Aruba 832x Diagnostics and Supportability Guide for ArubaOS-CX 10.02

a Hewlett Packard Enterprise company

Part Number: 5200-5305a
Published: January 2019
Edition: 2

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Applicable products

This document applies to the following products:

Aruba 8320 Switch Series (JL479A, JL579A, JL581A)

Aruba 8325 Switch Series (JL624A, JL625A, JL626A, JL627A, JL635A, JL636A)

Latest version available online

Updates to this document can occur after initial publication. For the latest versions of product documentation, see the links provided in the Websites chapter of this document.

About the examples

Examples in this document are representative and might not match your particular switch or environment.

The slot and port numbers in this document are for illustration only and might be unavailable on your device.

The software notation for identifying interfaces uses member/slot/port notation, such as 1/1/1. For standalone switches such as the 8320, slot is always 1.

Switch prompts in examples

The switch prompts used in this document are examples and might not match your particular switch or environment.

In examples:

- The switch prompt starts with the word `switch`.
- The switch prompt also indicates the command context.

  For example:

  switch>

  Indicates the operator command context.

  switch#

  Indicates the manager command context.

  switch(config)#

  Indicates the global configuration context.

  In your environment, the switch prompt can vary because the prompt is user-configurable.

  - Typically, the switch prompt begins with the host name of the switch.
  - The switch prompt contains specifiers in certain configuration command contexts, such as interface name or VLAN ID. For example: `switch(config-vlan-100)#`

    In these cases, examples in this document might contain placeholders such as `n` or `if`.

Overview

The debug logging framework provides an improved, customizable, and conditional logging framework with feature and entity based filtering options. Debug logging is a verbose, on-demand logging mechanism which customers and support can enable in order to obtain more information that will assist with troubleshooting.

Each debug logging event has both a Severity and a Module. Customers/support are required to enable a given Module in order to have those events logged. The log operation is not run when a Module is not enabled. All debug log events classified with a Severity of Error and above will always be logged. This ensures that both support and customers will be able to see these important events even when their respective debug log Module isn't enabled.

NOTE: Debug logging is disabled by default.

Debug logging

debug {all | module}

Syntax

```
debug {all | <MODULE-NAME>} [<SUBMODULE-NAME>] [severity (emer|crit|alert|err|
notice|warning|info|debug)] {port <PORT-NAME> | vlan <VLAN-ID> | ip <IP-ADDRESS> |
mac <MAC-ADDRESS> | vrf <VRF-NAME> | instance <INSTANCE-ID>}

no debug {all | <MODULE-NAME>} [<SUBMODULE-NAME>] {port | vlan | ip | mac | vrf |
instance}
```

Description

Enables debug logging for modules or submodules by name, with optional filtering by specific criteria.

The `no` form of this command disables debug logging.

Command context

Manager (`#`)

Parameters

`all`

Enables debug logging for all modules.

`<MODULE-NAME>`

Enables debug logging for a specific module.

`<SUBMODULE-NAME>`

Enables debug logging for a specific submodule.

`severity (emer|crit|alert|err|notice|warning|info|debug)`

Selects the minimum severity log level for the destination. If a severity is not provided, the default log level is`debug`. Optional.

emer

Specifies storage of debug logs with a severity level of `emergency` only.

crit

Specifies storage of debug logs with severity level of `critical` and above.

alert

Specifies storage of debug logs with severity level of `alert` and above.

err

Specifies storage of debug logs with severity level of `error` and above.

notice

Specifies storage of debug logs with severity level of `notice` and above.

warning

Specifies storage of debug logs with severity level of `warning` and above.

info

Specifies storage of debug logs with severity level of `info` and above.

debug

Specifies storage of debug logs with severity level of `debug` (default).

port

Displays debug logs for the specified port, for example `1/1/1`.

vlan *<VLAN-ID>*

Displays debug logs for the specified VLAN. Provide a VLAN from 1 to 4094.

ip *<IP-ADDRESS>*

Displays debug logs for the specified IP Address.

mac *<MAC-ADDRESS>*

Displays debug logs for the specified MAC Address, for example `A:B:C:D:E:F`.

vrf <VRF-NAME>

Displays debug logs for the specified VRF.

instance *<INSTANCE-ID>*

Displays debug logs for the specified instance. Provide an instance ID from 1 to 255.

Authority

Administrators

Examples

```
switch# debug all
```

debug destination

Syntax

```
debug destination {syslog | file | console | buffer} [severity (emer|crit|alert|err|notice|warning|info|debug)]

no debug destination {syslog | file | console}
```

Description

Sets the destination for debug logs and the minimum severity level for each destination

The `no` form of this command unsets the destination for debug logs.

Command context

Manager (`#`)

Parameters

`{syslog | file | console | buffer}`

Selects the destination to store debug logs. Required.

`syslog`

Specifies that the debug logs are stored in the `syslog`.

`file`

Specifies that debug logs are stored in `file`.

`console`

Specifies that debug logs are stored in `console`.

`buffer`

Specifies that debug logs are stored in `buffer`.

`severity (emer|crit|alert|err|notice|warning|info|debug)`

Selects the minimum severity log level for the destination. If a severity is not provided, the default log level is`debug`. Optional.

`emer`

Specifies storage of debug logs with a severity level of `emergency` only.

`crit`

Specifies storage of debug logs with severity level of `critical` and above.

`alert`

Specifies storage of debug logs with severity level of `alert` and above.

`err`

Specifies storage of debug logs with severity level of `error` and above.

`notice`

Specifies storage of debug logs with severity level of `notice` and above.

`warning`

Specifies storage of debug logs with severity level of `warning` and above.

`info`

Specifies storage of debug logs with severity level of `info` and above.

`debug`

Specifies storage of debug logs with severity level of `debug` (default).

Authority

Administrators

Usage

Events that have a severity equal to or higher than the configured severity level are stored in the designated destination. The product defaults to `buffer` for destination and `debug` as a severity level.

Examples

```
switch# debug destination syslog severity alert

switch# debug destination console severity info

switch# debug destination file severity warning

switch# debug destination buffer severity err
```

show debug

Syntax

```
show debug [vsx-peer]
```

Description

Displays the enabled debug types.

Command context

Manager (#)

Parameters

[vsx-peer]

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed.

Authority

Administrators

Examples

```
switch# show debug
--------------------------------------------------------------------------------
module sub_module severity vlan port    ip        mac             instance   vrf

--------------------------------------------------------------------------------
all     all          err    1   1/1/1   10.0.0.1  1a:2b:3c:4d:5e:6f   2      abcd
```

show debug buffer

Syntax

```
show debug buffer [module <MODULE-NAME> | severity (emer|crit|alert|err|notice|warning|info|debug)]
```

Description

Displays debug logs stored in the specified debug buffer with optional filtering by module or severity.

Command context

Manager (#)

Parameters

<MODULE-NAME>

Filters debug logs displayed by the specified module name.

severity (emer|crit|alert|err|notice|warning|info|debug)

Displays debug logs with a specified severity level. Defaults to`debug`. Optional.

emer

Displays debug logs with a severity level of `emergency` only.

crit

Displays debug logs with a severity level of `critical` and above.

alert

Displays debug logs with a severity level of `alert` and above.

err

Specifies storage of debug logs with severity level of `error` and above.

notice

Specifies storage of debug logs with severity level of `notice` and above.

warning

Displays debug logs with a severity level of `warning` and above.

info

Displays debug logs with a severity level of `info` and above.

debug

Displays debug logs with a severity level of `debug` (default).

Authority

Administrators

Examples

```
switch# show debug buffer

--------------------------------------------------------------------------------
show debug buffer
--------------------------------------------------------------------------------
2017-03-06:06:51:15.089967|hpe-sysmond|SYSMON|SYSMON_CONFIG|LOG_INFO|Sysmon poll interval changed to 20
```

show debug destination

Syntax

```
show debug destination [vsx-peer]
```

Description

Displays the configured debug destination and severity.

Command context

Manager (#)

Parameters

[vsx-peer]

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed.

Authority

Administrators

Examples

```
switch# show debug destination
------------------------------------------------------------------------
                show debug destination
------------------------------------------------------------------------
 CONSOLE:info
 FILE:warning
```

Overview

Log rotation provides an ability for a system administrator to systematically rotate and archive any log files produced by the system. Log rotation reduces the disk space requirement of an operating system. The feature uses the Linux log-rotate utility for log rotation. Log rotation rotates and compresses the log files either based on size and/or period. Rotated log files are stored locally or transferred to the remote destination using Trivial File Transfer Protocol (TFTP).

By default the log rotation feature rotates the log files daily. If the maximum file size exceeds 100 MB, log rotation is also triggered. Whichever condition occurs first (period or size) triggers the log rotation.

Changing the size of the log rotation file

By default, the product rotates the log files when the maximum file size exceeds 100 MB. When the size of the log file exceeds the configured value, the rotation is triggered for that particular log file. Log rotation does not occur immediately after the maximum file size for the log file is reached since the cron job runs with an hourly periodicity.

```
logrotate maxsize <10-200 MB>
```

If you are planning to transfer the log rotation file by TFTP, set the log rotation file to no more than 32 MB.

Prerequisites

You must be in the configuration context:

```
switch(config)#
```

Changing the time frequency for log rotation

By default, the product rotates the log files daily. Enter the command at the configuration context in the CLI.

Prerequisites

You must be in the configuration context:

```
switch(config)#
```

Procedure

At the configuration context, enter:

```
logrotate period {daily | hourly | weekly | monthly }
```

daily: Rotates the log files daily. It is the default option.

hourly: Rotates the log files hourly.

weekly: Rotates the log files every week.

monthly: Rotates the log files every month.

Example command

```
switch(config)# logrotate period weekly
```

Identifying a remote host for receiving rotated log files

You can send the rotated log files to a specified remote host Universal Resource Identifier (URI) by using the TFTP protocol. If no URI is specified, the rotated and compressed log files are stored locally in `/var/log/`. Only the TFTP protocol is supported for remote transfer, and the log rotation file cannot be more than 32 MB. Use the Linux TFTP command to transfer the file. Rotated log files are removed from the local path `/var/log/` when it is moved to TFTP server.

Prerequisites

You must be in the configuration context:

```
switch(config)#
```

Procedure

Provide the target IP address (IPv4 or IPv6) at the configuration context in the CLI:

```
switch(config)# logrotate target {tftp://A.B.C.D | tftp://X:X::X:X}
```

IPv4 Example

```
switch(config)# logrotate target tftp://192.168.1.132
```

IPv6 Example

```
switch(config)# logrotate target tftp://2001:db8:0:1::128
```

Log rotation paths

Only logs stored in the following files are rotated:

- Event logs stored in the `/var/log/event.log` file.
- Authentication logs stored in the `/var/log/auth.log` file.
- Audit logs stored in the `/var/log/audit/audit.log` file

Management of rotated log files

Rotated log files are compressed and stored locally in `/var/log/`, regardless of the remote host configuration. Rotated log files are stored with respective time extension to the granularity of hour in the format `file1-YYYYMMDDHH.gz` (for example, `messages-2015080715.gz`). Rotated log files are replaced when the number of old rotated log files exceeds three. The newly rotated log file replaces the oldest rotated log file.

Remote transfer of rotated log files

Only the TFTP protocol is supported for remote transfer, and both IPv4 and IPv6 addresses are supported.

Only newly rotated log files are transferred to the remote host during the log rotation. Previously rotated log files are not transferred. After a file is successfully transferred, it is removed from the switch local path.

Packet level failures with TFTP are handled in the protocol itself. With each TFTP session failure, TFTP retries the file transfer three times. Retries have a timeout of five seconds.

Verifying the log rotation parameters

Procedure

At the command prompt, enter:

```
switch# show logrotate
```

Example output

```
switch# show logrotate
Logrotate configurations :
Period             : daily
Maxsize            : 10MB
switch#
```

Resetting the size of the log rotation file

Prerequisites

You must be in the configuration context:

```
switch(config)#
```

Procedure

At configuration context, enter the `no` form of the `logrotate maxsize` command:

```
switch(config)# no logrotate maxsize
```

Resetting the time frequency to daily

Prerequisites

You must be in the configuration context:

```
switch(config)#
```

Procedure

At configuration context, enter the `no` form of the `logrotate period` command:

```
switch(config)# no logrotate period
```

Resetting the remote host for receiving rotated log files

Prerequisites

You must be in the configuration context:

```
switch(config)#
```

Procedure

At configuration context, enter the `no` form of the `logrotate target` command:

```
switch(config)# no logrotate target
```

Example:

```
switch(config)# logrotate target tftp://1.1.1.1
switch(config)# do show logrotate
Logrotate configurations :
Period            : daily
Maxsize           : 10MB
Target            : tftp://1.1.1.1
switch(config)# no logrotate target
switch(config)# do show logrotate
Logrotate configurations :
Period            : daily
Maxsize           : 10MB
switch(config)#
```

Log rotation not occurring immediately after reaching threshold

Symptom

Log rotation does not occur immediately after the maximum file size for the log file is reached.

Cause

The log rotation checks the size of the file on the first minute of every hour. If the maximum file size is reached in the meantime, the log rotation does not occur until the next hourly check of the file size.

Action

Log rotation is working as designed. The log rotation feature is designed to check the file size on an hourly basis.

Log files not transferred remotely

Symptom

Rotated log files are not transferred to a remote host.

Cause

- The remote host might not be reachable.
- The TFTP server on the remote host might not have sufficient privileges for file creation.

Action

1. Verify that the remote host is reachable.
2. Ensure that the TFTP server is configured with the required file creation permissions.
3. For example, on the TFTPD-HPA server, change the configuration file in `/etc/default/tftpd-hpa` to include `-c` in `TFTP_OPTIONS`. (for example, `TFTP_OPTIONS="--secure -c`.).

Log rotation not occurring regardless of `period` value

Symptom

Log rotation is not happening regardless of the `period` value.

Cause

Log files are not rotated when they are empty files (the log file size is zero).

Action

Log rotation occurs when the log file size is greater than zero.

Log rotation commands

`logrotate maxsize`

Syntax

```
logrotate maxsize <MAX-SIZE>

no logrotate maxsize
```

Description

Specifies the maximum allowed log file size.

The `no` form of this command resets the size of the log file to the default (100 MB).

Command context

`config`

Parameters

<MAX-SIZE>

Specifies the allowed size the log file can reach before it is compressed and stored locally or transferred to a remote host. The size is a value in the range of 10- 200 MB, and it cannot exceed 32 MB for transferred files.

Authority

Administrators

Usage

A log file that exceeds either the configured *<MAX-SIZE>* value or the `logrotate period` , triggers rotation for that log file. Log rotation occurs during the next hourly maintenance cycle.

Logs are stored locally (event logs in the `/var/log/event.log` file, and authentication logs in the `/var/log/auth.log` file) or transferred to the configured remote destination target using TFTP.

Examples

```
switch(config)# logrotate maxsize 32

switch(config)# no logrotate maxsize
```

logrotate period

Syntax

```
logrotate period {daily | hourly | monthly | weekly}

no logrotate period
```

Description

Sets the rotate period for the event logs, stored in the `/var/log/event.log` file, and authentication logs, stored in the `/var/log/auth.log` file. Defaults to `daily`.

A log file that exceeds either the `logrotate <MAX-SIZE>` value or the `logrotate period` (whichever happens first), triggers rotation for that log file.

The `no` form of this command resets the log rotation period to the default.

Command context

```
config
```

Parameters

`daily`

Rotates log files on a daily basis (default) at 1:00 am local time.

`hourly`

Rotates log files every hour at the first second of the hour.

`monthly`

Rotates log files monthly on the first day of the month.

`weekly`

Rotates log files once a week on Sunday.

Authority

Administrators

Examples

```
switch(config)# logrotate period weekly
```

logrotate target

Syntax

```
logrotate target {tftp://<IPV4_ADDR> | tftp://<IPV6_ADDR>}

no logrotate target
```

Description

Specifies the target remote host Universal Resource Identifier (URI) using TFTP protocol to allow transfer of rotated and compressed files to a remote target. Rotated log files are stored locally (event logs in the `/var/log/event.log` file, and authentication logs in the `/var/log/auth.log` file) or transferred to the configured remote destination target.

The `no` form of this command resets the target to the default, which stores the rotated and compressed log files locally in `/var/log/` .

Command context

`config`

Parameters

<IPV4_ADDR>

Specifies an IPv4 IP Address location for log file storage.

<IPV6_ADDR>

Specifies an IPv6 IP Address location for log file storage.

Authority

Administrators

Usage

To transfer rotated log files remotely, use the TFTP protocol only, and make sure that the rotated log file is less than 32 MB in size. Use the Linux TFTP command to transfer the file. The rotated log file is removed from the local path`/var/log/` when the log file is moved to a TFTP server.

Examples

Setting an IPv4 target:

```
switch(config)# logrotate target tftp://192.168.1.132
```

Setting an IPv6 target:

```
switch(config)# logrotate target tftp://2001:db8:0:1::128
```

Removing a `logrotate` target :

```
switch(config)# logrotate target tftp://1.1.1.1
switch(config)# do show logrotate
Logrotate configurations :
Period : daily
Maxsize : 10MB
Target : tftp://1.1.1.1

switch(config)# no logrotate target
switch(config)# do show logrotate
Logrotate configurations :
Period : daily
Maxsize : 10MB

switch(config)#
```

show logrotate

Syntax

`show logrotate [vsx-peer]`

Description

Displays `logrotate` configuration details.

Command context

Manager (#)

Parameters

[vsx-peer]

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed.

Authority

Administrators

Examples

```
switch# show logrotate
Logrotate configurations :
Period            : daily
Maxsize           : 100MB
switch#
```

Overview

Event logging logs events generated by daemons, processes, and plug-ins running within the switch software. The event logging framework captures the event logs in a system journal by updating the journal fields and meta data.

The `show event` CLI command offers various filtering options to display the event logs as per user requirements.

See the *ArubaOS-CX Security Guide* for information about accounting logs.

Event Logs

The time stamp for event log messages generated from the Service OS indicates when the event log messages were transferred to the event log after an ArubaOS-CX boot and not when the issue occurred.

show events

Syntax

```
show events [ -e <EVENT-ID> |
     -s {alert | crit | debug | emer | err | info | notice | warn} |
     -r | -a | -n <count> |
     -c {lldp | ospf | ... | } |
     -d {lldpd | hpe-fand | ... |}]
```

Description

Shows event logs generated by the switch modules since the last reboot.

Command context

Manager (#)

Parameters

`-e <EVENT-ID>`

Shows the event logs for the specified event ID. Event ID range: 101 through 99999.

`-s {alert | crit | debug | emer | err | info | notice | warn}`

Shows the event logs for the specified severity. Select the severity from the following list:

- `alert`: Displays event logs with severity alert and above.
- `crit`: Displays event logs with severity critical and above.
- `debug`: Displays event logs with all severities.
- `emer`: Displays event logs with severity emergency only.
- `err`: Displays event logs with severity error and above.

- `info`: Displays event logs with severity info and above.
- `notice`: Displays event logs with severity notice and above.
- `warn`: Displays event logs with severity warning and above.

`-r`

Shows the most recent event logs first.

`-a`

Shows all event logs, including those events from previous boots.

`-n <count>`

Displays the specified number of event logs.

`-c {lldp | ospf | ... | }`

Shows the event logs for the specified event category. Enter `show event -c` for a full listing of supported categories with descriptions.

`-d {lldpd | hpe-fand | ... |}`

Shows the event logs for the specified process. Enter `show event -d` for a full listing of supported daemons with descriptions.

Authority

Administrators or Auditors.

Examples

Showing event logs:

```
switch# show events
-------------------------------------------------
show event logs
-------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to up for bridge_normal interface
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1 in Hardware
```

Showing the most recent event logs first:

```
switch# show events -r
-------------------------------------------------
show event logs
-------------------------------------------------
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1 in Hardware
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to up for bridge_normal interface
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
```

Showing all event logs:

```
switch# show events -a
-------------------------------------------------
show event logs
-------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to up for bridge_normal interface
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1 in Hardware
```

Showing event logs related to the DHCP relay agent:

```
switch# show events -c dhcp-relay
2016-05-31:06:26:27.363923|hpe-relay|110001|LOG_INFO|DHCP Relay Enabled
2016-05-31:07:08:51.351755|hpe-relay|110002|LOG_INFO|DHCP Relay Disabled
```

Showing event logs related to the DHCPv6 relay agent:

```
switch# show events -c dhcpv6-relay
2016-05-31:06:26:27.363923|hpe-relay|109001|LOG_INFO|DHCPv6 Relay Enabled
2016-05-31:07:08:51.351755|hpe-relay|109002|LOG_INFO|DHCPv6 Relay Disabled
```

Showing event logs related to IRDP:

```
switch# switch# show events -c irdp
2016-05-31:06:26:27.363923|hpe-rdiscd|111001|LOG_INFO|IRDP enabled on interface %s
2016-05-31:07:08:51.351755|hpe-rdiscd|111002|LOG_INFO|IRDP disabled on interface %s
```

Showing event logs related to LACP:

```
switch# show events -c lacp
-----------------------------------------------------
show event logs
-----------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
```

Showing event logs as per the specified process:

```
switch# show events -d lacpd
-----------------------------------------------------
show event logs
-----------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
```

Displaying the specified number of event logs:

```
switch# show events -n 5
-----------------------------------------------------
show event logs
-----------------------------------------------------
2018-03-21:06:12:15.500603|arpmgrd|6101|LOG_INFO|AMM|-|ARPMGRD daemon has started
2018-03-21:06:12:17.734405|lldpd|109|LOG_INFO|AMM|-|Configured LLDP tx-delay to 2
2018-03-21:06:12:17.740517|lacpd|1307|LOG_INFO|AMM|-|LACP system ID set to 70:72:cf:d4:34:42
2018-03-21:06:12:17.743491|vrfmgrd|5401|LOG_INFO|AMM|-|Created a vrf entity 42cc3df7-1113-412f-b5cb-e8227b8c22f2
2018-03-21:06:12:17.904008|vrfmgrd|5401|LOG_INFO|AMM|-|Created a vrf entity 4409133e-2071-4ab8-adfe-f9662c06b889
```

Overview

To effectively diagnose various issues arising at the switch, different types of data are copied out using copy commands for further analysis.

Use the `copy core-dump` command to copy the core-dump of a daemon crash.

Use the `copy show-tech` command to capture the status of the feature.

If there is feature misbehavior, use the `copy support-files feature` command to copy all feature related information for further analysis. Additionally use `copy support-log` and `copy diag-dump` to copy information that helps to analyze the internal behavior of a feature/daemon.

Use `copy command-output` to copy any `show` command's output to remote destinations or USB storage.

These files can be copied to a remote destination using sftp/tftp, additionally they can also be stored in the USB storage.

Supportability copy commands

copy command-output

Syntax

`copy command-output "<COMMAND>" {<STORAGE-URL> | <REMOTE-URL> [vrf <VRF-NAME>]}`

Description

Copies the specified command output using TFTP, SFTP, or USB.

Command context

Manager (#)

Parameters

<COMMAND>

Specifies the command from which you want to obtain its output. Required.

NOTE: Users with auditor rights can specify these two commands only:

`show accounting log`

`show events`

{*<STORAGE-URL>* | *<REMOTE-URL>* [vrf *<VRF-NAME>*]}

Select either the storage URL or the remote URL for the destination of the copied command output. Required.

<STORAGE-URL>

Specifies the USB to copy command output.

Syntax: `{usb}:/<FILE>`

<REMOTE-URL>

Specifies the URL to copy the command output.

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE>`

`vrf <VRF-NAME>`

Specifies the VRF name. The default VRF name is default. Optional.

Authority

Administrators or Auditors.

Examples

Copying the output from the `show events` command to a remote URL:

```
switch# copy command-output "show events" tftp://10.100.0.12/file
```

Copying the output from the `show tech` command to a remote URL with a VRF named *mgmt*:

```
switch# copy command-output "show tech" tftp://10.100.0.12/file vrf mgmt
```

Copying the output from the `show events` command to a file named `events` on a USB drive:

```
switch# copy command-output "show events" usb:/events
```

copy core-dump daemon

Syntax

`copy core-dump daemon <DAEMON-NAME>[:<INSTANCE-ID>] <REMOTE-URL> [vrf <VRF-NAME>]`

Description

Copies the core-dump from the specified daemon using TFTP, SFTP, or USB.

Command context

Manager (#)

Parameters

<DAEMON-NAME>

Specifies the name of the daemon. Required.

`[:<INSTANCE-ID>]`

Specifies the instance of the daemon core dump. Optional.

<REMOTE_URL>

Specifies the remote destination URL. Required. The syntax of the URL is the following:

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE>`

`vrf <VRF-NAME>`

Specifies the VRF name. If no VRF name is provided, the VRF named *default* is used. Optional.

Authority

Administrators

Examples

Copying the core dump from daemon ops-vland to a remote URL with a VRF named mgmt:

```
switch# copy core-dump daemon ops-vland sftp://abc@10.0.14.211/vland_coredump.xz vrf mgmt
```

Copying the core dump from daemon ops-switchd to a USB drive:

```
switch# copy core-dump daemon ops-switchd usb:/switchd
```

copy core-dump kernel

Syntax

```
copy core-dump kernel <REMOTE-URL> [vrf <VRF-NAME>]
```

Description

Copies a kernel core dump using TFTP or SFTP.

Command context

Manager (#)

Parameters

<REMOTE-URL>

Specifies the URL to copy the command output. Required.

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE>`

vrf *<VRF-NAME>*

Specifies the VRF name. The default VRF name is default. Optional.

Authority

Administrators

Examples

Copying the kernel core dump to the URL:

```
switch# copy core-dump kernel tftp://10.100.0.12/kernel_dump.tar.gz
```

Copying the kernel core dump to the URL with the VRF named mgmt:

```
switch# copy core-dump kernel tftp://10.100.0.12/kernel_dump.tar.gz vrf mgmt
```

copy core-dump kernel *<STORAGE-URL>*

Syntax

```
copy core-dump kernel <STORAGE-URL>
```

Description

Copies the kernel core dump to a USB drive.

Command context

Manager (#)

Parameters

<STORAGE-URL>

Specifies the USB to copy command output. Required.

Syntax: `{usb}:/<FILE>`

Authority

Administrators

Examples

Copying the kernel core dump to a USB drive:

```
switch# copy core-dump kernel usb:/kernel.tar.gz
```

copy diag-dump feature <FEATURE>

Syntax

```
copy diag-dump feature <FEATURE> {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}
```

Description

Copies the specified diagnostic information using TFTP, SFTP, or USB.

Command context

Manager (#)

Parameters

<FEATURE>

The name of a feature, for example `aaa` or `vrrp`. Required.

{*<REMOTE-URL>* [vrf *<VRF-NAME>* |*<STORAGE-URL>*]}

Select either the remote URL or the storage URL for the destination of the copied command output. Required.

<REMOTE-URL>

Specifies the remote destination URL. Required. The syntax of the URL is the following:

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE>`

vrf *<VRF-NAME>*

Specifies the VRF name. If no VRF name is provided, the VRF named *default* is used. Optional.

<STORAGE-URL>

Specifies the USB to copy command output. Required.

Syntax: `{usb}:/<FILE>`

Authority

Administrators

Examples

Copying the output from the aaa feature to a remote URL with a specified VRF:

```
switch# copy diag-dump feature aaa tftp://10.100.0.12/diagdump.txt vrf mgmt
```

Copying the output from the vrrp feature to a USB drive:

```
switch# copy diag-dump feature vrrp usb:/diagdump.txt
```

copy diag-dump local-file

Syntax

`copy diag-dump local-file {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}`

Description

Copies the diagnostic information stored in a local file using TFTP, SFTP, or USB.

Command context

Manager (#)

Parameters

{*<REMOTE-URL>* [vrf *<VRF-NAME>*] |*<STORAGE-URL>*}

Select either the storage URL or the remote URL for the destination of the copied command output. Required.

<REMOTE-URL>

Specifies the URL to copy the command output.

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE>`

vrf *<VRF-NAME>*

Specifies the VRF name. The default VRF name is default. Optional.

<STORAGE-URL>

Specifies the USB to copy command output.

Syntax: `{usb}:/<FILE>`

Authority

Administrators

Usage

The `copy diag-dump local-file` command can be used only after the information is captured. Run the `diag-dump <FEATURE-NAME> basic local-file` command before you enter the `copy diag-dump local-file` command to capture the diagnostic information for the specified feature into the local file.

Examples

Copying the output from the local file to a remote URL:

```
switch# diag-dump aaa basic local-file
switch# copy diag-dump local-file tftp://10.100.0.12/diagdump.txt
```

Copying the output from the local file to a USB drive:

```
switch# diag-dump aaa basic local-file
switch# copy diag-dump local-file usb:/diagdump.txt
```

copy show-tech feature

Syntax

```
copy show-tech feature <FEATURE> {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}
```

Description

Copies show tech output using TFTP, SFTP, and USB.

Command context

Manager (#)

Parameters

{*<REMOTE-URL>* [vrf *<VRF-NAME>* | *<STORAGE-URL>*]}

Select either the remote URL or the storage URL for the destination of the copied command output. Required.

<REMOTE-URL>

Specifies the URL to copy the command output. Required.

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE>`

vrf *<VRF-NAME>*

Specifies the VRF name. The default VRF name is default. Optional.

<STORAGE-URL>

Specifies the USB to copy command output. Required.

Syntax: `{usb}:/<FILE>`

Authority

Administrators

Example

Copying show tech output using SFTP:

```
switch# copy show-tech feature aaa sftp://user@10.0.0.12/file.txt vrf mgmt
```

copy show-tech local-file

Syntax

```
copy show-tech local-file {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}
```

Description

Copies show tech output stored in a local file.

Command context

Manager (#)

Parameters

{*<REMOTE-URL>* [vrf *<VRF-NAME>*] | *<STORAGE-URL>*]}

Select either the remote URL or the storage URL for the destination of the copied command output. Required.

<REMOTE-URL>

Specifies the URL to copy the command output.

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE>`

vrf *<VRF-NAME>*

Specifies the VRF name. The default VRF name is default. Optional.

<STORAGE-URL>

Specifies the USB to copy command output.

Syntax: `{usb}:/<FILE>`

Authority

Administrators

Usage

Before entering the `copy show-tech local-file` command, run the `show tech` command with the `local-file` parameter for the specified feature.

Examples

Copying the output to a remote URL:

```
switch# copy show-tech local-file tftp://10.100.0.12/file.txt
```

Copying the output to a remote URL with a VRF:

```
switch# copy show-tech local-file tftp://10.100.0.12/file.txt vrf mgmt
```

Copying the output to a USB:

```
switch# copy show-tech local-file usb:/file
```

copy support-files

Syntax

```
copy support-files [feature <FEATURE-NAME> | previous-boot | all] {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}
```

Description

Copies a set of support files using TFTP, SFTP, or USB.

Command context

Manager (#)

Parameters

<FEATURE-NAME>

The feature name, for example, `aaa`.

{*<REMOTE-URL>* [vrf *<VRF-NAME>* | *<STORAGE-URL>*]}

Select either the remote URL or the storage URL for the destination of the copied command output. Required.

<REMOTE-URL>

Specifies the URL to copy the command output.

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE>`

vrf <VRF-NAME>

Specifies the VRF name. The default VRF name is default. Optional.

<STORAGE-URL>

Specifies the USB to copy command output.

Syntax: `{usb}:/<FILE>`

Usage

If feature name is not provided, the command collects generic system-specific support information. If a feature name is provided, the command collects feature-specific support information.

Authority

Administrators

Examples

Copying the files to a remote URL:

```
switch# copy support-files tftp://10.100.0.12/file.tar.gz
```

Copying the files of a feature *lldp* to a remote URL with a specified VRF:

```
switch# copy support-files feature lldp tftp://10.100.0.12/file.tar.gz vrf mgmt
```

Copying the files from the previous boot to a remote URL with a specified VRF:

```
switch# copy support-files previous-boot sftp://root@10.0.14.206/file.tar.gz vrf mgmt
```

Copying the files to a USB:

```
switch# copy support-files usb:/file.tar.gz
```

Copying all the support-files to a remote URL:

```
switch# copy support-files all sftp://root@10.0.14.216/file.tar.gz vrf mgmt
```

copy support-log

Syntax

```
copy support-log <DAEMON-NAME> {<STORAGE-URL> | <REMOTE-URL> [vrf <VRF-NAME>]}
```

Description

Copies the specified support log for a daemon TFTP, SFTP, or USB.

Command context

Manager (#)

Parameters

<DAEMON-NAME>

Specifies the name of the daemon. Required.

{*<STORAGE-URL>* | *<REMOTE-URL>* [vrf *<VRF-NAME>*]}

Selects either the storage URL or the remote URL for the destination of the copied command output. Required.

<STORAGE-URL>

Specifies the USB to copy command output.

Syntax: `{usb}:/<FILE>`

<REMOTE-URL>

Specifies the URL to copy the command output.

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE>`

vrf *<VRF-NAME>*

Specifies the VRF name. If no VRF name is provided, the VRF named *default* is used. Optional.

Usage

Fast log is a high performance, per-daemon binary logging infrastructure used to debug daemon level issues by precisely capturing the per daemon/module/functionalities debug traces in real time. Fast log, also referred to as support logs, helps users to understand the feature internals and its specific happenings. The fast logs from one daemon are not overwritten by other daemon logs because fast logs are captured as part of a daemon core dump. Fast logs are enabled by default.

Authority

Administrators

Examples

Copying the support log from the daemon hpe-fand to a remote URL:

```
switch# copy support-log hpe-fand tftp://10.100.0.12/file
```

Copying the support log from the daemon hpe-fand to a remote URL with a VRF named mgmt:

```
switch# copy support-log hpe-fand tftp://10.100.0.12/file vrf mgmt
```

Copying the support log from the daemon hpe-fand to a USB:

```
switch# copy support-log hpe-fand usb:/support-log
```

Overview

Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of User Datagram Protocol (UDP) packets addressed to a destination host. The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.

Traceroute commands

traceroute

Syntax

```
traceroute {IPv4-address | hostname} [ip-option loosesourceroute <IPV4-ADDR>]
     [dstport <NUMBER> | maxttl <NUMBER> | minttl <NUMBER> |
     probes <NUMBER> | timeout <TIME>] [vrf {<VRF-NAME> | mgmt}]
```

Description

Uses traceroute for the specified IPv4 address or hostname with or without optional parameters.

Command context

Operator (>) or Manager (#)

Parameters

IPv4-address

Specifies the IPv4 address of the device to use traceroute.

hostname

Specifies the hostname of the device to use traceroute.

ip-option

Specifies the IP option.

loosesourceroute *<IPV4-ADDR>*

Specifies the route for loose source record route. Enter one or more intermediate router IP addresses separated by ',' for loose source routing.

dstport *<NUMBER>*

Specifies the destination port, *<1-34000>*. Default: 33434

maxttl *<NUMBER>*

Specifies the maximum number of hops to reach the destination, *<1-255>*. Default: 30

minttl *<NUMBER>*

Specifies the Minimum number of hops to reach the destination, *<1-255>*. Default: 1

probes *<NUMBER>*

Specifies the number of probes, *<1-5>*. Default: 3

timeout *<TIME>*

Specifies the traceroute timeout in seconds, *<1-60>*. Default: 3 seconds

vrf *<VRF-NAME>*

Specifies the virtual routing and forwarding (VRF) to use, *<VRF-NAME>*.

mgmt

Specifies use of the management interface.

Authority

Operators or Administrators. Users without administrator authority can execute this command from the operator context (>) only.

Usage

Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of User Datagram Protocol (UDP) packets addressed to a destination host. The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.

Examples

```
switch# traceroute 10.0.10.1
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3 probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute localhost
traceroute to localhost (127.0.0.1), 1 hops min, 30 hops max, 3 sec. timeout, 3 probes
  1   127.0.0.1  0.018ms  0.006ms  0.003ms

switch# traceroute 10.0.10.1 maxttl 20
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 20 hops max, 3 sec. timeout, 3 probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute 10.0.10.1 minttl 1
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3 probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute 10.0.10.1 dstport 33434
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3 probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute 10.0.10.1 probes 2
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 2 probes
  1   10.0.40.2  0.002ms  0.002ms
  2   10.0.30.1  0.002ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms

switch# traceroute 10.0.10.1 timeout 5
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 5 sec. timeout, 3 probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute localhost vrf red
traceroute to localhost (127.0.0.1), 1 hops min, 30 hops max, 3 sec. timeout, 3 probes
  1   127.0.0.1  0.003ms  0.002ms  0.001ms

switch# traceroute localhost mgmt
traceroute to localhost (127.0.0.1), 1 hops min, 30 hops max, 3 sec. timeout, 3 probes
  1   127.0.0.1  0.018ms  0.006ms  0.003ms

switch# traceroute 10.0.10.1 maxttl 20 timeout 5 minttl 1 probes 3 dstport 33434
```

```
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 20 hops max, 5 sec. timeout, 3 probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute 10.0.10.1 ip-option loosesourceroute 10.0.40.2
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3 probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute 10.0.10.1 ip-option loosesourceroute 10.0.40.2 maxttl 20 timeout 5 minttl 1 probes 3 dstport 33434
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 20 hops max, 5 sec. timeout, 3 probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms
```

traceroute6

Syntax

```
traceroute6 {IPv6-address | hostname} [dstport <NUMBER> | maxttl <NUMBER> |
 probes <NUMBER> | timeout <TIME>] [vrf {<VRF-NAME> | mgmt}]
```

Description

Uses traceroute for the specified IPv6 address or hostname with or without optional parameters.

Command context

Operator (>) or Manager (#)

Parameters

IPv6-address

Specifies the IPv6 address of the device to use traceroute.

hostname

Specifies the hostname of the device to use traceroute.

dstport *<NUMBER>*

Specifies the destination port, *<1-34000>*. Default: 33434

maxttl *<NUMBER>*

Specifies the maximum number of hops to reach the destination, *<1-255>*. Default: 30

probes *<NUMBER>*

Specifies the number of probes, *<1-5>*. Default: 3

timeout *<TIME>*

Specifies the traceroute timeout in seconds, *<1-60>*. Default: 3 seconds

vrf *<VRF-NAME>*

Specifies the virtual routing and forwarding (VRF) to use, *<VRF-NAME>*.

mgmt

Specifies use of the management interface.

Authority

Operators or Administrators. Users without administrator authority can execute this command from the operator context (>) only.

Usage

Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of User Datagram Protocol (UDP) packets addressed to a destination host. The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.

Examples

```
switch# traceroute6 0:0::0:1
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24 byte packets
 1  localhost (::1)  0.117 ms  0.032 ms  0.021 ms

switch# traceroute6 localhost
traceroute to localhost (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24 byte packets
 1  localhost (::1)  0.089 ms  0.03 ms  0.014 ms

switch# traceroute6 0:0::0:1 maxttl 30
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24 byte packets
 1  localhost (::1)  0.117 ms  0.032 ms  0.021 ms

switch# traceroute6 0:0::0:1 dsrport 33434
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24 byte packets
 1  localhost (::1)  0.117 ms  0.032 ms  0.021 ms

switch# traceroute6 0:0::0:1 probes 2
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 2 probes, 24 byte packets
 1  localhost (::1)  0.117 ms  0.032 ms

switch# traceroute6 0:0::0:1 timeout 3
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24 byte packets
 1  localhost (::1)  0.117 ms  0.032 ms  0.021 ms

switch# traceroute6 localhost vrf red
traceroute to localhost (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24 byte packets
 1  localhost (::1)  0.077 ms  0.051 ms  0.054 ms

switch# traceroute6 localhost mgmt
traceroute to localhost (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24 byte packets
 1  localhost (::1)  0.089 ms  0.03 ms  0.014 ms

switch# traceroute6 0:0::0:1 maxttl 30 timeout 3 probes 3 dstport 33434
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24 byte packets
 1  localhost (::1)  0.117 ms  0.032 ms  0.021 ms
```

Overview

The ping (Packet Internet Groper) command is a common method for troubleshooting the accessibility of devices. It uses Internet Control Message Protocol (ICMP) echo requests and ICMP echo replies to determine if another device is alive. It also measures the amount of time it takes to receive a reply from the specified destination. The ping command is mostly used to verify IP connectivity between two endpoints which could be switch to switch, host to host, or host to switch. The reply packet tells if the host received the ping and the amount of time it took to return the packet.

Ping commands

ping

Syntax

```
ping <IPv4-address | hostname> [ data-fill <pattern> | datagram-size <size> |
interval <time> | repetitions <number> | timeout <time> | tos <number> | ip-option
(include-timestamp | include-timestamp-and-address |record-route ) | vrf <vrfname>]
```

Description

Pings the specified IPv4 address or hostname with or without optional parameters.

Command context

Operator (>) or Manager (#)

Parameters

<IPv4-ADDR>

Selects the IPv4 address to ping.

<HOSTNAME>

Selects the hostname to ping. Range: 1-256 characters

data-fill *<PATTERN>*

Specifies the data pattern in hexadecimal digits to send. A maximum of 16 "pad" bytes can be specified to fill out the ICMP packet. Default: AB

datagram-size *<SIZE>*

Specifies the ping datagram size. Range: 0-65399, default: 100.

interval *<TIME>*

Specifies the interval between successive ping requests in seconds. Range: 1-60 seconds, default: 1 second.

repetitions *<NUMBER>*

Specifies the number of packets to send. Range: 1-10000 packets, default: Five packets.

timeout *<TIME>*

Specifies the ping timeout in seconds. Range: 1-60 seconds, default: 2 seconds.

tos *<NUMBER>*

Specifies the IP Type of Service to be used in Ping request. Range: 0-255

ip-option [include-timestamp | include-timestamp-and-address | record-route]

Specifies an IP option (`record-route` or `timestamp` option).

include-timestamp

Specifies the intermediate router time stamp.

include-timestamp-and-address

Specifies the intermediate router time stamp and IP address.

record-route

Specifies the intermediate router addresses.

vrf *<VRF-NAME>*

Specifies the virtual routing and forwarding (VRF) to use. When VRF option is not given, the default VRF is used.

Authority

Operators or Administrators. Users without administrator authority can execute this command from the operator context (>) only.

Examples

Pinging an IPv4 address:

```
switch# ping 10.0.0.0
PING 10.0.0.0 (10.0.0.0) 100(128) bytes of data.
108 bytes from 10.0.0.0: icmp_seq=1 ttl=64 time=0.035 ms
108 bytes from 10.0.0.0: icmp_seq=2 ttl=64 time=0.034 ms
108 bytes from 10.0.0.0: icmp_seq=3 ttl=64 time=0.034 ms
108 bytes from 10.0.0.0: icmp_seq=4 ttl=64 time=0.034 ms
108 bytes from 10.0.0.0: icmp_seq=5 ttl=64 time=0.033 ms

--- 10.0.0.0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.033/0.034/0.035/0.000 ms
```

Pinging the localhost:

```
switch# ping localhost
PING localhost (127.0.0.1) 100(128) bytes of data.
108 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.060 ms
108 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.035 ms
108 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.043 ms
108 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.041 ms
108 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.034 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.034/0.042/0.060/0.011 ms
```

Pinging a server with a data pattern:

```
switch# ping 10.0.0.2 data-fill 1234123412341234acde123456789012
PATTERN: 0x1234123412341234acde123456789012
PING 10.0.0.2 (10.0.0.2) 100(128) bytes of data.
108 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.207 ms
108 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.187 ms
```

```
108 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.225 ms
108 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.197 ms
108 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.210 ms

--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.187/0.205/0.225/0.015 ms
```

Pinging a server with a datagram size:

```
switch# ping 10.0.0.0 datagram-size 200
PING 10.0.0.0 (10.0.0.0) 200(228) bytes of data.
208 bytes from 10.0.0.0: icmp_seq=1 ttl=64 time=0.202 ms
208 bytes from 10.0.0.0: icmp_seq=2 ttl=64 time=0.194 ms
208 bytes from 10.0.0.0: icmp_seq=3 ttl=64 time=0.201 ms
208 bytes from 10.0.0.0: icmp_seq=4 ttl=64 time=0.200 ms
208 bytes from 10.0.0.0: icmp_seq=5 ttl=64 time=0.186 ms

--- 10.0.0.0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.186/0.196/0.202/0.016 ms
```

Pinging a server with an interval specified:

```
switch# ping 9.0.0.2 interval 2
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.199 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.192 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.208 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.182 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.194 ms

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 7999ms
rtt min/avg/max/mdev = 0.182/0.195/0.208/0.008 ms
```

Pinging a server with a specified number of packets to send:

```
switch# ping 9.0.0.2 repetitions 10
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.213 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.204 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.201 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.184 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.202 ms
108 bytes from 9.0.0.2: icmp_seq=6 ttl=64 time=0.184 ms
108 bytes from 9.0.0.2: icmp_seq=7 ttl=64 time=0.193 ms
108 bytes from 9.0.0.2: icmp_seq=8 ttl=64 time=0.196 ms
108 bytes from 9.0.0.2: icmp_seq=9 ttl=64 time=0.193 ms
108 bytes from 9.0.0.2: icmp_seq=10 ttl=64 time=0.200 ms

--- 9.0.0.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8999ms
rtt min/avg/max/mdev = 0.184/0.197/0.213/0.008 ms
```

Pinging a server with a specified timeout:

```
switch# ping 9.0.0.2 timeout 3
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.175 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.192 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.190 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.181 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.197 ms
```

```
--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.175/0.187/0.197/0.007 ms
```

Pinging a server with the specified IP Type of Service:

```
switch# ping 9.0.0.2 tos 2
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.033 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.034 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.031 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.034 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.031 ms

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.031/0.032/0.034/0.006 ms
```

Pinging a local host with the specified VRF.

```
switch# ping localhost vrf red
PING localhost (127.0.0.1) 100(128) bytes of data.
108 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.048 ms
108 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.052 ms
108 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.044 ms
108 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.036 ms
108 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.055 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.036/0.047/0.055/0.006 ms
```

Pinging the localhost with the default VRF:

```
switch# ping localhost vrf mgmt
PING localhost (127.0.0.1) 100(128) bytes of data.
108 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.085 ms
108 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.057 ms
108 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.047 ms
108 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.038 ms
108 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.059 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.038/0.057/0.085/0.016 ms
```

Pinging a server with the intermediate router time stamp:

```
switch# ping 9.0.0.2 ip-option include-timestamp
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.031 ms
TS:     59909005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.034 ms
TS:     59910005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.038 ms
```

```
TS:     59911005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.035 ms
TS:     59912005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.037 ms
TS:     59913005 absolute
        0
        0
        0


--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.031/0.035/0.038/0.002 ms
```

Pinging a server with the intermediate router time stamp and address:

```
switch# ping 9.0.0.2 ip-option include-timestamp-and-address
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.030 ms
TS:     9.0.0.2 60007355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.037 ms
TS:     9.0.0.2 60008355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.037 ms
TS:     9.0.0.2 60009355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.038 ms
TS:     9.0.0.2 60010355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.039 ms
TS:     9.0.0.2 60011355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0


--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.030/0.036/0.039/0.005 ms
```

Pinging a server with the intermediate router address:

```
switch# ping 9.0.0.2 ip-option record-route
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.034 ms
RR:     9.0.0.2
        9.0.0.2
        9.0.0.2
        9.0.0.2

108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.038 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.036 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.037 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.035 ms (same route)

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.034/0.036/0.038/0.001 ms
```

ping6

Syntax

```
ping6 {<IPv6-ADDR> | <HOSTNAME>} [data-fill <PATTERN> | datagram-size <SIZE> |
 interval <TIME> | repetitions <NUMBER> | timeout <TIME> | vrrp <VRID> | vrf <VRF-NAME>]
```

Description

Pings the specified IPv6 address or hostname with or without optional parameters. The VRRP option is provided to self-ping the configured link-local address on the VRRP group.

Command context

Operator (>) or Manager (#)

Parameters

IPv6-ADDR

Selects the IPv6 address to ping.

HOSTNAME

Selects the hostname to ping. Range: 1-256 characters

data-fill *<PATTERN>*

Specifies the data pattern in hexadecimal digits to send. A maximum of 16 "pad" bytes can be specified to fill out the ICMP packet. Default: AB

datagram-size *<SIZE>*

Specifies the ping datagram size. Range: 0-65399, default: 100.

interval *<TIME>*

Specifies the interval between successive ping requests in seconds. Range: 1-60 seconds, default: 1 second.

repetitions *<NUMBER>*

Specifies the number of packets to send. Range: 1-10000 packets, default: Five packets.

timeout *<TIME>*

Specifies the ping timeout in seconds. Range: 1-60 seconds, default: 2 seconds.

vrrp *<VRID>*

Specifies the VRRP group ID.

vrf *<VRF-NAME>*

Specifies the virtual routing and forwarding (VRF) to use. When this option is not provided, the default VRF is used.

Authority

Operators or Administrators. Users without administrator authority can execute this command from the operator context (>) only.

Examples

Pinging an IPv6 address:

```
switch# ping6 2020::2
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.386 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.235 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.249 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.240 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.252 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.235/0.272/0.386/0.059 ms
```

Pinging the localhost:

```
switch# ping6 localhost
PING localhost(localhost) 100 data bytes
108 bytes from localhost: icmp_seq=1 ttl=64 time=0.093 ms
108 bytes from localhost: icmp_seq=2 ttl=64 time=0.051 ms
108 bytes from localhost: icmp_seq=3 ttl=64 time=0.055 ms
108 bytes from localhost: icmp_seq=4 ttl=64 time=0.046 ms
108 bytes from localhost: icmp_seq=5 ttl=64 time=0.048 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.046/0.058/0.093/0.019 ms
```

Pinging a server with a data pattern:

```
switch# ping6 2020::2 data-fill ab
PATTERN: 0xab
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.038 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.074 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.075 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.077 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.038/0.068/0.077/0.015 ms
```

Pinging a server with a datagram size:

```
switch# ping6 2020::2 datagram-size 200
PING 2020::2(2020::2) 200 data bytes
208 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.037 ms
208 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.076 ms
208 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms
208 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.077 ms
208 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.066 ms
```

```
--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.037/0.066/0.077/0.016 ms
```

Pinging a server with an interval specified:

```
switch# ping6 2020::2 interval 5
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.043 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.075 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.074 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.075 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.075 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 19999ms
rtt min/avg/max/mdev = 0.043/0.068/0.075/0.014 ms
```

Pinging a server with a specified number of packets to send:

```
switch# ping6 2020::2 repetitions 6
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.039 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.070 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.076 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.071 ms
108 bytes from 2020::2: icmp_seq=6 ttl=64 time=0.078 ms

--- 2020::2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.039/0.068/0.078/0.015 ms
```

Pinging a local host with the specified VRF.

```
switch# ping6 localhost vrf red
PING localhost(localhost) 100 data bytes
108 bytes from localhost: icmp_seq=1 ttl=64 time=0.038 ms
108 bytes from localhost: icmp_seq=2 ttl=64 time=0.050 ms
108 bytes from localhost: icmp_seq=3 ttl=64 time=0.039 ms
108 bytes from localhost: icmp_seq=4 ttl=64 time=0.040 ms
108 bytes from localhost: icmp_seq=5 ttl=64 time=0.027 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.027/0.038/0.050/0.010 ms
```

Pinging the localhost with the default VRF:

```
switch# ping6 localhost vrf mgmt
PING localhost(localhost) 100 data bytes
108 bytes from localhost: icmp_seq=1 ttl=64 time=0.032 ms
108 bytes from localhost: icmp_seq=2 ttl=64 time=0.022 ms
108 bytes from localhost: icmp_seq=3 ttl=64 time=0.040 ms
108 bytes from localhost: icmp_seq=4 ttl=64 time=0.022 ms
108 bytes from localhost: icmp_seq=5 ttl=64 time=0.046 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.022/0.032/0.046/0.010 ms
```

Troubleshooting

Operation not permitted

Symptom

The switch displays an "operation not permitted" message when a user attempts to send a ping request.

Example:

```
switch# ping 100.1.2.10
PING 100.1.2.10 (100.1.2.10) 100(128) bytes of data
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted


--- 100.1.2.10 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4000ms
```

Cause

When an ACL is applied on egress or an ACL is applied to the Control Plane, sending a ping request may be denied. If the ping packet matches a drop entry in the ACL, applying an egress ACL may block traffic sent from the switch CLI ping command.

When this situation occurs, the following error message is displayed: `ping: sendmsg: Operation not permitted`. The message indicates that the ICMP echo request packet has not been sent and is blocked by an egress ACL.

When this message is not displayed, the ping request packet has been sent correctly. A ping failure in this case represents a failure to receive the ICMP echo reply packet.

Action

1. Modify the ACL to allow the ping traffic.
2. Unapply the ACL from egress.
3. Ping a destination which is not matched by the ACL. For example, if the ACL is blocking traffic based on destination IP. Depending on the ACL content, this might not always be possible like when the ACL blocks all ICMP packets.

Network is unreachable

Symptom

User receives a "network is unreachable" message on sending a ping request.

Cause

The ping packet did not get sent, because the switch cannot find an interface with a route that leads to the destination for one of the following reasons:

- A configuration error, such as an interface having an incorrect IP address or subnet defined.
- DHCP having failed to assign an address at all.
- The user meant to ping out the management vrf, but forgot to add `vrf mgmt` to the ping command.

Action

Adjust the switch configuration to ensure that a route to the destination network exists.

Destination Host Unreachable

Symptom

User receives a "Destination host unreachable" message on sending a ping request.

Cause

This issue typically indicates that the host is down or otherwise not returning ICMP echo requests. It is also possible that an intermediate network hop is dropping the packets.

Action

Investigate whether an intermediate hop is not returning pings by using the `traceroute` command. Check the intermediate hop, and then the endpoint. If the destination is another Aruba switch, it is possible that Ingress ACLs on that switch are blocking ping packets. In such cases, the configuration option on the destination switch should be examined.

Remote syslog enables the forwarding of syslog messages to the remote syslog server. The feature supports a maximum of four remote syslog servers. Only one configuration per remote syslog server is allowed. The remote syslog server supports TCP and UDP transport protocols and TLS to establish a connection.

Remote syslog commands

logging

Syntax

```
logging {<IPV4-ADDR> | <IPV6-ADDR> | <HOSTNAME>}
     [udp [<PORT-NUM>] | tcp [<PORT-NUM>]| tls [<PORT-NUM>]]
     [include-auditable-events] [severity <LEVEL>] [vrf <VRF-NAME>]
```

```
logging {<IPV4-ADDR> | <IPV6-ADDR> | <HOSTNAME>}
     [tls [<PORT-NUM>]] [auth-mode {certificate|subject-name}]
     [legacy-tls-renegotiation] [include-auditable-events] [severity <LEVEL>]
     [vrf <VRF-NAME>]
```

```
no logging {<IPV4-ADDR> | <IPV6-ADDR> | <HOSTNAME>}
```

Description

Enables syslog forwarding to a remote syslog server.

The `no` form of this command disables syslog forwarding to a remote syslog server.

Command context

```
config
```

Parameters

{*<IPV4-ADDR>* | *<IPV6-ADDR>* | *<HOSTNAME>*}

Selects the IPv4 address, IPv6 address, or host name of the remote syslog server. Required.

[udp [*<PORT-NUM>*] | tcp [*<PORT-NUM>* | tls [*<PORT-NUM>*]]

Specifies the UDP port, TCP port, or TLS port of the remote syslog server to receive the forwarded syslog messages.

udp [*<PORT-NUM>*]

Range: 1 to 65535. Default: 514

tcp [*<PORT-NUM>*]

Range: 1 to 65535. Default: 1470

tls [*<PORT-NUM>*]

Range: 1 to 65535. Default: 6514

include-auditable-events

Specifies that auditable messages are also logged to the remote syslog server.

severity *<LEVEL>*

Specifies the severity of the syslog messages:

- `alert`: Forwards syslog messages with the severity of `alert (6)` and `emergency (7)`.
- `crit`: Forwards syslog messages with the severity of `critical (5)` and above.
- `debug`: Forwards syslog messages with the severity of `debug (0)` and above.
- `emerg`: Forwards syslog messages with the severity of `emergency (7)` only.
- `err`: Forwards syslog messages with the severity of `err (4)` and above
- `info`: Forwards syslog messages with the severity of `info (1)` and above. Default.
- `notice`: Forwards syslog messages with the severity of `notice (2)` and above.
- `warning`: Forwards syslog messages with the severity of `warning (3)` and above.

auth-mode

Specifies the TLS authentication mode used to validate the certificate.

- `certificate`: Validates the peer using trust anchor certificate based authentication. Default.
- `subject-name`: Validates the peer using trust anchor certificates as well as subject-name based authentication.

legacy-tls-renegotiation

Enables the TLS connection with a remote syslog server supporting legacy renegotiation.

vrf *<VRF-NAME>*

Specifies the VRF used to connect to the syslog server. Optional. Default: `default`

Authority

Administrators

Examples

Enabling the syslog forwarding to remote syslog server 10.0.10.2:

```
switch(config)# logging 10.0.10.2
```

Enabling the syslog forwarding of messages with a severity of `err (4)` and above to TCP port 4242 on remote syslog server 10.0.10.9 with VRF `lab_vrf`:

```
switch(config)# logging 10.0.10.9 tcp 4242 severity err vrf lab_vrf
```

Disabling syslog forwarding to a remote syslog server:

```
switch(config)# no logging
```

Enabling syslog forwarding over TLS to a remote syslog server using subject-name authentication mode:

```
switch(config)#logging example.com tls auth-mode subject-name
```

logging facility

Syntax

```
logging facility {local0 | local1 | local2 | local3
     | local4 | local5 | local6 | local7}

no logging facility
```

Description

Sets the logging facility to be used for remote syslog messages. Default: `local7`

The `no` form of this command disables the logging facility to be used for remote syslog messages.

Command context

`config`

Parameters

`{local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}`

Selects the logging facility to be used for remote syslog messages. Required.

Specifies the severity of the syslog messages:

- `local0`
- `local1`
- `local2`
- `local3`
- `local4`
- `local5`
- `local6`
- `local7`

Authority

Administrators

Examples

Sets the local5 logging facility to be used for remote syslog messages:

```
switch(config)# logging facility local5
```

Troubleshooting

Remote syslog server is not receiving messages

Symptom

The syslog messages are not received on the remote syslog server.

Cause

One or more of the following might be possible causes:

- The remote syslog server is not running.
- The remote syslog server is not reachable from the switch through the specified VRF.
- The source IP is set for the syslog protocol which is not reachable from the syslog server within the specified VRF.
- The remote syslog server has an improper configuration.
- An incorrect TLS Certificate is used in case the switch is in TLS mode.

Action

- Verify that the remote syslog server is running. Refer to the documentation for your remote syslog server.
- Test the reachability of the remote syslog server from the switch by using ping over the specific VRF.
- Test the reachability of the remote syslog server from the source IP of the syslog protocol over the specific VRF.
- Verify that the remote syslog server is configured to receive remote syslog messages. Refer to the documentation for your remote syslog server for more information.
- Make sure that the peer certificate is valid and as per the remote server configuration.

Overview

Service OS is an operating system that the customer only uses to fix filesystem corruption, download new ArubaOS-CX images, update firmware, and other support related issues. HPE Service OS is a Linux distribution that acts as a standalone bootloader and recovery OS for ArubaOS-CX-based switches. It is only accessible if the user is consoled into the switch. The main high level features provided include:

- Access to file system partitions for retrieval of logs, coredumps, and configuration for supportability purposes.
- Filesystem utilities to format and partition a corrupted storage disk.
- Management interface networking with TFTP to download and update a product image.
- Ability to boot primary and secondary ArubaOS-CX product images (.SWI file) on the storage disk.
- Support for clearing the ArubaOS-CX startup-config.
- Ability to not only clear the admin password for ArubaOS-CX, but also change it in SVOS.
- Ability to set the secure mode to enhanced or standard.

This document covers the customer CLI commands available in Service OS, as well as a few non-CLI features.

Service OS CLI login

Description

If the user enters 0 at the boot menu prompt, they will be presented with a Service OS CLI login prompt. The user must enter the login account "admin" to log in. By default, Service OS does not require a password.

To reboot without logging in, enter **`reboot`** as the login user name.

There are two additional login accounts that execute a command without requiring a password: **`reboot`** and **`zeroize`**. Enter the login account **`reboot`** to reboot the management module and **`zeroize`** to initiate a zeroization process. The zeroize user account helps a user reset the admin user account's password.

Example

```
ServiceOS GT.01.01.0001 switch ttyS0

To reboot without logging in, enter 'reboot' as the login user name.

switch login: admin

   Hewlett Packard
   Enterprise
SVOS>
```

```
ServiceOS GT.01.01.0001 switch ttyS0

To reboot without logging in, enter 'reboot' as the login user name.

switch login: reboot
```

```
   Hewlett Packard
   Enterprise
reboot: Restarting system
```

```
ServiceOS login: zeroize
This will securely erase all customer data, including passwords, and
reset the switch to factory defaults.
This action requires proof of physical access via a USB drive.
  * Create a FAT32 formatted USB drive
  * Create a file in the root directory of the USB drive named zeroize.txt
  * Type the following serial number into the zeroize.txt file: 772632X1830018
  * Insert the USB drive into the target module
  * Confirm the following prompt to continue

Continue (y/n)? y
##############################WARNING###############################
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
##############################WARNING###############################

Continue (y/n)? y

reboot: Restarting system
```

Service OS user accounts

Service OS provides a single admin login account. By default, no password is required to log in. Service OS will require a password if the Service OS admin user account password feature is enabled. This setting can be enabled or disabled in ArubaOS-CX.

Service OS boot menu

Description

On boot, the user is presented with a Service OS version banner with version, build date, build time, build ID, and SHA strings.

The user is then shown the boot image profiles.

- Enter 0 to boot the Service OS login CLI.
- Enter 1 to boot the primary ArubaOS-CX image.
- Enter 2 to boot the secondary ArubaOS-CX image.
- If no input is given within 5 seconds, the default boot profile is selected. Alternatively, press **Enter** to select the default boot profile.

The image selected by the user during boot is a run-time decision only and will not persist across reboots. The default image can be configured using the ArubaOS-CX `boot set-default` command.

Example

```
ServiceOS Information:
    Version:          GT.01.01.0001
    Build Date:       2017-07-19 14:52:31 PDT
    Build ID:         ServiceOS:GT.01.01.0001:461519208911:201707191452
    SHA:              46151920891195cdb2267ea6889a3c6cbc3d4193
```

```
Boot Profiles:

0. Service OS Console
1. Primary Software Image [XL.01.01.0001]
2. Secondary Software Image [XL.01.01.0002]

Select profile(primary):
```

NOTE: The (primary) string in the boot menu displays the default boot profile that will be booted after the timeout period. This string will change to (secondary) or (Service OS) depending on the current default boot option.

Console configuration

During boot, Service OS communicates with the RJ45 serial console with a baud rate of 115200. There is no option to change the baud rate during boot.

Additionally, if a USB console is connected to the management module console port, input will automatically be switched over to use the USB console. Automatic switching to USB is consistent with the ArubaOS-CX USB console behavior.

NOTE: Console output always displays on both the RJ45 console port and the USB console port.

ArubaOS-CX boot

Description

After the user has input a boot profile selection at the boot menu or the 5-second selection timeout has expired, Service OS will boot an ArubaOS-CX image.

Service OS displays the following boot strings embedded in the product image header:

- Image name
- Image version
- Build ID
- Build date

Service OS will then present status and boot the image.

Example

```
Booting primary software image...
Verifying Image...
Image Info:

        Name: ArubaOS-CX
     Version: XL.01.01.0001
    Build Id: ArubaOS-CX:XL.01.01.0001:1a36111da4e0:201707171452
  Build Date: 2017-07-17 14:52:27 PDT


Extracting Image...
Loading Image...
Done.
kexec: Starting new kernel
```

File system access

Description

When the user logs in to the Service OS CLI, they are presented with a limited file system. The user can use standard file system commands of cd, ls, and pwd to view and move through the file system.

On login, the user is first placed in the /home directory:

```
(C) Copyright 2017 Hewlett Packard Enterprise Development LP

                        RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP required for possession, use or copying. Consistent with FAR
12.211 and 12.212, Commercial Computer Software, Computer Software
Documentation, and Technical Data for Commercial Items are licensed to the
U.S. Government under vendor's standard commercial license.

To reboot without logging in, enter 'reboot' as the login user name.

ServiceOS login: admin
SVOS> pwd
/home
SVOS>
```

The home directory and the USB device (/mnt/usb and any sub directory) are the only writable directories available. These directories can be used as a staging location for downloading product images using TFTP. /home can also be used as temporary storage before copying files from the management module through TFTP or USB. Any changes made to /home will not persist across reboots or after booting an ArubaOS-CX image.

The root / directory displays viewable directories:

```
SVOS> ls /
bin        coredump   lib        mnt        selftest
cli        home       logs       nos
SVOS>
```

The directories coredump, selftest, nos, and logs each provide the user access to an SSD partition mount. The user may read, but not write any file on these partitions.

These mount points allow the user to copy files on the SSD to a USB storage device or upload files using TFTP. Copying files from the SSD is intended to be used under the guidance of a support engineer (to upload logs or coredumps to HPE support).

USB storage device access is provided through the mount at /mnt/usb.

The remaining directories in the root file system bin, cli, and lib are not intended to be used by the customer.

Service OS mount failure

Description

If the SSD is detected as missing or any of the partitions could not be mounted, Service OS will force the user to boot to the Service OS console and display an error message indicating that recovery should be attempted using the format command.

Example

```
(C) Copyright 2017 Hewlett Packard Enterprise Development LP

                        RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
```

```
Development LP required for possession, use or copying. Consistent with FAR
12.211 and 12.212, Commercial Computer Software, Computer Software
Documentation, and Technical Data for Commercial Items are licensed to the
U.S. Government under vendor's standard commercial license.

To reboot without logging in, enter 'reboot' as the login user name.

 Error, Could not mount the primary storage device.
 This may be due to filesystem or device corruption.
 Please attempt to recover using the "format" command.

ServiceOS login:
```

Service OS CLI command list

Description

After login to Service OS CLI, the user may enter the commands help or ? to get a full list of commands and a terse description for each command. The user may also enter <command> followed by --help to get more detailed help and usage for a specific command.

Example

```
SVOS> ?
Available Commands:

           ? - Display help screen
          cd - Change the working directory
         pwd - Print the current working directory
        help - Display help screen
        boot - Boot a product image
config-clear - Clears the startup-config
enable-shell - Enable support shell access
       erase - Securely erase storage devices on the management module
      format - Formats and partitions the primary storage device
    identify - Prints hardware identification information
          ip - Sets the OOBM Port Network Configuration
       mount - Mount a storage device
        ping - Send ICMP ECHO_REQUEST to network hosts (IPv4)
      reboot - Reboots the Management Module
    password - Set the admin account password
 secure-mode - Sets or retrieves the secure mode setting
          sh - Launch support shell
      umount - Unmounts a storage device
      update - Update a product image
     version - Prints ServiceOS release version information
         cat - Prints files to stdout
          cp - Copy files and directories
          du - Estimate file space usage
          ls - List directory contents
      md5sum - Compute and check md5 message digest
       mkdir - Make directories
          mv - Move (rename) files
          rm - Remove files or directories
       rmdir - Remove empty directories
        tftp - Allows transfer of files to/from a remote machine
        exit - Logout

Enter '<command> --help' for more info
```

Service OS CLI features and limitations

Description

The Service OS CLI provides basic shell functionality that allows you to execute commands and pass arguments to those commands only. The following features are not available:

- Input/output redirection (<, >, >>)
- Job control (&, fg, bg)
- Process piping (|)
- File globbing (*)

NOTE: Even though the Service OS CLI does not provide file globbing capabilities, some commands may provide this functionality internally. An example is the `ls` command.

The following common features are available:

- Command history (**Up Arrow**) and search (**Ctrl-R**)
- Tab completion for file and folder names (not CLI commands)
- Command abort using **Ctrl-C**

Service OS CLI commands

boot

Syntax

`boot`

Description

Presents you with the boot menu prompt. You can then specify which boot profile: primary, secondary, or Service OS console.

Command context

Service OS (`SVOS>`)

Authority

Administrators

Example

Presenting the boot menu prompt:

```
SVOS> boot

ServiceOS Information:
    Version:          GT.01.01.0005
    Build Date:       2017-07-19 14:52:31 PDT
    Build ID:         ServiceOS:GT.01.01.0001:461519208911:201707191452
    SHA:              46151920891195cdb2267ea6889a3c6cbc3d4193

Boot Profiles:
```

```
0. Service OS Console
1. Primary Software Image [XL.01.01.0001]
2. Secondary Software Image [XL.01.01.0001]

Select profile(primary):
```

cat

Syntax

`cat <FILENAME/DIRECTORY-NAME>`

Description

Prints the contents of a file to the console. The Service OS does not allow command output redirection, so this command is only useful for reading short text files.

Command context

Service OS (`SVOS>`)

Parameters

<FILENAME/DIRECTORY-NAME>

Shows the contents of the specified file or directory.

Authority

Administrators

Example

Showing the contents of /nos/hosts:

```
SVOS> cat /nos/hosts
127.0.0.1       localhost.localdomain           localhost

SVOS>
```

cd path

Syntax

`cd path`

Description

Changes the current working directory.

Command context

Service OS (`SVOS>`)

Authority

Administrators

Example

Changing the current working directory:

```
cd /
```

config-clear

Syntax

```
config-clear [primary | secondary]
```

Description

Configures the system to clear the startup-config for the specified boot profile on the next boot. The `startup-config` will be set to use default values and the existing configuration will be renamed to `startup-config-fixme`.

This command is not available if enhanced secure mode is set.

Command context

Service OS (`SVOS>`)

Parameters

`primary`

Clears the `startup-config` for the primary boot profile.

`secondary`

Clears the `startup-config` for the secondary boot profile.

Authority

Administrators

Example

Configuring the system to clear the startup-config:

```
SVOS> config-clear primary

The primary switch configuration will be cleared.

Continue (y/n)? y

The system has been configured to clear the startup-config associated with the
primary boot profile. Please reboot and select the primary boot profile to
complete this action.
SVOS>
```

cp

Syntax

```
cp [options] <SOURCE-FILENAME/SOURCE-DIRECTORY> <DESTINATION-FLENAME/DESTINATION-DIRECTORY>
```

Description

Copies files or directories.

Command context

Service OS (`SVOS>`)

Parameters

`[options]`

Selects the options for the command.

`-d,-P`

Specifies the preservation of symlinks (default if `-R`).

`-a`

Same as `-dpR`.

`R,-r`

Specifies recursiveness, all files, and subdirectories are copied.

`-L`

Specifies the following of all symlinks.

`-H`

Specifies the following of symlinks on command line.

`-p`

Specifies the preservation of file attributes if possible.

`-f`

Specifies the overwriting of a file or directory.

`-i`

Specifies the prompting before an overwrite.

`-l,-s`

Specifies the creation of (sym) links.

`<SOURCE-FILENAME/SOURCE-DIRECTORY>`

Specifies the name of the source file or directory.

`<DESTINATION-FLENAME/DESTINATION-DIRECTORY>`

Specifies the name of the destination file or directory.

Authority

Administrators

Example

Copying /home/customers directory to the /home/clients directory:

```
SVOS> cp /home/customers /home/clients
```

du

Syntax

```
du [options] <FILENAME/DIRECTORY-NAME>...
```

Description

Shows estimated disk space used for each file or directory or both.

Command context

Service OS (`SVOS>`)

Parameters

`[options]`

Selects the options for the command.

`-a`

Show file sizes.

`-L`

Shows all symlinks.

`-H`

Shows symlinks on a command line.

`-d, N`

Shows limited output to directories (and files with `-a`) of depth less than `N`.

`-c`

Shows the total disk space usage of all files or directories or both.

`-l`

Shows the count sizes if hard linked.

`-s`

Shows only a total for each argument.

`-x`

Does not show directories on different file systems.

`-h`

Show sizes in human readable format (1K, 243M, and 2G).

`-m`

Show sizes in megabytes.

`-k`

Show sizes in kilobytes (default).

`<FILENAME/DIRECTORY-NAME>`

Specifies the file or directory or both for displaying a size estimate.

Authority

Administrators

Example

Estimating disk space for the /nos directory:

```
SVOS> du -ah /nos
196.4M  /nos/primary.swi
196.4M  /nos
SVOS>
```

erase zeroize

Syntax

```
erase zeroize
```

Description

Securely erases any user data contained on the SSD or other storage devices on the management module.

NOTE: Back up all data before running this command or all user/config data will be lost.

Command context

Service OS (`SVOS>`)

Authority

Administrators

Example

Erasing user data:

```
SVOS> SVOS> erase --help
Usage: erase zeroize

Securely erases storage devices on the management module.
SVOS>
```

```

```
SVOS> erase zeroize
##############################WARNING###############################
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
##############################WARNING###############################

Continue (y/n)? y
reboot: Restarting system

ServiceOS Information:
    Version: GT.01.01.0001
    Build Date: 2017-07-19 14:52:31 PDT
    Build ID: ServiceOS:GT.01.01.0001:461519208911:201707191452
    SHA: 46151920891195cdb2267ea6889a3c6cbc3d4193

################ Preparing for zeroization #################

################ Storage zeroization ########################
################ WARNING: DO NOT POWER OFF UNTIL ###########
################   ZEROIZATION IS COMPLETE ###########
################ This should take several minutes ###########
################ to one hour to complete   ###########

################ Restoring files ############################
```
```

exit

Syntax

`exit`

Description

Logs the user out from the `SVOS>` prompt.

Command context

Service OS (`SVOS>`)

Authority

Administrators

Example

Loging the user out from the `SVOS>` prompt:

```
SVOS> exit

(C) Copyright 2017 Hewlett Packard Enterprise Development LP

                      RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP required for possession, use or copying. Consistent with FAR
12.211 and 12.212, Commercial Computer Software, Computer Software
Documentation, and Technical Data for Commercial Items are licensed to the
U.S. Government under vendor's standard commercial license.

To reboot without logging in, enter 'reboot' as the login user name.

ServiceOS login:
```

format

Syntax

`format`

Description

Configures the primary storage device with the correct partition and file system formatting. This command removes all pre-existing data on the primary storage device.

Command context

Service OS (`SVOS>`)

Authority

Administrators

Example

Configuring the primary storage device with the correct partition and file system formatting:

```
SVOS> format
####################WARNING#####################
```

```
The following action will cause all data on
the primary storage device to be lost. After
formatting has completed, a reboot will be
initiated to complete storage initialization.
####################WARNING####################

Continue? (y/n): y

Working...This may take a few minutes...
```

identify

Syntax

```
identify
```

Description

Prints the version of the SVOS and of the UEFI BIOS.

Command context

Service OS (`SVOS>`)

Authority

Administrators

Example

Printing the version of the SVOS and of the UEFI BIOS:

Output from an 8320 switch:

```
SVOS> identify
mc svos_primary           : TL.01.01.0004
mc svos_secondary         : TL.01.01.0004
mc cpld/1                 : 8
mc cpld/2                 : 7
mc cpld/3                 : 7
mc uefi                   : TL-01-0013
mc uefi_capsule           : TL-01-0013
Support Info              : SE:0
```

Output from an 8325 switch:

```
SVOS> identify
mc svos_primary           : GL.01.03.0002
mc svos_secondary         : GL.01.03.0002
mc uefi                   : GL-01-0010
mc uefi_capsule           : GL-01-0010
mc cpld_cpu               : 0xF
mc cpld_main/1            : 0x10
mc cpld_main/2            : 0x10
mc cpld_main/3            : 0x10
mc cpld_fan               : 0x9
mc xgig_single            : 0.86_800005B0
Support Info              : SE:0
SVOS>
```

ip

Syntax

`ip {show | dhcp | disable | addr <ADDR-NETMASK-GATEWAY>}`

Description

Shows or configures the port with a static IP address (IPv4 only) or enables the DHCP client on the port. An address is set only if a DHCP server is available to provide one.

Command context

Service OS (`SVOS>`)

Parameters

`{show | dhcp | disable | addr <ADDR-NETMASK-GATEWAY>}`

Selects the options for the OOBM port.

`show`

Shows the OOBM port.

`dhcp`

Configures the port with a DHCP address.

`disable`

Disables the OOBM port.

`addr <addr netmask gateway>`

Configures the port with a static IP address (IPv4 only). Specify address, netmask, and gateway as A.B.C.D.

Authority

Administrators

Example

Configuring the port with a DHCP IP address:

```
SVOS> ip dhcp
SVOS> ip show
Interface  : Link Up
IP Address : 10.0.26.17
Subnet Mask: 255.255.252.0
Gateway    : 10.0.24.1

SVOS> ip disable
SVOS> ip show
Interface : Disabled
SVOS>
```

ls

Syntax

`ls [<OPTIONS>] [<FILE-NME>]`

Description

This command lists directory contents.

Command context

Service OS (`SVOS>`)

Parameters

<OPTIONS>

Specifies options for the command.

`-1`

Shows one-column output.

`-a`

Shows entries which start with a period (.).

`-A`

Shows output similar to `-a`, but excludes a period (.) and a double period (..).

`-C`

Shows output list by columns.

`-x`

Shows output list by lines.

`-d`

Shows listing of directory entries instead of contents

`-L`

Follows symlinks.

`-H`

Follows symlinks on the command line.

`-R`

Recurse.

`-p`

Appends a slash (/) to directory entries.

`-F`

Appends an indicator to entries. An indicator can be as an asterisk (*) or slash (/) or equal sign (=) or at sign (@) or pipe (|).

`-l`

Shows the output in a long listing format.

`-i`

Shows the list inode numbers.

`-n`

Shows a list of numeric UIDs and GIDs instead of names.

-s

Shows a list of allocated blocks.

-e

Shows in one column a list with the full date and time.

-h

Shows list sizes in human readable format (1K, 243M, 2G) with a one-column output.

-r

Shows in one column a sort in reverse order.

-S

Shows in one column a sort by size.

-X

Shows in the output sort by extension.

-v

Shows in one column a sort by version.

-c

With `-l`, it shows a sort in one column by `ctime`.

-t

With `-l`, it shows a sort by `mtime`.

-u

With `-l`, sort by `atime`.

-c

With `-l`, it shows a sort in one column by `ctime`.

-w *<N>*

Assumes that the terminal has the number of columns wide as specified by <*N*>.

--color[={always | never | auto}]

Controls color in the output.

<FILE-NAME>

Specifies the name of the file to list.

Authority

Administrators

Example

Listing directory contents:

```
SVOS> ls -la /nos
drwxr-xr-x    3 0        0             4096 Nov 21 03:19 .
drwxr-xr-x   11 0        0              220 Nov 21 03:21 ..
drwx------    2 0        0            16384 Nov 21 03:20 lost+found
-rwxr-xr-x    1 0        0        205957424 Nov 21 03:19 primary.swi
SVOS>
```

md5sum

Syntax

```
md5sum [-c | -s | -w] [<FILE-NAME>]
```

Description

This command computes and checks the MD5 message digest.

Command context

Service OS (SVOS>)

Parameters

[-c | -s | -w]

Selects the options for the command.

-c

Specifies to check the sums against the list in files.

-s

Specifies not output anything, status code shows success.

-w

Specifies to warn about improperly formatted checksum lines.

<FILE-NAME>

Specifies the file name to run the checksum against.

Authority

Administrators

Example

Computing and checking the MD5 message digest for /nos/primary.swi:

```
SVOS> md5sum /nos/primary.swi
93ffc89e7ec357854704d8e450c4b7ab  /nos/primary.swi
SVOS>
```

mkdir

Syntax

```
mkdir [-m | -p] [<DIRECTORY-NAME>]
```

Description

This command makes directories.

Command context

Service OS (SVOS>)

Parameters

[-m | -p]

Specifies the options for the command.

-m

Specifies the mode.

-p

Specifies to make parent directories as needed with no errors for pre-existing directories.

<DIRECTORY-NAME>

Specifies the directory to create.

Authority

Administrators

Example

Making the dir directory:

```
SVOS> mkdir dir
```

mount

Syntax

`mount <DEVICE>`

Description

This command mounts the SSD partitions to the following locations: `/coredump`, `/logs`, `/nos`, `/selftest`, and mounts the USB device to `/mnt/usb`.

Users can mount USB flash drives formatted as either FAT16 or FAT32 with a single partition.

Command context

Service OS (`SVOS>`)

Parameters

<DEVICE>

Specifies the device to be mounted. Supported device options include `all` and `usb`.

Authority

Administrators

Examples

Mounting all of the SSD partitions:

```
SVOS> mount all
SVOS> mount usb
```

mv

Syntax

```
mv [-f | -i | -n] <TARGET-DIRECTORY>
```

Description

This command moves (renames) files.

Command context

Service OS (SVOS>)

Parameters

-f

Specifies not to prompt before overwriting.

-i

Specifies to prompt before overwriting.

-n

Specifies to not overwrite an existing file.

Authority

Administrators

Example

Moving the file named myfile:

```
SVOS> mv myfile
```

password

Syntax

```
password
```

Description

Sets the admin user account password for both Service OS and ArubaOS-CX once the user boots into ArubaOS-CX and saves the configuration. This will overwrite the previous password if one exists. User input is masked with asterisks.

This command is not available if enhanced secure mode is set.

Command context

Service OS (SVOS>)

Authority

Administrators

Example

Setting the admin account password:

```
SVOS> password
Enter password:********
Confirm password:********
SVOS>
```

ping

Syntax

`ping <HOST-IP-ADDRESS>`

Description

Pings network hosts for debug purposes.

Command context

Service OS (`SVOS>`)

Parameters

<HOST-IP-ADDRESS>

Specifies the host IP address.

Authority

Administrators

Example

Pinging a network host:

```
SVOS> ping 10.0.8.10
PING 10.0.8.10 (10.0.8.10): 56 data bytes
64 bytes from 10.0.8.10: seq=0 ttl=63 time=3.496 ms
64 bytes from 10.0.8.10: seq=1 ttl=63 time=0.367 ms
64 bytes from 10.0.8.10: seq=2 ttl=63 time=0.380 ms
64 bytes from 10.0.8.10: seq=3 ttl=63 time=0.282 ms
64 bytes from 10.0.8.10: seq=4 ttl=63 time=0.669 ms
^C
--- 10.0.8.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.282/1.038/3.496 ms
SVOS>
```

pwd

Syntax

`pwd`

Description

Displays the current working directory.

Command context

Service OS (`SVOS>`)

Authority

Administrators

Example

Displaying the current working directory:

```
SVOS> pwd
/home
SVOS>
```

reboot

Syntax

```
reboot
```

Description

Reboots the Management Module.

Command context

Service OS (SVOS>)

Authority

Administrators

Example

Rebooting the management module:

```
SVOS> reboot
reboot: Restarting system
```

rm

Syntax

```
rm [-f | -i | -R | -r] <FILE-NAME>
```

Description

Removes files or directories.

Command context

Service OS (SVOS>)

Parameters

[-f | -i | -R | -r]

Selects the options for removing files or directories.

-f

Never prompt before removing files or directories.

-i

Always prompt before removing files or directories.

-R | -r

Recursive.

Authority

Administrators

Example

Removing the file named `foo`:

```
SVOS> rm foo
```

rmdir

Syntax

`rmdir [-p] <DIRECTORY-NAME>`

Description

Removes empty directories.

Command context

Service OS (`SVOS>`)

Parameters

-p

Specifies to remove parent directories.

Authority

Administrators

Example

Removing the empty `foo` directory:

```
SVOS> rmdir foo
SVOS>
```

secure-mode

Syntax

`secure-mode <enhanced | standard | status>`

Description

Sets the secure mode to enhanced or standard secure mode. Also can display the current secure mode. A zeroization is required before switching between enhanced and standard secure modes.

The command also displays a message notifying the user that they are already in the targeted secure mode.

Command context

Service OS (`SVOS>`)

Authority

Administrators

Example

Setting the secure mode to enhanced or standard:

```
SVOS> secure-mode --help
Usage: secure-mode <enhanced | standard | status>

Set or retrieve the secure mode setting. Requires a zeroization to change modes.
SVOS>
```

```
SVOS> secure-mode enhanced
##############################WARNING###############################
This will set the switch into enhanced secure mode.  Before
enhanced secure mode is enabled, the switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
This should take several minutes to one hour to complete.
##############################WARNING###############################

Continue (y/n)? y
reboot: Restarting system
```

```
SVOS> secure-mode standard
##############################WARNING###############################
This will set the switch into standard secure mode.  Before
standard secure mode is enabled, the switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
This should take several minutes to one hour to complete.
##############################WARNING###############################

Continue (y/n)? y
reboot: Restarting system
```

```
SVOS> secure-mode standard
##############################WARNING###############################
Secure mode is already set to standard.  Setting it again will
repeat the zeroization process.  The switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
This should take several minutes to one hour to complete.
##############################WARNING###############################

Continue (y/n)? y
reboot: Restarting system
```

```
SVOS> secure-mode status
enhanced secure mode is set.
SVOS>
```

sh

Syntax

`sh`

Description

Launches a bash shell for support purposes. To quit bash, enter `exit`.

This command is not available if enhanced secure mode is set.

Command context

Service OS (`SVOS>`)

Authority

Administrators

Example

Launching a bash shell:

```
SVOS> sh
switch:/cli/fs/home#
```

umount

Syntax

`umount <DEVICE>`

Description

Unmounts the SSD partitions mounted to the following locations: `/coredump`, `/logs`, `/nos`, `/selftest`, and unmounts the USB device mounted to `/mnt/usb`.

Command context

Service OS (`SVOS>`)

Parameters

<DEVICE>

Specifies the device to be unmounted. Supported device options include `all` and `usb`.

Authority

Administrators

Examples

Unmounting all devices:

```
SVOS> umount all
SVOS> umount usb
```

Unmounting a USB device:

```
SVOS> umount all
SVOS> umount usb
```

update

Syntax

```
update {primary | secondary} <IMAGE>
```

Description

Verifies and installs a product image. The user can select the primary or secondary boot profile to update and the location of the file.

Command context

Service OS (`SVOS>`)

Parameters

`{primary | secondary}`

Selects either the primary or secondary image.

`<IMAGE>`

Specifies the image name.

Authority

Administrators

Examples

Updating the software image using TFTP:

NOTE: The OOBM port is disabled on first boot and must be enabled using the `ip` command.

```
SVOS> ip dhcp
SVOS> ip show
Interface  : Link Up
IP Address : 192.0.2.22
Subnet Mask: 255.255.200.20
Gateway    : 10.0.24.1
SVOS> tftp -g -r XL.10.00.0001.swi -l image.swi 192.4.8.10
XL.10.00.0001.swi 100% |*****************************|   178M  0:00:00 ETA
SVOS> ls
image.swi
SVOS> update primary image.swi
Updating primary software image...
Verifying image...
Done
```

Update the software image using USB:

NOTE: This example assumes that the user has preloaded a USB flash drive with the image to be updated. The image name on the flash drive is not important.

```
SVOS> mount usb
SVOS> ls /mnt/usb
image.swi
SVOS> update primary /mnt/usb/image.swi
Updating primary software image...
```

```
Verifying image...
Done
```

tftp

Syntax

```
tftp {-b | -g | -l <LOCAL-FILE> | -p | -r <REMOTE-FILE>} host [<PORT>]
```

Description

Transfers files to and from a remote machine (TFTP a file).

Command context

Service OS (SVOS>)

Parameters

{-b | -g | -l | -p | -r *<REMOTE-FILE>*}

Selects the options for transferring a file.

-b

Specifies the transfer blocks of size octets. The default blocksize is set to 1468, which can be overridden with the -b option.

-g

Specifies to get a file.

-l

Specifies a local file.

-p

Specifies to put a file in remote location.

-r *<REMOTE-FILE>*

Specifies a remote file.

<PORT>

Specifies the port for transfer. If no port option is specified, TFTP uses the standard UDP port 69 by default.

Authority

Administrators

Example

Transfering files:

```
SVOS> tftp -b 65464 -g -r XL.10.00.0002.swi.swi 192.0.2.1
XL.10.00.0002 100% |*******************************|   178M  0:00:00 ETA
SVOS>
```

version

Syntax

```
version
```

Description

Displays the following build strings:

- Version.
- Build date.
- Build time.
- Build ID.
- SHA.

Command context

Service OS (`SVOS>`)

Authority

Administrators

Example

Displaying version build strings:

```
SVOS> version
ServiceOS Information:
    Version:          GT.01.01.0001
    Build Date:       2017-07-19 14:52:31 PDT
    Build ID:         ServiceOS:GT.01.01.0001:461519208911:201707191452
    SHA:              46151920891195cdb2267ea6889a3c6cbc3d4193
SVOS>
```

In-System Programming Overview

The ISP (In-System Programming) feature provides an automated way to roll out updates to various programmable devices in an ArubaOS-CX network switch, after the product has shipped. ISP is intended to run automatically either at boot time or as new modules are inserted into the chassis at runtime.

`Show tech` command list for the ISP feature

Task	Command
Displaying versions of all present programmable devices.	`show tech isp`
Displaying stored log files from any ISP updates on the system.	`show tech update-log`

See the *Aruba 832x Command-Line Interface Guide for ArubaOS-CX* for additional information about the `show tech` commands.

In-System Programming commands

`clear update-log`

Syntax

```
clear update-log
```

Description

Clears stored log files of any In-System Programming updates on the system.

When run on the active management module, this command also clears log files from most other CPUs in the system. It must be run separately in standby context to clear log files on the standby management module.

Command context

Manager (#)

Authority

Administrators

`show needed-updates`

Syntax

```
show needed-updates [next-boot [primary|secondary]]
```

Description

Displays whether any programmable devices are in need of an update.

Without the `next-boot` parameter, this command displays needed updates relative to the currently running ArubaOS-CX image.

With the `next-boot` parameter, this command displays needed updates relative to an ArubaOS-CX image file in the persistent storage of the switch, which might be different from the currently running image. If either the `primary` or `secondary` parameter is specified, this command queries that specific ArubaOS-CX image file. Otherwise, it queries the default ArubaOS-CX image file as set by the most recent `boot system` or `boot set-default` command.

Command context

Manager (`#`)

Authority

Administrators

Overview

The 8320 switch only supports Boot-up Diagnostics (Power On Selftest aka POST).

Power On Self Test (POST) is the first task which verifies the hardware functionality of various modules during boot-up. Based on the criticality of the test, the selftest module decides whether to go ahead with the boot-up sequence of a particular subsystem or interface during a POST failure.

POST comprises of the following:

- **Front-end Port Loopback tests**

  This test verifies the physical port front-end interface.

  These tests check if a particular interface can function properly. A test failure would mean that the particular interface is marked as "Failed" and thus it would become unavailable for use.

  This test is run when "no fastboot" is configured.

- **Register read/write**

  This test checks for the registers and tables in the ingress pipeline of ASIC. It is always run during platform initialization only.

Selftest commands

fastboot

Syntax

```
fastboot

no fastboot
```

Description

Enables fastboot for the system.

The `no` form of this command disables fastboot for the system.

Command context

`config`

Authority

Administrators

Usage

When fastboot is enabled, all tests under a Power On Self Test (POST) are skipped. By default, fastboot is enabled.

After disabling fastboot, save switch configurations and then reboot for POST to run. POST verifies the hardware functionality of various modules during boot-up. Based on the criticality of the test, the selftest module decides whether to go ahead with the boot-up sequence of a particular subsystem or interface during a POST failure.

POST runs memory built-in selftest (BISTs) and front-end port loopback tests. Memory BISTs verify the internal and external memory blocks present in the module. The memory tables are critical for proper functionality of the system so any failures in these tests results in the corresponding subsystem to be marked as "Failed" and thus that subsystem is not available for use.

Front-end port loopback tests verify the physical port front-end interface. These tests check if a particular interface can function properly. A test failure means that a particular interface has been marked as "Failed" and is now unavailable for use.

Examples

Enabling fastboot:

```
switch# configure terminal
switch(config)# fastboot
switch(config)# end
switch# show running-config
Current configuration:
!
!Version ArubaOS-CX XL.10.00.0002
module 1/1 product-number jl363a
!
!
!
!
!
!
!
vlan 1
interface 1/1/1
    no shutdown
    no routing
```

Disabling fastboot:

```
switch# configure terminal
switch(config)# no fastboot
switch(config)# end
switch# show running-config
Current configuration:
!
!Version ArubaOS-CX XL.10.00.0002
module 1/1 product-number jl363a
!
!
!
no fastboot
!
!
!
!
vlan 1
interface 1/1/1
    no shutdown
    no routing
```

show selftest

Syntax

```
show selftest
show selftest interface [<PORT-NUM>] [vsx-peer]
```

Description

Displays selftest results.

Command context

Manager (#)

Parameters

<SLOT-ID>

Shows the selftest results for the slot ID of the line or fabric module.

<PORT-NUM>

Shows the selftest results for the port number.

[vsx-peer]

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed.

Authority

Operators or Administrators. Users without administrator authority can execute this command from the operator context (>) only.

Examples

Displaying the output when fastboot is disabled:

```
8320# show selftest
interface




Name       Status            ErrorCode
LastRunTime

---------- ----------------- ----------------
-------------------

1/1/2      skipped
0x0

1/1/44     skipped
0x0

1/1/46     skipped           0x0

8320# show selftest interface 1/1/1

Name       Status            ErrorCode        LastRunTime
---------- ----------------- ---------------- -------------------
1/1/1      skipped           0x0
```

Displaying the output when fastboot is enabled:

```
8320# show selftest interface

Name       Status            ErrorCode        LastRunTime
---------- ----------------- ---------------- -------------------
1/1/12     passed            0x0              2018-02-16 18:15:53
1/1/47     passed            0x0              2018-02-16 18:15:53
1/1/15     passed            0x0              2018-02-16 18:15:53
```

```
8320# show selftest interface 1/1/1

Name       Status            ErrorCode        LastRunTime
---------- ----------------- ---------------- --------------------
1/1/1      passed            0x0              2018-02-16 18:15:53
```

Testing to register read/write:

NOTE: This test is run irrespective of fastboot being enabled or disabled.

```
8320# show selftest

Name       Id   Status          ErrorCode  LastRunTime
---------- ---- --------------- ---------- --------------------
LineModule 1/1  passed          0x0        2018-02-16 18:15:53
```

Overview

Device zeroization lets you remove all user files from flash storage, including solid-state drives (SSDs). User files cannot be retrieved after the zeroization is complete.

NOTE: Zeroization can occur in both ArubaOS-CX and Service OS. This section covers zeroization and ArubaOS-CX. For information about zeroization and Support OS, see **erase zeroize** on page 62 .

Zeroization preserves the primary and secondary software images on the SSD. Zeroization also preserves manufacturing information.

The sensitive user files stored on an SSD or SPI flash/EEPROM storage or both include:

- Switch configurations.
- System generated private keys.
- User installed private keys.
- Admin/operator password files.

Zeroization commands

erase all zeroize

Syntax

```
erase all zeroize
```

Description

Erases customer data on the management modules in a secure manner. The command prompts for confirmation of zeroization.

Command context

```
config
```

Authority

Administrators

Example

Erasing customer data on the management modules in a secure manner:

```
8320# erase all zeroize
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
Continue (y/n)? y
The system is going down for zeroization.
8320#

Looking for SvOS.

Primary SvOS:  Checking... Loading... Booting...
```

```
ServiceOS Information:
    Version:          TL.01.01.0004
    Build Date:       2017-12-08 11:42:26 PST
    Build ID:         ServiceOS:TL.01.01.0004:2cb864c7ff6f:201712081142
    SHA:              2cb864c7ff6f9fcb89ea48575dac552ca64336b9


################ Preparing for zeroization #################


################ Storage zeroization ######################
################ WARNING: DO NOT POWER OFF UNTIL  ##########
################          ZEROIZATION IS COMPLETE ##########
################ This should take several minutes ##########
################ to one hour to complete          ##########


################ Restoring files ############################

Boot Profiles:

0. Service OS Console
1. Primary Software Image [TL.10.00.0003]
2. Secondary Software Image [TL.10.00.0003]

Booting primary software image...
Verifying Image...
Image Info:

        Name: ArubaOS-CX
     Version: TL.10.00.0003
    Build Id: ArubaOS-CX:TL.10.00.0003:39244ea0eab9:201803032112
  Build Date: 2018-03-03 13:17:58 PST
```

HTTP 404 error when accessing the switch URL

Symptom

The switch is operational and you are using the correct URL for the switch, but attempts to access the REST API or Web UI result in an HTTP 404 "Page not found" error.

Cause

REST API access is not enabled on the VRF that corresponds to the access port you are using. For example, you are attempting to access the REST API or Web UI from the management (OOBM) port, and access is not enabled on the `mgmt` VRF.

Action

Use the `https-server vrf` command to enable REST API access on the specified VRF.

For example:

```
switch(config)# https-server vrf mgmt
```

HTTP 401 error "Login failed: session limit reached"

Symptom

A REST request or Web UI login attempt returns response code 401 and the response body contains the following text string:

```
Login failed: session limit reached
```

Cause

A user attempted to log into the REST API or the Web UI but that user already has the maximum number of concurrent sessions running.

Action

1. Log out from one of the existing sessions.

   Browsers share a single session cookie across multiple tabs or even windows. However, scripts that POST to the login resource without later posting to the logout resource can easily create the maximum number of concurrent sessions.

2. If the session cookie has been lost and it is not possible to log out of the session, wait for the session idle time limit to expire.

   When the session idle timeout expires, the session is terminated automatically.

3. If it is important enough to stop all HTTPS sessions on the switch instead of waiting for the session idle time limit to expire, you can stop all HTTPS sessions using the `https-server session close all` command.

   This command stops and starts the `hpe-restd` service, so using this command affects all existing REST sessions, Web UI sessions, and real-time notification subscriptions.

Networking Websites

Hewlett Packard Enterprise Networking Information Library

www.hpe.com/networking/resourcefinder

Hewlett Packard Enterprise Networking Software

www.hpe.com/networking/software

Hewlett Packard Enterprise Networking website

www.hpe.com/info/networking

Hewlett Packard Enterprise My Networking website

www.hpe.com/networking/support

Hewlett Packard Enterprise My Networking Portal

www.hpe.com/networking/mynetworking

Hewlett Packard Enterprise Networking Warranty

www.hpe.com/networking/warranty

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

For additional websites, see **Support and other resources**.

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.