统计信息是指相关的协议检测引擎。

```
> perfmon verbose
> perfmon settings
interval: 120 (seconds)
verbose
> show console-output
...
Message #109 :
```

```
Message #110 : PERFMON STATS:                      Current      Average
Message #111 : Xlates                                 0/s          0/s
Message #112 : Connections                            0/s          0/s
Message #113 : TCP Conns                              0/s          0/s
Message #114 : UDP Conns                              0/s          0/s
Message #115 : URL Access                             0/s          0/s
Message #116 : URL Server Req                         0/s          0/s
Message #117 : TCP Fixup                              0/s          0/s
Message #118 : TCP Intercept Established Conns        0/s          0/s
Message #119 : TCP Intercept Attempts                 0/s          0/s
Message #120 : TCP Embryonic Conns Timeout            0/s          0/s
Message #121 : FTP Fixup                              0/s          0/s
Message #122 : AAA Authen                             0/s          0/s
Message #123 : AAA Author                             0/s          0/s
Message #124 : AAA Account                            0/s          0/s
Message #125 : HTTP Fixup                             0/s          0/s
Message #126 :
...
```

以下示例显示如何关闭详细模式。您必须从诊断 CLI 执行此操作。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password: <Press return, do not enter a password>

firepower# perfmon quiet
firepower# perfmon settings
interval: 120 (seconds)
quiet
firepower# <Press Ctrl+a, d>

Console connection detached.
> perfmon settings
interval: 120 (seconds)
quiet
```

Related Commands

命令	Description
show perfmon	显示性能信息。

pigtail commands

只能在思科技术支持中心的指导下使用 **pigtail** 命令。

如果要查看写入的日志，请使用 **tail-logs** 命令而不是 **pigtail**。

⚠

注意 请勿让尾纤进程继续运行，因为它可能会导致磁盘使用率过高。如果此过程在部署期间运行，也可能会干扰策略部署。有关如何停止尾纤流程的信息，请联系思科技术支持中心。

ping

要测试从指定接口到 IP 地址的连接，请使用 **ping** 命令。常规基于 ICMP 的 ping、TCP ping 和“系统”ping 的可用参数有所不同。此外，系统 ping 操作来自管理接口，而其他类型的 ping 操作则通过数据接口。请务必使用正确的 ping 类型进行测试。

ping [**interface** *if_name* | **vrf** *name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]
ping tcp [**interface** *if_name* | **vrf** *name*] *host port* [**repeat** *count*] [**timeout** *seconds*] [**source** *host port*]
ping system *host*

Syntax Description

data *pattern*	（可选，仅限 ICMP。）指定十六进制格式的 16 位数据模式，范围为 0 到 FFFF。默认值为 0xabcd。
host	指定要 ping 的主机的 IPv4 地址或名称。对于 ICMP ping，您还可以指定 IPv6 地址。TCP 或系统 ping 不支持 IPv6。 ping 操作是否可以使用完全限定域名（例如 www.example.com）取决于 DNS 服务器是否可以解析名称。系统 ping 使用管理接口的 DNS 服务器，但其他类型的 ping 不使用管理 DNS 服务器。必须为数据接口配置 DNS，才能使非系统主机名 ping 正常工作。 如果 **ping** 无法解析主机名，请使用 **nslookup** 确定与该名称关联的 IP 地址，然后 ping 通该 IP 地址。
interface *if_name*	（可选）对于ICMP，这是可通过其访问主机的接口的名称。如果不提供，则主机将解析为 IP 地址，并会参考路由表来确定目标接口。对于 TCP，这是来源用来发送 SYN 数据包的输入接口。 如果在启用虚拟路由和转发 (VRF) 时指定 **interface** 关键字，则 ping 将使用指定接口的虚拟路由表。
port	（仅限 TCP。）为您正在 ping 的主机指定 TCP 端口号 (1-65535)。
repeat *count*	（可选）指定重复 ping 请求的次数。默认值为 5。
size *bytes*	（可选，仅限 ICMP。）指定数据报大小（以字节为单位）。默认值为 100。
source *host port*	（可选，仅限 TCP。）指定从其发送 ping 的某个 IP 地址和端口（对于随机端口，使用端口 = 0）。
system	通过管理接口 ping 通主机。不同于通过数据接口进行 ping 操作，系统 ping 没有默认计数。ping 操作会持续执行，直到您使用 Ctrl+c 将其停止。

tcp	（可选）测试基于 TCP 的连接（默认为 ICMP）。TCP ping 发送 SYN 数据包，如果目标发送了 SYN-ACK 数据包，则认为 ping 取得了成功。您还可以同时运行最多 2 个 TCP ping 操作。
timeout *seconds*	（可选）指定超时间隔的秒数。默认值为 2 秒。
validate	（可选，仅限 ICMP。）验证回复数据。
vrf 名称	（可选。）如果启用虚拟路由和转发 (VRF)，也称为虚拟路由器，则可以通过指定虚拟路由器的名称来选择使用哪个虚拟路由表。此关键字与 **interface** 关键字互斥。 如果在启用虚拟路由和转发 (VRF) 时指定 **interface** 关键字，则 ping 将使用指定接口的虚拟路由表。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 **vrf** 关键字。

使用指南

ping 命令使您能够确定设备是否已连接或某主机在网络上是否可用。

使用基于 ICMP 的常规 ping 时，请确保您没有禁止这些数据包的 ICMP 规则（如果不使用 ICMP 规则，则允许所有 ICMP 流量）。

使用 TCP ping 时，您必须确保访问策略允许在您指定的端口上的 TCP 流量。

需要此配置，以允许设备响应和接受通过 **ping** 命令生成的消息。 **ping** 命令输出显示是否接收了响应。如果输入 **ping** 命令后主机未响应，将出现如下所示的类似消息：

```
> ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

使用 **show interface** 命令可确保设备连接到网络并正在传递流量。指定的指定接口的地址用作 ping 的源地址。

示例

以下示例显示如何确定是否可通过数据接口访问 IP 地址。由于未指定接口，因此使用路由表来确定如何到达该地址。

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

以下示例使用 TCP ping 来确定是否可通过数据接口访问主机。

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

> ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms
```

以下示例执行系统 ping 操作，以确定是否可通过管理接口访问 www.cisco.com。必须使用 Ctrl+c 停止 ping（在输出中用 ^C 表示）。

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

以下示例使用名为 red 的虚拟路由器的路由表对地址执行 ping 操作。

```
> ping vrf red 2002::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/20 ms
```

Related Commands

命令	Description
nslookup	对主机名或 IP 地址执行 DNS 查找。
show interface	显示有关接口配置的信息。

pmtool commands

只能在思科技术支持中心的指导下使用 **pmtool** 命令。

reboot

要重新启动设备，请使用 **reboot** 命令。

reboot

Command History

版本	修改
6.1	引入了此命令。

示例

```
> reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': yes

Broadcast message from root@firepower

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

redundant-interface

要设置冗余接口的哪个成员接口处于活动状态，请使用 **redundant-interface** 命令。

redundant-interface redundant *number* **active-member** *physical_interface*

Syntax Description

active-member *physical_interface*	设置活动成员。使用 show interface 命令查看可用的物理接口名称，例如 GigabitEthernet0/0。两个成员接口均必须为相同的物理类型。
redundant *number*	指定标识冗余接口 ID，例如 **redundant 1**。数字为 1-8。

Command Default

默认情况下，主用接口是在配置中列出的第一个成员接口（如果可用）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

在 设备管理器中创建冗余接口。创建冗余接口时，需要指定主接口。使用此命令可更改运行时处于活动状态的接口。

要查看哪个接口处于活动状态，请输入以下命令：

show interface redundant*number* **detail** | **grep Member**

例如：

```
> show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

示例

以下示例更改了冗余接口 1 的活动接口。

```
> show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2

> redundant-interface redundant 1 active-member gigabitethernet0/2
```

Related Commands

命令	Description
clear interface	清除 **show interface** 命令的计数器。
show interface	显示接口的运行时间状态和统计信息。

restore

要从 Cisco Secure Firewall Management Center管理的 Cisco Secure Firewall Threat Defense 设备恢复本地备份的配置，请使用**restore**命令。要恢复保存到远程位置的备份，请为备份文件的位置和用户名指定其他参数。

restore remote-manager-backup[*backup tar-file*|**location** [*scp-hostname username filepath backup tar-file*]]

Syntax Description

remote-manager-backup *backup tar-file*	恢复 Cisco Secure Firewall Management Center 创建的本地备份。本地备份文件保存在 Cisco Secure Firewall Threat Defense 设备上。
remote-manager-backup location *scp-hostname username filepath backup tar-file*	恢复 Cisco Secure Firewall Management Center 创建的远程备份。远程备份保存在用户配置的位置，可由 SCP 服务器访问，并由主机名、用户名和文件路径标识。

Command History

版本	修改
6.3	引入了此命令。

使用指南

restore 命令用于恢复新/替换设备上的 Cisco Secure Firewall Threat Defense 系统文件、Snort 数据库表和 LINA 运行配置 Cisco Secure Firewall Threat Defense。 **restore** 命令还可以确保在实际恢复操作继续之前删除 Cisco Secure Firewall Threat Defense 设备上的现有 LINA 运行配置。这可确保 Cisco Secure Firewall Threat Defense 设备仅传输进行备份时存在的配置。恢复操作成功后，除替换设备的序列号外，所有设备配置都将被替换。

恢复操作可确保使用分配给原始设备的通用唯一标识符 (UUID) 重新建立替换设备/新 Cisco Secure Firewall Threat Defense 设备与原始 Cisco Secure Firewall Management Center 设备之间的连接。成功恢复后， Cisco Secure Firewall Management Center 会将设备的所有策略标记为过期，以便在设备更换程序完成后， Cisco Secure Firewall Management Center 将可能影响替换的任何配置 Cisco Secure Firewall Threat Defense 更改部署到该设备。这可确保新的 Cisco Secure Firewall Threat Defense 和 Cisco Secure Firewall Management Center配置同步。

示例

以下示例显示从本地备份文件执行的恢复操作：

```
> restore remote-manager-backup 10.10.1.168_PRIMARY_20180614055906.tar
```

以下示例显示从远程备份文件执行的恢复操作：

```
>restore remote-manager-backup location 10.106.140.100 admin /Volume/home/admin
10.10.1.168_PRIMARY_20180614055906.tar
```

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。