t - z

tail-logs

要打开系统日志以查看在与思科技术支持中心 (TAC) 合作解决问题时编写的消息，请使用 **tail-logs** 命令。

tail-logs

Command History

版本	修改
6.1	引入了此命令。

使用指南

tail-logs 命令会打开系统日志，以便您可以查看写入的消息。请在配合思科技术支持中心 (TAC) 解决问题时使用此命令，以便他们帮助您解释输出内容并选择要查看的相应日志。

命令会显示一个列出所有可用日志的菜单。按照命令提示符选择日志。如果日志很长，您将看到 More 行；按 Enter 键一次前进一行，按 Space 键一次进入一页。查看完日志后，按 Ctrl+C 返回命令提示符。

示例

以下示例显示了如何跟踪 ngfw.log 文件。文件列表首先在顶部列出目录，然后列出当前目录下的文件。

```
> tail-logs
===Tail Logs===
============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>

2016-10-06 15:38:22.630001 | 9194       | ngfw.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s
```

```
Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> ngfw.log
2016-10-06 15:38:22 Running [rm -rf /etc/logrotate-dmesg.conf /etc/logrotate.conf
/etc/logrotate.d
/etc/logrotate_ssp.conf /etc/logrotate_ssp.d] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate-size.conf /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate-size.d /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate.conf /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate.d /etc/] ... success
2016-10-06 15:38:22 Running [rm -f /usr/sbin/ntpd] ... success
```

Related Commands

命令	Description
system support view-files	打开日志文件。

test aaa-server

要检查设备是否能够使用特定 AAA 服务器验证或授权用户，请使用 **test aaa-server** 命令。

test aaa-server {**authentication** *groupname* [**host** *ip_address*] [**username** *username*] [**password** *password*] | **authorization** *groupname* [**host** *ip_address*] [**username** *username*}

Syntax Description

groupname	指定 AAA 服务器组或领域名称。
host *ip-address*	指定服务器 IP 地址。如果没有在命令中指定 IP 地址，系统将提示您输入地址。
password *password*	指定用户密码。如果没有在命令中指定密码，系统将提示您输入密码。
username *username*	指定用于测试 AAA 服务器设置的帐户的用户名。确保 AAA 服务器中存在该用户名；否则，测试将失败。如果没有在命令中指定用户名，系统将提示您输入用户名。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

此命令允许您验证系统是否可以使用特定AAA服务器对用户进行身份验证或授权。此命令可让您测试 AAA 服务器而无需尝试验证的实际用户。它还可帮助您隔离 AAA 故障是由于 AAA 服务器参数配置错误、AAA 服务器连接问题还是其他配置错误。

示例

以下是成功进行身份验证的示例：

```
> test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

以下是不成功的身份验证尝试：

```
> test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: mypassword
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10
          seconds)
ERROR: Authentication Rejected: Unspecified
```

Related Commands

命令	Description
aaa-server active **aaa-server fail**	重新激活标记为发生故障的 AAA 服务器或使活动 AAA 服务器失效。
clear aaa-server statistics	清除 AAA 服务器统计信息。
show aaa-server	显示 AAA 服务器统计信息。

traceroute

要确定通过数据接口将传送至其目标的路由数据包，请使用 **traceroute** 命令。要确定数据包经过管理IP地址时到达目的地的路由，请使用 **traceroute system** 命令。

traceroute *destination* [**source** {*source_ip* | *source-interface*}] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]
traceroute system *destination*

Syntax Description

destination	要跟踪的主机的 IPv4 或 IPv6 地址或主机名。例如，10.100.10.10 或 www.example.com。必须配置 DNS 服务器才能解析主机名。 使用 **system** 关键字的跟踪使用为管理接口配置的 DNS 服务器。其他跟踪使用为数据接口配置的 DNS 服务器。如果没有为数据接口定义 DNS，请先使用 **nslookup** 命令确定主机的 IP 地址，然后使用 IP 地址而不是 FQDN。
numeric	指定只输出打印中间网关的 IP 地址。如果未指定此关键字，跟踪路由会尝试查找跟踪时到达的网关主机名。
port *port_value*	用户数据报协议 (UDP) 探测消息使用的目标端口。默认值为 33434。
probe *probe_num*	在每个 TTL 级别要发送的探测次数。默认计数为 3。
source {*source_ip* | *source_interface*}	指定 IP 地址或接口将用作跟踪数据包的源。此 IP 地址必须是其中一个数据接口的 IP 地址。在透明模式下，它必须是管理 IP 地址。如果指定接口名称，则使用接口的 IP 地址。
system	表示跟踪路由应通过管理接口，而不是数据接口。
timeout *timeout_value*	指定在连接超时前等待响应的时间（秒）。默认值为 3 秒。
ttl *min_ttl max_ttl*	指定探测中要使用的“生存时间”值范围。 • *min_ttl*-第一次探测的 TTL 值。默认值为 1，但也可以设置为更高的值来抑制已知跃点的显示。 • *max-ttl*-可以使用的最大 TTL 值。默认值为 30。此命令在跟踪路由数据包到达目标或达到该值时终止。
use-icmp	指定使用 ICMP 探测数据包而不是 UDP 探测数据包。

Command History

版本	修改
6.1	引入了此命令。

使用指南

traceroute 命令可打印发送的每个探测的结果。每行输出以递增顺序对应一个 TTL 值。以下是 **traceroute** 命令打印的输出符号：

输出符号	Description
*	在超时期限内未收到对探测的响应。
nn msec	各节点指定探测数的往返时间（以毫秒为单位）。
!N.	无法访问 ICMP 网络。
!H	无法访问 ICMP 主机。
!P	ICMP 协议不可达。
!A	管理性禁止 ICMP。
?	未知 ICMP 错误。

示例

以下示例展示指定了目标 IP 地址时产生的跟踪路由输出：

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

以下示例显示了通过管理接口到主机名的跟踪路由。

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

Related Commands

命令	Description
capture	捕获数据包信息，包括跟踪数据包。

命令	Description
show capture	在未指定选项时显示捕获配置。
packet-tracer	启用数据包跟踪功能。

undebug

要禁用给定功能调试，请使用 **undebug** 命令。此命令与 **no debug** 命令的效果相同。

undebug {*feature* [*subfeature*] [*level*] | **all**}

Syntax Description

all	禁用所有功能调试。
feature	指定要为其禁用调试的功能。若要查看可用功能，请使用 **undebug ?** 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禁用调试消息。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 History

版本	修改
6.1	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

以下示例禁用所有已启用调试的调试。

```
> undebug all
>
```

Related Commands

命令	Description
debug	启用功能调试。
show debug	显示当前活动的调试设置。

upgrade

要重试、取消或恢复系统软件升级，请使用 **upgrade** 命令。

upgrade { **cancel** | **cleanup-revert** | **revert** | **retry** }

Syntax Description

cancel	取消主要升级的安装。如果升级失败，但系统认为升级仍在进行中，则必须取消升级，才能将作业状态更改为可以重试升级的状态。在大多数情况下，系统应该能够自动取消失败的升级。
cleanup-revert	永久删除以前的版本以释放磁盘空间。如果清理可恢复版本，则无法使用 **revert** 关键字返回到该可恢复版本。
revert	如果有可恢复的版本，则通过返回到上一个版本来撤消系统软件升级。首先使用 **show upgrade revert-info** 命令验证是否存在可恢复版本，以及它是哪个版本。如果该版本可接受，则可以使用此命令恢复为该版本。 在高可用性/可扩展性 部署中，当所有设备同时恢复时，恢复更成功。使用CLI恢复时，打开所有设备的会话，验证每个设备是否可以恢复，然后同时启动进程。 恢复后，必须向智能软件管理器重新注册设备。 在版本 6.7 至 7.1 中， **upgrade revert** 仅可用于本地管理的系统。您不能在 管理中心管理的系统上使用此命令。 在版本 7.2+ 中， 如果 管理中心和设备之间的通信中断，则在 管理中心 部署中支持此命令。 注意 从 CLI 恢复可能会导致设备和管理中心之间的配置不同步，具体取决于您在升级后所做的更改。这可能会导致进一步的通信和部署问题。
retry	重试未能完成的主要升级。升级必须被系统视为失败，而不是正在进行。您可能需要输入 **upgrade cancel** ，然后才能重试升级。

Command History

版本	修改
6.7	引入了此命令。
7.0	**upgrade revert** 命令现在会自动从智能软件管理器注销设备。恢复升级后，必须重新注册设备。
7.2	如果管理中心和设备之间的通信中断， 管理中心 部署中现在支持 **upgrade revert** 命令。

示例

以下示例显示如何取消正在进行的系统软件更新。升级取消成功完成后，设备将自动重启。

```
> upgrade cancel
Warning: Upgrade in progress (11%,  8 mins remaining).
Are you sure you want to cancel it(yes/no)? yes
```

以下示例显示如何重试失败的升级。您需要先更正导致升级失败的问题，如失败消息所示。您可能需要使用 **upgrade cancel**，然后才能重试升级。并非所有失败的升级都可以重试。

```
> upgrade retry
Tue Dec  3 23:50:31 UTC 2020: Resuming upgrade for
Cisco_FTD_Upgrade-6.7.0-32.sh.REL.tar
```

以下示例显示如何在本地管理的系统上恢复到以前的版本。使用 **show upgrade revert-info** 命令确定是否有可用于恢复的版本。

```
> upgrade revert
Current version is 6.7.0.50
Detected previous version 6.6.1.20
Are you sure you want to revert (Yes/No)? Yes
```

以下示例显示如何删除以前的版本以清理磁盘空间。使用此命令后，您将无法恢复到以前的版本。

```
> upgrade cleanup-revert
Version 6.6 was cleaned up successfully.
```

Related Commands

命令	Description
show last-upgrade status	显示有关上次系统软件升级的信息。
show upgrade	显示有关当前系统软件升级的信息。

verify

要检验文件的校验和，请使用 **verify** 命令。

verify ［**sha-512** | **/signature**］ *path*
verify/md5 *path* ［*md5-value*］

Syntax Description

/md5	（可选）计算并显示指定软件映像的 MD5 值。将此值与 Cisco.com 上此映像的可用值进行比较。
sha-512	（可选）计算并显示指定软件映像的 SHA-512 值。将此值与 Cisco.com 上此映像的可用值进行比较。
/signature	（可选）验证存储在闪存中的映像的签名。
md5-value	（可选）指定映像的已知 MD5 值。在此命令中指定 MD5 值后，系统将计算指定映像的 MD5 值并显示一条验证 MD5 值匹配或不匹配的消息。

path	• *filename* 当前目录中的文件的名称。使用 **dir** 查看目录内容， **cd** 以更改目录。 • **disk0:**/[*path*/]*filename* 此选项表示内部闪存。您还可以使用 **flash:** 代替 **disk0**；它们是别名。 • **disk1:**/[*path*/]*filename* 此选项表示外部闪存卡。 • **flash:**/[*path*/]*filename* 此选项表示内部闪存卡。对于 ASA 5500 系列， **flash** 是 **disk0:** 的别名。 • **ftp:**//[*user*[**:***password*]**@**]*server*[: *port*]/[*path*/]*filename*[**;type=***xx*] **type** 可以是以下关键字之一： • **ap**- ASCII 被动模式 • **an**- ASCII 正常模式 • **ip**-（默认）二进制被动模式 • **in**- 二进制正常模式 • **http**[**s**]**:**//[*user*[:*password*] **@**]*server*[: *port*]/[*path*/]*filename* • **tftp:**//[*user*[:*password*]@]*server*[: *port*]/[*path*/]*filename*[**;int=***interface_name*] 如果要覆盖到服务器地址的路由，请指定接口名称。路径名不能包含空格。

Command Default

当前的闪存设备是默认文件系统。

注释 在指定 **/md5** 选项时，可使用网络文件（如 FTP、HTTP 和 TFTP）作为源。不带 **verify** 选项的 **/md5** 命令仅允许验证闪存中的本地映像。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **verify** 命令验证文件的校验和，然后再使用文件。

分布在磁盘上的每个软件映像对整个映像使用单个校验和。当映像复制到闪存中时才显示此校验和；当映像文件从一个磁盘复制到另一个磁盘时，不会显示。

在加载或复制新的映像之前，记录映像的校验和与MD5信息，以便当您将映像复制到闪存中或服务器上时可验证校验和。Cisco.com 上提供多种映像信息。

要显示闪存的内容，请使用 **show flash:** 命令。闪存的内容列表不包含各个文件的校验和。要重新计算和验证映像复制到闪存后的校验和，请使用**verify**命令。但请注意，当文件保存到文件系统之后，**verify** 命令才检查其完整性。损坏的映像可能会传输到设备并保存在文件系统中，不进行检测。如果损坏的映像成功传输到设备，则软件无法识别映像已损坏，而文件将成功验证。

要使用消息摘要 5 (MD5) 散列算法确保文件验证，请使用带 **/md5** 选项的 **verify** 命令。MD5 是一种通过创建唯一的 128 位消息摘要来验证数据完整性的算法（在 RFC 1321 中定义）。 **verify** 命令的 **/md5** 选项通过将映像的MD5校验和值与该映像的已知MD5校验和值进行比较，检查安全设备软件映像的完整性。目前 Cisco.com 提供了所有安全设备软件映像的 MD5 值，以供与本地系统映像值进行比较。

要执行 MD5 完整性检查，请执行使用 **/md5** 关键字的 **verify** 命令。例如，执行 **verify /md5 flash:cdisk.bin** 命令将计算并显示软件映像的 MD5 值。将此值与 Cisco.com 上此映像的可用值进行比较。

或者，您可以先从 Cisco.com 获取 MD5 值，然后在命令语法中指定此值。例如，执行 **verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** 命令将显示验证 MD5 值匹配或不匹配的消息。MD5 值不匹配表示映像已损坏或输入了错误的 MD5 值。

示例

以下示例验证映像文件。如果包含 **/signature** 关键字，则会看到相同的结果。

```
> verify os.img
Verifying file integrity of disk0:/os.img
Computed Hash   SHA2: 4916c9b70ad368feb02a0597fbef798e
                      ca360037fc0bb596c78e7ef916c6c398
                      e238e2597eab213d5c48161df3e6f4a7
                      66e4ec15a7b327ee26963b2fd6e2b347
Embedded Hash   SHA2: 4916c9b70ad368feb02a0597fbef798e
                      ca360037fc0bb596c78e7ef916c6c398
                      e238e2597eab213d5c48161df3e6f4a7
                      66e4ec15a7b327ee26963b2fd6e2b347
Digital signature successfully validated
```

以下示例计算映像的 MD5 值。为简洁起见，大多数感叹号已被删除。

```
> verify /md5 os.img
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!Done!
verify /MD5 (disk0:/os.img) = 0940c6c71d3d43b3ba495f7290f4f276
>
```

以下示例计算 MD5 值并将其与预期值进行比较。在这种情况下，决策为“已验证”，即计算值与预期值匹配。

```
> verify /md5 os.img 0940c6c71d3d43b3ba495f7290f4f276
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
```

```
Verified (disk0:/os.img) = 0940c6c71d3d43b3ba495f7290f4f276
>
```

以下示例计算映像的 SHA-512 值。

```
> verify /sha-512 os.img
!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
verify /SHA-512 (disk0:/os.img) = 77421c0f6498976fbe5300e62bd8b7e8140b52a851f055265080
a392299848a77227d6047827192f34d969d36944abf2bddd215ec4127f9503173f82a2d6c7e2
```

Related Commands

命令	Description
copy	复制文件。
dir	列出系统中的文件。

vpn-sessiondb logoff

要注销所有或选定的 VPN 会话，请使用 **vpn-sessiondb logoff** 命令。

vpn-sessiondb logoff {**all** | **index** *index_number* | **ipaddress** *IPaddr* | **l2l** | **name** *username* | **protocol** *protocol-name* | **tunnel-group** *groupname*} **noconfirm**

Syntax Description

all	注销所有 VPN 会话。
index *index_number*	按索引编号注销单个会话。您可以使用 **show vpn-sessiondb detail** 命令查看每个会话的索引编号。
ipaddress *IPaddr*	注销您指定的 IP 地址的会话。
l2l	注销所有 LAN 到 LAN 会话。
name *username*	注销您指定的用户名的会话。
protocol *protocol-name*	注销您指定的协议的会话。这些协议包括： • **ikev1**-互联网密钥交换第 1 版 (IKEv1) 会话。 • **ikev2**-互联网密钥交换第 2 版 (IKEv2) 会话。 • **ipsec**-使用 IKEv1 或 IKEv2 的 IPsec 会话。 • **ipseclan2lan**—IPsec LAN-to-LAN 会话。 • **ipseclan2lanovernatt**—IPsec LAN-to-LAN-over NAT-T 会话。
tunnel-group *groupname*	注销您指定的隧道组（连接配置文件）会话。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何注销企业隧道组（连接配置文件）的会话。

```
> vpn-sessiondb logoff tunnel-group Corporate noconfirm
INFO: Number of sessions from TunnelGroup "Corporate" logged off : 1
```

write net

要将运行配置保存到 TFTP 服务器，请使用 **write net** 命令。

write net ［**interface** *if_name*］ *server***:**［*filename*］

Syntax Description

:*filename*	指定路径和文件名。
interface *if_name*	可以通过其访问服务器的接口的名称。
*server***:**	设置 TFTP 服务器的 IP 地址或名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

运行配置是内存中当前运行配置。

示例

以下示例通过内部接口将运行配置复制到 TFTP 服务器。

```
> write net interface inside 10.1.1.1:/configs/contextbackup.cfg
```

Related Commands

命令	Description
show running-config	显示运行配置。

write terminal

要在终端上显示运行配置，请使用 **write terminal** 命令。

write terminal

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令与 **show running-config** 命令等效：

示例

以下示例将运行配置写入终端：

```
> write terminal
: Saved
:
: Serial Number: XXXXXXXXXXX
: Hardware:   ASA5516, 8192 MB RAM, CPU Atom C2000 series 2416 MHz, 1 CPU (8 cores)
:
NGFW Version 6.2.0
!
hostname firepower
(...remaining output deleted...)
```

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。