

# Veritas Access Appliance Commands Reference Guide

7.3.2 Revision 2

# Veritas Access Appliance Commands Reference Guide

Last updated: 2018-06-14

## Legal Notice

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC  
500 E Middlefield Road  
Mountain View, CA 94043

<http://www.veritas.com>

.

## 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](mailto:CustomerCare@veritas.com)

Japan

[CustomerCare\\_Japan@veritas.com](mailto:CustomerCare_Japan@veritas.com)

## Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

<https://sort.veritas.com/documents>

## 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](mailto:APPL.docs@veritas.com)

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

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

## 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](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# Contents

Chapter 1	Overview .....	7
	Scope of the Veritas Access Commands Reference Guide .....	7
	Where to find the documentation .....	7
	Changes in the Access Appliance document revision .....	9
	Using the Access Appliance shell menu .....	9
Appendix A	Main > Appliance .....	11
	Main > Appliance > Status .....	12
Appendix B	Main > Manage > Cluster .....	13
	Main > Manage > Cluster > Configure .....	14
Appendix C	Main > Manage > Software .....	15
	Main > Manage > Software > Cancel .....	16
	Main > Manage > Software > Delete .....	17
	Main > Manage > Software > Download .....	18
	Main > Manage > Software > DownloadProgress .....	19
	Main > Manage > Software > Install .....	20
	Main > Manage > Software > List .....	21
	Main > Manage > Software > Readme .....	22
	Main > Manage > Software > Rollback .....	24
	Main > Manage > Software > Share .....	25
	Main > Manage > Software > UpgradeStatus .....	26
Appendix D	Main > Manage > Storage .....	27
	Main > Manage > Storage > Show .....	28
	Main > Manage > Storage > Scan .....	29
	Main > Manage > Storage > Erase .....	30
Appendix E	Main > Network .....	32
	Main > Network > Configure .....	33
	Main > Network > Date .....	34
	Main > Network > DNS .....	35

Main > Network > Gateway .....	37
Main > Network > Hosts .....	39
Main > Network > IPv4 .....	40
Main > Network > IPv6 .....	41
Main > Network > SetProperty .....	42
Main > Network > Show .....	43
Main > Network > TimeZone .....	44
Main > Network > NetStat .....	45
Main > Network > NTPServer .....	46
Main > Network > Unconfigure .....	47
Main > Network > VLAN .....	48
Main > Network > TraceRoute .....	51
Main > Network > Ping .....	52
Main > Network > Hostname Show .....	53
Main > Network > Proxy .....	54

## Appendix F      Main > Monitor ..... 57

Main > Monitor > MemoryStatus .....	58
Main > Monitor > NetworkStatus .....	61
Main > Monitor > SDCS .....	62
Main > Monitor > Top .....	64
Main > Monitor > Uptime .....	65
Main > Monitor > Who .....	66
Main > Monitor > Hardware .....	67

## Appendix G      Main > Settings ..... 70

Main > Settings > Password .....	71
Main > Settings > Alerts > CallHome .....	72
Main > Settings > Alerts > Email .....	74
Main > Settings > Alerts > Hardware .....	77
Main > Settings > Alerts > SNMP .....	78
Main > Security > DeviceCertificate > Export .....	86
Main > Security > DeviceCertificate > Import .....	87

## Appendix H      Main > Support ..... 88

Main > Support > DataCollect .....	89
Main > Support > Logs .....	91
Main > Support > RAID .....	93
Main > Support > Shutdown .....	94
Main > Support > Storage Reset .....	95
Main > Support > Test .....	96

Main > Support > FactoryReset .....	98
Main > Support > InfraServices .....	103
Main > Support > IPMI .....	105
Main > Support > Maintenance .....	108
Main > Support > Reboot .....	109
Main > Support > Services .....	110

# Overview

This chapter includes the following topics:

- [Scope of the Veritas Access Commands Reference Guide](#)
- [Where to find the documentation](#)
- [Using the Access Appliance shell menu](#)

## Scope of the Veritas Access Commands 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 initial configuration. For example, the `Network > Configure` command for configuring `eth1`, the `Cluster > Configure` command for setting up the Access cluster on the appliance.
- Access Appliance node-level management. For example, the `Network > Date` command for setting the date and time, and the `Monitor > Hardware` command for monitoring the node hardware.

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

See [“Where to find the documentation”](#) on page 7.

## 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://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 and Administration Guide*

---

**Note:** This guide replaces the *Veritas Access Appliance Getting Started Guide*

---

- *Veritas Access Appliance Commands Reference Guide*
- *Veritas Access Appliance Release Notes*

---

**Note:** For the 7.3.2 release, this guide has been removed. The content has been moved into the *Veritas Access Release Notes*.

---

- *Veritas Access 3340 Appliance Product Description*
- *Veritas Access 3340 Appliance Hardware Installation Guide*
- *Veritas Appliance AutoSupport 2.0 Reference Guide*
- *Veritas Access Safety and Maintenance Guide*
- Veritas Access documentation set

## Veritas Access documentation set

The corresponding version of the Access application documentation is available on the same page of the Veritas Services and Operations Readiness Tools (SORT) website.

The following guides are available for the Access application:

- Veritas Access Administrator's Guide
- Veritas Access Command Reference Guide
- Veritas Access NetBackup Solutions Guide
- Veritas Access Online Help
- Veritas Access RESTful API Guide
- Veritas Access Release Notes
- Veritas Access Troubleshooting Guide



## Changes in the Access Appliance document revision

In the 7.3.2 release, the Access Appliance documentation set has been revised. The following changes are made:

- The *Veritas Access Appliance Getting Started Guide* has been renamed as *Veritas Access Appliance Initial Configuration and Administration Guide*
- The *Veritas Access Appliance Release Notes* has been removed for the 7.3.2 release. The content has been merged into the *Veritas Access Release Notes*.

## 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 `Main_Menu` view is displayed.

```
access-cluster_01.Main_Menu>
```

```
Appliance  Access Appliance node configuration.
Exit       Logout and exit from the current shell.
Manage     Manage Access Appliance node.
Monitor    Monitor appliance activities.
Network    Network Administration.
Settings   Change appliance settings.
Shell      Shell operations.
Support    Appliance Support.
```

To navigate to sub-views or execute available commands, type the name of the option you want from the list of available options. For example, from the `Main_Menu` view, type **Manage** and press Enter to go to the `Manage` view.

### 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, from the `Main_Menu > Settings > Alerts` view, the following command has one mandatory parameter and two optional parameters:

```
Email SMTP Add <Server> [Account] [Password]
```

Where `<Server>` is the mandatory SMTP server address, and `[Account]` and `[Password]` are the optional account credentials if the SMTP server requires them.

## Main > Appliance

This appendix includes the following topics:

- [Appliance > Status](#)

# Appliance > Status

`Appliance > Status` – Show status information about the appliance node.

## SYNOPSIS

`Status`

## DESCRIPTION

Use this command to show status information about the appliance and the current node.

- Appliance model
- Access software version
- Appliance software version
- Appliance node status
- Access cluster name
- Access management console virtual IP address

## OPTIONS

`Status`

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

## Main > Manage > Cluster

This appendix includes the following topics:

- [Cluster > Configure](#)

# Cluster > Configure

Cluster > Configure – Configure the Access cluster on the appliance.

## SYNOPSIS

Configure

## 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 reserved enough IP addresses for use as the physical and the virtual IP addresses of the Access cluster. At least four continuous IP addresses must be reserved for each type.

Do not run the `Configure` 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 on the other node.
- When the node is an unconfigured node that is used to replace a faulty node in an Access cluster.

## OPTIONS

Configure

Use the command to configure the Access cluster on the appliance.

# Main > Manage > Software

This appendix includes the following topics:

- [Manage > Software > Cancel](#)
- [Manage > Software > Delete](#)
- [Manage > Software > Download](#)
- [Manage > Software > DownloadProgress](#)
- [Manage > Software > Install](#)
- [Manage > Software > List](#)
- [Manage > Software > Readme](#)
- [Manage > Software > Rollback](#)
- [Manage > Software > Share](#)
- [Manage > Software > UpgradeStatus](#)

# Manage > Software > Cancel

Manage > Software > Cancel – Cancel the download process of a software update or the software patch, which can be in any of these installation stages - downloading or stopped or finished, or postcheck.

## SYNOPSIS

```
Cancel update_name
```

## DESCRIPTION

Use this command to cancel 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.
- Finished - The software update is downloaded completely. However, you must run the `Software > List Downloaded` command to view the software updates that are available for installation.
- 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.

## OPTIONS

```
Cancel update_name
```

This command cancels downloading of patch. Here, *update\_name* is the name of the software patch update.



# Manage > Software > Delete

Manage > Software > Delete – Delete a software update.

## SYNOPSIS

```
Delete update_name
```

## DESCRIPTION

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

## OPTIONS

```
Delete update_name
```

Delete a specific release update. Here *update\_name* is the specific name of the update that you want to delete.

# Manage > Software > Download

Manage > Software > Download – Download a software update.

## SYNOPSIS

Download *update\_name*

## DESCRIPTION

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

## OPTIONS

Download *update\_name*

Download a specific update, where *update\_name* is the name of the update that you want to download.

# Manage > Software > DownloadProgress

Manage > Software > DownloadProgress – Show the progress of an online patch download.

## SYNOPSIS

DownloadProgress

## DESCRIPTION

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

## OPTIONS

DownloadProgress

Display the download progress of a software patch.

# Manage > Software > Install

Manage > Software > Install – Use to install an EEB or a software release update.

## SYNOPSIS

```
Install update_name
```

## DESCRIPTION

Use this command to install a new or an existing software update or an engineering binary (EEB) to an appliance node that you designate.

To use this command you must know the name of the software update or EEB that you want to install. To see a list of the software updates and EEB that are available for you to install, run `Software > List AvailablePatch` command. This command checks the Veritas site for the latest software update. Once you find the software update or EEB that you want to install, you must run the `Software > Download update_name` command, where *update\_name* is the name of the software update.

After you have downloaded the software update, you can now run the `Software > Install update_name` command.

## OPTIONS

```
Install update_name
```

Install a software release update.

*update\_name* is the name of the update that you want to install.

# Manage > Software > List

Manage > Software > List – Lists the available patch information.

## SYNOPSIS

```
List AvailablePatch
List Details All
List Downloaded
List Downloaded Details [update_name]
List EEBs
List Version
```

## DESCRIPTION

This command shows the patches that have been applied to a particular appliance. In addition, you can use this command to show the patches that are available for installation for a particular appliance node.

## OPTIONS

```
List AvailablePatch
    Use this command to check the Veritas site for any software updates that are
    available.

List Details All
    Use this command to view all of the release updates that are available.

List Downloaded
    List downloaded software updates.

List Downloaded Details update_name
    List the detailed information of a downloaded software update.

List EEBs
    Show a detailed listing of all of the factory-installed Emergency Engineering
    Binaries (EEBs).

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

# Manage > Software > Readme

Manage > Software > Readme – Defines the Access Appliance patch process.

## SYNOPSIS

Readme

## DESCRIPTION

This command defines the patch process for the appliance node.

## OPTIONS

Readme

This command defines the patch process for the appliance node.

## EXAMPLES

This command contains the following patch information.

Patch Readme

=====

The following procedures explain how to copy a software release update on to the Access Appliance and install the update.

To download software update directly from the Veritas Support website:

1. Use the 'List AvailablePatch' command to look for the latest release updates.
2. Use the 'Download' command to download the release update.
3. Use the 'List 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 'Share Open' command to open the NFS and CIFS shares so the appliance node can receive the release updates.  
For NFS: (access-appliance:/inst/patch/incoming)  
For CIFS: (\\access-appliance\\incoming\_patches)
3. On the local computer, perform the following steps:
  - a. Mount/Map the appropriate NFS/CIFS share.  
For CIFS, you must map using the appliance 'admin' user's credentials.
  - 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.
  - e. Unmap/Unmount the mounted share.
4. Use the 'Share Close' command to close the NFS and CIFS shares.
  5. Use the 'List Downloaded' command to list all of 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 Access Appliance upgrade process before you install the patch to this node.
2. Use the 'Install' 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 'List Downloaded' command.

For more detailed information about this process, see the *Product Long Name documentation*.

# Manage > Software > Rollback

Manage > Software > Rollback – Rollback a specific EEB.

## SYNOPSIS

```
Rollback eeb_name
```

## DESCRIPTION

Use this command to rollback any Emergency Engineering Binaries (EEBs) that are installed on your appliance node. You can use the `List` commands to view the software version and all installed EEBs. You can then specify which EEB you want to roll back.

You can only specify one EEB at a time with this command. However, you can use this command multiple times to roll back as many installed EEBs as you want.

## OPTIONS

```
Rollback eeb_name
```

Rollback a specified EEB, where *eeb\_name* is the name of the EEB to rollback.

For example, run the following command to roll back EEB ABC5200\_EEB\_1-1.2.3.4.

```
Software> Rollback ABC5200_EEB_1-1.2.3.4
```



# Manage > Software > Share

Manage > Software > Share – Share or unshare a directory for incoming patches

## SYNOPSIS

Share Open

Share Close

## 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) and Common Internet File System (CIFS) protocol shares.

## OPTIONS

Share Open

Open the NFS and the CIFS shares for the directory that receives incoming patches.

For CIFS, you must map using the appliance "admin" user's credentials.

Share Close

Close the NFS and the CIFS shares for the directory that receives incoming patches.

# Manage > Software > UpgradeStatus

Manage > Software > UpgradeStatus – View the version and the software upgrade status.

## SYNOPSIS

UpgradeStatus

## DESCRIPTION

This command displays the version and the upgrade status of the appliance node.

## OPTIONS

UpgradeStatus

View the version and the upgrade status of the appliance node.

## EXAMPLES

The following is an example output of the Main > Manage > Software > UpgradeStatus command:

```
abc123.Software> UpgradeStatus
```

```
Command backup_system_files is completed. The upgrade is 21% completed.
```

# Main > Manage > Storage

This appendix includes the following topics:

- [Manage > Storage > Show](#)
- [Manage > Storage > Scan](#)
- [Manage > Storage > Erase](#)

# Manage > Storage > Show

Manage > Storage > Show – View storage information.

## SYNOPSIS

Show Disk

## DESCRIPTION

This command enables you to view the storage information of the storage devices within your appliance.

## OPTIONS

Show Disk

This command shows the disk name, type, capacity, and nodes.

- **Disk name:** The Access disk name.

---

**Note:** For the System disk, the **Disk name** column shows the 32-character disk ID instead of the Access disk name. The System disk is an internal disk that belongs to the node that you are currently on.

---

- **Type:** The disk type is Configuration, Data, or Fencing.
- **Capacity:** The disk size in MB or TB.
- **Nodes:** If it is the system disk that locates on the node, this column shows the node host name. If it is a shared disk, this column shows Shared between all nodes.

# Manage > Storage > Scan

`Manage > Storage > Scan` – Use this command to refresh the storage disks and devices information.

## SYNOPSIS

`Scan`

## DESCRIPTION

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

## OPTIONS

`Scan`

Use to refresh the storage disks and devices information.

# Manage > Storage > Erase

Manage > Storage > Erase – Used to manage the non-certified disk erasure process.

## SYNOPSIS

Erase Configure

Erase Show

Erase Abort

## DESCRIPTION

The non-certified disk erasure enables you to erase the Configuration, Data and Fencing disks on the appliance shared storage. When you erase a disk, all the data stored on the disk is destroyed and cannot be recovered.

The command enables you to manage the non-certified disk erasure process as follows:

- Configure disk erasure to erase all the disks on the appliance shared storage. You can specify a pass algorithm for overwriting the data on the disks.
- View disk erasure tasks in progress. You can also view the disk erasure history for each storage disk on the appliance.
- Abort the disk erasure operation.

## OPTIONS

Erase Configure

Configure disk erasure to erase all the disks on the appliance shared storage. This command requires you to enter the pass algorithm to be used. The available options are 1, 3, and 7.

Erase Show

View the disk erasure tasks in progress. You can also view the disk erasure history for each storage disk on the appliance.

Erase Abort

Abort the disk erasure operation for all the disks.

Aborting a disk erasure operation results in the corruption of all data on the disk. Once the data is corrupted, it cannot be recovered.

---

**Note:** When you abort a disk erasure operation, any erasure progress on the disk is lost. You must configure disk erasure again to erase the disk.

---

# Main > Network

This appendix includes the following topics:

- [Network > Configure](#)
- [Network > Date](#)
- [Network > DNS](#)
- [Network > Gateway](#)
- [Network > Hosts](#)
- [Network > IPv4](#)
- [Network > IPv6](#)
- [Network > SetProperty](#)
- [Network > Show](#)
- [Network > TimeZone](#)
- [Network > NetStat](#)
- [Network > NTPServer](#)
- [Network > Unconfigure](#)
- [Network > VLAN](#)
- [Network > TraceRoute](#)
- [Network > Ping](#)
- [Network > Hostname Show](#)
- [Network > Proxy](#)



# Network > Configure

Network > Configure – Configure the appliance to a network.

## SYNOPSIS

```
Configure IPAddress Netmask GatewayIPAddress InterfaceNames
```

## DESCRIPTION

You can use the `Configure` command to configure 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 `Network > Gateway` command to add the routing information for default route or to add route for VLAN interfaces.

## OPTIONS

```
Configure IPAddress Netmask GatewayIPAddress InterfaceNames
```

Configure the IP address and default gateway for the appliance. The command configures the IP address and sets the default gateway.

Where *IPAddress* is the IPv4 address, *Netmask* is the netmask, *GatewayIPAddress* is the default gateway IP address, and *InterfaceNames* is the name of the device.

## EXAMPLES

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

```
Network > Configure 10.180.2.3 255.255.255.0 eth1
```

# Network > Date

Network > Date – Set or show the computer system time.

## SYNOPSIS

```
Date Set Month Day HHMMSS Year
```

```
Date Show
```

## DESCRIPTION

You can use this command to set or show the system time.

## OPTIONS

```
Date Set Month Day HHMMSS Year
```

Set the system time.

Where *Month* is the name of the month. *Day* is the day of the month and has a range of one to 31. The variable *HHMMSS* is the hour, minute, and seconds in a 24-hour format and the fields are separated by semi-colons, for example, HH:MM:SS. The variable *Year* is the current year and the range for this field is 1970 through 2037.

The following is sample entry for this command:

```
Date Set Apr 29 23:44:34 2011
```

```
Date Show
```

Show the system date and time.

# Network > DNS

Network > DNS – Configure the DNS information for the appliance.

## SYNOPSIS

DNS Add NameServer *IPAddress*

DNS Add SearchDomain *DomainName*

DNS Delete Domain

DNS Delete NameServer *IPAddress*

DNS Delete SearchDomain *DomainName*

DNS Domain *Name*

DNS Show

## DESCRIPTION

You can use this command to perform the following tasks:

- Add or delete a name server to the DNS configuration.
- Add or delete a domain name to the DNS search list.
- Set the appliance DNS domain name.
- Show the current DNS information.

## OPTIONS

DNS Add NameServer *IPAddress*

Add a DNS nameserver to the DNS configuration.

Where *IPAddress* is the IP address of the DNS name server.

DNS Add SearchDomain *DomainName*

Add a DNS search domain to the configuration.

Where *DomainName* is the target domain to add for searching.

DNS Delete Domain

Delete a DNS domain name.

DNS Delete NameServer *IPAddress*

Delete a DNS named server from the configuration.

Where *IPAddress* is the IP address of the DNS name server.

DNS Delete SearchDomain *DomainName*

Delete a DNS search domain from the configuration.

Where *IPAddress* is the IP address of the DNS name server.

DNS Domain *Name*

Set the appliance domain name, where *Name* is the domain name of the appliance

DNS Show

Show the current DNS information.

# Network > Gateway

Network > Gateway — Add or delete routing information.

## SYNOPSIS

```
Gateway Add GatewayIPAddress [TargetNetworkIPAddress] [Netmask]  
[InterfaceName]  
  
Gateway Delete TargetNetworkIPAddress [Netmask]  
  
Gateway Show IPVersion
```

## DESCRIPTION

Use this command to add or delete a route from the kernel routing table. With this command you can also view the kernel routing table. Refer to Linux route man page for more advanced use cases.

With this command you can define the IPv4 address that you plan to add or delete as well as display the current gateway information. If multiple networks are added to the appliance configuration, you can use the `Gateway Add` command to add the gateway to all of the destination networks.

## OPTIONS

```
Gateway Add GatewayIPAddress [TargetNetworkIPAddress] [Netmask]  
[InterfaceName]
```

Add a route to a kernel routing table.

Where the *GatewayIPAddress* variable is the new IPv4 gateway address. The *TargetNetworkIPAddress* is the target network IPv4 address. The *Netmask* variable is the target network netmask, and *InterfaceName* is the interface name. The *TargetNetworkIPAddress*, *Netmask*, and *InterfaceName* are optional when you set up the default gateway. After the default gateway has been added, you must use these fields to add any additional gateways.

```
Gateway Delete TargetNetworkIPAddress [Netmask]
```

Delete the route from the kernel routing table.

Where *TargetNetworkIPAddress* is the target network address. The *Netmask* variable is the target network netmask.

```
Gateway Show [IPVersion]
```

Display the gateway and the route information. Here, [*IPVersion*] parameter is an optional parameter. It defines the IP protocols - IPv4 and IPv6. If you do

not enter a value for the [IPVersion] parameter, the information is displayed for IPv4.

To know the gateway information for a VLAN interface, enter the VLAN interface ID for the [IPVersion] parameter.

## EXAMPLES

Use the following example to set the default gateway.

```
Gateway Add 10.180.1.1
```

Use the following example to add a route to the destination network 192.168.2.0.

```
Gateway Add 191.168.2.1 192.168.2.0 255.255.255.0
```

```
Gateway Add 9ffe::49 6ffe:: 64 eth1
```

Use the following example to delete the default gateway.

```
Gateway Del default
```

Use the following example to delete a route to the destination network, 10.180.0.0 or 6ffe::/64.

```
Gateway Delete 10.180.0.0
```

```
Gateway Delete 6ffe::/64
```

# Network > Hosts

Network > Hosts – Manage the IP address and host name mapping.

## SYNOPSIS

```
Hosts Add IPAddress FQHN ShortName
```

```
Hosts Delete IPAddress
```

```
Hosts Show
```

## DESCRIPTION

You can use this command to view the hosts configuration information, such as the IP address and host name mapping. You can also use this command to add or delete an IP address from the hosts file.

## OPTIONS

```
Hosts Add IPAddress FQHN ShortName
```

Add an IP address to the host name mapping.

*IPAddress* is the IPv4 or IPv6 address to add.

*FQHN* is the fully qualified host name. And *ShortName* is the short host name.

```
Hosts Delete IPAddress
```

Delete an IP address from the host name mapping.

*IPAddress* is the IPv4 or the IPv6 address to be deleted.

```
Hosts Show
```

Display the IP address and host name mapping.

# Network > IPv4

Network > IPv4 – Change the IPv4 address of a network interface.

## SYNOPSIS

```
IPv4 IPAddress NetMask [InterfaceNames]
```

## DESCRIPTION

Use this command to change the IPv4 address of a network interface. You can use this command to configure multiple network interfaces. To do that, you must repeat the command for each network that you want to add.

## OPTIONS

```
IPv4 IPAddress NetMask [InterfaceNames]
```

Change the IPv4 address of a network interface.

Where *IPAddress* is the name of the new IPv4 address. The *NetMask* variable is the name of the netmask. The [*InterfaceNames*] parameter is a comma-separated list of interface names. The [*InterfaceNames*] field is optional. If an interface name is not provided, the command searches for an interface and configures it.



# Network > IPv6

Network > IPv6 – Add an IPv6 address without specifying a gateway address.

## SYNOPSIS

```
IPv6 IPAddress Prefix [InterfaceNames]
```

## DESCRIPTION

Use this command to configure the IPv6 address of a network interface. You cannot use this command to configure multiple interfaces.

## OPTIONS

```
IPv6 IPAddressPrefix [InterfaceNames]
```

Change the IPv6 address of a network interface.

Where *IPAddress* is the IPv6 address, *Prefix* is the prefix length, and [*InterfaceNames*] is the name of the device.

The [*InterfaceNames*] parameter is a comma-separated list of interface names. The [*InterfaceNames*] parameter is an optional field. If an interface name is not provided, the command searches for an interface and configures it.

## EXAMPLES

Use the following example to assign an IPv6 address to a specific interface:

```
IPv6 9ffe::9 64 eth1
```

# Network > SetProperty

Network > SetProperty – Set the Ethernet interface property.

## SYNOPSIS

```
SetProperty InterfaceName Property Value
```

## DESCRIPTION

You can use this command to set Ethernet interface property. You can define the name of the device, the property name such as an MTU. And you can define the property value, such as 1500 for the MTU.

## OPTIONS

```
SetProperty InterfaceName Property Value
```

Set Ethernet interface property.

Enter the name of the interface name in the *InterfaceName* variable. An example of this value is **eth1**. The *Property* variable is the property name, such as **mtu**. The *Value* variable is the property value, for example 1500.

The following is sample entry for this command:

```
SetProperty eth1 mtu 1500
```

This command changes the Maximum transmission unit (MTU) of interface (eth1) to 1500.

# Network > Show

Network > Show – List the network properties.

## SYNOPSIS

Show Configuration

Show Properties [InterfaceNames]

Show Status

## DESCRIPTION

Use this command to list the network properties.

## OPTIONS

Show Configuration

Display the network interface properties.

Show Properties [InterfaceNames]

Display the network properties. The `InterfaceNames` is an optional parameter.

Show Status

View the following network status information:

- Device status
- Routing status

# Network > TimeZone

Network > TimeZone – Set the time zone.

## SYNOPSIS

TimeZone Reset

TimeZone Set

TimeZone Show

## DESCRIPTION

You can use this command to set time zone for which your appliance is located. You can reset the time zone to the Coordinated Universal Time (UTC) or show the currently configured time zone.

## OPTIONS

TimeZone Reset

Reset the time zone to UTC.

TimeZone Set

Set the time zone.

TimeZone Show

Show the currently configured time zone.

# Network > NetStat

Network > NetStat — Identify network statistical information

## SYNOPSIS

NetStat a

NetStat an

NetStat ia

NetStat s

## DESCRIPTION

The `NetStat` command displays various network-related information such as network statistical information.

## OPTIONS

NetStat a

Examine network connections for all interfaces textually.

NetStat an

Examine network connections for all interfaces numerically.

NetStat ia

Examine network interface stats.

NetStat s

Examine network summary stats for all interfaces numerically.

# Network > NTPServer

Network > NTPServer – Manage the NTP Servers.

## SYNOPSIS

NTPServer Add *Server*

NTPServer Delete *Server*

NTPServer Show

## DESCRIPTION

Use this command manage the NTP servers. With this command, you can to do the following:

- Add an NTP server to the sync time.
- Delete an NTP server.
- Show the known NTP Servers.

## OPTIONS

NTPServer Add *Server*

Add an NTP Server. Where *Server* is the name of the server to add.

NTPServer Delete *Server*

Delete an NTP Server. Where *Server* is the name of the server to delete.

NTPServer Show

Show the known NTP Servers.

# Network > Unconfigure

Network > Unconfigure – Remove the IP address and shut down the interface.

## SYNOPSIS

```
Unconfigure InterfaceNames [IPAddress]
```

## DESCRIPTION

Use this command to remove the IP address and shut down the interface.

This network interface can be a physical interface, or a VLAN interface.

## OPTIONS

```
Unconfigure InterfaceNames [IPAddress]
```

Remove the IP address and shut down the interface. *InterfaceNames* is the name of the interface.

[*IPAddress*] is the IPv4 address. [*IPAddress*] is an optional parameter.

The *InterfaceNames* can be a VLAN interface, or a ethernet interface.

# Network > VLAN

`Network > VLAN` – Tag a VLAN, view its properties and status, or delete a tagged VLAN.

## SYNOPSIS

`VLAN Delete VLANID`

`VLAN Show Properties Interfaces InterfaceNames`

`VLAN Show Status Interfaces InterfaceNames`

`VLAN Tag VLANID InterfaceNames [IPAddress] [Netmask]`

## DESCRIPTION

Use these commands to configure and manage VLAN for your appliance in your existing network environments.

To tag a VLAN using a physical interface, conform to the following guidelines

- Ensure that the selected interface or ethernet device is plugged.
- The selected interface must not have an IP address configured to it. If the selected interface is configured with an IP address, you must first unconfigure the IP address and then tag a VLAN to it. To unconfigure the IP address, run the `Network > Unconfigure` command.

Use the `VLAN Show` command options to view the properties and statuses of your network interfaces.

## OPTIONS

`VLAN Delete VLANID`

Delete a protocol-based VLAN. Here, *VLANID* is a numeric identifier for a tagged VLAN.

If the VLAN interface is configured with an IP address, you must first unconfigure the IP address to delete the VLAN.

`VLAN Show Properties Interfaces InterfaceNames`

View all the properties of a VLAN, where *InterfaceNames* is the name of the interface to which a VLAN is tagged. If you do not provide a value for the `[InterfaceNames]` parameter, the command displays properties for all the network interfaces that are available. Some of the property types that are included are MAC address, speed, and port type.



VLAN Show Status Interfaces *InterfaceNames*

View the status of a VLAN. The VLAN status can be *PLUGGED* or *UNPLUGGED*. Here, *InterfaceNames* is the name of the interface to which a VLAN is tagged.

VLAN Tag *VLANID* *InterfaceNames* [*IPAddress*] [*Netmask*]

Tag a VLAN to a physical interface. Here, *VLANID* is the VLAN identifier, which is numeric value and it can range between 1 - 4094. *InterfaceNames* is the name of the interface to which you want to tag the VLAN. [*IPAddress*] is an IPv4 address and [*Netmask*] is netmask for IPv4. The *VLANID* and *InterfaceNames* are mandatory variables; whereas [*IPAddress*] and [*Netmask*] are optional parameters.

## EXAMPLES

The following is an example of information that is displayed when you run the `Main > Network > VLAN Show Properties` command.

```
nb-appliance.Network> VLAN Show properties
```

```
Card: vlan12 [ PLUGGED|UP ]
      BOOTPROTO           : |static           |
      DESCRIPTION         : |test         |
      DEVICE              : |vlan12       |
      ETHERDEVICE          : |eth1         |
      ETHTOOL_OPTIONS      : |undef        |
      IPADDR               : |10.10.10.10   |
      MTU                  : |1400         |
      NETMASK              : |255.255.255.0 |
      NETWORK             : |undef        |
      REMOTE_IPADDR        : |undef        |
      STARTMODE            : |auto         |
      USERCONTROL         : |no           |
      VLAN                 : |yes          |
      BUS_ID               : |undef        |
      FLAGS                : |RBMU         |
      ID                   : |12           |
      LINK                 : |yes          |
      MAC                  : |00:50:56:B5:74:13 |
      MASTER               : |undef        |
      MODEL                : |undef        |
      PORT_TYPE            : |Twisted Pair  |
      SERIAL               : |undef        |
      SKIP_ADDITIONAL_DISCOVERY : |0           |
      SKIP_LINKSTATE_DISCOVERY : |0           |
```

SPEED	:	1Gb/s	
VIRTUAL_DEV	:	undef	
VLANCOUNT	:	0	
ADMINPORT	:	No	
VIRTUAL	:	No	
IPADDR_V6	:	undef	

# Network > TraceRoute

Network > TraceRoute – Display the network packet route

## SYNOPSIS

TraceRoute *Host*

## DESCRIPTION

Use this command to display the network path of Internet routers that a packet takes as it travels from the appliance to the destination IP address or host.

## OPTIONS

TraceRoute *Host*

Display the network route that a packet took to a destination host name or the IPv4 or IPv6 address of the target computer.

Where *Host* is the hostname or the IPv4 or IPv6 address of the target computer.

# Network > Ping

Network > Ping – An attempt to reach a host or IP address with ICMP ECHO\_REQUESTs

## SYNOPSIS

Ping *Host*

## DESCRIPTION

Use this command to test whether a particular host is reachable across an Internet Protocol (IP) network. The command sends a small packet of information to a hostname or an IP address to test network communications. It then provides information on how long the packet took to come back to its origin.

## OPTIONS

Ping *Host*

Send a small packet of ICMP ECHO\_REQUESTs to a host name or an IPv4 or IPv6 address of the target computer to test the network communications.

Where *Host* is the hostname or the IPv4 or IPv6 address of the target computer.

# Network > Hostname Show

Network > Hostname Show – View the appliance node hostname.

## SYNOPSIS

Hostname Show

## DESCRIPTION

This command enables you to view your appliance node hostname.

## OPTIONS

Show

Display the host name.

# Network > Proxy

`Network > Proxy` – Use this command to manage proxy server settings for the appliance.

## SYNOPSIS

```
Proxy > Enable
Proxy > Disable
Proxy > Set Proxy [Tunnel] [Username]
Proxy > Unset
Proxy > Show
```

## DESCRIPTION

Use this command to do the following:

- Set and use a proxy for this appliance.
- Enable the use of a proxy server for this appliance.
- Disable the use of a proxy server for this appliance.
- Unset a proxy by removing the proxy settings from this appliance.
- Show the current proxy settings and status of the proxy for this appliance.

## OPTIONS

```
Proxy Set Proxy [Tunnel] [Username]
```

Configure the proxy for this appliance. By default, the proxy is enabled automatically after the configuration.

*Proxy*

Specifies 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]*

Specifies the optional proxy server tunnelling settings. The available options are `TunnelOn` and `TunnelOff`. The default option is `TunnelOff`.

*[Username]*

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

Proxy > Enable

Enables the use of a proxy server for this appliance.

Proxy > Disable

Disables the proxy server settings for this appliance.

Proxy > Unset

Unset a proxy for this appliance. The proxy sever settings are removed from this appliance.

Proxy > Show,

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

## EXAMPLES

The following is an example output of the `Proxy Set` command.

```
abc.Network.Proxy> Set 10.182.27.100:3128 TunnelOn admin
Enter password for user "admin":
Enter password for user "admin" again:
[Info] The default proxy server is set successfully.
```

The following is an example output of the `Proxy Show` command.

```
abc.Network.Proxy> Show
+-----+-----+-----+-----+-----+
| Proxy server | Access port | User   | Tunnel | Status |
+-----+-----+-----+-----+-----+
| 10.182.27.100 | 3128       | mukesh | On     | Enabled |
+-----+-----+-----+-----+-----+
```

The following is an example output of the `Proxy Enable` command.

```
abc.Network.Proxy> Enable
[Info] Enabled connection to the default proxy server.
```

The following is an example output of the `Proxy Disable` command.

```
abc.Network.Proxy> Disable
[Info] Disabled connection to the default proxy server.
```

The following is an example output of the `Proxy Unset` command.

```
abc.Network.Proxy> Unset
[Info] Are you sure you want to unset the default proxy server?
```

```
[yes, no] yes  
[Info] The default proxy server is unset successfully.
```



# Main > Monitor

This appendix includes the following topics:

- [Monitor > MemoryStatus](#)
- [Monitor > NetworkStatus](#)
- [Monitor > SDCS](#)
- [Monitor > Top](#)
- [Monitor > Uptime](#)
- [Monitor > Who](#)
- [Monitor > Hardware](#)

# Monitor > MemoryStatus

Monitor > MemoryStatus – Displays memory usage statistics of the host in KB.

## SYNOPSIS

MemoryStatus

## DESCRIPTION

Use this command to report memory usage statistics in KB.

## OPTIONS

MemoryStatus

Use this command to report memory usage statistics in KB.

## EXAMPLES

The following is an example of information that is displayed when you run the Main > Monitor > MemoryStatus command.

```
abc123.Monitor> MemoryStatus
```

	total	used	free	shared	buffers	cached
Mem:	8065028	6617948	1447080	0	347384	5111668
-/+ buffers/cache:		1158896	6906132			
Swap:	10993656	0	10993656			
Total:	19058684	6617948	12440736			

  

	total	used	free	shared	buffers	cached
Mem:	8065028	6617940	1447088	0	347384	5111664
-/+ buffers/cache:		1158892	6906136			
Swap:	10993656	0	10993656			
Total:	19058684	6617940	12440744			

  

	total	used	free	shared	buffers	cached
Mem:	8065028	6617940	1447088	0	347384	5111664
-/+ buffers/cache:		1158892	6906136			
Swap:	10993656	0	10993656			
Total:	19058684	6617940	12440744			

  

	total	used	free	shared	buffers	cached
--	-------	------	------	--------	---------	--------

Mem:	8065028	6618328	1446700	0	347384	5111712
-/+ buffers/cache:		1159232	6905796			
Swap:	10993656	0	10993656			
Total:	19058684	6618328	12440356			

	total	used	free	shared	buffers	cached
Mem:	8065028	6618320	1446708	0	347384	5111716
-/+ buffers/cache:		1159220	6905808			
Swap:	10993656	0	10993656			
Total:	19058684	6618320	12440364			

	total	used	free	shared	buffers	cached
Mem:	8065028	6618320	1446708	0	347384	5111716
-/+ buffers/cache:		1159220	6905808			
Swap:	10993656	0	10993656			
Total:	19058684	6618320	12440364			

	total	used	free	shared	buffers	cached
Mem:	8065028	6618304	1446724	0	347384	5111716
-/+ buffers/cache:		1159204	6905824			
Swap:	10993656	0	10993656			
Total:	19058684	6618304	12440380			

	total	used	free	shared	buffers	cached
Mem:	8065028	6618148	1446880	0	347384	5111712
-/+ buffers/cache:		1159052	6905976			
Swap:	10993656	0	10993656			
Total:	19058684	6618148	12440536			

	total	used	free	shared	buffers	cached
Mem:	8065028	6617636	1447392	0	347384	5111720
-/+ buffers/cache:		1158532	6906496			
Swap:	10993656	0	10993656			
Total:	19058684	6617636	12441048			

	total	used	free	shared	buffers	cached
Mem:	8065028	6617636	1447392	0	347384	5111724
-/+ buffers/cache:		1158528	6906500			
Swap:	10993656	0	10993656			
Total:	19058684	6617636	12441048			

	total	used	free	shared	buffers	cached
Mem:	8065028	6618212	1446816	0	347384	5111724

-/+ buffers/cache:	1159104	6905924
Swap:	10993656	0 10993656
Total:	19058684	6618212 12440472

# Monitor > NetworkStatus

Monitor > NetworkStatus – Displays the network statistics for the host.

## SYNOPSIS

NetworkStatus

## DESCRIPTION

Use this command to view network statistics for the appliance node.

## OPTIONS

NetworkStatus

Use this command to view the network statistics for the appliance node.

## EXAMPLES

The following example display information that is displayed when you run the Main > Manage > NetworkStatus command.

abc123.Monitor> NetworkStatus							
eth0		eth1		eth2		eth3	
KB/s in	KB/s out	KB/s in	KB/s out	KB/s in	KB/s out	KB/s in	KB/s out
0.00	0.00	0.00	0.00	18.27	0.42	0.00	0.00
0.00	0.00	0.00	0.00	19.11	0.26	0.00	0.00
0.00	0.00	0.00	0.00	5.40	0.26	0.00	0.00
0.00	0.00	0.00	0.00	14.69	0.26	0.00	0.00
0.00	0.00	0.00	0.00	11.07	0.26	0.00	0.00
0.00	0.00	0.00	0.00	21.99	0.26	0.00	0.00
0.00	0.00	0.00	0.00	15.97	0.26	0.00	0.00
0.00	0.00	0.00	0.00	22.95	0.26	0.00	0.00
0.00	0.00	0.00	0.00	7.91	0.26	0.00	0.00
0.00	0.00	0.00	0.00	15.99	0.26	0.00	0.00
0.00	0.00	0.00	0.00	16.54	0.58	0.00	0.00
0.00	0.00	0.00	0.00	10.63	0.26	0.00	0.00
0.00	0.00	0.00	0.00	4.43	0.26	0.00	0.00
0.00	0.00	0.00	0.00	16.60	0.26	0.00	0.00

# Monitor > SDCS

Monitor > SDCS – Configure and monitor Symantec Data Center Security (SDCS).

## SYNOPSIS

Audit

## DESCRIPTION

Use this command to monitor Symantec Data Center Security (SDCS) events and configuration on the appliance node.

## OPTIONS

The following commands and options are available under Monitor > SDCS:

Audit

Search, filter, and edit the retention settings of the SDCS audit log.

- Use the `Audit Search <search_string>` command to search the audit log for the specified string. Use quotation marks if your search string contains multiple words.
- Use the `Audit SetSettings FileNumber <file_number>` command to set the number of SDCS audit files that are maintained.
- Use the `Audit SetSettings RetentionPeriod <days>` command to set the number of days that the audit files are maintained.
- Use the `Audit ShowSettings` command to view the retention period (days) of the audit files.
- Use the `Audit View` command and options to filter and display the audit log based on available criteria.
  - `Audit View Date <ToDate> [FromDate]`  
View audit records using the `FromDate` to `ToDate` parameters. The format is `mm/dd/yyyy[-hh:mm:ss]`. If `FromDate` is omitted, it equals `ToDate` with `hh:mm:ss` set to zeroes.
  - `Audit View EventID <ID#>`  
Retrieve the detailed view of the audit record that contains the given event ID.
  - `Audit View EventType <event_code>`

Retrieve the audit records that match the given event type. Each event type is represented by a four-letter code that appears in the SDCS audit log. You can view the available codes using the `Audit View EventTypeCodes` command.

- `Audit View EventTypeCodes`  
Display the event type codes that can be used with the `Audit View EventType` command, along with a brief description of each code.
- `Audit View Filter <criteria>`  
View the audit records that match the filter criteria.
- `Audit View Severity <severity_code>`  
Retrieve the audit records that match the given severity. Each event is represented by a one-letter code that appears in the SDCS audit log. You can view the available codes using the `Audit View SeverityCodes` command.
- `Audit View SeverityCodes`  
Display the severity codes that can be used with the `Audit View Severity` command, along with a brief description of each code.

# Monitor > Top

Monitor > Top – Display the top process information.

## SYNOPSIS

Top

## DESCRIPTION

This command exists under the `Main > Monitor` view. You can use this command to view the top process information.

## OPTIONS

Top

Provides the information (frequently refreshed) about the most CPU-intensive processes currently running.

## EXAMPLES

The following is an example of process information that is displayed for the `Main > Monitor > Top` command.

```
top - 00:36:33 up 1 day,  2:39, 11 users,  load average: 1.71, 1.50, 1.40
Tasks: 1765 total,   1 running, 1758 sleeping,   0 stopped,   6 zombie
%Cpu(s):  0.8 us,   0.6 sy,   0.0 ni, 98.6 id,   0.0 wa,   0.0 hi,   0.0 si,   0.0 st
KiB Mem : 19630064+total, 17126507+free, 16448444 used,  8587128 buff/cache
KiB Swap: 10240000+total, 10240000+free,    0 used. 17844412+avail Mem

   PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
162533 root        20   0       0       0       0 Z    7.6   0.0   0:00.39 fusemnt_res_scr
  4510 rabbitmq   20   0 18.122g 108516  4748 S    6.6   0.1 108:56.56 beam.smp
 20926 root        20   0 1201028  26468  2812 S    5.6   0.0  99:31.51 sisidsdaemon
151723 root        20   0  159492   4348  1832 R    1.3   0.0   0:00.46 top
 52546 mongod    20   0  553884 192032  7884 S    0.7   0.1   8:06.59 mongod
  7162 root        20   0       0       0       0 S    0.3   0.0   0:23.60 dmpdaemon
 33916 root        20   0  539652   3860  2568 S    0.3   0.0   1:11.08 CFSSMountAgent
 33945 root        20   0  473072   3676  2500 S    0.3   0.0  22:48.45 CVMVolDgAgent
 61355 mongod    30  10   38040   1052   724 S    0.3   0.0   0:01.19 xinetd
 81703 root        20   0 2994616 557924 15420 S    0.3   0.3   2:48.90 jsvc
```



# Monitor > Uptime

`Monitor > Uptime` – Display the uptime statistics for the current host.

## SYNOPSIS

`Uptime`

## DESCRIPTION

Use this command to display the uptime statistics for the current host.

## OPTIONS

`Uptime`

Prints the current time, how long the system has been running, the number of users currently logged in (which may include the same user multiple times) and system load averages.

# Monitor > Who

Monitor > Who – Display current logon sessions on the current host.

## SYNOPSIS

Who

## DESCRIPTION

Use this command to display current logon sessions on the current host.

## OPTIONS

Who

Lists the names of users currently logged in, their terminal, the time they have been logged in, and the name of the host from which they have logged in.

## EXAMPLES

The following is an example of information that is displayed when you run the Main > Monitor > Who command.

```
abc123.Monitor> Who
10:44:37 up 1 day, 23:05, 5 users, load average: 0.01, 0.02, 0.05
USER      TTY      LOGIN@  IDLE   JCPU   PCPU WHAT
admin     tty1     Mon11   46:59m 0.11s  0.01s login -- admin
admin     pts/0    Mon11   46:41m 0.09s  0.18s sshd: admin [priv]
admin     pts/1    Mon12   46:40m 0.11s  0.18s sshd: admin [priv]
admin     pts/2    09:43   1:01m  0.11s  0.02s sshd: admin [priv]
admin     pts/3    10:17   0.00s  0.14s  0.01s sshd: admin [priv]
```

# Monitor > Hardware

Monitor > Hardware – View the various hardware components, view the errors and the health status.

## SYNOPSIS

```
Hardware ShowErrors
```

```
Hardware ShowComponents
```

```
Hardware ShowHealth Appliance [Item]
```

## DESCRIPTION

Use this command to do the following:

- Display the hardware components such as the appliance or the compute node, or the storage shelves. The items that are associated with these components also display.
- 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.
- View the performance and status of various hardware components of the appliance node and the attached storage.

## OPTIONS

```
Hardware ShowComponents
```

Display all the hardware components and items of an appliance node.

```
Hardware ShowErrors
```

Display all the errors that are related to hardware status.

```
Hardware ShowHealth Appliance [Item]
```

The following options are available for the [Item] parameter. The default value is ALL.

```
(All/Fan/CPU/Disk/RAID/Power/Temperature/Product/PCI/Network/  
Firmware/Partition/Connection/StorageStatus/DIMM) [all]
```

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

**Hardware ShowHealth Appliance Product**

```
Hardware ShowHealth PrimaryShelf [Item]
```

View the performance and status of the primary storage shelf of the appliance.

The following options are available for the [Item] parameter. The default value is ALL.

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

```
Hardware ShowHealth ExpansionShelf [ExpansionShelfID] [Item]
```

View the performance and status of the expansion storage shelf(shelves) of the appliance.

Where [ExpansionShelfID] is the ID of a specific expansion shelf. By default, the data is displayed for all the storage shelves. To check the expansion shelf IDs, use the `Main > Monitor > Hardware ShowComponents` command.

The following options are available for the [Item] parameter. 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:

**Hardware ShowHealth ExpansionShelf 1 FAN**

## EXAMPLES

The following is an example output of the `Monitor > Hardware ShowHealth Appliance Product` command.

```
Compute Node syscluster_01
```

```
Time Monitoring Ran: Mon Jan 22 2018 22:52:21 PST
```

```
+-----+  
|           Hardware monitor information           |  
|+-----+-----+-----+-----+|  
|| Name          | Manufacturer | Serial      | |  
|+-----+-----+-----+-----+|  
|| Access 3340   | Veritas    | VTAS9000918 | |  
|+-----+-----+-----+-----+|  
|               |           |              | |  
+-----+
```

Hardware ShowHealth Appliance Connection  
Compute Node abc-cluster\_01

Time Monitoring Ran: Wed Jan 24 2018 18:34:13 PST

Appliance to Primary Storage Shelf Connections Information					
ID	Appliance Port	Primary Storage Shelf Port	Status	State	
SAS HBA 0	Slot1 Port1	Controller B Port 0	Connected	OK	
SAS HBA 0	Slot1 Port2	Controller A Port 0	Connected	OK	
SAS HBA 1	Slot4 Port1	Controller B Port 1	Connected	OK	
SAS HBA 1	Slot4 Port2	Controller A Port 1	Connected	OK	

# Main > Settings

This appendix includes the following topics:

- [Settings > Password](#)
- [Settings > Alerts > CallHome](#)
- [Settings > Alerts > Email](#)
- [Settings > Alerts > Hardware](#)
- [Settings > Alerts > SNMP](#)
- [Security > Certificates > DeviceCertificate > Export](#)
- [Security > Certificates > DeviceCertificate > Import](#)

# Settings > Password

Settings > Password – Change the user password.

## SYNOPSIS

Password *UserName*

## DESCRIPTION

Use this command to change the user password.

The following describes password restrictions:

- At least eight characters are required.
- At least one lower case character (a-z) and one number are required.
- Dictionary words are not allowed.
- The last seven passwords cannot be reused.
- The new password cannot be similar to the current and previous passwords.

## OPTIONS

Password *UserName*

Change the password on your appliance node. *UserName* is the name of the user.

# Settings > Alerts > CallHome

Settings > Alerts > CallHome – Manage CallHome settings.

## SYNOPSIS

```
CallHome Disable
CallHome Enable
CallHome Registration Show
CallHome Show
CallHome Test
```

## DESCRIPTION

The `CallHome Registration Show` command displays your appliance registration information and your contact information. The [MyAppliance portal](#) is the unified address where you register the appliance and edit registration details.

You can use the `CallHome Enable` and `CallHome Disable` commands to instruct the appliance whether or 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.

## OPTIONS

```
CallHome Disable
    Disable the Call Home feature. Disabling Call Home also disables the Product
    Improvement Program.

CallHome Enable
    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.

CallHome Registration Show
    View registration details for the appliance and the link to the MyAppliance portal
    to register and edit contact information.

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



#### CallHome Test

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

# Settings > Alerts > Email

Settings > Alerts > Email – Use to configure email support for the appliance.

## SYNOPSIS

```
Email Hardware Add Addresses
Email Hardware Delete Addresses
Email NotificationInterval Time
Email SenderID Reset
Email SenderID Set Address
Email Show
Email Test
Email SMTP Add Server [Account] [Password]
Email SMTP Delete
Email Software Add Addresses
Email Software Delete Addresses
```

## DESCRIPTION

Use this command to add, replace, or show the email address that the appliance uses. You can use this command to define one or more emails.

## OPTIONS

```
Email Hardware Add Addresses
```

Add or append a hardware administrator's email account for Access Appliance to use.

Where *Addresses* is the user's email address. To define multiple emails, separate them with a semi-colon.

```
Email Hardware Delete Addresses
```

Delete a hardware administrator's email account for Access Appliance to use.

Where *Addresses* is the user's email address. To define multiple emails, separate them with a semi-colon.

#### Email NotificationInterval *time*

Define the time span between the alert emails that are sent to the administrator.

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

#### Email SenderID Reset

Reset the current email ID to default email ID that is used for the emails that are received from the appliance.

#### Email SenderID Set Address

Set a sender email ID that is used for the emails that are received from appliance. Here, *Address* is the email address of the sender.

#### Email Show

View your email or SMTP settings

#### Email SMTP Add Server [Account] [Password]

Add an SMTP server that NetBackup can use.

The *Server* variable is the host name of the target SMTP server that is used to send emails. The *Account* option identifies the name of the account that was used or the authentication to the SMTP server. The *Password* option is the password for authentication to the SMTP server.

#### Email SMTP Delete

Delete the SMTP server that Access Appliance uses.

#### Email SMTP Enable

Enable the SMTP server that Access Appliance uses.

#### Email Software Add Addresses

Add or append a software administrator's email account for Access Appliance to use.

Where *Addresses* is the user's email address. To define multiple emails, separate them with a semi-colon.

#### Email Software Delete Addresses

Delete a software administrator's email account for Access Appliance to use.

Where *Addresses* is the user's email address. To define multiple emails, separate them with a semi-colon.

#### 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.

# Settings > Alerts > Hardware

Settings > Alerts > Hardware – Set or view a threshold value for the disk space of any partition.

## SYNOPSIS

```
Hardware DiskspaceThreshold Set
```

```
Hardware DiskspaceThreshold Show
```

## DESCRIPTION

You can set a threshold value for a disk space using this command and receive alerts when the disk space of any partition passes this threshold value.

## OPTIONS

```
Hardware DiskspaceThreshold Set DiskThreshold
```

Set a threshold value for the disk space. The default value for disk space threshold is 80%. Here, the *DiskThreshold* variable defines a threshold value for the disk space in the range 1-99 in percent.

```
Hardware DiskspaceThreshold Show
```

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

# Settings > Alerts > SNMP

Settings > Alerts > SNMP – Add SNMP information on your appliance that enables the host to send SNMP notifications for monitoring.

## SYNOPSIS

SNMP Disable

SNMP Enable

SNMP Set *Server* [Community] [Port]

SNMP Show

SNMP ShowMIB

## DESCRIPTION

The Product Long Name uses the SNMPv2-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.

The following list is an example of the types of hardware notifications that are monitored through SNMP for the appliance:

- CPU
- Disk
- Fan
- Power Supply
- RAID
- Temperature

## OPTIONS

### SNMP Disable

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

### SNMP Enable

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

### SNMP Set *Server* [Community] [Port]

Add information about SNMP. Here, *Server* is the name of the SNMP server, [Community] is the SNMP community, and [Port] is the SNMP port.

---

**Note:** The Product Long Name supports all the SNMP servers in the market. However, the ManageEngine™ SNMP server and the HP OpenView SNMP server are tested and certified.

---

### SNMP Show

Displays the parameters that are set after you have run an `SNMP Set Server` 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 *Server*.

### SNMP ShowMIB

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

## EXAMPLES

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

```
abc123.Alerts> SNMP Set pqr222.xyz.com public 8080
Successfully set SNMP manager
```

When you run the `Settings> Alerts > SNMP ShowMIB` 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 }
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 }

vrt RAIDgroupTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Traps RAID failures"
:= { systems 9 }

vrtenclosurefanTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Traps enclosure fan failures"
:= { systems 10 }

vrtenclosurepowerTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Traps enclosure power failures"
:= { systems 11 }

vrtenclosuretemperatureTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Traps enclosure temperature failures"
```

```
:= { systems 12 }

vrtssenclosediskTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Traps enclosure disk failures"
:= { systems 13 }

vrtssadapterTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Traps adapter failures"
:= { systems 14 }

vrtssfirmwareTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Traps firmware failures"
:= { systems 15 }

vrtsspciTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Traps pci failures"
:= { systems 16 }

vrtssnetworkcardTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Traps network card failures"
:= { systems 17 }

vrtssvolumeTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Traps volume failures"
:= { systems 18 }

vrtssbbuTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Traps BBU failures"
:= { systems 19 }
```

```
vrtsconnectionTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
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

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"
:= { software 6 }

vrtssuccessTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Software rollback success trap"
:= { software 7 }

vrtssuccessFailedTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "Software rollback failed trap"
```

```
 ::= { software 8 }

vrtscclusterStateTrap 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 }

vrtsassettTagTrap NOTIFICATION-TYPE
OBJECTS { vrtssystemName }
STATUS current
DESCRIPTION "AssetTag"
 ::= { software 12 }

END
```

# Security > Certificates > DeviceCertificate > Export

Security > Certificates > DeviceCertificate > Export – Export the device certificate.

## SYNOPSIS

```
Export [EnterPasswd] [PathValue]
```

## DESCRIPTION

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

---

**Note:** The device certificate is removed during a reimage process. The certificate is unique for each appliance node and is included as part of the original factory image.

The device certificate is not included on the USB drive that is used to reimage the appliance node.

---

## OPTIONS

```
Export [EnterPasswd] [PathValue]
```

Use this command to export the device certificate. The `EnterPasswd` 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. In addition, you must specify a path that defines where you want to place the exported credentials.

# Security > Certificates > DeviceCertificate > Import

Security > Certificates > DeviceCertificate > Import – Import the device certificate.

## SYNOPSIS

```
Import [EnterPasswd] [PathValue]
```

## DESCRIPTION

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

## OPTIONS

```
Import [EnterPasswd] [PathValue]
```

Use this command to import the device certificate. The `EnterPasswd` 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. In addition, you must specify a path that defines where you want to place the imported credentials.

## Main > Support

This appendix includes the following topics:

- [Support > DataCollect](#)
- [Support > Logs](#)
- [Support > RAID](#)
- [Support > Shutdown](#)
- [Support > Storage Reset](#)
- [Support > Test](#)
- [Support > FactoryReset](#)
- [Support > InfraServices](#)
- [Support > IPMI](#)
- [Support > Maintenance](#)
- [Support > Reboot](#)
- [Support > Services](#)



# Support > DataCollect

Support > DataCollect – Gather device logs.

## SYNOPSIS

DataCollect

## DESCRIPTION

Use this command to gather appliance device logs.

## OPTIONS

DataCollect

Use to gather appliance device logs.

## EXAMPLES

The following procedure is executed after you run the `DataCollect` command.

```
abc123.Support> DataCollect
Gathering release information
Gathering disk performance logs
Gathering command output logs
Gathering dmidecode logs
Gathering ipmitool sel list logs
Gathering ipmitool sel writeraw logs
Gathering fwtermlog logs
Gathering AdpEventLog logs
Gathering smartctl logs
Gathering ipmiutil command output
Gathering BMC Debug logs
Gathering Seagate storage array logs
Gathering cpu information
Gathering memory information
Gathering os logs
Gathering dfinfo logs
Gathering vxprint logs
Gathering patch logs
Gathering autosupport logs
Gathering sysinfo logs
Gathering sdr logs
```

```
Gathering adpallinfo logs
Gathering encinfo logs
Gathering cfgdsply logs
Gathering ldpdinfo logs
Gathering pdlist logs
Gathering fru logs
Gathering adpbucmd logs
Gathering sas3ircu logs
Gathering sas3ircu display logs
Gathering adpalilog logs
Gathering Test Hardware logs
Gathering Access product logs
```

```
All logs have been collected in /tmp/DataCollect.zip
Log file can be collected from the appliance shared folder - \\abc123example.
Share can be opened using Main->Support->Logs->Share Open
The Log files DataCollect-xxxxXXXX-20180122233305.tar.gz collected from the a
The data transmission may complete in several minutes or longer due to file s
=====End of DataCollect=====
```

# Support > Logs

Support > Logs – Manage logging setting, view and share logs files.

## SYNOPSIS

Browse

Share

VxLogView Minutes *minutes\_ago*

VxLogView Module

## DESCRIPTION

Use this command to do the following functions:

- Browse the appliance log directories and files.  
You can use the `Browse` command to view the log directories and log files that are configured in your appliance node. When you run the `Browse` command the command prompt changes to `LOGROOT/>`. From the `LOGROOT/` command prompt you can run the following commands to list, view, and change directories:
  - `ls` - List the directories and files
  - `tree` - Provides a tree-view of the directories and files.
  - `cd DIR` - Use to change the directory, where *DIR* is the directory name. For example, you can use `cd .`, `cd ..`, and `cd -`.
  - `less FILE` - Provides a read-only view of a file. You must enter the letter `q` or `quit` to exit this view.
  - `exit|quit` - Enables you to exit the log shell.
  - `help|?` - Use either of these two commands to display help.

From the `LOGROOT/>` command prompt, you can use the `ls` command to see the following log directories on the host:

- `APPLIANCE`
- `OS`
- `COREDUMP`
- `ACCESS`

To see the log files from within a log directory, you must change directories to the log directory that contains the log files that you want to view. After you change

directories, the same commands that were available under the `LOGROOT/` view are available for each of the log directories.

For example, to see the operating system (OS) log files, you must first enter `cd OS` at the `LOGROOT/>` command prompt. The command prompt changes to `LOGROOT/OS>/.`  Then you can enter `ls` to see the file names. Finally, you can use the `less filename` command to view a read-only version of the log file.

- Export or remove CIFS and NFS shares for the logs.  
Use the `Share Open` command to export the CIFS and the NFS shares for the logs. The `Share Close` command removes the CIFS and the NFS shares for the logs.
- Display debug information from the VxLog files.  
Use the `VxLogView` command to display log files for specific job or by a set duration of time.

## OPTIONS

### Browse

Use the show the appliance logs on the current node.

### Share

Use to extract the CIFS and the NFS shares for the logs.

For CIFS, you must map the share using the appliance "admin" user's credentials.

### VxLogView Minutes *minutes\_ago*

Display debug information from the log files using time (in minutes) as the criteria by which the information is parsed.

Where *minutes\_ago* is the amount of time, in minutes, used to determine how much of the past debug information to display.

### VxLogView Module

Use the command to display debug information from the log files by designating a specific logging module as the criteria by which the information is parsed.

Type the number that corresponds to the appliance system component that contains the module that you want to view the VxLog of.

# Support > RAID

`Support > RAID` – Used to clear data on the storage disks and to reset the disk RAID configuration.

## SYNOPSIS

`RAID Clear`

## DESCRIPTION

The RAID commands is available on a 3340 appliance only when it is newly out-of-box or has been re-imaged or factory reset.

Use the `RAID Clear` command to remove external RAID storage that includes only the LUNs and volume groups.

## OPTIONS

`RAID Clear`

This command removes all data on the storage and resets the disk RAID configuration. It also reassigns all the host-spare disks. The RAID volume groups are completely cleared out and then re-created. The complete operation results in an initialization overhead.

# Support > Shutdown

Support > Shutdown – Turn off the system

## SYNOPSIS

Shutdown

## DESCRIPTION

Use the command to turn off the system and power off the appliance node.

## OPTIONS

Shutdown

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

# Support > Storage Reset

Support > Storage Reset – Reset the appliance storage.

## SYNOPSIS

Storage Reset

## DESCRIPTION

Use the `Storage Reset` command to delete the data on the attached storage that is shared among the appliance nodes.

This command is available when the appliance node is in a factory install state. An appliance node is in a factory install state when it has not been configured.

# Support > Test

Support > Test – Test the current status of the various appliance components.

## SYNOPSIS

Test Hardware

Test Software

## 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 `Test` command to verify the current status of the various appliance components.

## OPTIONS

Test Hardware

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

Test Software

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

## EXAMPLES

The following is an example of information that is displayed when you run the `Main > Support > Test Software` command.

```
abc-cluster_01.Support> Test Software
```

```
Starting self-test at Thu Jan 25 00:16:12 2018
```

```
Running validation tests on the host 'abc-cluster_01'.
```

Testing the database service ...	[PASS]
Testing the message queue service ...	[PASS]
Testing the required RPM package installation ...	[PASS]
Testing the serial number ...	[PASS]
Testing the SSH server and settings ...	[PASS]
Testing the web server service ...	[PASS]



Testing the LUNs ...	[PASS]
Testing the S3 service ...	[PASS]
Testing the Access services ...	[PASS]

Validation tests are complete.

Appliance self-test result: PASS

# Support > FactoryReset

Support > FactoryReset – Reset the node to factory default settings.

## SYNOPSIS

```
FactoryReset
```

```
FctoryReset ResetAll
```

## DESCRIPTION

This command exists under the `Main_Menu > Support` view. You can use this command to reset the current node to the factory default settings. If you have changed the initial password to something else and you run this command, your password is reset to the initial default value.

---

**Note:** This command only applies to the current single node. If you want to reset the entire cluster, you must reset each node in the cluster one at a time. For more information, see the *Veritas Access™ Appliance Getting Started Guide*.

---

## OPTIONS

```
FactoryReset
```

Use this command to reset the node to the factory default settings.

```
FactoryReset ResetAll
```

Use this command to reset the node factory installed image in non-interactive mode.

## EXAMPLES

The following is an example output when you run the `FactoryReset` command.

**To begin a factory reset from the appliance node shell menu**

- 1** Open an SSH session and log on to the appliance node as an administrator.

**2 Enter `Main_Menu > Support > FactoryReset`. This command shows the following messages and requires you to answer the following questions before the factory reset begins.**

A factory reset returns a single appliance node to a clean, factory-installed image. The following components are reset to a factory state:

- Appliance Operating System
- Appliance Software
- Access Software
- (Optional) Storage configuration and data
- (Optional) Networking configuration

There are two supported factory reset scenarios:

**\*Single node reset\***

Use this mode if you want to reset just one node and then add it back into the cluster. All of the data on the attached storage is preserved.

Requirements:

- Before you reset the node you must use the Access shell menu to remove the node from the cluster and then physically disconnect the Ethernet cables connecting the node to the cluster.
- Once the factory reset is complete, you may need to upgrade the appliance software before you add the node back into the cluster. This is to make the two nodes have the same appliance software version.

**\*Full cluster reset\***

Use this mode if you want to reset the entire cluster and delete all data on the attached storage.

Requirements:

- You must reset each node in the cluster one by one.
- Do not select to reset the storage when you factory reset the first node.
- Ensure that you select to reset the storage when you reset the last node.

Select networking configuration reset [Optional]

- Removes the IP and routing configuration.
- Removes the DNS configuration.

Note: If you reset the network configuration, you may lose the ability to remotely access the appliance over IP. Once the factory reset is complete, you can connect to the appliance either directly or remotely using the IPMI interface.

>> Do you want to reset the network configuration as part of the factory reset? [yes, no] (yes) no

Select storage configuration and backup data reset [Optional]

- Removes all data and backup images from the attached storage.
- Resets the storage partitions.

- [WARNING] Do not reset the storage unless you plan to factory reset the entire cluster. If you are resetting the entire cluster:

Select 'no' when you are resetting the first node.

Select 'yes' when you are resetting the last node.

>> Do you want to reset the storage configuration and delete the data on the attached storage as part of the factory reset? (Select 'no' if you are resetting just a single node and want to preserve the cluster.) [yes, no] (no) no

>> A system restart is required to complete the factory reset.  
Do you want to automatically restart the node at the end of the factory reset process? [yes, no] (no) yes

- 3 After you respond to these questions, the following summary information displays:

```
-----
Review factory reset selections
-----

Reset OS and software configuration:           [Required]
Reset networking configuration:               [Yes]
Reset storage configuration (remove data):     [No]
Automatic restart:                           [Yes]


Factory reset makes the following version changes to the node:
+-----+
| Current Version | Reverted Version |
+-----+-----+
| Access 7.3.1    | Access 7.3.1     |
| Appliance 7.3.1 | Appliance 7.3.1  |
+-----+-----+
```

- 4 The following warning appears. If you want to begin the factory reset operation, enter **yes**.

```
>> WARNING: The node is ready for factory reset. This process
cannot be reversed! Do you want to proceed? [yes, no] (no) yes
```

The following summary messages appear as the factory reset continues:

```
-[Info] Running factory reset. This process can take up to 20 minutes...
-[Info] The appliance is restarting...
```

# Support > InfraServices

Support > InfraServices – Display and control the infrastructure services.

## SYNOPSIS

```
Show All
Start All
Stop All
Show Database
Start Database
Stop Database
Show MessageQueue
Start MessageQueue
Stop MessageQueue
Show Webserver
Start Webserver
Stop Webserver
```

## DESCRIPTION

These commands exist under the `Main > Support > InfraServices` view. 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.

---

## OPTIONS

```
Show All
```

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

Start All

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

Stop All

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

Show Database

Show the status of the database.

Start Database

Start the database.

Stop Database

Stop the database.

Show MessageQueue

Show the status of the message queue service.

Start MessageQueue

Start the message queue service.

Stop MessageQueue

Stop the message queue service.

Show Webserver

Show the status of the web server service.

Start Webserver

Start the web server service.

Stop Webserver

Stop the web server service.



# Support > IPMI

Support > IPMI – Use these commands to manage the IPMI configuration.

## SYNOPSIS

```
IPMI Network Configure<IPAddress> <Netmask> <GatewayIPAddress>
```

```
IPMI Network Show
```

```
IPMI Reset
```

```
IPMI User Add <User_name>
```

```
IPMI User Delete <User_name>
```

```
IPMI User List
```

## 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 sub-system
- View the current IPMI settings
- Reset the IPMI
- Add users
- Delete users
- List users

## OPTIONS

IPMI Network Configure

This command is used to configure the IPMI sub-system using the IPMI port.

IPMI Network Show

This command is used to view the current IPMI port information.

IPMI Reset

This command is used to reset the IPMI. You must reset IPMI only if the IPMI interface stops responding or hangs.

IPMI User Add

This command is used to add new users to access the IPMI sub-system.

#### IPMI User Delete

This command is used to delete existing users that can access the IPMI sub-system.

#### IPMI User List

This command is used to view the list of users who can access the IPMI sub-system.

The following procedure is executed after you run the `IPMI Network Configure` command.

```
Support> IPMI Network Configure 10.182.8.70 255.255.240.0 10.182.1.1
Network is configured successfully.
```

The following information is displayed when you run the `IPMI Network Show` command.

```
Support> IPMI Network Show
IP Address Source      : STATIC
IP Address              : 10.182.8.70
Subnet Mask             : 255.255.240.0
Gateway IP Address     : 10.182.1.1
```

The following information is displayed when you run the `IPMI Reset` command.

```
Resetting the IPMI disconnects all current IPMI users.
Are you sure you want to reset the IPMI? [yes, no]: yes
```

In case other users are not affected, type **yes** and press **Enter** to continue. The following message is displayed:

```
-[Info] The IPMI is being reset...
-[Info] Wait for two minutes before attempting to reconnect to the
IPMI console. If you cannot access the IPMI console, the appliance
must be shut down and then restarted. First schedule a convenient time
for the shutdown, alert all users and shut down the appliance.
Then disconnect all appliance power cables for 15 seconds, reconnect
them and turn on power to the appliance.
```

Type **no** in case other users are affected. Alert all users and schedule a convenient time for reset. Run the `IPMI Reset` command again at the scheduled time.

The following procedure is executed after you run the `IPMI User Add <User_name>` command.

```
Support> IPMI User Add abc
New password:
```

```
Confirm password:  
Operation successful
```

The following procedure is executed after you run the `IPMI User Delete <User_name>` command.

```
Support> IPMI User Delete abc  
User abc has been deleted successfully.
```

The following information is displayed after you run the `IPMI User List` command.

```
Support > IPMI User List  
  
User name      : Anonymous User  
User privilege : ADMIN  
  
User name      : sysadmin  
User privilege : ADMIN  
  
User name      : root  
User privilege : ADMIN
```

# Support > Maintenance

Support > Maintenance – Enables the user to open an interactive shell menu.

## SYNOPSIS

Maintenance

## DESCRIPTION

Your appliance node is pre-configured with a **Maintenance** user account. When you log into this account, you open an interactive shell menu that you can use to troubleshoot or manage underlying operating system tasks.

The default password is, P@ssw0rd. Veritas recommends that you change this password at your earliest convenience. Use the following command to reset the password.

```
Main > Settings > Password UserName
```

In this case, the user name is `maintenance`.

If you require customer support to resolve an issue, you may be required to provide this password to your support representative. In addition, if you change this password and then run the `FactoryReset` command, this password is reset to the initial default value.

## OPTIONS

Maintenance

Used to enter an interactive shell menu that you can use to troubleshoot or manage underlying operating system tasks.

## EXAMPLES

To enter your Maintenance account, run the following command, and provide the password when you receive a prompt.

```
NBApl.Support> Maintenance
<!--Maintenance Mode--!>
maintenance's password:
```

# Support > Reboot

Support > Reboot – Reboot the system

## SYNOPSIS

```
Reboot [Force]
```

## DESCRIPTION

Use this command to reboot the current system on the appliance node. You cannot use this command to restart another system remotely.

## OPTIONS

```
Reboot [Force]
```

Use this command to restart the system.

The `Force` parameter forces the system to restart even if services are not able to be stopped. Use this parameter if a previous attempt failed.

# Support > Services

Support > Services – Show and control the Access services.

## SYNOPSIS

Show

Start

Stop

## DESCRIPTION

These commands exist under the `Main > Support > Services` view. Enter the `Support > Services` view, and then you can use these commands to control the Access services on the appliance node, and view the service status.

## OPTIONS

Show

Show the Access services on all the nodes in the cluster.

Start

Start the Access services on the appliance node.

Stop

Stop the Access services on the appliance node.