NetBackup Access Appliance Command Reference Guide

Release 8.5

Veritas

Oct 29, 2025

Contents:

1 Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054
http://www.veritas.com

1.1 Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan) CustomerCare@veritas.com

Japan CustomerCare_Japan@veritas.com

1.2 Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 3. The latest documentation is available on the Veritas website:

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

1.3 Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

APPL.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

1.4 Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

2 Overview

This chapter includes the following topics:

- *Scope of the Veritas Access Appliance Command Reference Guide*
- *Where to find the documentation*
- *Using the Access Appliance shell menu*

2.1 Scope of the Veritas Access Appliance Command Reference Guide

This document describes the commands that are used in the Access Appliance shell menu. These commands are used in the following scenarios:

- Access Appliance node-level management. For example, the `set network` command for setting network, and the `show hardware` command for monitoring the node hardware.

For cluster-level management commands that are used in the Access CLI, refer to the Veritas Access Command Reference Guide.

See "Where to find the documentation" on page 8.

2.2 Where to find the documentation

The latest version of the Veritas Access Appliance documentation is available on the Veritas Support website and the Veritas Services and Operations Readiness Tools (SORT) website.

https://www.veritas.com/content/support/en_US/Appliances.html

https://sort.veritas.com/documents

You need to specify the product and the platform and apply other filters for finding the appropriate document. The following guides are available for the Access Appliance:

- Veritas Access Appliance Initial Configuration Guide
- Veritas Access Appliance Command Reference Guide
- Veritas Access 3350 Appliance Product Description
- Veritas Access 3350 Appliance Hardware Installation Guide
- Veritas Access Appliance Safety and Maintenance Guide
- Veritas Access Appliance Third-Party Legal Notices Guide
- Veritas Access Appliance Upgrade Guide
- Veritas™ Appliance AutoSupport Reference Guide
- Veritas Access Appliance Cloud Storage Tiering Solutions Guide
- Veritas Access Appliance Solutions Guide for Enterprise Vault
- Veritas Access Appliance Troubleshooting Guide
- Veritas Access Appliance Administrator's Guide
- Veritas Access Appliance Solutions Guide for NetBackup
- Veritas Access Appliance Release Notes

2.3 Using the Access Appliance shell menu

The Access Appliance shell menu provides a menu-based interactive shell interface through which an administrator can manage the Veritas Access Appliance. The interface is made up of hierarchical views that contain the administrative commands and options. When you log onto the Access Appliance shell menu, the shell view is displayed.

To navigate to execute available commands, type the name of the option you want from the list of available options. For example, from the shell view, type support and press Enter to view the list of available options. A command consists of three keywords and an attribute, sometimes attribute is not necessary for different commands. For example, for the `support logbrowser start <active-time=10>` command, support, logbrowser and start are the keywords, active-time is the attribute and 10 is the value set for the attribute. The `show network interface` command does not have any attribute.

Helpful tips

The following list contains some helpful tips for using the Access Appliance shell menu:

- Press Tab or Enter to auto-complete a command.
- Press the spacebar key to display the next parameter that needs to be entered.
- Type a question mark (?) to show more information about the commands or sub-views that are available in the current view. If you type ? after you enter a command or option, more information about that command is shown, such as the format and usage of the command parameters.
- When you press the Enter key, the next mandatory parameter that needs to be entered is displayed. A mandatory parameter is one that does not have predefined values.
- Command parameters that are in angular brackets (< >) are mandatory; whereas the command parameters that are in square brackets ([ ]) are optional. For example, in the `system import iso` view command, there is one mandatory parameter: <*path*=>; and in the `import certificate device-certificate`, the following command has two optional parameters: *[password=] [path=]*.
- In the Veritas Access Appliance shell menu, use the exit command to logout and exit from the current shell.

3 Alerts commands

3.1 delete alerts

delete alerts - Disable Call Home feature and delete email accounts.

3.1.1 SYNOPSIS

delete alerts callhome

delete alerts email-hardware *email_address*

delete alerts email-smtp

delete alerts email-software *email_address*

delete alerts snmp

3.1.2 DESCRIPTION

You can use the `delete alerts callhome` commands to instruct the appliance not to send the appliance health status to Veritas Technical Support. Veritas uses the health status to automatically open Support cases to resolve problems faster. The functionality is enabled by default.

3.1.3 OPTIONS

delete alerts callhome

Disable the Call Home feature.

delete alerts email-hardware *email_address*

Delete a hardware administrator's email account for Access Appliance to use. Where *email_address* is the user's email address.

delete alerts email-smtp

Delete the SMTP server that Access Appliance uses.

delete alerts email-software *email_address*

Delete a software administrator's email account for Access Appliance to use. Where *email_address* is the user's email address.

delete alerts snmp

Disable the ability to send SNMP notifications (traps) for monitoring.

3.2 set alerts

set alerts - Alerts and Call Home settings, configure email, set a threshold value for the disk space of any partition, add SNMP information.

3.2.1 SYNOPSIS

set alerts callhome

set alerts email-hardware *email_address*

set alerts email-notification-interval *time*

set alerts email-smtp *port*

set alerts email-smtp *smtp_server smtp_sender_id [smtp_account]*

set alerts email-software *email_address*

set alerts hardware-threshold

set alerts snmp enable *version*

set alerts snmp disable

set alerts snmp *community*

set alerts snmp *server port*

set alerts snmp-security *security*

3.2.2 DESCRIPTION

You can use the `set alerts callhome` commands to instruct the appliance to send the appliance health status to Veritas Technical Support. Veritas uses the health status to automatically open Support cases to resolve problems faster. The functionality is enabled by default.

Use `set alerts email` command to add email address that the appliance uses. You can use this command to define one or more emails.

Use `set alerts hardware-threshold` set a threshold value for a disk space, CPUIdle, MemorySwap,MemoryUsage, IOWait, disklog, diskroot, DiskSystemSwap, receive alerts when the disk space of any partition passes this threshold value.

The Access Appliance uses the SNMPv2-SMI or the SNMPv3-SMI application protocol to monitor the appliance node. Use this command to add or change SNMP parameters on the server. You can use the following commands to display the current parameters and the changes that were made to the SNMP information. You can use this command to enable and disable SNMP notifications for appliance monitoring. When you create and enable an SNMP community you enable appliance monitoring to occur on the appliance node through the SNMP protocol. Notifications or traps are programmed to occur on the appliance node. In addition, you can use this command to see the notification traps that have been configured for the appliance node.

3.2.3 OPTIONS

set alerts callhome

Enable the Call Home feature. Enabling the feature lets you send the health status of the appliance to Veritas Technical Support. In case of any failure, Veritas Technical Support uses this information to resolve the issue.

set alerts email-hardware *email_address*

Add or append a hardware administrator's email account for Access Appliance to use. Where *email_address* is the user's email address. To define multiple emails, separate them with a semi-colon.

set alerts email-notification-interval *interval*

Define the time span between the alert emails that are sent to the administrator. Where *interval* is the time between the alert emails that are sent to the administrator. This variable is defined in minutes.

set alerts email-smtp *port*

Set the port for SMTP. You need to add the SMTP server details first.

set alerts email-smtp *smtp_server smtp_sender_id [smtp_account]*

Add an SMTP server that Access Appliance can use. The *smtp_server* variable is the host name of the target SMTP server that is used to send emails. The *smtp_account* option identifies the name of the account that was used or the authentication to the SMTP server, which is optional. The *smtp_sender_id* is the email address of the sender. It is used for the emails that are received from appliance. The port is set to a default value of 25. You have to manually enter the password for authentication to the SMTP server.

set alerts email-software *email_address*

Add or append a software administrator's email account for Access Appliance to use. Where *email_address* is the user's email address. To define multiple emails, separate them with a semi-colon.

set alerts hardware-threshold

Set a threshold value for the disk space, CPUIdle, MemorySwap,MemoryUsage, IOWait, disklog, diskroot, DiskSystemSwap. The default value for threshold is 80%.

set alerts snmp enable *version*

V2

Enable the ability to send SNMP version 2 notifications (traps) for monitoring.

V3

Enable the ability to send SNMP version 3 notifications (traps) for monitoring. The appliance sends traps only if you have set snmp security.

set alerts snmp *community*

Sets the SNMP community string. The default setting is public. This setting is required for SNMP V2, and is optional for SNMP V3.

set alerts snmp *server port*

Sets the SNMP server name and the port assignment. The default setting is 162.

Note: Access Appliance supports all of the SNMP servers in the market. However, the ManageEngine™ SNMP server and the HP OpenView SNMP server are tested and certified.

set alerts snmp-security *security*

Lets you configure the following security parameters when SNMP version 3 is enabled:

- *None [Username]*

Sets the security level to no authentication and no privileges for a specific SNMP user.

- *authentication [Username] [Authentication Protocol] [Authentication Password]*

  Sets the security level to authentication with no privileges for a specific SNMP user. Authentication Protocol can be set to SHA256 or SHA512. An Authentication Password is required.

- *authentication privacy [Username] [Authentication Protocol] [Encryption Policy] [Authentication Password] [Encryption Passphrase]*

  Sets the security level to authentication with privileges for a specific SNMP user. Authentication Protocol can be set to SHA256 or SHA512. Encryption Policy can be set to AES128, AES192, or AES256. Authentication Password and Encryption Passphrase are mandatory parameters.

  Rules for Username, Authentication Password, and Encryption Passphrase: Username can have 1-32 characters.

  Authentication Password and Encryption Passphrase must have 8 or more characters.

  Username, passwords, and passphrases may include uppercase letters, lowercase letters, numbers, and the following punctuation marks: period, hyphen/dash, underscore.

  Spaces, commas, and special characters are not allowed.

3.2.4 EXAMPLES

You can use following methods to configure a public SNMP community on port 8080. The example uses the [Port] options.

```
[access-8.1] access-appliance > set alerts snmp server=pqr222.xyz.com
port=

    (default:  162)

>> port of snmp server:  8080

Successfully set SNMP manager
```

3.3 show alerts

show alerts - View the Call Home, email, threshold value, and SNMP information.

3.3.1 SYNOPSIS

show alerts callhome

show alerts callhome-test

show alerts email

show alerts email-test

show alerts hardware-threshold

show alerts snmp

3.3.2 DESCRIPTION

View the Call Home, proxy server settings, email, threshold value, and SNMP information.

3.3.3 OPTIONS

show alerts callhome

View the Call Home and proxy settings that are currently configured for your appliance.

CallHome is enabled by default

show alerts callhome-test

Validate whether or not the appliance is able to send Call Home information to Veritas Technical Support.

show alerts email

View your email or SMTP settings.

show alerts email-test

A test email is sent to the email addresses configured above. Check if a test email is received in your mail inbox. The email transmission is decided by the network connections, the SMTP settings and the email address settings of your appliance. Follow the prompted error messages to troubleshoot if the test email is not received.

show alerts hardware-threshold

View the threshold value that is set for your disk space.

show alerts snmp

Displays the parameters that are set after you have run an set alerts snmp server port command. If you run this command before you have run a SNMP set server command, then default values for [Community] and [Port] are displayed and no value is displayed for the server.

show alerts snmp mib

Display the contents of the Management Information Base (MIB) file. This file contains the notification traps that are configured to monitor the appliance.

3.3.4 EXAMPLES

When you run the `show alerts snmp mib` command, an output similar to the following is displayed.

```
VERITAS-APPLIANCE-MONITORING-MIB DEFINITIONS ::= BEGIN

IMPORTS

DisplayString, mib-2 FROM RFC1213-MIB

enterprises, OBJECT-TYPE, NOTIFICATION-TYPE, MODULE-IDENTITY FROM SNMPv2-SMI;

applianceMonitoringMib MODULE-IDENTITY

LAST-UPDATED "2016083000Z"

ORGANIZATION "Veritas Technologies LLC"

CONTACT-INFO "500 East Middlefield Road

Mountain View, CA 94043 US

Subject: appliance.mib"

DESCRIPTION "The MIB module for Veritas Appliance Monitoring"

REVISION "201609060000Z"

DESCRIPTION "Changed symc strings to vrts."

::= { products 9 }

veritassoftware OBJECT IDENTIFIER ::= { enterprises 48328 }

products OBJECT IDENTIFIER ::= { veritassoftware 3 }

systems OBJECT IDENTIFIER ::= { applianceMonitoringMib 1 }

software OBJECT IDENTIFIER ::= { applianceMonitoringMib 2 }

-- system traps

vrtssystemName OBJECT-TYPE

SYNTAX DisplayString (SIZE(0..80))

MAX-ACCESS read-only

STATUS current

DESCRIPTION "System Name"

::= { systems 1 }

vrtsfanTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }
```

(continues on next page)

(continued from previous page)

```
STATUS current

DESCRIPTION "Traps fan failures"

::= { systems 3 }

vrtspowerTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps power failures"

::= { systems 4 }

vrtsfibrechannelTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps FibreChannel failures"

::= { systems 5 }

vrtstemperatureTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps temperature failures"

::= { systems 6 }

vrtscpuTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps cpu failures"

::= { systems 7 }

vrtsdiskTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps disk failures"

::= { systems 8 }

vrtsraidgroupTrap NOTIFICATION-TYPE
```

(continues on next page)

(continued from previous page)

```
OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps raid failures"

::= { systems 9 }

vrtsenclosurefanTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps enclosure fan failures"

::= { systems 10 }

vrtsenclosurepowerTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps enclosure power failures"

::= { systems 11 }

vrtsenclosuretemperatureTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps enclosure temperature failures"

::= { systems 12 }

vrtsenclosurediskTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps enclosure disk failures"

::= { systems 13 }

vrtsadapterTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps adapter failures"
```

(continues on next page)

(continued from previous page)

```
::= { systems 14 }

vrtsfirmwareTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps firmware failures"

::= { systems 15 }

vrtspciTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps pci failures"

::= { systems 16 }

vrtsnetworkcardTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps network card failures"

::= { systems 17 }

vrtsvolumeTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps volume failures"

::= { systems 18 }

vrtsbbuTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps BBU failures"

::= { systems 19 }

vrtsconnectionTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current
```

(continues on next page)

(continued from previous page)

```
DESCRIPTION "Traps connection failures"

::= { systems 20 }

vrtspartitionTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Partition alert traps"

::= { systems 21 }

vrtsstoragestatusTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps StorageArray HealthStatus failures"

::= { systems 22 }

vrtsdimmTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps Dimm failures"

::= { systems 23 }

vrtsiscsiTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps Iscsi failures"

::= { systems 24 }

vrtsethernetTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Traps Ethernet failures"

::= { systems 25 }

-- software traps
```

(continues on next page)

(continued from previous page)

```
vrtsfailedJobsTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Job failures Trap"

::= { software 1 }

vrtsprocessTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Processes stopped traps"

::= { software 2 }

vrtsdiskSpaceTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Low disk space traps"

::= { software 3 }

vrtssoftwareUpdateSuccessTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Software update success trap"

::= { software 4 }

vrtssoftwareUpdateFailedRollbackSuccessTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Software update failed but rollback was successful trap"

::= { software 5 }

vrtssoftwareUpdateFailedRollbackFailedTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Software update and rollback failed trap"
```

(continues on next page)

(continued from previous page)

```
::= { software 6 }

vrtsrollbackSuccessTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Software rollback success trap"

::= { software 7 }

vrtsrollbackFailedTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Software rollback failed trap"

::= { software 8 }

vrtsclusterStateTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Cluster node failed trap"

::= { software 9 }

vrtsdiskPerfTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Disk performance alert trap"

::= { software 10 }

vrtscollectorserviceTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }

STATUS current

DESCRIPTION "Collector plugin loading failed trap"

::= { software 11 }

vrtsassetTagTrap NOTIFICATION-TYPE

OBJECTS { vrtssystemName }
```

(continues on next page)

(continued from previous page)

```
STATUS current

DESCRIPTION "AssetTag"

::= { software 12 }

END``
```

4 Appliance commands

- *configure cluster*
- *show appliance*
- *system factory-reset*
- *system restart*
- *system self-test*
- *system shutdown*
- *system import iso*
- *start appliance preupgrade-check*
- *show appliance preupgrade-check*

4.1 configure cluster

configure cluster - Configure the Access cluster on the appliance

4.1.1 SYNOPSIS

configure cluster

4.1.2 DESCRIPTION

Use this command to configure the Access cluster on the appliance from the current node.

Note the following before you run the command:

- The Access cluster configuration is only allowed to run from one node. Make sure that the Access cluster configuration process is not already ongoing on the current node or other nodes.
- Make sure that you have the node management IP addresses of the appliance nodes for clustering.
- Make sure that you have sufficient physical and virtual IP addresses for the cluster configuration. The IP addresses need not be contiguous.
- Disk-based fencing is configured when you configure the cluster. You cannot change the configured fencing.

Do not run the command on the current node in the following scenarios:

- When the cluster configuration process is already running on another node of the Access appliance.
- When the node has been factory reset without resetting the storage, and the Access cluster remains active on the other node.
- When the node is an unconfigured node that is used to replace a faulty node in an Access cluster.

4.2 show appliance

show appliance status – Show status information about the appliance node.

4.2.1 SYNOPSIS

show appliance status

4.2.2 DESCRIPTION

Use this command to show status information about the appliance and the current node. such as appliance model, access software version, appliance software version, appliance node status, access cluster name, access management console virtual IP address.

4.2.3 OPTIONS

show appliance status Show the status information about the node, such as appliance model, software release version, and the node status.

4.3 system factory-reset

system factory-reset - Initialize factory reset

system factory-reset status - Check on-going factory reset status

4.3.1 SYNOPSIS

system factory-reset

system factory-reset status

4.3.2 DESCRIPTION

You can use the `system factory-reset` command to begin factory reset process. You must confirm a number of options before starting. If you are running factory reset with disk erase option selected, the process will begin in the background and open a status screen after beginning.

You can also use the `system factory-reset status` command to open the status screen mentioned above, the status is synced across nodes in cluster scenario. When factory reset is running in foreground, `system factory-reset status` is still available from a seperate session or remote node.

4.3.3 OPTIONS

status Open status screen of on-going factory reset

4.3.4 EXAMPLES

The following command shows how to run factory reset on your appliance:

```
system factory-reset
```

The following command shows how to check on-going factory reset status on your appliance:

```
system factory-reset status
```

4.4 system restart

system restart - Restart the system.

4.4.1 SYNOPSIS

system restart [force]

4.4.2 DESCRIPTION

Use this command to restart the current system on the appliance node when the node is not a part of the cluster. You cannot use this command to restart another system remotely.

4.4.3 OPTIONS

restart [force] Use this command to restart the system. The *force* parameter forces the system to restart even if services cannot be stopped. Use this parameter if a previous attempt failed.

4.5 system self-test

system self-test – Test the current status of the various appliance components.

4.5.1 SYNOPSIS

system self-test hardware

system self-test software

4.5.2 DESCRIPTION

The appliance runs a test at regular intervals to check the status of its components. This ability of the appliance is referred to as self test. Use the `system self-test` command to verify the current status of the various appliance components.

4.5.3 OPTIONS

hardware Use this command to view the enhanced hardware monitoring page that displays the status of various hardware components.

software Use this command to test the current status of the various appliance software components.

4.5.4 EXAMPLES

`system self-test software`

```
Starting self-test on Fri Dec 31 13:21:59 2021

Running validation tests on the host 'access-appliance'.

    Checking eth1 configuration...                                  [PASS]

    Checking the database service...                                [PASS]

    Checking the message queue service...                           [PASS]

    Checking the required RPM package installation...               [PASS]

    Checking the serial number...                                   [PASS]

    Checking the SSH server and settings...                         [PASS]

    Checking the web server service...                              [PASS]

    Checking the LUNs...                                            [PASS]

    Checking the accessServices...                                  [PASS]

    Checking the storage_s3test...                                  [PASS]

    Checking the SDCS policy settings...                            [PASS]
```

(continues on next page)

(continued from previous page)

```
Validation tests are complete.

Appliance self-test result: PASS``
```

4.6 system shutdown

system shutdown - Turn off the system.

4.6.1 SYNOPSIS

system shutdown

4.6.2 DESCRIPTION

Use the command to turn off the system and power off the appliance node when the node is not a part of the cluster.

4.6.3 OPTIONS

shutdown Use to turn off the current system and power off the appliance node.

4.7 system import iso

4.7.1 SYNOPSIS

system import iso <*path*=>

4.7.2 DESCRIPTION

You can use this command to import an ISO image to SSD to replace the existing ISO image. After that, you can choose boot from SSD option in the boot menu with the imported ISO.

4.7.3 OPTIONS

iso Import a specific ISO image.

path= The absolute path of the specific ISO file you want to imported.

4.8 start appliance preupgrade-check

start appliance preupgrade-check – Check if the appliance is ready for an upgrade.

4.8.1 SYNOPSIS

start appliance preupgrade-check <*patch*=>

4.8.2 DESCRIPTION

The preupgrade check determines if the appliance is ready for an upgrade and displays potential issues that might prevent a successful upgrade. You can also view a summary of the tests performed and their status. Some of the tests that are performed during the preupgrade check are as follows:

- Upgrade path is supported
- All the service groups are online
- Relevant certificates exist and are configured correctly
- Connectivity to the MongoDB database
- Passwords are valid and do not expire within seven days
- Sufficient free space is available for the upgrade

4.8.3 OPTIONS

start appliance preupgrade-check <*patch*=>

patch The name of the upgrade release update.

4.8.4 EXAMPLES

The following example shows how to run the preupgrade-check:

```
start appliance preupgrade-check patch=VRTSaccess-app-update-8.1-1.x86_64.rpm
```

4.9 show appliance preupgrade-check

show appliance preupgrade-check – Display the preupgrade check status.

4.9.1 SYNOPSIS

show appliance preupgrade-check status

4.9.2 DESCRIPTION

Use this command to view the result of the preupgrade tests.

4.9.3 OPTIONS

show appliance preupgrade-check status Display the details of the preupgrade tests and whether the tests passed or failed.

5

Logs commands

5.1 show log-forwarding

show log-forwarding - View the current Logforwarding configuration

5.1.1 SYNOPSIS

show log-forwarding

5.1.2 DESCRIPTION

You can use the `show log-forwarding` command to show the log forwarding configuration on the appliance.

If log forwarding is enabled, the command will also return configuration details of log forwarding, including target server, port, protocol, forward interval and TLS status.

5.1.3 EXAMPLES

The following example shows how to check log forwarding configuration on your appliance:

```
show log-forwarding
```

Output if log forwarding is configured:

```
- [Info] Forwarding syslogs to an external log management server is enabled.
Target server: 10.188.132.100
Server port: 514
Protocol: TCP
Interval: 15 minutes
TLS: Disabled
```

Output if log forwarding is not configured:

```
- [Info] Forwarding syslogs to an external log management server is disabled.
```

5.2 support data-collect

support data-collect – Gather device logs.

5.2.1 SYNOPSIS

support data-collect *advanced*

support data-collect *delete* <*file*=>

support data-collect *list*

support data-collect *status*

support data-collect *upload* <*file*=>

support data-collect *sanitize-data status*

support data-collect *sanitize-data enable*

support data-collect *sanitize-data disable*

5.2.2 DESCRIPTION

Use this command to

- Collect default/additional diagnostic logs.
- Delete the log package that were generated using the data-collect command.
- List all the generated log packages from the /log/data-collect directory.
- Display the status of the ongoing data-collect command.
- Disable the use of a proxy server for this appliance.
- Upload the log package that were generated using the data-collect command.
- Enable, disable, and view the current setting for sanitizing sensitive data.

5.2.3 OPTIONS

support data-collect advanced Collect additional diagnostic logs.

support data-collect list List all the generated log packages from the /log/data-collect directory.

support data-collect status Display the status of the ongoing data-collect command.

support data-collect delete <*file*=> Delete the log packages that were generated using the data-collect command.

support data-collect upload <*file*=> Upload the log package that was generated using the data-collect command.

support data-collect sanitize-data *status* Display the data sanitization status.

support data-collect sanitize-data *enable* Mask sensitive data such as personally identifiable information (PII) in the generated data-collect log package. Data-sanitization is enabled by default.

support data-collect sanitize-data *disable* Disable masking of sensitive data such as personally identifiable information (PII) in the generated data-collect log package

5.2.4 EXAMPLES

```
support data-collect

[INFO] The data-collect command is initiated. Use the support data-collect
status command to check the current status.

Operation completed successfully
```

5.3 support logbrowser

support logbrowser - Show/control log transfer console processes.

5.3.1 SYNOPSIS

support logbrowser start

support logbrowser status

support logbrowser stop

5.3.2 DESCRIPTION

Use this command to manage the log transfer web service, which is used by the Log Transfer Console to download the logs to your local system.

5.3.3 OPTIONS

support logbrowser start Start the log transfer web service. The time period can range from 1 to 720 minutes. The default time is 720 minutes. When the set time expires, the log transfer web service stops automatically.

support logbrowser status Show the status of the log transfer web service.

support logbrowser stop Stop the log transfer service manually.

6

Monitor commands

6.1 set beacon

Start or stop the LED(s) of HDD or NVMe SSD drive(s)

6.1.1 SYNOPSIS

set beacon hdd <*sid*=> <*eid*=> <*operation*=> <*minutes*=>

set beacon wwid <*wwid*=> <*operation*=> <*minutes*=>

set beacon nvme <operation=> <deviceid=>

6.1.2 DESCRIPTION

You can use the `set beacon` to start or stop flashing the LED(s) of one or more HDD/NVMe SSD drive(s).

Use the `set beacon hdd` command to flash LED according to disk enclosure and slot Ids of the hard disk or use `set beacon wwid` to flash LED according to SCSI controller WWID.

When you provide an invalid WWID value for `set beacon wwid`, a list of available WWIDs will be returned.

Use the `set beacon nvme` command to flash LED according to the NVMe device ID on the 3360 appliance.

6.1.3 OPTIONS

`set beacon hdd`

hdd Start or Stop the LED(s) of HDD drive(s) by EnclosureId and SlotId

sid The enclosure number you want to locate, should be integer number of {0,62}

eid The slot number of the disk you want to locate, should be integer number or 'ALL'

operation Start or Stop flashing the target LEDs, should be: [start or stop]

minutes The duration of time, in minutes, that LEDs can flash

`set beacon wwid`

wwid Start or Stop the LED(s) of HDD drive(s) by WWID

wwid The wwid of the disk you want to locate

operation Start or Stop flashing the target LEDs, should be: [start or stop]

minutes The duration of time, in minutes, that LEDs can flash

Start or stop the LED(s) of NVMe SSD drive(s) on the 3360 appliance.

operation Start or stop flashing the target LEDs. It can be: [start or stop].

deviceid NVMe device ID that you want to locate. EXAMPLES ^^^^^^^^

The following example shows how to set beacon to flash an LED of a disk with slot and enclosure id for 3 minutes:

```
set beacon hdd sid=0 eid=62 operation=start minutes=3
```

The following example shows how to set beacon to flash an LED of disks with SCSI controller wwid for 3 minutes:

```
set beacon wwid wwid=600C0FF0003C2C1EABF33E6001000000 operation=start
minutes=3
```

The following example shows how to set beacon to flash an LED of an NVMe SSD with device ID:

```
set beacon nvme operation=start deviceid=/dev/nvme0n1
```

6.2 set sdcs-audit

set sdcs-audit settings - Manage Symantec data center security logs

6.2.1 SYNOPSIS

set sdcs-audit settings <*file-number*=>

set sdcs-audit settings <*retention-period*=>

6.2.2 DESCRIPTION

You can use the `set sdcs-audit settings` command to set SDCS audit log file number and their retention period.

Use either file-number or retention-period to specify the attribute you want to set.

6.2.3 OPTIONS

```
set sdcs-audit settings file-number=
set sdcs-audit settings retention-period=
```

settings Only one of the following options below can be used for each set command

file-number Number of audit log files to retain. Size of each file is 10 MB

retention-period Number of days to retain the audit log files

6.2.4 EXAMPLES

The following example shows how to set the number of audit log files to retain to 10:

```
set sdcs-audit settings file-number=10
```

The following example shows how to set the period of retaining the audit log files to 7 days:

```
set sdcs-audit settings retention-period=7
```

6.3 show hardware-errors

show hardware-errors - View the errors that are related to hardware components.

6.3.1 SYNOPSIS

show hardware-errors

6.3.2 DESCRIPTION

View the errors that are related to the hardware components of an appliance. You can use this information to notify Veritas Technical Support of the errors.

6.3.3 OPTIONS

show hardware-errors Display all the errors that are related to hardware status.

6.4 show hardware-health

show hardware-health - View the health of the various hardware components.

6.4.1 SYNOPSIS

show hardware-health appliance *[component=][export]*

6.4.2 DESCRIPTION

View the performance and status of various hardware components of the appliance node and the attached storage.

6.4.3 OPTIONS

show hardware-health appliance *[component=][export]*

The following options are available for the [component] parameter. The default value is all.

(All/Product/Fan/Power/Temperature/CPU/Network/PCI/Adapter/Firmware/ Partition/RAID/DIMM/Certificate/CMOSBattery/DIMMP StorageStatus/Connection)[all]

The following options are available for the [component] parameter by model specific Model 3340/3350 - Disk Model 3360 - VROC

For example, to view the serial number of the appliance node, run the following command:

```
show hardware-health appliance component=Product
```

show hardware-health primary-shelf *[component=][export]*

View the performance and status of the primary storage shelf of the appliance. The following options are available for the [component] parameter. The default value is all.

(All/Fan/Disk/Power/Temperature/Product/Firmware/BBU/ Controller/Volume/VolumeGroup)[all]

show hardware-health expansion-shelf *[component=][export][tray-id=]*

View the performance and status of the expansion storage shelf(shelves) of the appliance.Where [tray-id=] is the ID of a specific expansion shelf. By default, the data is displayed for all the storage shelves. The default value is all.

(All/Fan/Disk/Power/Temperature/Product/Volume/ VolumeGroup) [all]

For example, to view the status of fan on the expansion storage shelf with an ID of 1, run the following command:

```
show hardware-health expansion-shelf component=FAN tray-id=1
```

6.4.4 EXAMPLES

The following is an example output of the `show hardware-health appliance component=Product` command.

```
Time Monitoring Ran:  Fri Dec 31 2021 04:36:59 PST
```

```
+-------------+-------------+-------------+------------------+
|    Name     | Manufacturer | Serial      | I/O Configuration|
+-------------+-------------+-------------+------------------+
| Access 3340 | Veritas      | VTAS9000909 |        A         |
+-------------+-------------+-------------+------------------+
```

```
show hardware-health appliance component=connection
```

```
Compute Node access-appliance
```

```
Time Monitoring Ran:  Fri Dec 31 2021 04:54:54 PST
```

```
+---------------+----------------------------+-----------+-------+
|      ID       | Primary Storage Shelf Port | Status    | State |
+---------------+----------------------------+-----------+-------+
| SAS HBA0 Port1|    Controller B Port 0     | Connected |  OK   |
+---------------+----------------------------+-----------+-------+
```

6.4.5 Error Messages - Negative Scenarios

The following is an example output of the `show hardware-health appliance k` command.

Invalid command: show hardware-health appliance k

component Appliance components to query for data, choose one from below:
All/Fan/CPU/RAID/Power/Temperature/Product/PCI/Network DIMM/SSD/Adapter/Firmware/Partition/Connection/Certific
StorageStatus/DIMMPopulation Additional options: Model 3340/3350 - Disk

3360 - VROC

export Export historical health status data for particular appliance component

The following is an example output of the `show hardware-health appliance component=k` command.

Model 3340/3350 Invalid component, please enter one of the following:

All/Product/Fan/Power/Temperature/CPU/Network/PCI/Firmware/Raid/Disk/DIMM/Partition/Certificate/CMOSBattery/DIMMP

Model 3360 Invalid component, please enter one of the following:

All/Product/Fan/Temperature/CPU/Network/PCI/Firmware/Raid/DIMM/Partition/Certificate/CMOSBattery/DIMMPopulation/SS

6.5 show sdcs-audit

show sdcs-audit - Display Symantec data center security logs

6.5.1 SYNOPSIS

show sdcs-audit settings

show sdcs-audit view severity-codes

show sdcs-audit view event-type-codes

show sdcs-audit search *<event-id=><event-type=><from-date=><to-date=><severity=><search-string=>*

6.5.2 DESCRIPTION

You can use the `show sdcs-audit settings` to show the current setting of retaining SDCS audit log files.

Use the `show sdcs-audit view` to view the dictionary of all available severity codes or event type codes.

Use the `show sdcs-audit search` with one or more arguments to search for SDCS audit logs matching the specified conditions.

6.5.3 OPTIONS

`show sdcs-audit settings`

settings Show and set SDCS audit log file number and retention period

`show sdcs-audit view`

view Display EventTypeCodes or SeverityCodes dictionary

severity-codes SDCS SeverityCodes dictionary

event-type-codes SDCS EventTypeCodes dictionary

`show sdcs-audit search`

search Display SDCS audit log records based on specific conditions

to-date Date format mm/dd/yyyy[-hh:mm:ss]

event-type These 4 letter codes represent the various event types of audit log

event-id SDCS audit log event ID

search-string Specific string

severity These 1 letter codes represent the various severities of audit log

from-date Date format mm/dd/yyyy[-hh:mm:ss]

6.5.4 EXAMPLES

The following example shows how to show the SDCS audit log file retention settings:

`show sdcs-audit settings`

The following example shows how to display SDCS SeverityCodes dictionary:

```
show sdcs-audit view severity-codes
```

The following example shows how to display SDCS audit log records based on event type:

```
show sdcs-audit search event-type=MSTA
```

The following example shows how to display SDCS audit log records based on several conditions:

```
show sdcs-audit search severity=I to-date=08/31/2021 from-date=08/21/2021
search-string=retranslation
```

7 Network commands

7.1 delete network

delete network - Delete the configured network settings.

7.1.1 SYNOPSIS

delete network interface

delete netowrk vlan

7.1.2 DESCRIPTION

Use the `delete network interface` command to remove the IP address and shut down the interface.

Use the `delete netowrk vlan` command to delete a protocol-based VLAN.

7.1.3 OPTIONS

interface Unconfigure an IP address for a network interface

vlan Delete a protocol-based VLAN

7.2 delete proxy-server

delete proxy-server - Unset the proxy server.

7.2.1 SYNOPSIS

delete proxy-server

7.2.2 DESCRIPTION

Unset the settings of the proxy server for this appliance.

7.2.3 EXAMPLES

The following is an example output of the `delete proxy-server` command.

```
[access-8.1] node-01 > delete proxy-server
[Info] Are you sure you want to unset the proxy server? [yes, no](no) yes
[Info] Removing the proxy server settings. This might take a few minutes...
[Info] Removed the configured proxy server.
```

7.3 modify network

modify network - Modify existing network settings.

7.3.1 SYNOPSIS

modify network vlan <*device*=> <*vlanid*=> <*ip*=> <*netmask*=> <*gateway*=>

7.3.2 DESCRIPTION

You can use the `modify network vlan` command to modify the network settings of a pre-existing VLAN interface to which you want to connect your appliance to. To modify the settings, specify the existing VLAN interface and the new VLAN ID, IP address, netmask and gateway that you want to assign to the VLAN interface.

7.3.3 OPTIONS

vlan Tag a protocol-based VLAN

device Existing vlan interface name

vlanid VLAN identifier [1-4095]

ip IPv4 or IPv6 address

netmask Netmask for an IPv4 address or the prefix length for an IPv6 address

gateway Default gateway IP address

7.3.4 EXAMPLES

following example shows how to configure your appliance network settings:

```
modify network vlan device=eth1.400 vlanid=501 ip=192.168.60.2 netmask=255.
255.255.0 gateway=192.168.60.1
```

7.4 set network

set network - Configure network settings.

7.4.1 SYNOPSIS

set network interface <*ip*=> <*netmask*=> <*gateway*=>

set network vlan <*vlanid*=> <*ip*=> <*netmask*=> <*gateway*=>

7.4.2 DESCRIPTION

You can use the `set network interface` command to set the IP address of a single interface on the network that you want to connect your appliance to. When you use this command, you need to define the IP address, the netmask address, and the gateway address.

Use the `set network vlan` command to set VLAN for your appliance in your existing network environments.

7.4.3 OPTIONS

interface Configure an IP address for a network interface

ip IPv4 or IPv6 address

netmask Netmask for an IPv4 address or the prefix length for an IPv6 address

gateway Default gateway IP address

vlan Tag a protocol-based VLAN

vlanid VLAN identifier [1-4095]

ip IPv4 or IPv6 address

netmask Netmask for an IPv4 address or the prefix length for an IPv6 address

gateway Default gateway IP address

7.4.4 EXAMPLES

The following example shows how to configure your appliance network settings:

```
set network interface ip=10.180.2.3 netmask=255.255.255.0 gateway=10.180.2.1
```

7.5 set proxy-server

set proxy-server - Set and use a proxy for this appliance.

7.5.1 SYNOPSIS

set proxy-server settings <*server*=> <*tunnel*=> <*user*=>

set proxy-server enable

set proxy-server disable

7.5.2 DESCRIPTION

Use this command to

- Set and use a proxy-server for this appliance.
- Enable the use of a proxy server for this appliance.
- Disable the use of a proxy server for this appliance.

7.5.3 OPTIONS

settings Configure the proxy for this appliance.

server Specify the proxy server address and port number (0-65535). Use a host name or an IPv4/IPv6 address for the proxy server. A colon (:) is required between the server address and the port number. For example: 192.0.2.0:80

tunnel Specify the optional proxy server tunneling settings. The available options are TunnelOn and TunnelOff. The default option is TunnelOff.

user Specify the optional proxy server user name. Alphanumeric characters and four special characters(@,-,_,.) are supported.

enable Enables the use of a proxy server for this appliance.

disable Disables the proxy server settings for this appliance.

7.5.4 EXAMPLES

The following is an example output of the `set proxy-server` command.

```
[access-8.1] node-01 > set proxy-server settings server=10.182.27.100:3128
tunnel=TunnelOn user=admin

Enter password for the user "admin":

Enter password for the user "admin" again:

[Info] Saving the proxy server settings. This might take a few minutes...

[Info] Configured the proxy server for the appliance.
```

7.6 show network

show network - Show network settings.

7.6.1 SYNOPSIS

show network interface

show network vlan status

7.6.2 DESCRIPTION

Use the `show network interface` command to list the network properties.

Use the `show network vlan status` command to show VLAN for your appliance in your existing network environments.

7.6.3 OPTIONS

interface Display status of a network interface

vlan Display VLAN status

status VLAN status

7.7 show proxy-server

show proxy-server - Show the current proxy settings and status.

7.7.1 SYNOPSIS

show proxy-server

7.7.2 DESCRIPTION

Show the current proxy settings and status of the proxy for this appliance.

7.8 system ipmi

system ipmi - Manage the IPMI configuration.

7.8.1 SYNOPSIS

system ipmi user show

system ipmi user <*add*=>

system ipmi user <*delete*=>

system ipmi reset

system ipmi network show

system ipmi network <*ip*=> <*netmask*=> <*gateway*=>

7.8.2 DESCRIPTION

The IPMI commands let you configure the IPMI network and manage users accessing the appliance using the IPMI connection. Use the IPMI commands to:

- Configure IPMI network settings
- View the current IPMI network settings
- Reset the IPMI
- Add users
- Delete users
- List users

7.8.3 OPTIONS

user Manage the users in the IPMI sub-system.

show View the list of users who can access the IPMI sub-system.

add Specify a new user to be created in the IPMI sub-system.

delete Specify an existing user to be deleted from the IPMI sub-system.

reset Reset the IPMI. You must reset IPMI only if the IPMI interface stops responding or hangs.

system ipmi network Configure the IPMI network settings.

show View the current IPMI network settings.

ip Specify the IP address to be configured in the IPMI sub-system.

netmask Specify the netmask for an IPv4 address or the prefix length for an IPv6 address.

gateway Specify the IP address of default gateway.

7.8.4 EXAMPLES

The following example shows how to add a new user into your appliance IPMI sub-system:

```
[access-8.1] node-01 > system ipmi user add=user01
```

The following example shows how to delete an user from your appliance IPMI sub-system:

```
[access-8.1] node-01 > system ipmi user delete=user01
```

The following example shows how to configure your appliance IPMI network settings:

```
[access-8.1] node-01 > system ipmi network ip=10.180.2.3 netmask=255.255.255.0
gateway=10.180.2.1
```

8

Security commands

8.1 export certificate

export certificate - Export the device certificate.

8.1.1 SYNOPSIS

export certificate device-certificate <*need-password*=> <*cert-file*=>

8.1.2 DESCRIPTION

Use this command to export the device certificate to a specified location. The device certificate is unique for each appliance and is factory installed. The certificate is stored on a storage device in the appliance. When you reimage the appliance, the certificate on the storage device is preserved. The certificate is copied to the appliance after the appliance is reimaged.

8.1.3 OPTIONS

export certificate device-certificate <*need-password*=> <*cert-file*=>

Use this command to export the device certificate. The *need-password* field is used to answer the question, "Do you want to enter a password?". You must enter a value of yes or no in this field. The *cert-file* parameter specifies the location where you want to store the exported certificate. By default, the certificate is exported to the /inst/certs/host.pfx location.

8.2 import certificate

import certificate - Import the device certificate.

8.2.1 SYNOPSIS

import certificate device-certificate <*need-password*=> <*cert-file*=>

8.2.2 DESCRIPTION

Use this command to import the device certificate to a specified location.

8.2.3 OPTIONS

import certificate device-certificate <*need-password*=> <*cert-file*=>

Use this command to import the device certificate. The need-password parameter is used to answer the question, "Do you want to enter a password?". You must enter a value of yes or no in this field. The cert-file parameter specifies the location where the encrypted device certificate is saved. By default, the encrypted certificate is stored in the /inst/certs/host.pfx location.

9 Software commands

9.1 system software available-patch

system software available-patch – Lists the available patch information.

9.1.1 SYNOPSIS

system software available-patch

9.1.2 DESCRIPTION

You can use this command to show the patches that are available for installation for a particular appliance node.

9.1.3 OPTIONS

system software available-patch Use this command to check the Veritas site for any software updates that are available.

9.2 system software delete-update

system software delete-update – Delete a software update.

9.2.1 SYNOPSIS

system software delete-update <*update-name*=>

9.2.2 DESCRIPTION

You can use this command to delete a specific software release update, sometimes referred to as a patch. Use the `system software downloaded` command to obtain the list of software release updates that are downloaded.

9.2.3 OPTIONS

system software delete-update <*update-name*=> Delete a specific release update.

update-name= The specific name of the update that you want to delete.

9.3 system software downloaded

system software downloaded – List downloaded software updates.

9.3.1 SYNOPSIS

system software downloaded

system software downloaded <*update-name*=>

system software downloaded <*list*>

9.3.2 DESCRIPTION

List downloaded software updates.

9.3.3 OPTIONS

system software downloaded List all downloaded software updates.

update-name= The specific name of the update that you want to list detail.

list List only the names of all downloaded software updates.

9.4 system software download-progress

system software download-progress – Show the progress of an online patch download.

9.4.1 SYNOPSIS

system software download-progress

9.4.2 DESCRIPTION

Use this command to display the download progress of a software patch.

9.4.3 OPTIONS

system software download-progress Display the download progress of a software patch. The progress bar displays the download progress. Press Ctrl+C to exit this command. Exiting the command does not stop the download process.

9.5 system software download-update

system software download-update – Download a software update.

9.5.1 SYNOPSIS

system software download-update <*update-name*=>

9.5.2 DESCRIPTION

You can use this command to download a specific release update.

9.5.3 OPTIONS

system software download-update <*update-name*=> Download a specific update.

update-name= The file name of the update that you want to download.

9.6 system software installed-addons

system software installed-addons – List the detailed information of the software add-ons that are installed on the appliance node.

9.6.1 SYNOPSIS

system software installed-addons

9.6.2 DESCRIPTION

List the detailed information of the software add-ons that are installed on the appliance node.

9.6.3 OPTIONS

system software installed-addons List the detailed information of the software add-ons that are installed on the appliance node.

9.7 system software installed-eebs

system software installed-eebs – Show the list of the Emergency Engineering Binaries (EEBs) that are installed on each node of the appliance.

9.7.1 SYNOPSIS

system software installed-eebs

9.7.2 DESCRIPTION

Show the list of the Emergency Engineering Binaries (EEBs) that are installed on each node of the appliance.

9.7.3 OPTIONS

system software installed-eebs Show the list of the Emergency Engineering Binaries (EEBs) that are installed on each node of the appliance.

9.8 system software install-update

system software install-update – Use to install an EEB, an add-on, or a software release update.

9.8.1 SYNOPSIS

system software install-update <*update-name*=>

9.8.2 DESCRIPTION

Use this command to install a new or an existing software update, an engineering binary (EEB), or an add-on to an appliance node that you designate. To use this command you must know the name of the software update, the EEB, or the add-on that you want to install. To see a list of the software updates that are available for you to install, run `system software available-patch` command. This command checks the Veritas site for the latest software updates. Once you find the software update that you want to install, you must run the `system software download-update update_name=` command, where *update_name* is the name of the software update. To see the list of the EEBs and ADDONs that are available for you to install, check the Veritas Download Center and download these manually. You can then run the `system software share open` command on the appliance and copy the downloaded EEB or add-on to the appliance. After you have downloaded the software update, EEB, or add-on you can now run the `system software install-update update-name=` command.

9.8.3 OPTIONS

system software install-update <*update-name*=> Install a software release update.

update-name= The name of the update that you want to install.

9.9 system software readme

system software readme – Defines the Access Appliance patch process.

9.9.1 SYNOPSIS

system software readme

9.9.2 DESCRIPTION

This command defines the patch process for the appliance node.

9.9.3 OPTIONS

system software readme Show the patch process for the appliance node.

9.9.4 EXAMPLES

This command contains the following patch information.

```
Patch Readme
============
The following procedures explain how to copy a software release update to
the Access Appliance node and install the update.

  To download software update directly from the Veritas Support website:

  1. Use the 'system software available-patch' command to look for the latest
     release updates.

  2. Use the 'system software download-update' command to download the release update.

  3. Use the 'system software downloaded' command to list all of the downloaded
    release updates. Note the name of the update to install.

  To upload a software update from a local computer:

  1. Log in as the user 'admin' to the Appliance node.

  2. Use the 'system software share open' command to open the share so the
     Appliance node can receive the release updates. Access to the share:
     (access-appliance:/system/inst/patch/incoming)

  3. On the local computer, perform the following steps:

    a. Mount/Map the appropriate share.

    b. Download the release update from the Veritas Support website.

    c. Unzip the release update and review the README file in the zip.

    d. Upload the unzipped release update to the mounted share.
```

(continues on next page)

(continued from previous page)

```
    e. Unmap/Unmount the mounted share.

  4. Use the 'system software share close' command to close the share.

  5. Use the 'system software downloaded' command to list all the downloaded
     release updates. Note the name of the update to install.

  To install a release update on the Access Appliance node:

  1. Make sure that you follow the correct upgrade process in the Access
     Appliance documentation before you install the patch on this node.

  2. Use the 'system software install-update' command to install the release
     update to the node.

     Use the name of the release update that you noted in the procedures

     above when you entered the 'system software downloaded' command.

For more detailed information about this process, refer to the Access
Appliance documentation.
```

9.10 system software rollback-update

system software rollback-update – Rollback a specific EEB or a software add-on.

9.10.1 SYNOPSIS

system software rollback-update <*update-name*=>

9.10.2 DESCRIPTION

Use this command to rollback any Emergency Engineering Binaries (EEBs) or software add-ons that are installed on your appliance. You can use the `system software installed-eebs` and `system software installed-addons` commands to view the software version and all installed EEBs and add-ons. You can then specify which EEB or add-on you want to roll back. You can only specify only one EEB or an add-on at a time with this command. However, you can use this command multiple times to roll back as many installed EEBs or add-ons as you want.

9.10.3 OPTIONS

system software rollback-update <*update-name*=> Roll back a specific EEB or an add-on.

update-name= The name of the EEB or add-on that you want to roll back.

9.11 system software share

system software share – Share or unshare a directory for incoming patches

9.11.1 SYNOPSIS

system software share open

system software share close

9.11.2 DESCRIPTION

You can use this command to share or not share the directory that is used to receive incoming patches for your appliance. This operation is accomplished by opening and closing the Network File System (NFS) protocol shares.

9.11.3 OPTIONS

system software share open Open the NFS shares for the directory that receives incoming patches.

system software share close Close the NFS shares for the directory that receives incoming patches.

9.12 system software stop-download

system software stop-download – Stop the download process of a software update or the software patch, which can be in any of these installation stages - Downloading, Stopped, or Postcheck.

9.12.1 SYNOPSIS

system software stop-download <*update-name*=>

9.12.2 DESCRIPTION

Use this command to stop a patch download in one of the following stages:

- Downloading - The software update is in the process of being downloaded.
- Stopped - The downloading process has stopped abruptly; therefore the download cannot be completed.
- Postcheck - During downloading, the software update splits into several files.
- Once the split files are downloaded, they need to be merged into the software

update. The merging is termed as Postcheck.

9.12.3 OPTIONS

system software stop-download <*update-name*=> This command stops the patch downloading process.

update-name= The name of the software patch update.

9.12.4 NOTE

You cannot use the stop-download command if the software update has been downloaded completely and the download process is in Completed stage.

9.13 system software upgrade-status

system software upgrade-status - View the version and the software upgrade status.

9.13.1 SYNOPSIS

system software upgrade-status

9.13.2 DESCRIPTION

This command displays the upgrade status, including the target version, percentage completion, upgrade process status, and some of latest operations.

9.13.3 OPTIONS

system software upgrade-status View the version and the upgrade status of the appliance node.

9.13.4 EXAMPLE

The following is an example output of the `system software upgrade-status` command:

```
access-appliance.Software> system software upgrade-status

The target verison is: 8.1

Current upgrade status: COMPLETED. The upgrade is 100% completed.

Latest operations:

-[2020-12-16 21:31:56] [INFO] V-409-777-1318: Completed switching root to
the upgraded system.

-[2020-12-16 21:31:57] [INFO] V-409-777-1511: Rebooting nodes...

-[2020-12-16 21:41:03] [INFO] V-409-777-1517: Upgrade completed
successfully.
```

9.14 system software version

system software version - Use this command to view the version of your appliance node.

9.14.1 SYNOPSIS

system software version

9.14.2 DESCRIPTION

Use this command to view the version of your appliance node.

9.14.3 OPTIONS

system software version Use this command to view the version of your appliance node.

10

Storage commands

10.1 system storage-scan

system storage-scan - Use this command to refresh the storage disks and devices information.

10.1.1 SYNOPSIS

system storage-scan

10.1.2 DESCRIPTION

This command enables you to refresh the storage disks and devices information.

10.1.3 OPTIONS

system storage-scan

Use to refresh the storage disks and devices information.

11

Support commands

11.1 support collect

support collect - Collect appliance details and transmit to Veritas AutoSupport server.

11.1.1 SYNOPSIS

support collect inventory support collect config

11.1.2 DESCRIPTION

Use this command to collect appliance details on-demand without waiting for a scheduled collection. Ensure that Call Home is enabled on the appliance before you run this command.

11.1.3 OPTIONS

support collect config Use this command to collect configuration information about the appliance and transmit it to the Veritas AutoSupport server.

support collect inventory Use this command to collect all component-specific metadata including the appliance model and serial number and transmit it to the Veritas AutoSupport server.

11.1.4 EXAMPLES

The following example shows the output that is displayed when you run the `support collect config` command:

```
[access-8.1] access-appliance > support collect config

[Info] Collecting configuration data. This process may take several minutes.

[Info] V-475-4-30000 Configuration data collection completed.

Transmitting this data to the Veritas AutoSupport server may

take up to 30 seconds.

The following example shows the output that is displayed when you run the ``support␣
↪collect inventory`` command:

[access-8.1] access-appliance > support collect inventory

Collecting inventory data.The data collecting process may take

several minutes. Inventory collection completed. It may take 10 to 30

seconds to transmit the data to Veritas.
```

11.2 support data-collect

support data-collect – Gather device logs.

11.2.1 SYNOPSIS

support data-collect *advanced*

support data-collect *delete* <*file*=>

support data-collect *list*

support data-collect *status*

support data-collect *upload* <*file*=>

support data-collect *sanitize-data status*

support data-collect *sanitize-data enable*

support data-collect *sanitize-data disable*

11.2.2 DESCRIPTION

Use this command to

- Collect default/additional diagnostic logs.
- Delete the log package that were generated using the data-collect command.
- List all the generated log packages from the /log/data-collect directory.
- Display the status of the ongoing data-collect command.
- Disable the use of a proxy server for this appliance.
- Upload the log package that were generated using the data-collect command.
- Enable, disable, and view the current setting for sanitizing sensitive data.

11.2.3 OPTIONS

support data-collect advanced Collect additional diagnostic logs.

support data-collect list List all the generated log packages from the /log/data-collect directory.

support data-collect status Display the status of the ongoing data-collect command.

support data-collect delete <*file*=> Delete the log packages that were generated using the data-collect command.

support data-collect upload <*file*=> Upload the log package that was generated using the data-collect command.

support data-collect sanitize-data *status* Display the data sanitization status.

support data-collect sanitize-data *enable* Mask sensitive data such as personally identifiable information (PII) in the generated data-collect log package. Data-sanitization is enabled by default.

support data-collect sanitize-data *disable* Disable masking of sensitive data such as personally identifiable information (PII) in the generated data-collect log package

11.2.4 EXAMPLES

```
support data-collect

[INFO] The data-collect command is initiated. Use the support data-collect
status command to check the current status.

Operation completed successfully
```

11.3 support elevate

support elevate - Enables the user to open a root shell.

11.3.1 SYNOPSIS

support elevate

11.3.2 DESCRIPTION

You can use this command to open a root shell in which you can troubleshoot or manage underlying operating system tasks. The maintenance passowrd is required for running this command.

NOTE: If current appliance node is in lockdown mode, you need assistance from Veritas Support to generate One-Time Password (OTP) and unlock root shell access before you can successfully open the root shell. In this case, a passphrase, which your Support representative specified while generating the security key, is needed.

11.4 support lock

support lock - Lock root shell access.

11.4.1 SYNOPSIS

support lock

11.4.2 DESCRIPTION

You can use the this command to lock root shell access if the appliance node has been unlocked by command `support unlock` , when this appliance node is in lockdown mode.

NOTE:

- When it is run, all the active root shell sessions in current node will be terminated.
- The system will lock root shell access automatically after 12 hours even if you do not manually run this command.

11.5 support shell

support shell - Enables the user to open a read-only shell.

11.5.1 SYNOPSIS

support shell

11.5.2 DESCRIPTION

You can use this command to open a shell in which you can monitor and troubleshoot the appliance node as a non root user in read-only mode.

11.6 support unlock

support unlock - Unlock root shell access.

11.6.1 SYNOPSIS

support unlock

11.6.2 DESCRIPTION

You can use the this command to unlock root shell access when this appliance node is in lockdown mode. When it is run, you are prompted for the security key which your support representative must generate.

11.7 system infraservices

system infraservices - Show and manage the infrastructure services

11.7.1 SYNOPSIS

system infraservices show all

system infraservices start all

system infraservices stop all

system infraservices show database

system infraservices start database

system infraservices stop database

system infraservices show webserver

system infraservices start webserver

system infraservices stop webserver

system infraservices show messagequeue

system infraservices start messagequeue

system infraservices stop messagequeue

11.7.2 DESCRIPTION

You can use these commands to monitor, start, and stop the infrastructure services.

Note: The infrastructure service commands are mainly used for troubleshooting and support. These should be used under the guidance of Technical Support. Stopping the infrastructure services may lead to failure of running operations.

11.7.3 OPTIONS

system infraservices *show all*

Show the status of all the infrastructure services. The infrastructure services include the database, message queue, and the web server service.

system infraservices *start all*

Start all the infrastructure services. The infrastructure services include the database, message queue, and the web server service.

system infraservices *stop all*

Stop all the infrastructure services. The infrastructure services include the database, message queue, and the web server service.

system infraservices *show database*

Show the status of the database.

system infraservices *start database*

Start the database.

system infraservices *stop database*

Stop the database.

system infraservices *show messagequeue*

Show the status of the message queue service.

system infraservices *start messagequeue*

Start the message queue service.

system infraservices *stop messagequeue*

Stop the message queue service.

system infraservices *show webserver*

Show the status of the web server service.

system infraservices *start webserver*

Start the web server service.

system infraservices *stop webserver*

Stop the message queue service.

11.7.4 EXAMPLES

The following example shows the output that is displayed when you run the `system infraservices show database` command:

```
[access-8.1] access-appliance > system infraservices show database

Database is running.

Operation completed successfully
```

11.8 system hardware DIMM cleanup-errors

system hardware DIMM cleanup-errors - Resets the uncorrectable error count of specific failed DIMMs (dual in-line memory modules) to zero.

11.8.1 SYNOPSIS

system hardware DIMM cleanup-errors

11.8.2 DESCRIPTION

You might need to run this command after a failed DIMM has been replaced. Use this command if after replacing some DIMMs the uncorrectable error count is not reset (to zero) automatically. After replacing a DIMM, you can verify the uncorrectable error count by running the `show hardware-health node component=DIMM`

NOTE: Ensure that you contact the Technical Support before you run this command.

11.8.3 OPTIONS

system hardware DIMM cleanup-errors

After the failed DIMMs have been replaced, this command might be needed to reset the uncorrectable error count of the specific DIMMs. By default, the command resets the uncorrectable error count of all the failed DIMMs that are shown in the output. You can specify specific IDs to reset the uncorrectable error count for specific failed DIMMs. If alerts are configured for the appliance, after the uncorrectable error count is reset, you will receive one or more alerts indicating that the DIMM error is resolved.

11.8.4 EXAMPLES

The following example shows the sample output that is displayed when you run the `system hardware DIMM cleanup-errors`: Showing the DIMMs (dual in-line memory modules) with a failed state:

```
+-------+-------------+------------+------+------+----+----+-----+-------------+------
|IDName |Status       |Manufacturer|Part  |Serial|Type|Size|Speed|Uncorrectable|State
|       |             |            |Number|Number|    |    |     |Error Count  |
+-------+-------------+------------+------+------+----+----+-----+-------------+------
|CPU1   |Uncorrectable|  Samsung   |M393A1|313C6 |DDR4|8192|2133 |   2         |Failed
|Channel|Error        |            |G40DB0|2CB   |    | MB |MT/s |             |
|A Slot |             |            |-CPB  |      |    |    |     |             |
|1      |             |            |      |      |    |    |     |             |
+-------+-------------+------------+------+------+--------+-----+-------------+------
|CPU1   |Uncorrectable|  Samsung   |M393A1|313C5 |DDR4|8192|2133 |   2         |Failed
|Channel|Error        |            |G40DB0|3CA   |    | MB |MT/s |             |
|A Slot |             |            |-CPB  |      |    |    |     |             |
|2      |             |            |      |      |    |    |     |             |
+-------+-------------+------------+------+------+----+----+-----+-------------+------
```

To reset the uncorrectable error count of specific DIMMs from the table, enter the IDs separated by commas. To reset the uncorrectable error count for all the DIMMs shown in the table, type all(default): CPU1 Channel A Slot1, CPU1 Channel A Slot 2 Are you sure you want to reset the uncorrectable error count for CPU1 Channel A Slot1, and CPU1 Channel A Slot2?[yes, no](no): yes The reset has been initiated. It may take some time to complete. If alerts are

configured, you will receive one or more alerts indicating that the DIMM error is resolved. Showing the DIMMs (dual in-line memory modules) with a failed state:

```
+-------+-------------+------------+------+------+----+----+-----+-------------+------
|ID     |Status       |Manufacturer|Part  |Serial|Type|Size|Speed|Uncorrectable|State
|       |             |            |Number|Number|    |    |     |Error Count  |
+-------+-------------|------------+------+------+----+----+-----|-------------+------
|CPU1   |Uncorrectable|  Samsung   |M393A1|313C6 |DDR4|32  |2400 | 1           |Failed
|Channel|Error        |            |G40DB0|2CB   |    |GB  |MT/s |             |
|A Slot |             |            |-CPB  |      |    |    |     |             |
|1      |             |            |      |      |    |    |     |             |
+-------+-------------+------------+------+------+----+----+-----+-------------+------
```

Are you sure you want to reset the uncorrectable error count for CPU1 Channel A Slot 1?[yes, no](no):yes

The reset has been initiated. It may take some time to complete. If alerts are configured, you will receive one or more alerts indicating that the DIMM error is resolved