Veritas Flex Appliance Getting Started and Administration Guide

Release 3.x

VERITAS™

Veritas Flex Appliance Getting Started and Administration Guide

Last updated: 2023-10-25

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

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

Documentation feedback

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

APPL.docs@veritas.com

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

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

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

Contents

Chapter 1

Product overview

This chapter includes the following topics:

Introduction to Veritas Flex Appliance

Veritas Flex Appliance is a customizable data management solution that lets you consolidate multiple applications on a single hardware platform. With Flex Appliance, you can run concurrent instances of the following applications:

- NetBackup primary server
  You can also configure a BMR primary server with this application. However, the BMR boot server cannot be configured on the appliance.
- NetBackup media server with the following storage options:
  - Media Server Deduplication Pool (MSDP)
    You can also configure MSDP cloud storage with this application. Refer to the *NetBackup Deduplication Guide* after the instance is created.
  - AdvancedDisk
- NetBackup WORM storage

The NetBackup applications must follow the same compatibility requirements between NetBackup versions as any other NetBackup environment. See the *NetBackup Release Notes* for specifics.

For a full list of supported applications and versions for each Flex Appliance release, see the following article on the Veritas Support website:

Flex Appliance supported applications and usage information

Flex Appliance is currently available in English only.

This release is compatible with the following hardware:

- The Veritas 5360 Appliance, supporting all PCIe-based I/O configurations (supported on Flex Appliance version 3.2 and later).
- The Veritas 5350 Appliance, supporting all PCIe-based I/O configurations.
- The Veritas 5340 Appliance, supporting PCIe-based I/O configurations A, G, and H.
- An additional 53xx compute node for high availability (HA).

  Note: Both nodes must have the same PCIe-based I/O configuration.

- The Veritas 5260 Appliance, supporting all PCIe-based I/O configurations (supported on Flex Appliance version 3.2 and later).
- The Veritas 5250 Appliance, supporting all PCIe-based I/O configurations.
- The Veritas 5150 Appliance, supporting all PCIe-based I/O configurations.

See the *Product Description* guides for additional details about the appliance hardware and the available I/O configurations.

Flex Appliance terminology

Table 1-1 defines some of the common terminology used in Flex Appliance:

Table 1-1 Common terms

Term	Definition
Application	A Veritas software program that can be installed and used on a Flex appliance. For example, NetBackup.
Instance	A single deployment of an application that was historically a standalone server. For example, a NetBackup primary server or a NetBackup media server.
Application add-on	A piece of software that can be installed on an application to modify or add to its capabilities. For example, a NetBackup Emergency Engineering Binary (EEB).

Table 1-1 Common terms *(continued)*

Term	Definition
Repository	The location on the appliance that stores your applications, application add-ons, and Flex Appliance updates. You must add these files to the repository before you can use them.
Tenant	A separate space that you can create for a specific group of users and for a specific use. For example, you may create separate tenants for the different teams within your company.

About the Flex Appliance documentation

The following documents contain information about the Flex Appliance and application software:

- The *Flex Appliance Getting Started and Administration Guide*
  Refer to this guide to configure and manage the Flex Appliance software, as well as for general information about creating and managing application instances.
- The *NetBackup Application Guides*
  Refer to these guides for more specific information about the NetBackup applications, including detailed instructions on how to create application instances of each supported version.

The following documents contain information about the appliance hardware:

- The *Veritas 5360 Appliance Hardware Installation Guide*
- The *Veritas 5360 Appliance Product Description*
- The *Veritas 5350 Appliance Hardware Installation Guide*
- The *Veritas 5350 Appliance Product Description*
- The *Veritas 5340 Appliance Hardware Installation Guide*
- The *Veritas 5340 Appliance Product Description*
- The *Veritas 5260 Appliance Hardware Installation Guide*
- The *Veritas 5260 Appliance Product Description*
- The *Veritas 5250 Appliance Hardware Installation Guide*
- The *Veritas 5250 Appliance Product Description*

- The *Veritas 5150 Appliance Hardware Installation Guide*
- The *Veritas 5150 Appliance Product Description*
- The *Veritas Appliance Safety and Maintenance Guide*

Flex Appliance also uses Veritas AutoSupport to monitor the appliance. You can find additional information about AutoSupport in the *Veritas Appliance AutoSupport Reference Guide*.

You can find the latest documentation on the Documentation page of the Veritas Support website. Navigate to the **Documentation** tab, then select **Flex Appliance OS** on the left-hand side.

API documentation is also available from the **Knowledge Base** page on Veritas SORT.

Chapter 2

Release notes

This chapter includes the following topics:

Flex Appliance 3.0 new features, enhancements, and changes

The following list describes the new features, enhancements, and changes in the Flex Appliance 3.0 release:

- You can now remove applications and application add-ons from the repository. See “Removing files from the repository” on page 71.
- This release introduces the Network Access Control feature. You can use Network Access Control to control which IP addresses are allowed to access the appliance. Use HTTPS access control to control which IP addresses can

access the Flex Appliance Console or the APIs through HTTPS. Use SSH access control to control which IP addresses can access the Flex Appliance Shell through SSH.
See “Using network access control” on page 98.
You can customize the SSH port with the NetworkAccessControl API. For more information, see the API documentation on Veritas SORT.

- IPv6 is now supported on the appliance. It is also supported on NetBackup primary and media server application instances version 9.1.0.1 and later, and NetBackup WORM storage server versions 15.0.2 and later. You can edit your existing network interfaces to add IPv6 addresses, but the interfaces must not be in use by any instances when you make the change. See “Configuring or editing a network interface” on page 47.
  Note that IPv6 is not supported on the Appliance Management Console.
- The Flex Appliance Console now supports single sign-on (SSO). You must have a SAML 2.0 compliant identity provider configured in your environment.
  See “Managing single sign-on (SSO)” on page 58.
- Local Flex Appliance Console user accounts are now protected with an account lock if the appliance detects 3 failed sign-in attempts within 15 minutes.
  See “Unlocking a local user account in the Flex Appliance Console” on page 65.
- You can now edit network bonds to change the bonded interfaces.
  See “Editing a network bond” on page 46.
- The diagnostic logs now mask user information such as hostnames, IP addresses, usernames, etc. If needed, you can disable the masking option from the Flex Appliance Shell.
  See “Gathering logs” on page 129.
- On the Veritas 5150 and 5250 appliances, upgrades to this release remove all unused applications and add-ons from the repository.
- Call Home is now enabled by default unless you choose to disable it during the `setup configure-console` step of initial configuration. You can also disable it from the **Settings > Call Home** page.
  See “Configuring Call Home” on page 101.
- The following widgets have been added to the **Home** page on the Flex Appliance Console:
  - Call Home
    This widget shows whether Call Home is enabled or disabled and the connection status.
  - Security meter

This widget shows the security status of the appliance and offers recommendations.

- Performance
  This widget shows the CPU, memory, and network throughput metrics for the appliance.

- The bond modes balance-alb and balance-tlb are no longer supported for applications.
- The metrics API no longer collects metrics about application instances except for the storage utilization. For more information on the metrics API, see the API documentation on Veritas SORT.
- The appliance alerts have been enhanced to add visibility into the status of the appliance. If an application instance or an appliance service encounters an error, the monitoring service sends an SNMP alert and an event to the Veritas NetInsights Console. The monitoring service also sends an email alert if an application instance or one of the following services goes offline or fails over to another node: management server, the authorization service, the registry service, or the Flex Appliance Console.

Flex Appliance 3.1 new features, enhancements, and changes

The following list describes the new features, enhancements, and changes in the Flex Appliance 3.1 release:

- You can now run an update precheck to make sure that the appliance is ready for update. The precheck is available for updates from version 3.1 to a future release.
  See “Updating Flex Appliance” on page 87.
- The Data Collect log package advanced option now includes the logs in the `/var/log/appliance` directory.
- When you add a node to an appliance, both nodes must now be on the same update version. They can have different security patches installed.
- A factory reset now resets the appliance to the same version that is currently running. You no longer need to reinstall updates after the reset. However, you do need to reinstall security patches.

Flex Appliance 3.2 new features, enhancements, and changes

The following list describes the new features, enhancements, and changes in the Flex Appliance 3.2 release:

- This release introduces support of the Veritas 5360 Appliance and the Veritas 5260 Appliance.
  The Veritas 5360 Appliance is a hardware and software storage system that scales up to a total of 1,920TiB (2,111TB) of usable backup capacity. It consists of one or two 2U 5360 Appliance compute nodes and one required externally attached 5U84 Primary Storage Shelf, which is used for data storage purposes. By itself, the 5360 Appliance compute node does not provide internal disk space for data storage. You can add up to three optional 5U84 Expansion Storage Shelves if you require additional data storage space. For complete details, see the *Veritas 5360 Appliance Product Description Guide*.
  The Veritas 5260 Appliance is a hardware and software storage system that can scale to 429.4 TiB of available backup capacity. It consists of a Veritas 5260 Appliance and up to six optional Veritas 2U12 65.5TiB/72TB storage shelves. By itself, the 2U Veritas 5260 Appliance offers internal storage from 9.1 TiB to 36.4 TiB, depending on the appliance configuration purchased. For complete details, see the *Veritas 5260 Appliance Product Description Guide*.
- The term “upgrade” has been discontinued for Flex Appliance. The packages and procedures that were previously referred to as “upgrades” now use the term “updates.” The term “upgrade” still applies for application instances.
  As part of this change, you can now install all software updates from the Flex Appliance Console. The `system upgrade` command has been removed.
  See “Updating Flex Appliance” on page 87.
- You can now commit all software updates from the Flex Appliance Console. To commit an update, click **Commit** on the **Appliance updates** tab of the **Repository** page. The `system upgrade-commit` command has been removed.
- You can now schedule automatic updates for Flex Appliance from System Health Insights. See the *System Health Insights User Guide* for details.
- You can now change the port to use for SSH access to the Flex Appliance Shell.
  See “Changing the SSH port” on page 99.
- This release adds a new `show hardware-data storage-shelf` command that shows detailed information about the 53xx storage shelf components.
  See “Viewing storage shelf information on a Veritas 53xx Appliance” on page 106.
- You can now use the `support clear-hardware-status` command to clear the hardware monitoring status. You may need to clear the status if you replace a

hardware component or experience any issues with the hardware monitoring data.

See “Clearing the hardware status” on page 110.

- If you have configured an isolated recovery environment (IRE) on a WORM storage server instance, you can now view the live firewall settings from the Flex Appliance Console. To view the settings, navigate to the **Application instances** section of the **System topology** page and click the instance name, then **click Live firewall settings**.

Flex Appliance 3.3 new features, enhancements, and changes

The Flex Appliance 3.3 release includes a variety of fixes. It does not include any new features.

See “Flex Appliance 3.3 release content” on page 23.

Supported upgrade and update paths to this release

The following describes the supported upgrade and update paths to Flex Appliance version 3.x:

For upgrades to 3.0:

- Direct upgrade path
  You can upgrade directly from version 2.1 or 2.1.x to version 3.0.
- Multi-step upgrade path
  Any appliance running an earlier version must first be upgraded to version 2.1. If you have a multi-node appliance, upgrade both nodes to version 2.1 before you upgrade to version 3.0.

For updates to 3.1:

- Direct update path
  You can update directly from version 3.0 to version 3.1.
- Multi-step update path
  Any appliance running an earlier version must first be upgraded to version 3.0. If you have a multi-node appliance, upgrade both nodes to version 3.0 before you update to version 3.1.

For upgrades or updates to 3.2 or 3.3:

- Direct upgrade or update path
  You can upgrade or update directly from versions 2.1, 2.1.x, or 3.x to version 3.2 or 3.3.
- Multi-step upgrade path
  Any appliance running an earlier version must first be upgraded to version 2.1. If you have a multi-node appliance, upgrade both nodes to version 2.1 before you upgrade to version 3.2 or 3.3.

Operational notes

This topic explains important aspects of Flex Appliance 3.x operations that may not be documented elsewhere in the documentation.

The following list contains the notes and the known issues that apply for the Flex Appliance 3.x software:

- Once you upgrade to version 3.x, SAN client (Fibre Transport Media Server) backups no longer work on NetBackup application instances earlier than version 10.1. To use SAN client on earlier versions, you must install an EEB on versions 10.0.0.1 and 9.1.0.1. Versions other than 10.0.0.1 and 9.1.0.1 do not have an EEB and must be upgraded before you can install the EEB.
  You can find the EEBs at the following locations:
  - Version 10.0.0.1
  - Version 9.1.0.1

  Veritas recommends that you install the EEB before you upgrade the appliance to version 3.x so that scheduled backups are not interrupted.
- Once you upgrade to version 3.x, universal shares no longer work on NetBackup application instances earlier than version 10.1.1. To use universal shares on earlier versions, you must install an EEB on versions 10.1, 10.0.0.1, and 9.1.0.1. Versions other than 10.1, 10.0.0.1, and 9.1.0.1 do not have an EEB and must be upgraded before you can install the EEB.
  You can find the EEBs at the following locations:
  - Version 10.1
  - Version 10.0.0.1
  - Version 9.1.0.1

  Veritas recommends that you install the EEB before you upgrade the appliance to version 3.x so that scheduled backups are not interrupted.
- NetBackup 10.3 is not supported on Flex Appliance 3.x.

- When you access the Flex Appliance Shell through the Veritas Remote Management Interface, do not enter **alt+PrtScn** while a command is running. If you do, the command fails, and it still may not work when you try to rerun it.
- When you create an instance, if you change the unit for a volume in the **Storage** section but do not enter a new size, the unit does not update. To work around this issue, you must also enter a new size. Once the unit has updated, you can change the size back to the previous value if needed.
- For this release, the audit log may include incorrect username or group name values for user identifiers (for example, UID and GUID). The log shows the values for the user IDs or group IDs on the appliance instead of the user IDs or group IDs on the application instance.
- If you generate a Data Collect log package and stay on the **Activity Monitor** page for more than 15 minutes, you may see a new task appear on the monitor page. The new task stops immediately with the following message:
  “A Data Collect operation is already in progress. Retry after the task is completed.”
  This task displays in error and can be ignored. It has no impact on the generation of the log package.
- The Linux lspci utility shows an incorrect model number for the SAS storage controller. You can see the correct model number with the hardware-health commands in the Flex Appliance Shell.
- If you make configuration changes on the appliance while an update is in progress, the update may fail. To avoid this issue, do not make configuration changes or run the `system restart` command until the update is fully complete. If you were not aware of this issue and have encountered it, rerun the update to resolve it.
- For this release, the **Alt** + **s** shortcut in the Flex Appliance Shell is not enabled.
- When you add a node to the appliance either during initial configuration or after, the `system self-test` command fails on the new node if you run it before you run `setup add-node`. The following error appears:
  "Hostagent must not be active on unconfigured appliance"
  If you see this error in this scenario, it can be ignored. Run `setup add-node` to finish adding the node and then run `system self-test` again.
- For this release, the **Performance** graphs on the Flex Appliance Console **Home** page show data only in the UTC time zone.
- On a multi-node appliance, an issue can occur if you remove a node while that node is powered off. If the node comes back online before you have restarted the appliance, the removed node is added back to the appliance. If you

experience this issue, remove the node again and then immediately restart the appliance.

- When you run the following commands, messages that include the text `avc: denied` and `comm='iptables'` or `comm='ip6tables'` may appear in the logs at `/var/log/audit/audit.log`:
  - `setup configure-console`
  - `system restart`
  - `system appliance-recover`
  - `systemctl restart system-hostnamed`
  - `hostnamectl`

  The messages look similar to the following:

  ```
  node=localhost.localdomain type=AVC
  msg=audit(1668166429.323:16048): avc: denied { ioctl } for
  pid=612229 comm="iptables"
  ```

  These messages can be ignored.
- Alerts are not currently sent for the metrics that can be set with the `set alerts hardware-threshold` command.
- The `support data-collect` command may show the following error:
  "*** Error in `qaucli': double free or corruption"
  This error can be safely disregarded. The command still generates a Data Collect package.
- During a firmware update, an issue can occur with the storage shelf controller that causes an update failure message to appear. If you see a failure message, it may have appeared in error, and the update may still have worked. Run the following command to confirm the firmware version:

  ```
  show hardware-health primaryshelf component=controller
  ```
- For this release, while an update is in progress, do not perform any other operations in the Flex Appliance Shell or the Flex Appliance Console.
- When you install application add-ons on an instance, the Flex Appliance Console lets you select different versions of the same OST plug-in. However, this configuration is not supported, and if you select more than one version of the same plug-in, the **Install add-ons** page shows duplicate entries. Only install one version of each OST plug-in on an instance. If you need to change the version of an OST plug-in that is already installed, first uninstall it, and then install the new version.

- If the host0 or host1 port is not connected to the appliance node during initial configuration, the following error message appears that does not provide complete information:
  “Network card for *<interface name>* is missing. Make sure that all network interfaces are connected to the appliance.”
  If you encounter this message, verify that all ports are connected according to the initial configuration guidelines. See “Initial configuration guidelines and checklist” on page 24. Then restart the node to continue the configuration.
- When you create a new application instance, the **Application instances** section of the **System topology** page may show the instance status as **Partially Deleted** while the creation is in progress. The **Partially Deleted** status displays in error and can be safely ignored. You can track the instance creation progress from the Activity Monitor, and the instance status changes to **Online** when the instance creation has completed successfully.
- If you configure or change the configuration of a Call Home proxy server, the event does not display correctly in System Health Insights. The **Severity** column on the **Events** page shows as **Unknown**. You can ignore this status.
  This issue is fixed in version 3.3.
- A known issue can occur when you try to delete an application instance on a multi-node appliance. The following error message displays in the Activity Monitor:
  "Failed to delete instance. Check /var/log/nodeworker/worker.log and VCS logs for more details."
  This issue is fixed in version 3.2. To avoid this issue on earlier releases, relocate the instance to the other node before you delete it.
  If you were not aware of this issue and encounter it, contact Veritas Technical Support for assistance and ask your representative to reference article 100054665.
- Performing a power cycle from the Veritas Remote Management Interface can cause system downtime.
  This issue is fixed in version 3.2. If you need to restart the appliance on earlier releases, run the `system restart` command from the Flex Appliance Shell.
- For versions 3.0 and 3.1, if you add a node to the appliance and do not use DNS, you must perform the following steps after you add the hostname resolution information for the new node to the appliance Hosts file:
  - Log in to the Flex Appliance Shell from the preexisting node that was already part of the appliance.
  - Run the following command:
    `system ha-service restart service=infra_svc node=<node hostname>`

Where <*node hostname*> is the hostname of the node that you are logged in to.

Perform these steps after you run the system add-host command and before you run the setup add-node command. You do not need to perform these steps on version 3.2 and later.

- If you do not use DNS and you configure email alerts or configure Call Home with a proxy server, the alert tests fail, and alerts are not sent.

  This issue is fixed in version 3.2. To resolve this issue on earlier releases, perform the following steps after you configure the alerts:

  - Log in to the Flex Appliance Shell and run the following command:

    ```
    system add-host
    ```

  - Enter the required information for the SMTP server or the Call Home proxy server.

  - Run the following commands:

    ```
    system os-service restart service=autosupport
    system ha-server restart service=infra_svc node=<node hostname>
    ```

    Note: If you have a multi-node appliance, you must run these two commands on both nodes.

- If you configure a Fibre Channel port in target mode and then change it to initiator mode, a message should appear that advises you to rescan the ports. However, the message does not appear in versions 3.0 and 3.1. If you change a port from target mode to initiator mode, make sure that you rescan the ports after the change to discover all devices.

- If you try to remove a node that has crashed or is no longer working, the removal may fail with the following message:

  "Unable to remove node because an appliance update is in progress or pending. Complete the update, then commit or roll back. If any of these operations did not complete successfully, you must resolve the errors before you can remove a node."

  This issue is fixed in version 3.2. If you encounter this scenario on an earlier release, retry the remove node operation.

- If you have a multi-node appliance and update one of the nodes but have not updated the other node, the following message may appear on the Flex Appliance Console:

  "V-492-100-505: Internal server error occurred"

This issue is resolved in version 3.2. On earlier versions, this message can be ignored. To remove the message, update the other node.

Flex Appliance 3.0 release content

The following list contains the known issues that were fixed and that are now included in this release of Flex Appliance:

- When you upgraded and committed to the upgraded version, the Flex Appliance Console showed an error displaying the node information for a couple minutes after the commit. The error resolved on its own once all services were online.
- When you created an instance or configured a proxy server for Call Home, an issue could occur with the file uploads if you uploaded a file with incorrect data. If you edited the file to correct the issue and then attempted to upload it again, the upload still failed.
- If you upgraded the appliance and then rolled back, an issue could occur that caused the Flex Appliance Console to be unable to load.
- On a multi-node appliance, if a node was restarted while the other node was off, the Flex Appliance Console failed to load.
- When you created an instance, if you entered the IP address before you selected a network interface, the **IP address** field displayed the following error message: “IP address does not belong to the selected network’s subnet.”
  This message still displayed after you selected the network interface that corresponded to the IP address.
- If you created a bond with a bond name that was all numbers, you could no longer create any additional bonds on the appliance.

Flex Appliance 3.1 release content

This release includes fixes for customer-reported defects and security vulnerabilities. See the *Release Notes* PDF on the Downloads page for more information.

Flex Appliance 3.2 release content

The following list contains the known issues that were fixed and that are included in the Flex Appliance 3.2 release:

- A known issue could occur when you tried to delete an application instance on a multi-node appliance. The following error message displayed in the Activity Monitor:

"Failed to delete instance. Check /var/log/nodeworker/worker.log and VCS logs for more details."

- Performing a power cycle from the Veritas Remote Management Interface caused system downtime.
- If you added a node to the appliance and did not use DNS, you needed to restart the infrastructure services after you added the hostname resolution information for the new node to the appliance Hosts file.
- If you did not use DNS and you configured email alerts or configured Call Home with a proxy server, the alert tests failed, and alerts were not sent.
- If you configured a Fibre Channel port in target mode and then changed it to initiator mode, a message should have appeared that advised you to rescan the ports. However, the message did not appear.
- If you tried to remove a node that crashed or was no longer working, the removal failed with the following message:
  "Unable to remove node because an appliance update is in progress or pending. Complete the update, then commit or roll back. If any of these operations did not complete successfully, you must resolve the errors before you can remove a node."
- If you had a multi-node appliance and updated one of the nodes but had not updated the other node, the following message appeared on the Flex Appliance Console:
  "V-492-100-505: Internal server error occurred"

Flex Appliance 3.3 release content

The following list contains the known issues that were fixed and that are included in the Flex Appliance 3.3 release:

- If you configured or changed the configuration of a Call Home proxy server, the event did not display correctly in System Health Insights. The **Severity** column on the **Events** page showed as **Unknown**.

Chapter 3

Getting started

This chapter includes the following topics:

Initial configuration guidelines and checklist

Review the following information before you perform the initial configuration on a new Veritas Flex appliance:

Table 3-1 Flex Appliance configuration guidelines and checklist

Parameter	Description
Network cabling for the Veritas 53xx Appliance	The following Veritas 53xx Appliance ports must be connected to the network for initial configuration: ■ The remote management (IPMI) port Used to connect to the Veritas Remote Management Interface. **Note:** The remote management port must be configured before you begin initial configuration. If it is not configured, do one of the following: For a 5360 or a 5350 appliance, refer to the *Hardware Installation* guides for the procedure. For a 5340 appliance, contact Technical Support and ask your representative to reference article 100042482. ■ host1 or host0 Used to connect to the Flex Appliance Console. Veritas recommends that you connect both host1 and host0 for maximum resiliency, but only one of them is required. **Note:** These ports are labeled ETH0 and ETH1 on the 53xx nodes. ■ privnic1 and privnic0 (multi-node appliances only) Used for communication between nodes. **Note:** These ports are labeled ETH2 and ETH3 on the 53xx nodes. ■ Four to eight 25-10Gb Ethernet ports per node on the 5360 Two to eight 25-10Gb Ethernet ports per node on the 5350 Two to ten 10Gb Ethernet ports per node on the 5340 Used for the application instances. See the *Hardware Installation* or the *Product Description* guides for more details.
Network cabling for the Veritas 52xx Appliance	The following Veritas 52xx Appliance ports must be connected to the network for initial configuration: ■ The remote management (IPMI) port Used to connect to the Veritas Remote Management Interface. **Note:** The remote management port must be configured before you begin initial configuration. If it is not configured, refer to the *Hardware Installation* guides for the procedure. ■ host0 Used to connect to the Flex Appliance Console. ■ Two to eight 25-10Gb Ethernet ports on the 5260 Two to six 25-10Gb Ethernet ports on the 5250 Used for the application instances. See the *Hardware Installation* or the *Product Description* guides for more details.

Table 3-1 Flex Appliance configuration guidelines and checklist *(continued)*

Parameter	Description
Network cabling for the Veritas 5150 Appliance	The following Veritas 5150 Appliance ports must be connected to the network for initial configuration: ■ The remote management (IPMI) port Used to connect to the Veritas Remote Management Interface. **Note:** The remote management port must be configured before you begin initial configuration. If it is not configured, refer to the *Veritas 5150 Appliance Hardware Installation Guide* for the procedure. ■ host0 Used to connect to the Flex Appliance Console. ■ Two 25-10Gb Ethernet ports, two 10GBASE-T Ethernet ports, or four 1GBASE-T Ethernet ports, depending on the purchase configuration Used for the application instances. See the *Veritas 5150 Appliance Hardware Installation Guide* or the *Veritas 5150 Appliance Product Description* for more details.
Connectivity during initial configuration	When you perform the appliance initial configuration, you must take precautions to avoid loss of connectivity. Any loss of connectivity during initial configuration results in failure. The computer that you use to configure the appliance should be set up to avoid the following events: ■ Conditions that cause the computer to go to sleep ■ Conditions that cause the computer to turn off or to lose power ■ Conditions that cause the computer to lose its network connection

Table 3-1 Flex Appliance configuration guidelines and checklist *(continued)*

Parameter	Description

Required names and addresses	Before the configuration, gather the following information:
	■ (53xx appliance only) IP address for the Flex Appliance Console
	■ (53xx appliance only) Hostname for the Flex Appliance Console
	■ IP address for each node in the appliance
	■ Hostname for each node in the appliance
	■ Default gateway
	■ (Optional) DNS server IP address
	■ DNS domain
	■ (Optional) Search domain
	Note: The following subnets are reserved for internal use and cannot be used for the appliance network:
	192.168.227.0/24 and fdf8:192:168:227::/120
	192.168.228.0/24 and fdf8:192:168:228::/120
	192.168.229.0/24 and fdf8:192:168:229::/120
	192.168.230.0/24 and fdf8:192:168:230::/120
	If you plan to use DNS, make sure that forward and reverse DNS lookups are configured properly in your environment. If a forward or a reverse DNS lookup returns multiple records, the initial configuration may fail. You can check the DNS configuration with the following commands for each node. Each command should return only one entry.
	Linux:
	`dig +short @<DNS server IP address> a <node FQDN>`
	`dig +short @<DNS server IP address> -x <node IP address>`
	Windows:
	`nslookup <node IP address>`
	`nslookup <node hostname>`

Default username and password	New appliances are shipped with the following default login credentials: ■ Username: **hostadmin** ■ Password: **P@ssw0rd**
Firewall port usage	Make sure that the following ports are open if a firewall exists between the appliance and the network: ■ 22 (SSH) must be allowed to each node. ■ 443 (HTTPS) must be allowed to the Flex Appliance Console.

Performing the initial configuration

The following procedure explains how to configure the Veritas Flex Appliance software on a new appliance.

Note: If more than the Veritas-tested number of Fibre Channel devices or paths are connected to the appliance, Veritas recommends that you disable the ports or disconnect the devices before you begin this procedure. When the procedure is complete, reenable or reconnect them. You may need to rescan the ports from the Fibre Channel interfaces page.

See "Managing the appliance Fibre Channel ports" on page 48.

To configure Flex Appliance

1. Review the initial configuration guidelines and checklist to make sure that you have all of the necessary information to complete this procedure.

   See "Initial configuration guidelines and checklist" on page 24.

2. Use the following steps to access the Flex Appliance Shell from the Veritas Remote Management Interface:

   - Open a supported web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:
     - Google Chrome version 94 or later recommended (minimum version 80 or later)
     - Mozilla Firefox version 93 or later recommended (minimum version 80 or later)
   - Enter the IP address that is assigned to the remote management (IPMI) port of the appliance node. If you have a multi-node appliance, select one of the nodes to use to begin the initial configuration.
   - Log in to the Veritas Remote Management Interface with the following default credentials:
     - **Username**: **sysadmin**
     - **Password**: **P@ssw0rd**
   - Change the **sysadmin** password from the known default password as follows:
     - Navigate to **Configuration** > **Users** and select the **sysadmin** user.
     - Click **Modify User**.
     - Select the **Change Password** check box and enter a new password.

- Do one of the following to launch the Flex Appliance Shell:
  - Navigate to **Remote Control** > **Console Redirection** and click **Launch Console**.
  - If available, navigate to **Remote Control** > **iKVM over HTML5** and click **Launch Console over HTML5**.

Note: Availability of the HTML5 option depends on the appliance firmware version. You can check the version from the **System** > **System Information** page. The BIOS ID must show version 00.01.0016 or later.

---

3 Log in to the Flex Appliance Shell with the following default credentials:

- Username: **hostadmin**
- Password: **P@ssw0rd**

See "Accessing and using the Flex Appliance Shell" on page 35.

4 Enter the following command to change the password for the **hostadmin** user:

```
set user password
```

5 Enter the following command to configure the host network:

```
setup configure-network
```

Follow the prompts to enter the host network information. You can enter multiple DNS server IP addresses or search domains using a comma-separated list. You can enter up to three DNS server IP addresses. If you need to add more, you can use the `set network dns` command after initial configuration.

Note: The Flex Appliance Shell does not support changing host network settings other than the DNS and Hosts file settings after initial configuration has been completed. If you need to change any of the other host network settings, you must perform a factory reset and then restart the initial configuration process.

---

6 If you did not fill in the optional DNS parameters or want to bypass DNS for specific hosts, you must add the hostname resolution information to the appliance `Hosts` file. Use the following steps:

- Enter the following command:

  ```
  system add-host
  ```

- One at a time, enter the required hostname information for the following:
  - The node

- The Flex Appliance Console if the `setup configure-network` prompts asked for it

You can also add the information for the other node if you have a multi-node appliance, as well as any instances you plan to create, or you can add that information later.

7 Use the `set date` commands to set the date and time. See "Setting the date and time for appliance nodes" on page 41.

8 Enter the following command to configure the Flex Appliance Console:

```
setup configure-console
```

Follow the prompts as applicable to your appliance to enter the console network information.

Note: Depending on the number of storage shelves you have in the appliance, this step may take up to 15 minutes to complete. When it is complete, the shell refreshes with new command options.

---

9 If you have a single-node appliance, the initial configuration process is now complete. Proceed to the next steps that are listed at the end of this topic.

If you have a multi-node appliance, add the second node. Then proceed to the next steps that are listed at the end of this topic.

See "Adding a node" on page 31.

Note: If any part of the initial configuration fails, refer to the error message to resolve the issue and try again. If you resolve the error but experience the same failure, perform a factory reset and a storage reset to return the appliance to its factory configuration. Then restart the initial configuration process.

See "Performing a factory reset" on page 114.

See "Performing a storage reset" on page 124.

Next steps

After you have completed the initial configuration, you must perform the following tasks before you can create an application instance and start using Flex Appliance:

- Verify that you can access the Flex Appliance Console.
  See "Accessing and using the Flex Appliance Console" on page 37.
- Configure at least one network interface. You can configure a physical interface, add a VLAN tag, or create a bond.

See “Configuring or editing a network interface” on page 47.
See “Creating a network bond” on page 44.

- Add the applications that you want to use to the repository.
  See “Managing the repository” on page 69.
- Add at least one tenant.
  See “Adding a tenant” on page 54.
- Veritas also recommends that you register your appliance to ensure that you receive maximum support in the event of a failure. Registration helps Veritas to contact the right person and to dispatch field services to the correct location for repairs.

Once all of these tasks have been completed, you are ready to create an instance and start using Flex Appliance.

Adding a node

Flex Appliance supports up to two nodes on the Veritas 53xx Appliance. You can add a second node during initial configuration or any time after.

A multi-node appliance provides the following benefits:

- Increased efficiency with a shared workload
- Automatic failover for a single-node failure

Adding a second node consists of the following tasks:

- Perform the host network configuration on the new node.
- From the existing node, add the new node to the appliance.

Note: If you add a node to an appliance that has already been configured and is in lockdown mode, the same lockdown mode is automatically enabled on the new node. However, if you are configuring a new multi-node appliance, you must configure all nodes before you enable lockdown mode.

Tasks for adding a node

To perform the host network configuration on the new node

1. Verify the version compatibility between the new node and the node that you want to add it to. The nodes must be running the same version of Flex Appliance, but they can have different security patches installed.

   If the existing node is at a lower version that does not meet these requirements, upgrade or update that node before you add the new one. If the new node is at a lower version that does not meet these requirements, it must be reimaged to the later version.

2. Gather the following details for the new node that you want to add to the appliance:

   - IP address
   - Hostname

   Note: The following subnets are reserved for internal use and cannot be used for the appliance network:

   192.168.227.0/24 and fdf8:192:168:227::/120

   192.168.228.0/24 and fdf8:192:168:228::/120

   192.168.229.0/24 and fdf8:192:168:229::/120

   192.168.230.0/24 and fdf8:192:168:230::/120

   Gather the following details from the appliance that you want to add the node to:

   - Default gateway
   - (Optional) DNS server IP address
   - DNS domain
   - (Optional) Search domain

3. If the node that you want to add has Fibre Channel connections to external devices, disable all Fibre Channel ports that are connected to those devices. You do not need to disable the ports that are connected to the appliance storage shelves.

4. Use the following steps to access the Flex Appliance Shell from the Veritas Remote Management Interface:

   - Open a supported web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:

- Google Chrome version 94 or later recommended (minimum version 80 or later)
- Mozilla Firefox version 93 or later recommended (minimum version 80 or later)

- Enter the IP address that is assigned to the remote management port of the new node.
- Log in to the Veritas Remote Management Interface with the following default credentials:
  - **Username**: **sysadmin**
  - **Password**: **P@ssw0rd**
- Change the **sysadmin** password from the known default password as follows:
  - Navigate to **Configuration** > **Users** and select the **sysadmin** user.
  - Click **Modify User**.
  - Select the **Change Password** check box and enter a new password.
- Navigate to **Remote Control** > **Console Redirection** and click **Launch Console** to launch the Flex Appliance Shell.

5 Log in to the Flex Appliance Shell with the following default credentials:

- Username: **hostadmin**
- Password: **P@ssw0rd**

6 Enter the following command to change the password for the **hostadmin** user:

```
set user password
```

7 Enter the following command to configure the host network:

```
setup configure-network
```

Follow the prompts to enter the host network information. You can enter multiple DNS server IP addresses or search domains using a comma-separated list.

8 If you did not fill in the optional DNS parameters or want to bypass DNS for the new node, you must add the hostname resolution information for the new node to the appliance `Hosts` file. If you did not already add this information when you configured the first node, enter the following command:

```
system add-host
```

Follow the prompts to enter the required information for the new node.

9 Use the `set date` commands to set the date and time. Make sure that the settings are in sync with the other node. See "Setting the date and time for appliance nodes" on page 41.

To add the new node to the appliance

1 Log in to Flex Appliance Shell from the other, preexisting node that was previously configured for the appliance.

2 On versions 3.0 and 3.1, if you do not use DNS or bypassed DNS for the new node, run the following command:

```
system ha-service restart service=infra_svc node=<node hostname>
```

Where *<node hostname>* is the hostname of the node that you are logged in to.

You do not need to perform this step on version 3.2 and later.

3 From the preexisting node, enter the following command to add the new node to the appliance:

```
setup add-node
```

Follow the prompts to add the node. When you are prompted for the new node's password, enter the **hostadmin** password that you set in the previous procedure.

Note: Do not perform any other tasks on the appliance until the `add-node` operation is complete.

---

4 When the `add-node` operation is complete, exit the Flex Appliance Shell from the new node that you just added to the appliance. Then launch a new session from the Veritas Remote Management Interface or open an SSH session to the node. The shell should now display additional command options.

5 If the node that you added has existing Fibre Channel connections, enable them and then run the following command:

```
system sync-settings
```

Alternatively, you can first clean and then rescan the ports from the Flex Appliance Console. See "Viewing the devices that are connected to the Fibre Channel ports" on page 50.

6 If you added this node as part of the appliance initial configuration, return to the initial configuration procedure and refer to the next steps at the end of the procedure to get started using the appliance.

See "Performing the initial configuration" on page 28.

Accessing and using the Flex Appliance Shell

You can use the Flex Appliance Shell to perform the initial configuration, monitor the appliance hardware, and manage some of the settings.

Accessing the Flex Appliance Shell

To access the Flex Appliance Shell for most operations, open an SSH session to the appliance node and log in with the username **hostadmin** and the password that you set during initial configuration.

Note: If you have a multi-node appliance, you must log in to each node individually.

If you have not completed the initial configuration yet, you can access the shell through the Veritas Remote Management Interface. Refer to the initial configuration procedure for instructions.

Veritas recommends that you also log in through the remote management interface for the following operations:

- Restarting the node
- Factory resets
- Reimaging

To conform with the Federal Information Processing Standards (FIPS) and the Security Technical Implementation Guide (STIG), the Flex Appliance Shell supports only the following ciphers and message authentication codes (MACs):

- Ciphers:
  - aes256-ctr

  - aes192-ctr
  - aes128-ctr
- MACs:
  - hmac-sha2-512
  - hmac-sha2-256

Older SSH clients are likely to prevent access to the appliance. Check to make sure that your SSH client supports the listed ciphers and MACs, and update to the latest version if necessary. Default SSH client settings may not be FIPS- and STIG-compliant, which means you may need to select them manually in your SSH client configuration.

Navigating the Flex Appliance Shell

Note: When you log in for the first time, the available commands are limited to those that you can run on an unconfigured appliance. Complete the initial configuration to gain access to the rest of the command options. See "Performing the initial configuration" on page 28.

The Flex Appliance Shell includes the following command views:

- `setup`
  Includes all of the commands for initial configuration.
- `system`
  Includes the commands you can use to manage the appliance OS, system services, and hosts file settings.
- `show`
  Includes the commands you can use to show the current appliance settings and information about the appliance hardware.
- `set`
  Includes the commands you can use to modify the appliance settings.
- `support`
  Includes the commands you can use to access privileged operations and manage storage shelves. This view is primarily intended for Veritas Technical Support.
  - Also includes the `support shell`, which has a command prompt to let you view read-only information on the appliance, including performance metrics.

The following is a list of tips on how to use the Flex Appliance Shell:

- You can press the **?** key at any time to display more information about the commands or sub-views. If you press **?** after you enter a command, the format and usage of the parameters for that command is displayed.
- To type a **?** without displaying the help, first press **Ctrl** + **v**.
- The Flex Appliance Shell works similarly to the Bourne-Again Shell (BASH) and supports all of the same keyboard shortcuts.
- Additional Linux commands are available by typing the full path to the command. For example: `/usr/bin/top`.

  The available commands are dependent on the security permission settings of the user.
- In the documentation, command variables are italicized or in angular brackets (<>). Replace these variables with the appropriate information for each command.

See "Common tasks in Flex Appliance" on page 42.

Accessing and using the Flex Appliance Console

After you have configured Flex Appliance, you can sign in to the Flex Appliance Console to use and manage the appliance software.

Accessing the Flex Appliance Console

To access the Flex Appliance Console

1. Open a web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:
   - Google Chrome version 94 or later recommended (minimum version 80 or later)
   - Mozilla Firefox version 93 or later recommended (minimum version 80 or later)

   Note: These browsers may display a **Privacy error** or **Insecure Connection** page when you access the Flex Appliance Console. Use the **Advanced** option on the page to proceed.

   ---

2. Navigate to **https://*console.domain***, where *console.domain* is one of the following:
   - If you have a Veritas 52xx or 5150 Appliance, *console.domain* is the fully qualified domain name (FQDN) or the IP address that you entered during initial configuration.

- If you have a Veritas 53xx Appliance, *console.domain* is the fully qualified domain name (FQDN) or the IP address that you entered for the Flex Appliance Console during initial configuration.

3 When you sign in for the first time, use the following default credentials:

- **Username**: **admin**
- **Password**: **P@ssw0rd**

After you have signed in, you can create other users from the **User management** page. See "Managing Flex Appliance Console users and tenants" on page 53.

Navigating the Flex Appliance Console

To navigate the Flex Appliance Console, use the icons in the left-side navigation bar or the **Settings** drop-down menu in the upper-right corner. To see the page names in the navigation bar, hover over the icons or use the **>>** icon at the top to expand the entire bar.

The Flex Appliance Console includes the following pages:

Home

The home page includes various widgets that provide information about the status of the appliance. To return to the home page at any time, click the **Home** icon in the left-side navigation bar.

System topology

The **System topology** page shows a complete overview of the appliance nodes, storage, and instances. To access this page, click the **System topology** box on the home page or click the **System topology** icon in the left-side navigation bar.

Note: The **System topology** page shows the full capacity of the appliance storage. However, not all of the storage is available for use. You can see the usable storage capacity when you create or resize an instance.

Activity Monitor

The **Activity Monitor** page shows the tasks that have been performed on the Flex Appliance Console and their current status. To access this page, click the **Activity Monitor** icon in the left-side navigation bar.

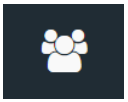
Repository

The **Repository** page lets you manage the applications, application add-ons, and update packages for Flex Appliance. To access this page, click the **Repository** icon in the left-side navigation bar.

Tenants

The **Tenants** page lets you manage tenants. To access this page, click the **Tenants** icon in the left-side navigation bar.

User management



The **User management** page lets you manage users for the Flex Appliance Console. To access this page, click the **User management** icon in the left-side navigation bar.

Network interfaces

The **Network interfaces** page lets you view and configure the appliance's network interfaces. To access this page, click the **Network interfaces** icon in the left-side navigation bar.

Fibre Channel interfaces

The **Fibre Channel interfaces** page lets you check the status of the appliance Fibre Channel ports and view the devices that are connected to them. To access this page, click the **Fibre Channel interfaces** icon in the left-side navigation bar.

Settings

The **Settings** pages let you manage the settings for security and compliance, alert configuration, and remote management. To access these pages, click the gear icon in the upper-right corner of the page.

See “Common tasks in Flex Appliance” on page 42.

Managing the appliance from the Appliance Management Console

The Veritas Appliance Management Console is a centralized management interface for multiple appliances that is hosted on an Appliance Management Server (AMS). You can use the Appliance Management Console for some management tasks of your appliance and your application instances. Flex appliances are supported on AMS version 2.0 or later.

For more information on how to configure and use the Appliance Management Console or how to add a Flex appliance to an existing setup, see the *Veritas Appliance Management Guide*.

Setting the date and time for appliance nodes

Follow these steps to set the date and time on the appliance nodes.

To set the date and time using NTP

1. Log in to the Flex Appliance Shell, and then type the following:

   ```
   set date ntp
   ```

2. Press **Enter**.
3. Follow the prompts to set the NTP server.
4. If you have a multi-node appliance, repeat this procedure on the other node.

To set the date and time by entering the date and time manually

1. Log in to the Flex Appliance Shell, and then type the following:

   ```
   set date manual-date
   ```

2. Press **Enter**.
3. Type the date and time, and then press **Enter**.
4. If you have a multi-node appliance, repeat this procedure on the other node.

To set the time zone

1. Log in to the Flex Appliance Shell, and then type the following:

   ```
   set date timezone
   ```

2. Press **Enter**.
3. Type the number that corresponds to your continent or ocean, and then press **Enter**.
4. Type the number that corresponds to your country, and then press **Enter**.
5. Type the number that corresponds to your time zone, and then press **Enter**.

6 Type **1** to verify that the time zone is correct, and then press **Enter**.

Note: After this step, the following message displays:

```
You can make this change permanent for yourself by appending the
line TZ='<timezone>'; export TZ to the file '.profile' in your
home directory; then log out and log in again.

Here is that TZ value again, this time on standard output so that
you can use the /usr/bin/tzselect command in shell scripts:
```

This message displays in error. You do not need to perform any additional steps to make the timezone change permanent.

7 If you have a multi-node appliance, repeat this procedure on the other node.

Common tasks in Flex Appliance

The following table contains quick links on how to perform common tasks in Veritas Flex Appliance.

Table 3-2

Task	Quick links
Configuring Flex Appliance	See "Performing the initial configuration" on page 28. See "Adding a node" on page 31.
Managing tenants and users	See "Managing Flex Appliance Console users and tenants" on page 53.
Modifying settings	See "Configuring or editing a network interface" on page 47. See "Creating a network bond" on page 44. See "Setting the date and time for appliance nodes" on page 41.
Configuring Call Home	See "About AutoSupport and Call Home" on page 101.
Monitoring the appliance	See "Viewing the hardware status" on page 105. See "Viewing hardware faults" on page 109. See "Viewing system data" on page 109.

Table 3-2 *(continued)*

Task	Quick links
Adding files to the repository	See “Managing the repository” on page 69.
Creating instances	See “Creating application instances” on page 72. See “Managing application instances from Flex Appliance” on page 73.

Chapter 4

Managing network settings

This chapter includes the following topics:

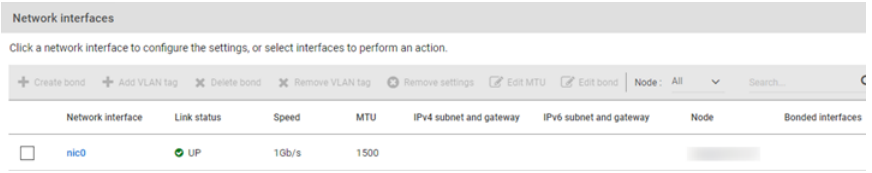
Creating a network bond

If you have more than one node, you must create a network bond on each appliance node after all of the nodes are added. Use the same network interfaces and bonding mode for the bond on each node.

To create a network bond

1. On the Flex Appliance Console, click the **Network interfaces** icon in the left-side navigation bar to open the **Network interfaces** page.

   It may take a few minutes to load.



2. Select the check box next to the name of each network interface that you want to include in the bond, then click **Create bond**.
3. Enter a unique bond name and select the bond mode.

   The following bond modes are available:

   - 802.3ad (LACP) - this is the default bond mode value

     Note: If you select this bond mode, all of the network interfaces in the bond must be on the same port channel. If they are not, the bond speed is less than the sum of the interface speeds. If the bond speed is not as expected after you create the bond, run the following command in the Flex Appliance Shell:

     `/bin/grep "Aggregator ID" /proc/net/bonding/<bond name>`

     The Aggregator IDs should all be the same. If they are not, run the following command and check the Aggregator ID of each interface to determine which one is on a different port channel:

     `/bin/cat /proc/net/bonding/<bond name>`

   - balance-rr
   - active-backup
   - balance-xor
   - broadcast
4. Click **Create**.
5. Configure the new bond.

   See “Configuring or editing a network interface” on page 47.

Editing a network bond

Follow these steps to edit a network bond to change the bonded interfaces.

To edit a network bond

1. From the **System topology** page on the Flex Appliance Console, click on each of your application instances and verify that the bond is not listed in the **IP address and interface pairs** field. If the bond is listed for one or more instances, edit the network of each instance to remove the bond. See "Editing instance network settings" on page 75.

   You may need to add a different IP address and interface pair if the bond that you want to edit is the only interface that is assigned to the instance. If you do not have another available configured interface, configure an interface with placeholder values that you can use until you complete the edits. See "Configuring or editing a network interface" on page 47.

2. Navigate to the **Network interfaces** page and select the bond that you want to edit.
3. Click **Edit bond**.
4. Make the required changes and click **Save**.

Deleting a network bond

Follow these steps to delete a network bond.

To delete a network bond

1. From the **System topology** page on the Flex Appliance Console, click on each of your application instances and verify that the bond is not listed in the **IP address and interface pairs** field.
2. If the bond is listed for one or more instances, edit the network of each instance to remove the bond. You may need to add a different IP address and interface pair if the bond is the only interface that is assigned to the instance.

   See "Editing instance network settings" on page 75.

3. Navigate to the **Network interfaces** page and select the bond that you want to delete.
4. Click **Remove settings**.
5. Click **Delete bond**.

Configuring or editing a network interface

Before you can create an instance, you must configure a network interface. The information that you enter when you configure an interface is used to populate the network information fields when you create a new instance.

To configure or edit a network interface

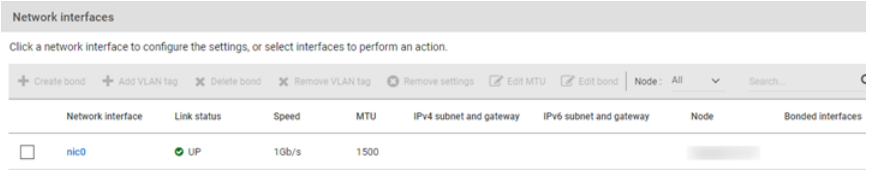
1. Before you edit an existing network interface, first make sure that it is not in use by any application instances, as follows:

   From the **System topology** page on the Flex Appliance Console, click on each of your application instances and verify that the interface is not listed in the **IP address and interface pairs** field. If the network interface that you want to edit is listed for one or more instances, edit the network of each instance to remove the interface. See “Editing instance network settings” on page 75.

   You may need to add a different IP address and interface pair if the interface that you want to edit is the only interface that is assigned to the instance. If you do not have another available configured interface, use this procedure to configure an interface with placeholder values that you can use until you complete the edits.

2. On the Flex Appliance Console, click the **Network interfaces** icon in the left-side navigation bar to open the **Network interfaces** page.

   It may take a few minutes to load.



3. Do one of the following to enter network information:

Note: If you configure a network interface with both IPv4 and IPv6 addresses, all instances that use the interface must also be configured with both IPv4 and IPv6 addresses.

   - If you want to use VLAN tagging, select the check box next to the name of the network interface, click **Add VLAN Tag**, and then enter the VLAN ID and at least one subnet and gateway pair. Use CIDR notation for the subnet and gateway. For example, 1.1.1.0/24.

Do not enter the same VLAN ID or subnet and gateway pair for more than one interface.

Note: If you have more than one node, you must set the VLAN tag for each node.

- If you do not want to use VLAN tagging, click the name of the network interface, and then enter at least one subnet and gateway pair in CIDR notation. For example, 1.1.1.0/24.
  Do not enter the same subnet and gateway pair for more than one interface.

Note: The following subnets are reserved for internal use and cannot be used for the network interfaces:

192.168.227.0/24 and fdf8:192:168:227::/120

192.168.228.0/24 and fdf8:192:168:228::/120

192.168.229.0/24 and fdf8:192:168:229::/120

192.168.230.0/24 and fdf8:192:168:230::/120

4 Click **OK**.

See "Creating a network bond" on page 44.

Managing the appliance Fibre Channel ports

If your appliance has Fibre Channel ports, you can view and manage them from the **Fibre Channel interfaces** page on the Flex Appliance Console. To access the page, click the **Fibre Channel interfaces** icon in the left-side navigation bar.

On this page, you can view all of the Fibre Channel ports on the appliance. Click on any port to see additional information, such as the WWPN, the remote port, and the devices that are connected to it. See "Viewing the devices that are connected to the Fibre Channel ports" on page 50.

Note: The number of Fibre Channel ports on the appliance depends on your hardware configuration. For more information, see the *Product Description* for your specific hardware model.

This release supports the following types of backups over Fibre Channel:

- VMware SAN transport (initiator)

- Tape out (initiator)
- SAN client (Fibre Transport target) - supported on NetBackup 9.1.0.1 and later instances

If you want to perform backups over Fibre Channel, you must assign ports to your application instances. To assign or unassign ports, navigate to the **System topology** page and click on the instance name, then navigate to the **Fibre Channel** tab.

See "Assigning Fibre Channel ports to an instance" on page 77.

See "Unassigning Fibre Channel ports from an instance" on page 79.

Fibre Channel best practices

Veritas recommends the following best practices for connecting Fibre Channel devices:

- Flex Appliance 3.x has been tested for up to 6,000 storage devices or paths in the case of multipathing. If you zone more than the tested number of devices or paths, you may have to take additional steps to perform the following operations and avoid the associated issues:
  - Initial configuration and Flex Appliance updates
    These operations may take a long time or fail.
  - Factory reset
    During a factory reset, the Veritas Remote Management Interface may go blank and may not accept input.

  You should consult with Veritas Technical Support before you implement a Fibre Channel configuration of that size.
- VMware SAN transport mode only works with VMware Virtual Machine File System (VMFS) datastores version 6.0 or later. Other devices such as the raw device-mapping (RDM) format are not supported. Make sure that only VMFS devices are zoned to the appliance to avoid backup failures.
  Refer to the NetBackup Software Compatibility List to confirm the supported VDDK versions.
- Veritas recommends that you do not allocate more than four ports to the same device unless the storage array requires it.
- If you run VMware SAN backups to LSI storage, the LSI storage should be configured in Asymmetric Logical Access Unit (ALUA) mode by following the procedure from the storage vendor. The procedure may involve updating the storage array firmware to a version that supports ALUA mode. If the storage was connected before it was configured in ALUA mode, you also need to unmap and remap the LSI storage LUNs to the appliance. After the LSI storage LUNs

have been remapped, rescan the associated Fibre Channel ports from the **Fibre Channel interfaces** page on the Flex Appliance Console.

Viewing the devices that are connected to the Fibre Channel ports

You can view all the devices that are connected to the appliance Fibre Channel ports from the **Fibre Channel interfaces** page. You can also use this page to scan for new devices or clean stale device information from the system.

Use the following procedure to view the devices that are connected to a particular port.

To view the devices that are connected to a Fibre Channel port

1. On the Flex Appliance Console, click the **Fibre Channel interfaces** icon in the left-side navigation bar to access the **Fibre Channel interfaces** page.
2. Click on the port that you want to view the information for.
3. Under the **Devices** heading, click **Show**.

The appliance scans for devices when it starts up. If you connect or remove devices while the appliance is running, use the following procedure to rescan for newly connected devices or clean the removed devices from the system.

Note: You cannot rescan the ports that are assigned to instances as targets for SAN client.

To rescan or clean Fibre Channel ports

1. On the Flex Appliance Console, click the **Fibre Channel interfaces** icon in the left-side navigation bar to access the **Fibre Channel interfaces** page.
2. Select the check box next to the port or ports that you want to rescan or clean.
3. Click **Rescan** or **Clean**.

Changing DNS or Hosts file settings

Use the following procedures to change the DNS or `Hosts` file settings after initial configuration.

Changing DNS settings

To change the DNS server IP address or search domain

1 From the Flex Appliance Shell, run the following command:

```
set network dns
```

2 Follow the prompts to change the DNS settings as follows:

- To replace the existing settings with new parameters, enter the new information in the appropriate fields. You can enter multiple DNS server IP addresses or search domains using a comma-separated list.
- To remove the DNS settings, leave the fields blank.

Warning: If you remove existing DNS settings, you must add the hostname resolution information to the appliance `Hosts` file. See the section called "Changing Hosts file settings" on page 51.

Changing Hosts file settings

If you do not want to use DNS or want to bypass DNS for specific hosts, you can use the appliance `Hosts` file to manage the hostname resolution information.

To add entries to the `Hosts` file

1 Gather the following information for all appliance nodes and for the Flex Appliance Console, if applicable:

- IP address
- Hostname
- Domain

2 From the Flex Appliance Shell, run the following command:

```
system add-host
```

3 One at a time, enter the required information for the nodes and the Flex Appliance Console, if applicable.

To remove an entry from the `Hosts` file

1 From the Flex Appliance Shell, run the following command:

```
system remove-host
```

2 Enter the IP address of the host that you want to remove.

Chapter 5

Managing users

This chapter includes the following topics:

Overview of the Flex Appliance default users

Flex Appliance comes with default users for the Flex Appliance Console, the Flex Appliance Shell, and the application instances.

The following list describes the default users and their functions:

- The **admin** user
  This user is the default user for the Flex Appliance Console. Use this user to sign in to the console for the first time and for operations that require elevated privileges.
- The **hostadmin** user
  This user is the default user for the Flex Appliance Shell. Use this user to perform the initial configuration and for any other tasks that involve the shell.
- The **sysadmin** user
  This user is the default user for the Veritas Remote Management Interface. Use this user and the remote management interface to access the Flex Appliance Shell for initial configuration, or as an alternative to an SSH session.
- The default application user

Each application that is supported on Flex Appliance also has a default user. See the *NetBackup Application Guides* for specifics.

Managing Flex Appliance Console users and tenants

You can manage all of your Flex Appliance Console users from the **User management** page. To access the **User management** page, sign in to the console and click the **User management** icon in the left-side navigation bar.

Users are assigned to tenants. A tenant is a separate space for a specific group of users and for a specific use. Different tenants can be allocated for different user groups.

See "Adding a tenant" on page 54.

Note: In this version of Flex Appliance, all users are assigned to all tenants.

User types

The following types of users are supported on the Flex Appliance Console:

- Local users
  See "Adding a local user to the Flex Appliance Console" on page 56.
- Active Directory and LDAP users
  See "Connecting a remote user domain to the Flex Appliance Console" on page 56.
- Single sign-on (SSO) users
  See "Managing single sign-on (SSO)" on page 58.

User access roles

User roles determine the access privileges that a user has on the Flex Appliance Console.

The following user roles are available:

- Super administrator
  The default **admin** user is the only user with the super administrator role. The **admin** user has access to all areas of the Flex Appliance Console and can perform all operations.
- Administrator
  All other users have the administrator role. A user with the administrator role can perform most operations.

Adding a tenant

Follow these steps to add a tenant.

To add a tenant

1. On the Flex Appliance Console, click the **Tenants** icon in the left-side navigation bar to open the **Tenants** page.

2. Click **Add tenant**.
3. Enter a tenant name and location. Special characters are not allowed.

4 Complete the following network configuration settings:

Note: The network configuration information that you enter here is used to populate the network information fields when you create a new instance. You can also enter this information when you create an instance.

Domain name	Type the domain name for this tenant. You can enter only one domain name.
Search domains	To enter multiple search domains, type a comma and a space after each search domain.
Name servers	Type the IP addresses for the name servers for this tenant. To enter multiple name servers, type a comma and a space after each name server.
Hosts file entries	Type the `Hosts` file entries for this tenant if you do not want to use DNS or want to bypass DNS for specific hosts. Include entries for all hosts that you want your instances to communicate with.

5 Click **Save**.

After you add a tenant, you can assign instances to it.

Editing a tenant

Follow these steps to change the settings for a tenant.

To edit a tenant

1 On the Flex Appliance Console, click the **Tenants** icon in the left-side navigation bar.

2 Click the name of the tenant that you want to edit.

3 Change the appropriate settings.

4 Click **Save**.

Removing a tenant

Follow these steps to remove a tenant.

To remove a tenant

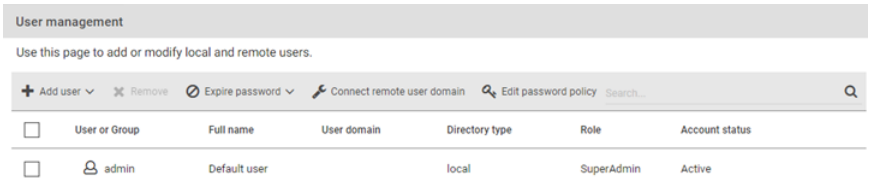
1. On the Flex Appliance Console, click the **Tenants** icon in the left-side navigation bar.
2. Select the tenant that you want to remove, then click **Remove**.

Adding a local user to the Flex Appliance Console

Follow these steps to add a local user.

To add a local user

1. On the Flex Appliance Console, click the **User management** icon in the left-side navigation bar to open the **User management** page.



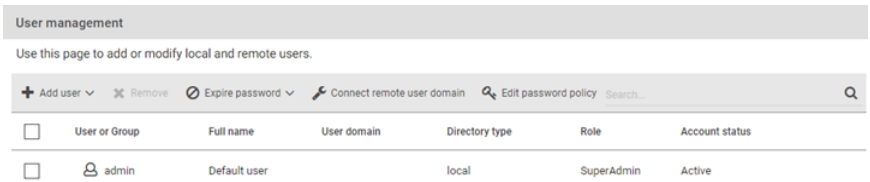
2. Click **Add user** > **Add local user**.
3. Enter a username, the user's full name, and a password.
4. Click **Save**.

Connecting a remote user domain to the Flex Appliance Console

Follow these steps to connect an Active Directory (AD) or LDAP domain.

To connect a remote user domain

1. On the Flex Appliance Console, click the **User management** icon in the left-side navigation bar to open the **User management** page.



2. Click **Connect remote user domain**.

3 Fill in the required parameters and select the connection type. If you do not enter a **Port** value, the following default ports are used:

- **Plain text** or **Plain text + TLS (encrypted)**: port 389
- **SSL (encrypted)**: port 636

4 Select a directory type. If you select **OpenLDAP**, additional parameters appear. Make sure that these parameters match your LDAP server configuration.

5 When you are finished, click **Save**.

If you selected the SSL connection type, a **Trust the certificate** window appears. Review the certificate details and click **Trust**.

Once the remote user domain has been connected, you can import remote users and user groups to grant them access to the Flex Appliance Console.

See "Importing a remote user or user group to the Flex Appliance Console" on page 57.

Editing a remote user domain in the Flex Appliance Console

Follow these steps to make changes to an Active Directory (AD) or LDAP domain that is connected to Flex Appliance.

To edit a remote user domain

1 From the **Home** page of the Flex Appliance Console, click the **User management** icon in the left-side navigation bar.

2 Click **Edit remote user domain**.

3 Modify the parameter fields as necessary and click **Save**.

Note: Changing the server name or IP address overwrites the existing remote user domain with a new domain. Any imported users or user groups that are not part of the new domain are then unable to sign in. If you do not plan to add these users to the new domain, you can remove them from the **User management** page.

See "Removing users from the Flex Appliance Console" on page 66.

Importing a remote user or user group to the Flex Appliance Console

Follow these steps to import an Active Directory (AD) or LDAP user or user group.

Note: Nested user groups are not supported. To import the users of a nested group, you must perform this procedure for the group that they directly belong to.

To import a remote user or user group

1. On the Flex Appliance Console, click the **User management** icon in the left-side navigation bar.
2. If you have not done so already, connect the remote user domain that the user or the user group belongs to.

   See "Connecting a remote user domain to the Flex Appliance Console" on page 56.
3. Click **Add user** > **Import remote users**.
4. Select **User** or **User group**.
5. Depending on your selection, enter the username or the group name. Do not include the domain name.
6. Click **Import**.

After you have imported the user or the user group, you can view the details on the **User management** page.

Note: You cannot view the members of a user group from the Flex Appliance Console. Use the remote server to manage the users within a group.

Managing single sign-on (SSO)

The Flex Appliance Console supports single sign-on (SSO). Note the following prerequisites and considerations:

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Only identity providers that use AD or LDAP directory services are supported.
- SSO users cannot use the APIs. API keys are used to authenticate a user and therefore cannot be used with a SAML-authenticated user.
- SSO users must use the fully qualified domain name (FQDN) in the URL to access the Flex Appliance Console. For example, **https://*consoleFQDN***. The IP address option does not work for SSO.
- Single logout (SLO) is supported if an SLO POST binding URL is present in the identity provider (IDP) metadata. If it is not present, you sign out only from the

appliance and not from the IDP. In this situation, Veritas recommends that you close your browser after signing out for security purposes.

Note: For some IDPs with SLO, you are not redirected to the sign-in page after you sign out of the console. Open a new session to sign back in.

Configuring SSO

Perform the following steps to configure SSO.

To configure SSO

1. Add the SSO identity provider (IDP).

   See the section called “Adding an IDP” on page 60.

2. From the **Single sign-on** page, select the check box next to **Enable single sign-on** to enable SSO.

3. Import the SSO users that you want to have access to the Flex Appliance Console.

   See “Importing a remote user or user group to the Flex Appliance Console” on page 57.

Enabling or disabling SSO

Use the following procedure to enable or disable SSO. You must have added at least one IDP.

To disable or enable SSO

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.

2. Select or deselect the check box next to **Single sign-on**.

Managing identity providers (IDPs)

You can configure single sign-on (SSO) with any identity provider (IDP) that uses the SAML 2.0 protocol and AD or LDAP directory services. You can add up to three IDPs to the appliance but can use only one at a time.

Note: The date and time of the appliance, the IDP, and the browser must be synchronized. Veritas recommends that the date and time are set using NTP.

Use the following procedures to manage your IDPs.

Adding an IDP

To add an IDP

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
2. Under **Appliance service provider URL**, copy or download the appliance metadata file. Upload that file to your IDP and add the appliance as a service provider. For more specific instructions, see the following articles on the Veritas Support website:
   - Active Directory Federation Services (ADFS)
   - IBM
   - Microsoft Azure Active Directory
   - Okta
   - Ping Federate
   - Shibboleth
3. From the IDP, download and save the IDP metadata XML file.
4. Gather the following information for the IDP:
   - Name: A name of your choosing to identify the IDP.
   - User field: The SAML attribute name that is mapped to the user attribute of the remote user domain. For example, **userPrincipalName**, **displayName**, **identifier**, **uid**, etc.
   - Group field: The SAML attribute name that is mapped to the group attribute of the remote user domain. For example, **memberOf**, **role**, etc.
5. From the **Single sign-on** page on the Flex Appliance Console, click **Add**.
6. Upload the IDP metadata file. Once the file has uploaded successfully, click **View details** and verify the certificate subject values and SHA-256 fingerprints.
7. Fill in the other required fields, then click **Save**.
8. If you have added only one IDP, enable SSO to start using it. See the section called “Enabling or disabling SSO” on page 59.

   If you have added more than one IDP, the first IDP is used by default. Switch to the new IDP if necessary. See the section called “Switching to a different IDP” on page 61.

Editing an IDP

To edit an IDP

1. If you need to change the IDP metadata XML file, download the file from the IDP.
2. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
3. Click the name of the IDP, then click **Edit**.
4. Make the required changes. If you uploaded a new IDP metadata file, click **View details** and verify the certificate subject values and SHA-256 fingerprints.
5. When you are done, click **Save**.

Switching to a different IDP

To switch to a different IDP

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
2. If you have not done so already, add the IDP that you want to use. See the section called “Adding an IDP” on page 60.
3. Make sure that SSO is enabled. Then select the IDP that you want to use and click **Use**.

Removing an IDP

To remove an IDP

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
2. Select the IDP that you want to remove and click **Remove**.

Note: If you have more than one IDP, you cannot remove the one that is in use unless you remove the others first. If you have only one IDP or have already removed the others, you must disable SSO before you can remove it. See the section called “Enabling or disabling SSO” on page 59.

Importing a single sign-on user or user group to the Flex Appliance Console

Follow these steps to import a single sign-on (SSO) user or user group.

Note: Nested user groups are not supported. To import the users of a nested group, you must perform this procedure for the group that they directly belong to.

To import an SSO user or user group

1. On the Flex Appliance Console, click the **User management** icon in the left-side navigation bar.
2. If you have not done so already, add the SSO identity provider (IDP) and enable SSO.

   See "Managing identity providers (IDPs)" on page 59.

   See "Managing single sign-on (SSO)" on page 58.
3. Click **Add user** > **Import single sign-on (SSO) users**.
4. Select **User** or **User group**.
5. Depending on your selection, enter the username or the group name in the format ***<user or group>@<domain>***. Note that the parameters are case sensitive. For example, **User@example.com** or **group@example.com**.

   If a group or user has multiple common names (CNs), enter them as a directory path. For example, **Users/testusers@example.com**.
6. Click **Import**.

After you have imported the user or the user group, you can view the details on the **User management** page.

Note: You cannot view the members of a user group from the Flex Appliance Console. Use the IDP to manage the users within a group.

Managing user authentication with smart cards or digital certificates

You can use smart cards or certificates for user validation with a remote user domain. This authentication method is not available for local users.

Prerequisites

Note the following prerequisites for smart card authentication:

- DNS must be configured on the appliance.
  See "Changing DNS or Hosts file settings" on page 50.
- The remote users who are associated with the smart cards or digital certificates must be imported to the appliance.

See “Importing a remote user or user group to the Flex Appliance Console” on page 57.

- Veritas recommends that the appliance date and time are set using NTP. See “Setting the date and time for appliance nodes” on page 41.

Configuring or editing smart card authentication

Follow these steps to configure user authentication with smart cards or digital certificates or to edit an existing configuration.

To configure or edit smart card authentication

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Smart card authentication**.
2. Click **Configure** or **Edit**.
3. Select a certificate mapping attribute and optionally enter the OCSP URI. If you do not provide the OCSP URI, the URI in the certificate is used.
4. Browse for or drag and drop the CA certificates that are associated with the user smart cards or the user digital certificates. Certificate file types must be in `.pem` format and less than 1,000 KB in size.

   To remove a certificate, click the **x** next to the file name. If the certificate is part of a certificate chain, make sure that you also remove the other certificates in the chain.

   Note: If you use Mozilla Firefox, you must also remove the certificate from the browser's certificate manager. See the browser documentation for instructions.

   ---

5. Click **Save**.
6. Open a new session to the Flex Appliance Console. The sign-in page should now display an option to sign in with a certificate or smart card.
7. Before a user can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser’s certificate manager. See the browser documentation for instructions.
8. Once a user inserts a smart card or uploads a certificate, they are prompted to select and authenticate the certificate when they open a new session to the Flex Appliance Console. Once they do so, they can use the certificate to sign in.

   If the user does not select and authenticate the certificate when prompted, they can still sign in with their username and password.

Disabling or enabling smart card authentication

Follow these steps to disable user authentication with smart cards or digital certificates or to enable it after it has been disabled.

To disable or enable smart card authentication

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Smart card authentication**.
2. Click **Disable** or **Enable**.

If you disable smart card authentication, users no longer see an option to sign in with a certificate or smart card.

Changing a local user password in the Flex Appliance Console

Follow these steps to change the password of a local user or the default **admin** user.

Note: Remote user passwords cannot be changed from the Flex Appliance Console. They must be changed from the server on which they reside.

To change a user password

1. Sign in to the Flex Appliance Console from the user account that you want to change the password for.
2. In the top-right corner of the screen, click the black circle icon that includes the user's initials. For example, if the user's full name is Default User, the icon includes the initials DU.

3. Click **Change password**.
4. Fill in the required fields. The password must adhere to the current password policy.

   See "Changing the password policy" on page 66.
5. Click **Save**.

Expiring local user passwords in the Flex Appliance Console

Expiring a user password forces that user to change their password the next time that they sign in to the Flex Appliance Console. If the user is currently signed in, the current session is not affected.

Use the following procedure to expire the password for local users or the default **admin** user.

To expire user passwords

1. Sign in to the Flex Appliance Console. If you want to expire the **admin** user password or all user passwords, you must sign in as the **admin** user.
2. Click the **User management** icon in the left-side navigation bar to open the **User management** page.
3. Do one of the following:
   - To expire the password for a specific user or users, select the user or users and click **Expire password** > **Expire selected users**.
   - To expire the password for all users, click **Expire password** > **Expire all users**.

Note: If you expire your own password, you are immediately signed out of the Flex Appliance Console.

Unlocking a local user account in the Flex Appliance Console

Local user accounts are protected with an account lock if the appliance detects 3 failed sign-in attempts within 15 minutes. If the default **admin** account becomes locked, it is unlocked automatically after 30 minutes. If a different local user account becomes locked, that user and the **admin** user must work together to unlock it. The locked user must know their password. Use the following procedures to unlock the account.

Steps for the admin user

The **admin** user must generate a secure unlock code for the local user.

To generate a secure unlock code

1. Sign in to the Flex Appliance Console and click the **User management** icon on the left.
2. Locate the locked user in the table and click **Unlock**.
3. Copy the code and send it to the local user. The code is valid for 24 hours. If you generate a new code during that time, the first one becomes invalid.

Steps for the locked user

Once the **admin** user has sent the secure unlock code, the locked user can unlock their account.

To unlock a local user account

1. Open a session to the Flex Appliance Console, enter your username and password, and click **Sign in**.
2. You are redirected to a page to enter your secure unlock code. Enter the code that you received from the **admin** user and click **Confirm**.
3. On the page that appears, enter your current password and a new password.
4. Use the new password to sign back in to the Flex Appliance Console.

Removing users from the Flex Appliance Console

Follow these steps to remove users.

Note: The default **admin** user cannot be removed, and users cannot remove their own user accounts.

To remove users

1. On the Flex Appliance Console, click the **User management** icon in the left-side navigation bar.
2. Select the users that you want to remove, then click **Remove**.

Changing the password policy

You can use the Flex Appliance Console to edit the password policy for user passwords. The password policy is enforced for local Flex Appliance Console users and the **hostadmin** user in the Flex Appliance Shell.

The default password policy is as follows:

Password complexity:

- Minimum characters: 8
- Minimum numbers: 1
- Minimum lowercase characters: 1
- Minimum uppercase characters: 1
- Minimum special characters: 0
- Minimum different characters: 0
- Maximum consecutive repeating characters: 99999
- Maximum consecutive characters of the same type: 99999

Password age:

- Days before password must be changed: 99999
- Days before password can be changed: 0
- Days before password expires to display warning message: 10
- Minimum different passwords before allowing reuse: 7

Use the following procedure if you need to make changes to this policy.

To edit the password policy

1. Sign in to the Flex Appliance Console as the **admin** user.
2. Click the **User management** icon in the left-side navigation bar to open the **User management** page.
3. Click **Edit password policy**.
4. If you want your password policy to adhere to the Security Technical Implementation Guides (STIGs), select the **Use STIG for validation** toggle. You can click **Reset to STIG default** to fill in the default values for all fields.
5. Fill in or adjust the required parameters as needed, then click **Save**.

Changing the hostadmin user password in the Flex Appliance Shell

Follow these steps to change the **hostadmin** user password.

To change a hostadmin user password

1. Log in to the Flex Appliance Shell, and then type the following:

   ```
   set user password
   ```

2. Press **Enter**.
3. Type a new password.

   The password must adhere to the password policy that is set on the Flex Appliance Console. In addition, dictionary words are not accepted.

   See “Changing the password policy” on page 66.

Changing the sysadmin user password in the Veritas Remote Management Interface

Follow these steps to change the **sysadmin** user password.

To change the sysadmin user password

1. Log in to the Veritas Remote Management Interface.
2. Navigate to **Configuration** > **Users** and select the **sysadmin** user.
3. Click **Modify User**.
4. Select the **Change Password** check box and enter a new password.

Chapter 6

Using Flex Appliance

This chapter includes the following topics:

Managing the repository

Before you can create an application instance, install an application add-on, or update the appliance software, you must first add the applicable files to the repository.

To access the repository, sign in to the Flex Appliance Console and click the **Repository** icon in the left-side navigation bar.

The **Repository** page consists of the following tabs:

- **Applications**
  Use this tab to manage your applications for creating and upgrading instances. The tab displays the applications that are in the repository and their versions.
- **Application add-ons**
  Use this tab to manage application add-ons for your instances. The tab displays the add-ons that are in the repository and details about each, such as type, version, and the application they can be installed on.

- **Appliance updates**
  Use this tab to manage update packages for Flex Appliance. The repository can only hold one update package at a time. The tab displays the package that is currently in the repository and details relevant to installing the update.

Use the Repository tabs to do the following:

- Add files to the repository
  See "Adding files to the repository" on page 70.
- Remove files from the repository
  See "Removing files from the repository" on page 71.
- Update Flex Appliance
  See "Updating Flex Appliance" on page 87.

Adding files to the repository

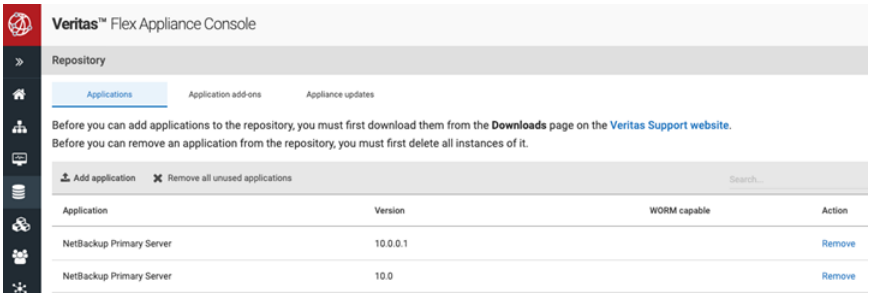
Use the following procedure to download and add files to the Flex Appliance repository.

Guidelines for adding files to the repository:

- Only add files that have been downloaded from or provided by Veritas.
- Do not change the file names.
- To avoid upload issues, ensure that your computer has a strong network connection with the appliance and is connected locally to the same network. Veritas recommends that you use a Windows lab computer if available.

To download and add files to the repository

1. From a computer within your appliance domain, download the appropriate file from the Download Center on the Veritas Support website.
2. From the same computer, sign in to the Flex Appliance Console and click the **Repository** icon in the left-side navigation bar to open the **Repository** page.



3 On the **Repository** page, navigate to the **Applications**, **Application add-ons**, or **Appliance updates** tab, depending on the type of file that you want to add.

4 Click **Add application**, **Add add-on**, or **Add package**.

5 In the dialog box that appears, do the following:

- At the top of the dialog box, click on the drop-down and navigate to the location where you downloaded the file from Veritas.
- Select the downloaded file from the list of items that appears, then click **Open**.

If you added an update package, a progress banner appears at the top of the screen. When the task is complete, the new file appears on the page.

If you added an application or application add-on, you are redirected to the Activity Monitor to view the progress. When the task is complete, return to the **Repository** page to see the new file at the top of the list.

Removing files from the repository

Use the following procedure to remove files from the Flex Appliance repository.

To remove files from the repository

1 Sign in to the Flex Appliance Console and click the **Repository** icon in the left-side navigation bar.

2 On the **Repository** page, navigate to the tab for the type of file that you want to remove.

3 Do one of the following:

- To remove an application, locate the row of the application that you want to remove and click **Remove**. You can also click **Remove all unused applications** to remove all of the applications that are not currently in use. You can also remove the unused add-ons that correspond to the application. To do so, select **Remove corresponding unused add-ons** in the confirmation window that appears. Then click **Remove**.
- To remove an add-on, locate the row of the add-on that you want to remove and click **Remove**. You can also click **Remove all unused add-ons** to remove all of the add-ons that are not currently installed on application instances.
- To remove an update package, click **Remove package**.

Creating application instances

You can create application instances from the **System topology** page of the Flex Appliance Console. Navigate to the **Application instances** section and click **Create instance** to open a new page that leads you through the instance creation process.

Note: You also need to complete additional configuration steps from within NetBackup. See the *NetBackup Application Guides* for detailed instructions for your specific version of NetBackup.

Depending on the application version, you can create instances of the following applications:

- NetBackup primary server
  You can also configure a BMR primary server with this application. However, the BMR boot server cannot be configured on the appliance.
- NetBackup media server with the following storage options:
  - Media Server Deduplication Pool (MSDP)
    You can also configure MSDP cloud storage with this application. Refer to the *NetBackup Deduplication Guide* after the instance is created.
  - AdvancedDisk
- NetBackup WORM storage server

The NetBackup applications must follow the same compatibility requirements between NetBackup versions as any other NetBackup environment. See the *NetBackup Release Notes* for specifics.

For a full list of supported applications and versions for each Flex Appliance release, see the following article on the Veritas Support website:

Flex Appliance supported applications and usage information

Managing application instances from Flex Appliance and NetBackup

After you have created your instances, the instance management is divided between Flex Appliance and NetBackup, depending on the type of operation. In general, use Flex Appliance for any tasks that are related to the appliance or the application files. Use NetBackup for any tasks that are related to your backups. Refer to the following information for more details.

Instance operations that you can perform from Flex Appliance

Use Flex Appliance to do the following:

- Resize instance storage
- Edit instance network settings
- Assign or unassign Fibre Channel ports
- View instance performance metrics
- Upgrade application instances
- Manage application add-ons, including NetBackup EEBs
- Delete application instances
- Clear a configuration error status

See "Managing application instances from Flex Appliance" on page 73.

Instance operations that you can perform from NetBackup

All other management tasks happen from NetBackup. The *NetBackup Application Guides* cover the information that is specific to the NetBackup application. For all other tasks, refer to the regular NetBackup documentation as you would for any other environment.

Managing application instances from Flex Appliance

You can manage some aspects of your application instances from the **System topology** page of the Flex Appliance Console. To access your existing instances, click on the **System topology** box on the home page or the **System topology** icon in the left-side navigation bar, then navigate to the **Application instances** section.

Under **Application instances**, you can perform the following tasks:

- Create a new instance.
  See "Creating application instances" on page 72.
- Select an existing instance to:
  - Relocate it to another node if you have a multi-node appliance.
  - Stop or start it.

Note: When you start an instance, Flex Appliance automatically determines which node to start it on for optimal load balancing. Therefore, it may not start on the same node that it was located on when it was stopped. If you want the instance to run on a specific node, you can relocate it after it starts.

- Use the **Manage** drop-down to delete it.
- Use the **Manage** drop-down to resize the storage.
  See "Resizing instance storage" on page 75.
- Use the **Manage** drop-down to upgrade it.
  See "Upgrading application instances" on page 83.

- Click on an existing instance to:
  - View the instance details.
  - Edit the network settings, including IP address and interface pairs.
    See "Editing instance network settings" on page 75.
  - Manage add-ons.
    See "Managing application add-ons on instances" on page 79.
  - Manage the assigned Fibre Channel ports.
    See "Assigning Fibre Channel ports to an instance" on page 77.
    See "Unassigning Fibre Channel ports from an instance" on page 79.

You can also view live performance metrics of all of the instances on your appliance from the Flex Appliance Shell. See "Viewing instance performance metrics" on page 82.

Note: Flex Appliance does not support adding local directories or manually editing most files on application instances. If you create a local directory or manually edit a file and the instance is relocated or stopped for any reason, the changes are not maintained when the instance restarts.

However, if you must store a small amount of critical data on an instance, you can store it in the `/mnt/nblogs` directory. Note that this directory has 250GB of storage space that cannot be resized. If you use too much storage space, the instance may be affected.

See the *NetBackup Application Guides* for specific details.

Resizing instance storage

Use the following procedure to change the storage allocations on an existing application instance in Flex Appliance.

To resize the instance storage

1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance that you want to modify. If it is running, select it and click **Stop**.
3. Select the instance, then click **Manage** > **Resize instance storage**.
4. Follow the prompts to enter new storage allocations for each volume, then click **Resize**.
5. Wait for the resize operation to complete. You can monitor the progress in the Activity Monitor, which is accessible from the left pane of the Flex Appliance Console.

   When the resize is complete, you can view the new storage allocations by clicking on the instance name under **System topology** > **Application instances**.

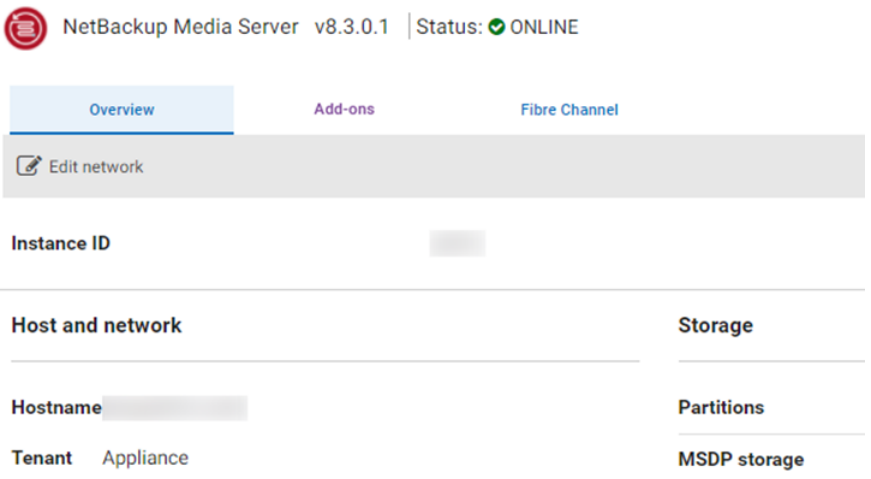
Editing instance network settings

Use the following procedure to edit the network settings of an existing application instance in Flex Appliance.

To edit the instance network settings

1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance that you want to edit. If you want to edit the IP address and interface pairs or the default gateway, select the instance and click **Stop**. You do not need to stop the instance to edit the other settings.

3 Click on the instance name to open the instance details page.



4 At the top of the details page, click **Edit network**.

5 Make the required changes. To add or remove IP address and interface pairs, click **Manage pairs**. To add or remove static routes, click **Manage routes**.

Note: If you change the protocol of the instance IP addresses, make sure that your configured NetBackup features support the new protocol. For example, if you have configured MSDP cloud on an instance and change the IP protocol to IPv6 only, the SSL setting **Check certificate revocation** must be disabled.

---

6 When you are done, click **Save**.

7 If you changed the IP address and interface pairs for the instance, make sure that you update your DNS configuration or add the new IP addresses to the `Hosts` file on all hosts that communicate with the instance. If the other hosts are application instances, you can add the new IP addresses to the `Hosts` file as follows:

- Follow the previous steps to edit the network of all application instances that need to communicate with the instance that you already edited. On the **Edit network** page, add the new IP addresses to the **Hosts file entries** field.
- Open an SSH session to each instance and run the following commands:
  - `sudo /usr/openv/netbackup/bin/bpclntcmd -clear_host_cache`

- `sudo mv /usr/openv/var/host_cache /usr/openv/var/host_cache.old`
- `sudo bp.kill_all`
- `sudo bp.start_all`

Assigning Fibre Channel ports to an instance

To perform backups over Fibre Channel, you must assign ports to your application instances.

This release supports the following types of backups over Fibre Channel:

- VMware SAN transport (initiator)
- Tape out (initiator)
- SAN client (Fibre Transport target) - supported on NetBackup 9.1.0.1 and later instances

Use the following procedure to assign one or more Fibre Channel ports to an application instance.

To assign Fibre Channel ports to an instance

1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance that you want to assign ports to. If it is running, select it and click **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.
3. Click on the instance name to open the instance details page, then navigate to the **Fibre Channel** tab.
4. Click **Assign ports** and follow the prompts to assign available ports. If you assign a port as an initiator that was previously used as a target, you are prompted to rescan the port before you can continue.

Note: Depending on the use case you select for the port, only the devices of that storage type are visible to the instance. If you want all devices to be visible to the instance, select all available options from the **Used for** drop-down menu.

Port sharing and multipathing support

Note the following information:

- You can assign an initiator port to multiple instances if the instances belong to the same tenant. You cannot assign a target port to multiple instances.
- You can use the same port for both VMware and Tape out backups.
- You can assign multiple ports to the same application instance or instances as long as they meet the following guidelines:
  - Used for VMware SAN transport:
    Multiple ports can be assigned to a single or to multiple application instances in any combination.
  - Used for Tape out or for both Tape out and VMware SAN transport:
    Multiple ports can be assigned to a single or to multiple application instances. However, the ports that are connected to the same tape devices must also be connected to the same application instances. The same tape devices cannot be assigned to different instances using different ports.
  - Used for SAN client:
    Multiple ports can be assigned to a single or to multiple application instances in any combination. Once you have assigned the ports, you cannot assign them to additional application instances or use them for another use case unless you unassign the existing instances.
- A Fibre Transport (FT) target port can handle data streams from multiple SAN client initiator ports concurrently. However, if you want it to handle streams from more than two SAN client initiator ports, consider changing the following NetBackup primary server setting:

  ```
  nbftconfig -setconfig -ncp4
  ```

  Caution: This setting applies to all FT target ports on all media servers in your NetBackup domain. This setting should only be increased from the default (2) when all of the following conditions exist:

  All FT target ports on all media servers are at least eight gBit/s link speeds.

  The mix of jobs is such that all of the media servers have unused FT pipes.

  A large number of jobs from other SAN clients are waiting for resources.

  The back-end storage units have a lot of unused throughput capacity.

  If you increase the `-ncp` setting too high, the load balancing between multiple FT media servers could become highly imbalanced.

Unassigning Fibre Channel ports from an instance

Use the following procedure to unassign Fibre Channel ports from an application instance.

To unassign Fibre Channel ports from an instance

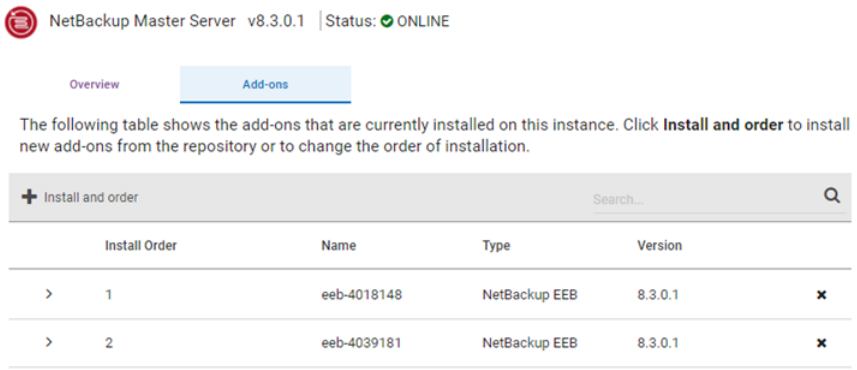
1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance that you want to unassign ports from. If it is running, select it and click **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.
3. Click on the instance name to open the instance details page, then navigate to the **Fibre Channel** tab.
4. Select the port or ports that you want to unassign and click **Unassign ports**.

Managing application add-ons on instances

Flex Appliance instances support the following types of add-ons:

- NetBackup emergency engineering binaries (EEBs)
- NetBackup EEB packages
- Veritas-provided plug-ins
- OpenStorage (OST) plug-ins

You can view and manage the add-ons on an instance from the **Application instances** section of the **System topology** page. Click on the instance name to open the instance details page, then navigate to the **Add-ons** tab. From there, you can view the currently installed add-ons and make changes.



You can also use the **Manage** drop-down in the **Application instances** section to install and order add-ons on the instance.

See “Installing application add-ons” on page 80.

See “Uninstalling application add-ons” on page 81.

See “Changing the application add-on installation order” on page 81.

Installing application add-ons

Use the following procedure to install an add-on on an instance.

To install add-ons

1. Make sure that the add-ons you want to install are located in the repository. See “Managing the repository” on page 69.
2. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
3. Locate the instance on which you want to install the add-ons. If it is running, select it and click **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.
4. Select the instance, then click **Manage** > **Install add-ons**. Alternatively, click on the instance name, navigate to the **Add-ons** tab, and click **Install and order**.
5. Select the appropriate add-ons from the repository list that appears. When you are done, click **Next**.
6. On the following page, you have the option to change the add-on installation order. In most cases, the install order does not affect operation, and you can skip this step. However, if recommended by Veritas Support or otherwise required, you can use the up and down arrows to change the order.

   If any of the add-ons have conflicting changes, alert messages appear to let you know of the conflicts and the resulting actions. Click **View report** at the top of the page for more detailed information. If you agree with the default resolution, proceed to the next step.

   Otherwise, resolve the conflicts manually as follows:

   - If a conflict exists between new add-ons, the add-on that is listed last takes precedence. You can use the up and down arrows to change the order and prioritize a different add-on.
   - If a conflict exists between a new add-on and an installed add-on, the new add-on is not installed. If you want to install the new-add-on, click **Cancel**

to back out of the procedure. Then remove the installed add-on and try again.

- If a conflict exists between installed add-ons, you must remove one of the add-ons before you can continue. Click **Cancel** to back out of the procedure.
- If all of the add-ons are required or if you are unsure which add-ons should be installed, contact Veritas Support for assistance. Before you do so, navigate to the **Conflict report** and click **Copy**. Share this report with your representative.

7 Click **Install**.

Uninstalling application add-ons

Use the following procedure to uninstall an add-on from an instance.

To uninstall an add-on

1 From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.

2 Locate the instance from which you want to uninstall the add-on. If it is running, select it and click **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.

3 Click on the instance name to open the instance details page.

4 At the top of the details page, navigate to the **Add-ons** tab.

5 Click the **X** icon next to the add-on that you want to uninstall.

Changing the application add-on installation order

In most cases, the order in which add-ons are installed on an instance does not affect operation. However, if recommended by Veritas Support or otherwise required, use the following procedure to change the order.

To change the add-on install order

1 From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.

2 Locate the instance that you want to modify. If it is running, select it and click **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.

3 Select the instance, then click **Manage** > **Install add-ons**. Alternatively, click on the instance name, navigate to the **Add-ons** tab, and click **Install and order**.

4 In the wizard that appears, click **Next** to skip the add-on installation step.

5 Use the up and down arrows to change the add-on install order as needed.

6 Click **Install**.

Viewing instance performance metrics

You can view live performance metrics of all of the instances on your appliance from the `support shell` command view in the Flex Appliance Shell.

To view instance performance metrics

1 Log in to the Flex Appliance Shell on the node that you want to view performance metrics for.

2 To view metrics for all instances, enter the following commands:

- `support shell`
- `podman stats --no-stream`

To view metrics for a specific instance, enter the following commands:

- `support shell`
- `podman stats --no-stream <instance name>`

The following information displays for each of the instances on the node, including the Flex Appliance infrastructure instances:

- `CID`: An instance identifier
- `CPU`: The CPU usage of the instance
- `MEM`: The memory usage of the instance
- `NET RX/TX`: The amount of data that is being transmitted and received
- `IO R/W`: The amount of data that is being read from and written to the instance storage disk(s)
- `PIDS`: The total number of processes that are running on the instance

3 When you are done reviewing the information, enter **q** to return to the main Flex Appliance Shell view.

Clearing a configuration error status on an application instance

If a configuration error occurs when you create or upgrade an application instance, the **Application instances** section shows one of the following error statuses:

- Instance creation error: **ONLINE | Configuration Failed**
- Instance upgrade error: **<*Version*> (upgrade failed)**

If you see one of these errors, use the following procedure to clear the error status.

To clear a configuration error status:

1. Before you can clear the error status, you must resolve the underlying configuration error or errors. Hover over the **Configuration Failed** status to see more specific information, and refer to the error messages that display in the Activity Monitor. Then log in to the instance and resolve all errors.
2. When you are sure that all errors have been resolved, navigate to the **System topology** > **Application instances** section.
3. Select the instance and click **Manage** > **Clear status**, then refresh the page to see the change.

Upgrading application instances

Use the following procedure to upgrade an existing instance in Flex Appliance.

To upgrade an instance

1. Make sure that the new version of the application is located in the repository. See "Managing the repository" on page 69.
2. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
3. Locate the instance that you want to upgrade. If it is stopped, select it and click **Start** before you begin the upgrade so that the upgrade precheck can run.
4. Stop all current backup operations on the instance.
5. From the **Application instances** section, select the instance, then click **Manage** > **Upgrade instance**.
6. Select the version that you want to upgrade to and click **Precheck**.
7. If the precheck passes, click **Next** to continue. If the application needs any additional configuration parameters, you are prompted to enter them. Enter the parameters and click **Next**. Then verify the selection summary and click **Upgrade** to begin the upgrade process.

   If the precheck returns with any error messages, resolve the issues before continuing with the upgrade.

   If the upgrade fails for any reason, the instance automatically rolls back to the previous version. You can find more detailed information on the failure in the Activity Monitor. Resolve any issues before restarting the upgrade procedure.
8. If your application does not support rollback, the upgrade is now complete.

If your application does support rollback, the instance version remains in a pending state for the next 24 hours. You must decide within that time period whether you want to commit to the new version or roll back to the previous version. Note that some operations are restricted until you commit or roll back. Complete the rest of this procedure to restore full functionality.

Warning: Performing a rollback may lead to inconsistencies between the NetBackup catalog and the media servers for all jobs that ran after the upgrade. These inconsistencies can affect future backups.

See "Warnings and considerations for instance rollbacks" on page 84.

To commit or roll back the instance version, navigate to the **System topology** > **Application instances** section and do one of the following:

- To commit to the new version, select the instance name and click **Manage** > **Upgrade instance** > **Commit**. You can also click on the instance name to open the instance details page, then click **Commit** at the top of the screen.
- To roll back to the previous version, stop all current backup operations on the instance. Then select the instance name and click **Manage** > **Upgrade instance** > **Roll back**. You can also click on the instance name to open the instance details page, then click **Roll back** at the top of the screen.

  Warning: Before you roll back the version of a primary server instance, check the versions of all media servers and clients that are used with it. The version of the primary server after rollback must be equal to or later than the versions of the connected hosts, including media server instances.

Caution: If you do not commit or roll back within 24 hours of the upgrade, the new instance version is committed automatically.

Warnings and considerations for instance rollbacks

If you need to roll back an instance upgrade, review the following information before you begin.

- Instances with MSDP storage do not support rollback. If you experience an upgrade failure that you cannot resolve, contact Veritas Technical Support for assistance.

- Rollback of other instances should only be attempted as a last resort if there were serious problems with the upgrade.
- A rollback restores the instance to a pre-upgrade checkpoint and reverses all operations that were performed after the upgrade, including backup data. For this reason, backup operations should be kept at a minimum for testing purposes only while the instance upgrade is in a pending state. Do not perform production operations until you commit or roll back the upgrade.
- You cannot resize the instance storage until you commit or roll back the upgrade.
- If you upgrade and roll back an application instance that has a lot of configured storage, the rollback can take a long time to complete. For example, an instance with 1 Petabyte of storage can take a little over an hour to roll back.
- If a rollback is performed, there is a risk of data loss and data leakage for all operations that are performed after the upgrade. The longer the system was up and running before a rollback, the greater the chance of data loss and leakage. The data loss is not limited to losing backup data for the jobs that ran before the rollback. Future backups can be affected as well.

  The following inconsistencies can occur if you decide to roll back:

  - Incremental or transaction log-based database backups:

    If transaction logs were truncated after the upgrade and before the rollback, the database may not be protected.

    To resolve this issue, perform a full database backup after the rollback.
  - Incremental Windows file system backups:

    If the archive bit is used for incremental backup, it is reset upon completion of an incremental backup. If a rollback occurs, the incremental backup is lost, and subsequent incremental backups do not detect that these files changed. The files are not backed up again until a full backup is performed.

    To resolve this issue, perform a full backup after the rollback. If any files were modified in the lost incremental and then deleted before the next full backup, those files are lost.
  - Backup expiration catalog and storage inconsistency:

    If backup images expire and cleanup begins after the upgrade and before the rollback, backup data may be removed from storage units external to the instance. For example, this behavior can happen with an MSDP media server, cloud storage, OST storage, or tape storage. When a rollback of the primary server catalog occurs, the catalog indicates that there is a valid backup even though the data was removed from storage. This inconsistency results in backup data that cannot be restored, duplicated, or replicated. It may also affect scheduling of subsequent backups (delaying backups or performing incrementals instead of fulls).

- Orphaned backups on storage:
  If backup images are created on external storage after the upgrade and before the rollback of the primary server, the backup images exist on storage but not in the NetBackup catalog. This discrepancy results in situations where the backups are never removed from storage (data leakage).
  To resolve this issue, import the images from storage or use the consistency check tools.
- Backup considerations if the instance is a media server:
  - The backups between the upgrade and rollback are not restorable even though NetBackup has them in the catalog.
  - Unfinished SLP jobs fail, causing inconsistencies between the NetBackup primary server and the storage.
    If any backups were deleted after the upgrade and before the rollback, those backups come back as storage leak.

Updating an application instance to a newer revision

Periodically, new revisions of applications are released to address security updates. When a new revision is released, it is posted on the Download Center with a new file name that includes the revision number after the version.

For example, the file `VRTSflex-netbackup-9.1.0.1-0043x86_64.rpm` indicates that the application version is 9.1.0.1, and the revision number is 0043.

Use the following procedure to update an application instance to a newer revision.

Note: The Flex Appliance Console does not currently show the revision numbers of your application instances. To determine the current revision of an instance, log in to the Flex Appliance Shell and run the following commands:

```
support shell
```

```
docker inspect flex.io/netbackup/main:<version> --format='{{index
.Config.Labels "image.revision"'}}
```

Where <*version*> is the version number of the application instance.

To update an instance to a newer revision

1. Add the new revision of the application to the repository.

   See "Adding files to the repository" on page 70.

2. Restart the instance.

Note: If you have more than one instance of the application, they all get updated to the newer revision the next time they are restarted.

About Flex Appliance updates

Flex Appliance provides product enhancements and fixes with the following types of releases:

- Software updates
  A software update contains new features, enhancements, and fixes for Flex Appliance. It modifies the operating system, the appliance interfaces, or both.
- Firmware updates
  A firmware update modifies the firmware on the appliance hardware components, including the BIOS, storage, network interface cards, and Fibre Channel ports. The version number for a firmware update is not related to the Flex Appliance version.

Veritas recommends that you install updates when available to make sure that you have the latest product features and fixes.

See "Updating Flex Appliance" on page 87.

Updating Flex Appliance

Use the following procedure to update the Flex Appliance software from version 3.x to a later release.

Note: To upgrade to version 3.x from a pre-3.0 version, refer to the *Getting Started and Administration Guide* for the version that you are currently on.

If more than the Veritas-tested number of Fibre Channel devices or paths are connected to the appliance, Veritas recommends that you disable the ports or disconnect the devices before you begin this procedure. When the procedure is complete, reenable or reconnect them. You may need to rescan the ports from the Fibre Channel interfaces page.

See “Managing the appliance Fibre Channel ports” on page 48.

To update Flex Appliance

1. Before you begin the software update, make sure that the appliance firmware is up to date. See “Updating the firmware” on page 90.
2. On the Flex Appliance Console, click the **Repository** icon in the left-side navigation bar and navigate to the **Appliance updates** tab.
3. Make sure that the update package you want to use is located in the repository. See “Managing the repository” on page 69.
4. Navigate to **System topology** > **Application instances** and do one of the following:
   - If you have a single-node appliance, stop all running instances.
   - If you have a multi-node appliance, stop all running instances or select the node that you want to update first and relocate all of its instances to the other node.
5. (Optional) If you want to check ahead of time if the appliance is ready for the update, run a precheck on each node. The precheck also runs as part of the update process, so you can skip this step if you prefer to wait for the system to run it.

   Note: The precheck is available on versions 3.1 and later.

   To run the precheck, select the node or nodes and click **Run precheck**. If you have a multi-node appliance and relocated the instances, run the precheck on the node that does not have any running instances.

   When the precheck completes, you can view the status in the table. If the precheck reports any issues, correct them before you proceed with the update.

6 Return to the **Appliance updates** tab on the **Repository** page. Select the node that you want to update and click **Update** or **Update and restart**.

Note: The **Update and restart** option does not appear for versions 3.1 and later.

If the update requires a restart, you can monitor the restart progress from the Veritas Remote Management Interface. To access the Veritas Remote Management Interface, refer to the initial configuration procedure. See "Performing the initial configuration" on page 28.

Warning: Do not start any application instances while the update is in progress.

---

7 When the update process is done, refresh your browser cache and sign back in to the Flex Appliance Console.

8 If you have a multi-node appliance, make sure that the update completed successfully on the first node. Then stop or relocate all instances on the other node and repeat the update on that node.

Do not attempt to update the second node if the update failed on the first node.

9 If the update release that you installed supports rollback, you must decide whether you want to commit the new version or roll back to the previous version.

Note: Some operations are restricted until you commit or roll back, or if the nodes are running different software versions. You also should not edit any settings during these times. Update both nodes and complete the rest of this procedure to restore full functionality.

Do one of the following:

- To commit the update to version 3.1, run the following command from the Flex Appliance Shell:

  ```
  system upgrade-commit
  ```

- To commit the update to version 3.2 or later, return to the **Appliance updates** tab on the **Repository** page and click **Commit**.

- To roll back to the previous version, stop all instances on the appliance and then run the following command from the Flex Appliance Shell:

  ```
  system rollback
  ```

  Restart the node when prompted. If you have a multi-node appliance, you must run this command on all nodes.

Warning: If you have a multi-node appliance, you must roll back all nodes before you perform any other operations, including retrying an update. Complete the rollback and restart on the first node before you proceed with the next node.

10 If you rolled back, refresh your browser cache before you sign back in to the Flex Appliance Console.

Updating the firmware

Use the following procedure to update the appliance firmware.

If you make any hardware changes after you install a firmware update, make sure that you install the update again for the new hardware.

You can check the supported firmware for your hardware model from the Appliance Compatibility List.

To update the firmware

1 On the Flex Appliance Console, click the **Repository** icon in the left-side navigation bar and navigate to the **Appliance updates** tab.

2 Make sure that the update package you want to use is located in the repository. See "Managing the repository" on page 69.

3 Navigate to **System topology** > **Application instances** to check the status of the application instances.

4 Do one of the following:

- If you have a single-node appliance, stop all running instances.
- If you have a multi-node appliance, stop all running instances or select the node that you want to update first and relocate all of its instances to the other node.

5 Return to the **Appliance updates** tab on the **Repository** page. Select the node that you want to update and click **Update** or **Update and restart**. If you already updated the firmware and want to update it again because of new hardware, the options are **Update again** or **Update again and restart**.

Note: The **Update and restart** and the **Update again and restart** options do not appear for versions 3.1 and later.

If the update requires a restart, you can monitor the restart progress from the Veritas Remote Management Interface. However, the interface briefly becomes unavailable during the update. To access the Veritas Remote Management Interface, refer to the initial configuration procedure. See "Performing the initial configuration" on page 28.

Warning: Do not start any application instances while the update is in progress.

---

6 When the update process is done, refresh your browser cache and sign back in to the Flex Appliance Console.

7 If you have a multi-node appliance, stop or relocate all instances on the other node.

Then repeat the update on the other node.

Chapter 7

Appliance security

This chapter includes the following topics:

Security overview

Flex Appliance includes multiple features to ensure the security of your data. Each element of the appliance is tested for vulnerabilities using both industry standards and advanced security products. These measures ensure that exposure to unauthorized access and resulting data loss or theft is minimized.

Flex Appliance also uses the Security Technical Implementation Guide (STIG) template to meet security requirements per the Defense Information Systems Agency (DISA) profile. See the *NetBackup Flex Appliance Security* white paper for more information.

The security features in this release include but are not limited to the following:

- OS security hardening, including Security-Enhanced Linux (SELinux).
- Forced password changes during initial configuration to make sure that the default password does not remain active on the system.
- The ability to set your own password policy, including the option to use STIG for validation.
  See “Changing the password policy” on page 66.

- Lockdown mode and WORM storage support, which let you set additional access restrictions and block data deletion during a specified retention period.
  See "About lockdown mode" on page 94.
- The ability to add a sign-in banner that appears before a user signs in to the Flex Appliance Console and the Flex Appliance Shell.
  See "Using a sign-in banner" on page 96.
- Support for external certificates.
  See "Using an external certificate" on page 97.
- Session timeouts that automatically sign users out of the Flex Appliance Console and the Flex Appliance Shell after 10 minutes of inactivity.
- Conformance to the Federal Information Processing Standards (FIPS) 140-2.
- Additional password protection in the Flex Appliance Console that locks local user accounts after three incorrect login attempts. If an account becomes locked, the locked user and the **admin** user must work together to unlock it.
- Additional password protection in the Flex Appliance Shell that locks the **hostadmin** account for 15 minutes after 3 incorrect login attempts.
- Password protection that restricts access to the **GRUB** menu except with assistance from Veritas Technical Support. If you need to edit GRUB, contact Technical Support and ask your representative to reference article 100048098.

Also note the following information regarding the appliance security:

- IP forwarding is enabled in Flex Appliance by design; it is used to facilitate network communication between application instances and external networks.
- Simultaneous multithreading (smt) is enabled by default on the Veritas 53xx Appliance.
  The following vulnerabilities affect this feature:
  - CVE-2018-12130
  - CVE-2018-12126
  - CVE-2018-12127
  - CVE-2019-11091

  You can disable smt to address these vulnerabilities; however, significant performance degradation may occur. If you want to disable smt, contact Veritas Technical Support and ask your representative to reference article 100046154.

About lockdown mode

Flex Appliance lockdown mode offers additional security levels to protect your appliance and data, in addition to the hardened, secure operating environment that comes out of the box.

Lockdown mode provides the following benefits:

- It prevents unauthorized access or modification to the underlying operating system (OS). Once lockdown mode is enabled, administrators cannot make changes to the OS or the internal components.
  If you need access to the OS for emergency operations, you must contact Veritas Technical Support to obtain a One-Time Password and temporarily unlock the appliance. This functionality prevents unauthorized changes even if a malicious actor gained access to stolen credentials.
- It includes the option to create WORM storage instances that prevent your data from being encrypted, modified, or deleted. WORM is the acronym for Write Once Read Many. Any data that is saved on these instances is protected with the following security measures:
  - Immutability
    This protection ensures that the backup image is read-only and cannot be modified, corrupted, or encrypted after backup.
  - Indelibility
    This property protects the backup image from being deleted before it expires. The data is protected from malicious deletion.

Flex Appliance includes the following lockdown modes:

- Normal mode
  This mode is the default mode of the appliance. Normal mode does not support WORM storage.
- Enterprise mode
  This mode adds additional access restrictions but retains a level of flexibility. In this mode:
  - You can create WORM storage instances and also delete them, including any existing data.
  - Any administrator can delete WORM storage instances if there is no immutable data. However, only the default **admin** user can delete them if immutable data is present.
  - When you delete a WORM storage instance as the default **admin** user, the instance can be running or stopped. When you delete a WORM instance as

any other user, the instance must be running so that the system can verify that there is no immutable data present.

- To change from enterprise mode to normal mode, you must first delete all WORM storage instances.

- Compliance mode
  This mode adds the highest level of access restrictions. In this mode:
  - You can create WORM storage instances. You can delete the instances only if there is no immutable data present.
  - Any administrator can delete WORM storage instances if there is no immutable data.
  - When you delete a WORM storage instance, the instance must be running so that the system can verify that there is no immutable data present.
  - To change from compliance mode to enterprise mode or normal mode, you must first wait for all data on the WORM storage instances to expire and then delete the instances.

In both enterprise mode and compliance mode, storage reset is disabled.

Veritas strongly recommends that you enable enterprise lockdown mode to prevent unauthorized access to the OS, even if you do not plan to create WORM storage instances.

Warning: Lockdown mode does not block access to the remote management (IPMI) port. Veritas recommends that you set up your network to restrict access and only allow security administrators or the users that manage the physical hardware to use the port.

The appliance must be in lockdown mode before you can create WORM storage instances. See "Changing the lockdown mode" on page 95.

For more information on creating and managing WORM storage instances, see the *NetBackup Application Guide for Flex Appliance*.

Changing the lockdown mode

You can use the Flex Appliance Console to change the lockdown mode on a Flex appliance. Note the following restrictions:

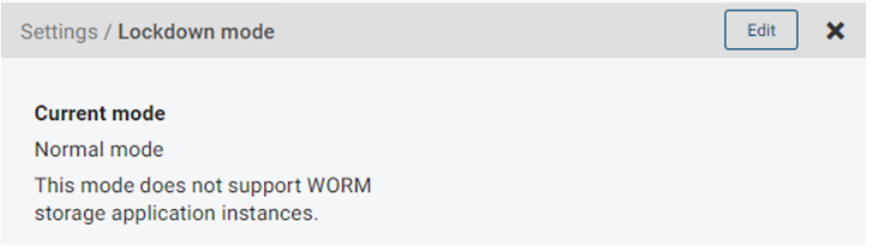
- Lockdown mode does not block access to the remote management (IPMI) port. Veritas recommends that you set up your network to restrict access and only allow security administrators or the users that manage the physical hardware to use the port.

- Only the default **admin** user can change the lockdown mode.
- To change from enterprise mode to normal mode, you must first delete all WORM storage instances.
- To change from compliance mode to enterprise mode or normal mode, you must first expire all data on the WORM storage instances, and then delete the instances.

Note: If you have a multi-node appliance, make sure that all nodes are configured before you enable lockdown mode.

To change the lockdown mode

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Lockdown mode**.



2. On the **Lockdown mode** page, click **Edit**.
3. Select the mode that you want to enable and click **Save**.

Using a sign-in banner

You can set a text banner that appears before a user signs in to the Flex Appliance Console and the Flex Appliance Shell. Typical uses for the login banner include legal notices, warning messages, and company policy information.

To add or edit a sign-in banner

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Sign-in banner**.
2. Click **Add** or **Edit**.
3. Enter the sign-in banner details. You can click **Preview** to see how it appears in the console. When you are finished, click **Save**.

To remove a sign-in banner

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Sign-in banner**.
2. Click **Remove**.

Using an external certificate

By default, the appliance uses a Flex Appliance self-signed certificate for host communication. You can configure the appliance to use an external certificate instead.

Importing an external certificate

To use an external certificate, you must have the following:

- Host certificate: An X.509 certificate for the appliance, in PEM format. This certificate is different from the certificate for your NetBackup primary and media servers.
- Private key: The PKCS #8 private key of the host certificate.
- Passphrase: The passphrase of the private key if the key is encrypted.

To prevent errors while importing certificates, ensure that the external certificate files meet the following requirements.

- All certificate files must have a suffix of .pem or .cer and include `-----BEGIN CERTIFICATE-----` at the beginning of the certificate.
- All certificate files must contain the Flex Appliance Console FQDN in the common name or the subject alternative name (SAN) field of the certificate.
- The subject name and common name fields must not be left empty.
- Only ASCII 7 characters can be used in the subject and SAN fields of the certificate.
- The private key must be in the PKCS #8 PEM format, and it must begin with a header line of `-----BEGIN ENCRYPTED PRIVATE KEY-----`, `-----BEGIN PRIVATE KEY-----`, or `-----BEGIN RSA PRIVATE KEY-----`.
- Flex Appliance's web service uses the PKCS #12 standard and requires certificate files to be in the X.509 (.pem) format. If you obtained the certificate and private key in any other format you must first convert them to the X.509 (.pem) format.

To import an external certificate

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **External certificate**.
2. Upload the required files and click **Next**.
3. Confirm the details and click **Import**.

Removing an external certificate

Use the following procedure to remove an external certificate that you imported. Note that if you remove an external certificate, the appliance reverts to use the default Flex Appliance self-signed certificate for host communication.

To remove an external certificate

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **External certificate**.
2. Click **Remove**.

Using network access control

You can use the network access control feature to control which IP addresses are allowed to access the appliance. Use HTTPS access control to control which IP addresses can access the Flex Appliance Console or the APIs through HTTPS. Use SSH access control to control which IP addresses can access the Flex Appliance Shell through SSH.

To configure or edit network access control

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Network Access Control**.
2. Depending on which service you want to configure, click **Configure** or **Edit** under **HTTPS access control** or **SSH access control**.
3. Follow the prompts to add the IP addresses or subnets that you want to have access to the appliance. Any IP addresses that are not included in the allowed list cannot access the appliance.

   Note the following information:

   - The IP protocol of the addresses in the allowed list must match the protocol of the appliance.
   - Subnets must be entered in CIDR notation. For example, 1.1.1.0/24.

- If you use the Dynamic Host Configuration Protocol (DHCP), add subnets instead of IP addresses.
- For HTTPS access control, you must include your current IP address in the allowed list. It can be entered by itself or as part of a subnet.
- For SSH access control, you can leave the allowed list empty to block all SSH access.

To disable or enable network access control

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Network Access Control**.
2. Depending on which service you want to disable or enable, click **Edit** under **HTTPS access control** or **SSH access control**.
3. Deselect or select the check box next to **Enable HTTPS access control** or **Enable SSH access control**.

Changing the SSH port

By default, SSH access to the Flex Appliance Shell uses port 22. If you need to use a different port, use the following procedure to change it.

Note: This feature is available on version 3.2 and later.

To change the SSH port

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Network Access Control**.
2. Under **SSH access control**, click **Configure** or **Edit**.
3. Enter a new port in the **SSH port** field and click **Save**.

Chapter 8

Monitoring the appliance

This chapter includes the following topics:

Registering an appliance

Registering your appliance is a vital step in allowing Veritas the ability to help maximize availability of your appliance and provide proactive monitoring support. Registration provides Veritas with accurate contact details and site-specific information, which aids in expediting support, field services, and customer notification of failures.

You can register your appliance by signing in to the System Health Insights portal (https://systemhealth.netinsights.veritas.com) with your Veritas Account Manager credentials. For more information, see the *Veritas Appliance AutoSupport Reference Guide* and the *System Health Insights User Guide*.

Configuring alerts

The appliance has the ability to monitor itself and send a notification if it detects a problem that needs attention. You can configure the following types of alerts from the Flex Appliance Console:

- Call Home
  Send notifications to Veritas and the NetInsights Console. Call Home is enabled by default.
  See "About AutoSupport and Call Home" on page 101.
  See "Configuring Call Home" on page 101.
- Email alerts
  Send notifications to an email address.
  See "Configuring email alerts" on page 102.
- SNMP alerts
  Send notifications to an SNMP manager.
  See "Configuring SNMP alerts" on page 103.

About AutoSupport and Call Home

Veritas AutoSupport is a set of infrastructures, processes, and systems that enhance the support experience through proactive monitoring of Veritas Appliance hardware and software. AutoSupport also provides automated error reporting and support case creation.

Call Home provides information regarding appliance component states and status. AutoSupport correlates the Call Home data with other site configuration data held by Veritas, for technical support and error analysis. With AutoSupport, Veritas greatly improves the customer support experience.

More information about AutoSupport and Call Home is available in the *Veritas Appliance AutoSupport Reference Guide* at the following site:

Appliance documentation

Configuring Call Home

The appliance can communicate with the Veritas Call Home server and upload hardware and software information. If required for your environment, you can also configure a proxy server.

Use the following procedures to manage the Call Home configuration.

To configure or edit Call Home

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Call Home**.
2. Click **Configure** or **Edit**.
3. If required, select **Enable proxy server** and fill in the required details. Then click **Configure** or **Save**.
4. To test the connection, wait at least 10 seconds and then click **Test Call Home**.

To disable or enable Call Home

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Call Home**.
2. Click **Disable** or **Enable**.

Configuring email alerts

You can configure the appliance to send emails with alerts about the hardware, the appliance services, and your application instances.

Note: NetBackup alerts must be configured separately from NetBackup. See the topic "Setting up mailx email client" in the *NetBackup Administrator's Guide, Volume I*.

Use the following procedures to manage email alerts.

To configure or edit email alerts

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Email alerts**.
2. Click **Configure** or **Edit**.

3 Fill in the required details and click **Configure** or **Save**.

Note: If your appliance is configured with an IPv6 address and your SMTP server is configured with both IPv4 and IPv6 addresses, you must do one of the following for alerts to work:

Enter the server IPv6 address instead of the hostname.

After alert configuration, add the server IPv6 address to the appliance Hosts file. See "Changing DNS or Hosts file settings" on page 50.

If you use DNS, modify your DNS configuration so that the server hostname only responds to the IPv6 address.

---

4 To test the connection, wait at least 10 seconds and then click **Test email alerts**.

To disable or enable email alerts

1 Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Email alerts**.

2 Click **Disable** or **Enable**.

Configuring SNMP alerts

The Simple Network Management Protocol (SNMP) enables you to monitor the appliance performance. You must have an existing SNMP manager before you can configure SNMP alerts.

Use the following procedures to manage SNMP alerts.

To configure or edit SNMP alerts

1 Locate the Flex Appliance MIB file at the following website:
https://sort.veritas.com/utility_tool

Copy the contents of this file to your SNMP manager to set it up to receive appliance monitoring traps.

2 Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **SNMP alerts**.

3 Click **Configure** or **Edit**.

4 Fill in the required details and click **Configure** or **Save**.

Note: If your appliance is configured with an IPv6 address and your SNMP server is configured with both IPv4 and IPv6 addresses, you must do one of the following for alerts to work:

Enter the server IPv6 address instead of the hostname.

After alert configuration, add the server IPv6 address to the appliance Hosts file. See "Changing DNS or Hosts file settings" on page 50.

If you use DNS, modify your DNS configuration so that the server hostname only responds to the IPv6 address.

---

5 To verify the connection, check your SNMP manager.

To disable or enable SNMP alerts

1 Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **SNMP alerts**.

2 Click **Disable** or **Enable**.

Setting the threshold values for disk usage alerts

You can set the threshold at which alerts are sent for high disk usage. The default value is 80%.

Note: Critical `diskspace` alerts are sent when disk usage exceeds 94%. This threshold cannot be changed. In some cases, backup jobs may fail before you reach the 94% threshold, so Veritas recommends that you add storage or otherwise address the issue as soon as you see an alert.

To set the threshold value

1 Log in to the Flex Appliance Shell.

2 Run the following command:

```
set alerts diskspace-threshold threshold=<value>
```

Where <*value*> is an integer between 0 and 93. If you enter 0, disk usage alerts are disabled. Veritas recommends that you do not set this value higher than 87.

3 If you have a multi-node appliance, repeat these steps on the other node.

To view the threshold value

1. Log in to the Flex Appliance Shell.
2. Run the following command:

```
show alerts diskspace-threshold
```

Monitoring the appliance from the System Health Insights portal

System Health Insights is a global appliance monitoring and insights portal that delivers telemetry-driven information to help you understand the health and operational state of your appliances. You can use System Health Insights to monitor storage use across appliances, monitor the hardware metrics, and reduce upgrade planning with automatic updates.

Note: Automatic updates are supported on version 3.2 and later.

For more information about System Health Insights, see the *System Health Insights User Guide*.

Viewing the hardware status

You can use the `show` command view in the Flex Appliance Shell to obtain information about the appliance hardware components. The hardware monitoring commands are available before initial configuration.

See "Viewing node information" on page 105.

See "Viewing storage shelf information on a Veritas 52xx Appliance" on page 108.

Viewing node information

Depending on the appliance model, you can view data about the following compute node components from the shell. Details are provided as needed.

- All (components)
- Adapter
- CMOSBattery
- Connection (between the appliance and the Primary Storage Shelf)
- CPU

- DIMM
- DIMMPopulation
- Disk
- Fan
- FibreChannel
- Firmware
- Network
- PCI
- Power
- Product
- RAID
- ReservedStorage
- SSD
- StorageConnections
- StorageStatus
- Temperature
- VROC

To view node component health

1. Log in to the Flex Appliance Shell, and type the following.

   `show hardware-health node component=<component>`

2. Press **Enter** to view the data.

Viewing storage shelf information on a Veritas 53xx Appliance

You can view data about the storage shelf components from the shell with the `show hardware-health primaryshelf` command, the `show hardware-health expansionshelf` command, and the `show hardware-data storage-shelf` command.

Note: The `show hardware-data storage-shelf` command is available on version 3.2 and later.

The `show hardware-health primaryshelf` command shows details about the following components for a primary shelf:

- All (components)
- BBU (battery backup unit)
- Controller
- Disk
- Fan
- Firmware
- Power
- Product
- Temperature
- Volume
- VolumeGroup

The `show hardware-health expansionshelf` command shows details about the following components for a specific expansion shelf:

- All (components)
- Disk
- Fan
- Firmware
- Power
- Product
- Temperature
- Volume
- VolumeGroup

The `show hardware-data storage-shelf` command shows more granular details about the following components for all storage shelves:

- configuration
- controllers
- disk-affinity
- disk-group-statistics
- disk-groups

- disk-statistics
- disks
- enclosures
- events
- pools
- ports
- sensor-status
- system
- volumes

To view storage shelf component status

1. Log in to the Flex Appliance Shell.
2. Run one of the following commands:
   - For a primary shelf:
     `show hardware-health primaryshelf component=<component>`
     Where <*component*> is the component that you want to see information for.
   - For an expansion shelf:
     `show hardware-health expansionshelf component=<component> shelf_id=<shelf number>`
     Where <*component*> is the component that you want to see information for and <*shelf number*> is the number of the expansion shelf, starting from 1.
   - For more granular details about all storage shelves:
     `show hardware-data storage-shelf <component>`
     Where <*component*> is the component that you want to see information for.

Viewing storage shelf information on a Veritas 52xx Appliance

You can view data about the following storage shelf components from the shell:

- All (components)
- Disk
- Fan
- Power

- Product
- Temperature

To view the storage shelf status

1. Log in to the Flex Appliance Shell.
2. Run the following command:

   ```
   show hardware-health storageshelf component=<component>
   ```

   Where *<component>* is the component that you want to see information for.

Viewing hardware faults

From the Flex Appliance Shell you can run a command that shows only hardware component faults.

To view hardware faults

1. Log in to the Flex Appliance Shell, and type the following.

   ```
   show hardware-errors
   ```

2. Press **Enter** to display the data.

Viewing system data

In addition to individual hardware component data you can obtain information about the appliance system. The `self-test` command captures more data than the `hardware-health` command. It includes a health check all the way to the NetBackup application layer.

This section provides the information that is specific to the output from the `self-test` commands. The available information is provided in the following table.

Table 8-1 Self-test data

Command	Description
`disk`	Shows the current status of the storage array.
`software`	Shows the current status of the various appliance software components.
`hardware`	Shows the current status of the various appliance hardware components.

Table 8-1 Self-test data *(continued)*

Command	Description
`network`	Shows the current status of the network connections.

To view appliance system data

1 Log in to the Flex Appliance Shell, and type any of the following as needed.

```
system self-test disk
system self-test software
system self-test hardware
system self-test network
```

2 Press Enter after each string to view the data.

See "Gathering logs" on page 129.

Clearing the hardware status

If you replace a hardware component or experience any issues with the hardware monitoring data, you may need to clear the hardware status. When you clear the status, all component statuses are reset. When you recheck the monitoring data, the most current information shows.

Note: This feature is available on version 3.2 and later.

To clear the hardware status

1 Log in to the Flex Appliance Shell.

2 Run the following command:

```
support clear-hardware-status
```

3 Follow the prompts to confirm.

Note: After the status is cleared, the collection of new data takes approximately 5 to 10 minutes. During that time, the hardware monitoring commands do not show any data.

Forwarding logs

You can forward the appliance system logs (syslogs) and the audit logs to an external log management server. Your log management server must support the Rsyslog client.

Flex Appliance supports the following:

- TLS Anonymous Authentication for log forwarding
- X.509 file format for certificate files

To configure or edit log forwarding:

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Log forwarding**.
2. Click **Configure** or **Edit**.
3. Enter the log forwarding settings. If you want to secure the log transmissions from the appliance to the log server, select **Enable TLS log transmission** and upload the required certificate files. Veritas recommends that you enable TLS for security purposes.
4. When you are finished, click **Save**.

To stop forwarding logs

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **Log forwarding**.
2. Click **Remove**.

Providing access for external monitoring

You can generate an API access token to provide access to the appliance for external monitoring or support.

The following token types are available:

- Metrics token: Monitor the performance metrics from a third-party analytics application. For example, Grafana.
- Support token: Grant permission to Technical Support to create, download, and clean up log packages on the appliance.

Only one token of each type is allowed at a time.

To generate an API access token

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **API access token**.
2. Click **Generate**.
3. Select the token type and enter the required details. When you are finished, click **Generate**.
4. A pop-up window appears with the token.

   Note: Make sure that you copy the token and save it to a safe location. You can no longer view it after you close the window.

5. Use the new token to provide access to your analytics application or share it with Veritas Technical Support. You can access the `metrics` APIs with the metrics token and the `logscollect` APIs with the support token. Check Veritas SORT for more information on the APIs.

Revoking access for external monitoring

Use the following procedure to delete an API access token and remove access privileges for an external monitoring service or Veritas Technical Support.

To delete an API access token

1. Sign in to the Flex Appliance Console as the default **admin** user and click the gear icon in the upper-right corner of the page, then click **API access token**.
2. Select the token that you want to delete and click **Delete**.

Chapter 9

Reconfiguring the appliance

This chapter includes the following topics:

Shutting down the appliance

Use the following procedure to shut down your appliance.

To shut down an appliance

1. Stop all instances from the Flex Appliance Console.
2. Log in to the Flex Appliance Shell and run the following command:

   ```
   system shutdown
   ```

3. If you also need to physically turn off the appliance hardware, press the power button on the storage shelves and unplug the appliance power cable.

Performing a factory reset

The purpose of a factory reset is to return a node to a clean, unconfigured, factory state. A factory reset discards all configuration data but does not affect the storage data. If you have a multi-node appliance, a factory reset only affects the node that you run this procedure from.

A factory reset resets the node to the current version. However, if you installed any security patches, they must be reinstalled after the factory reset.

After you perform a factory reset, you can also reset the storage if your appliance is not in lockdown mode. If it is in lockdown mode, storage reset is disabled.

Note: If more than the Veritas-tested number of Fibre Channel devices or paths are connected to the appliance, Veritas recommends that you disable the ports or disconnect the devices before you begin this procedure. When the procedure is complete, reenable or reconnect them. You may need to rescan the ports from the Fibre Channel interfaces page.

See "Managing the appliance Fibre Channel ports" on page 48.

To perform a factory reset

1. If you have a multi-node appliance, remove the node that you want to reset from the appliance. If you want to reset both nodes, choose a node to begin the procedure with and remove that node. See "Removing a node" on page 125.
2. Log in to the Flex Appliance Shell from the node that you want to reset.

   Note: Veritas recommends that you log in from the Veritas Remote Management Interface instead of an SSH session to perform a factory reset. To access the Veritas Remote Management Interface, refer to the initial configuration procedure. See "Performing the initial configuration" on page 28.

   ---

3. Enter the following command:

   ```
   system factory-reset
   ```

4 Type `yes` to continue, and then press **Enter**.

Note: Once you have started the `factory-reset` operation, do not perform any other tasks on the appliance until the reset is complete.

When the process is complete, you are prompted to restart. The factory reset is not complete until after the system is restarted. The system continues to run with the current configuration until after the restart is completed.

5 Do one of the following:

- To restart the node now, type `yes`, and then press **Enter**.
- To restart the node later, type `no`, and then press **Enter**.
  You can type the following command at any time to restart:
  `system restart`

6 When the restart is complete, the **hostadmin** user password resets to the default password (**P@ssw0rd**). Use the default password to log back in to the Flex Appliance Shell, then run the following command to change the password:

`set user password`

7 If you have a multi-node appliance and want to reset both nodes, repeat the procedure on the other node.

Next steps for a single-node appliance

After the factory reset is complete, do one of the following:

- If you want to delete the existing storage data, perform a storage reset and then perform the initial configuration again to reconfigure your settings.
  This option is not available if your appliance is in lockdown mode.
  See "Performing a storage reset" on page 124.
  See "Performing the initial configuration" on page 28.
- If you do not want to delete the storage data, you can recover the appliance with the existing storage data.
  See "Recovering storage data after a factory reset or a reimage" on page 122.
- If the node was never configured with the `configure-console` command, proceed with the initial configuration.
  See "Performing the initial configuration" on page 28.

Next steps for a multi-node appliance

After the factory reset is complete, do one of the following:

- If you performed the factory reset on only one of the nodes, add it back to the appliance. If the node was previously updated, reinstall the update after you add it back.
  See "Adding a node" on page 31.
  See "Updating Flex Appliance" on page 87.
- If you performed the factory reset on both nodes and want to delete the existing storage data, perform a storage reset and then perform the initial configuration again to reconfigure your settings.
  This option is not available if your appliance is in lockdown mode.
  See "Performing a storage reset" on page 124.
  See "Performing the initial configuration" on page 28.
- If you performed the factory reset on both nodes and do not want to delete the storage data, you can recover the appliance with the existing storage data.
  See "Recovering storage data after a factory reset or a reimage" on page 122.

Performing a reimage

The purpose of a reimage is to remove and reinstall the appliance software on a node. Veritas recommends that you always try a factory reset before resorting to a reimage.

A reimage does not affect the storage data. After you perform a reimage, you can also reset the storage if desired.

Warning: This procedure cannot be run on a Veritas 5340 Appliance. If you need to reimage a 5340 node, you must contact Veritas Technical Support. Ask your representative to reference article 100044669.

Use one of the following procedures to reimage an appliance.

Reimaging from the USB drive

To reimage an appliance from the USB drive

1. Before you begin the reimage process, Veritas recommends that you record the configuration information that you entered when you performed the initial configuration.
2. Verify that the following ports are connected to the network:
   - The remote management (IPMI) port
     Used to connect to the Veritas Remote Management Interface
   - host0

Used to connect to the Flex Appliance Console

3. Insert the USB drive into a USB port on the node that you want to reimage.
4. Use the following steps to access the Veritas Remote Management Interface:
   - Open a supported web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:
     - Google Chrome version 94 or later recommended (minimum version 80 or later)
     - Mozilla Firefox version 93 or later recommended (minimum version 80 or later)
   - Enter the IP address that is assigned to the remote management port of the node that you want to reimage.
   - Log in to the Veritas Remote Management Interface. If you have not previously logged in, use the following default credentials:
     - **User Name**: **sysadmin**
     - **Password**: **P@ssw0rd**
5. If you logged in with the default password, you must change the password before you can configure or recover the appliance after the reimage. Perform the following steps:
   - Navigate to **Configuration** > **Users** and select the **sysadmin** user.
   - Click **Modify User**.
   - Select the **Change Password** check box and enter a new password.
6. Do one of the following to launch the Flex Appliance Shell:
   - Navigate to **Remote Control** > **Console Redirection** and click **Launch Console**.
   - If available, navigate to **Remote Control** > **iKVM over HTML5** and click **Launch Console over HTML5**.

Note: Availability of the HTML5 option depends on the appliance firmware version. You can check the version from the **System** > **System Information** page. The BIOS ID must show version 00.01.0016 or later.

---

7. Return to the Veritas Remote Management interface and select **Server Power Control** on the left side of the **Remote Control** page.
8. On that page, do the following:

- Select the **Reset Server** radial option.
- Click **Perform Action**.

9 Return to the Flex Appliance Shell and wait for the system to turn on. When the splash screen appears, immediately press **F6** to enter the **boot** menu.

Note: You only get a window of a few seconds to perform this task. If you miss the window, the operating system loads, and you cannot access the **boot** menu.

---

10 When the **boot** menu appears, scroll down to the USB drive and press **Enter**.

11 The system begins to start from the USB drive. It then presents you with the following options:

- **Boot from local drive**
- **Install Veritas Optimised OS**
- **Rescue a Red Hat Enterprise Linux system**

Select **Install Veritas Optimised OS** and press **Enter**.

12 When the installation of the new appliance package is complete, you receive a **Welcome** message in the Flex Appliance Shell. The **hostadmin** user password resets to the default password (**P@ssw0rd**), so use the default password to log back in to the Flex Appliance Shell. Then run the following command to change the password:

```
set user password
```

13 Restart the node with the `system restart` command.

14 Proceed to the next steps that are listed at the end of this topic.

Reimaging from an ISO image

To reimage an appliance from an ISO image

1 Before you begin the reimage process, Veritas recommends that you record the configuration information that you entered when you performed the initial configuration.

2 Verify that the following ports are connected to the network:

- The remote management (IPMI) port
  Used to connect to the Veritas Remote Management Interface
- host0
  Used to connect to the Flex Appliance Console

3. From a computer within your appliance domain, download the appropriate ISO image from the Download Center on the Veritas Support website.
4. Save the ISO image to a local drive of the computer.
5. If a firewall exists between the appliance and the remote devices that manage the appliance, make sure that the following ports are open:
   - 627 RMM ISO/CD
   - 5902 RMM CLI
6. Turn off the appliance.
7. Use the following steps to access the Veritas Remote Management Interface:
   - Open a supported web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:
     - Google Chrome version 94 or later recommended (minimum version 80 or later).
     - Mozilla Firefox version 93 or later recommended (minimum version 80 or later). Note that reimaging over HTML5 is not supported on Firefox.
   - Enter the IP address that is assigned to the remote management port of the node that you want to reimage.
   - Log in to the Veritas Remote Management Interface. If you have not previously logged in, use the following default credentials:
     - **User Name**: **sysadmin**
     - **Password**: **P@ssw0rd**
8. If you logged in with the default password, you must change the password before you can configure or recover the appliance after the reimage. Perform the following steps:
   - Navigate to **Configuration** > **Users** and select the **sysadmin** user.
   - Click **Modify User**.
   - Select the **Change Password** check box and enter a new password.
9. Do one of the following to launch the Flex Appliance Shell:
   - (Recommended) Navigate to **Remote Control** > **Console Redirection** and click **Launch Console**.
   - If you are using Google Chrome and the option is available, navigate to **Remote Control** > **iKVM over HTML5** and click **Launch Console over HTML5**. Note that the performance of HTML5 is significantly slower.

Note: Availability of the HTML5 option depends on the appliance firmware version. You can check the version from the **System** > **System Information** page. The BIOS ID must show version 00.01.0016 or later.

10 If you clicked **Launch Console**, perform the following steps:

- When the shell launches, click on the **Device** drop-down menu on the console and select **Redirect ISO**.
- From the **Open** pop-up window that appears, choose the ISO image that you want to install and click **Open**.

11 If you clicked **Launch Console over HTML5**, perform the following steps:

- Navigate to **Virtual Media** > **Virtual Media over HTML5** and click **Launch virtual media over HTML5**.
- In the pop-up window that appears, click **Choose file** and select the ISO image that you want to install, then click **Open**.
- From the **Virtual Media** > **Virtual Media over HTML5** page, click **Mount**.

12 Return to the Veritas Remote Management interface and select **Server Power Control** on the left side of the **Remote Control** page.

13 On that page, since the server is currently off, the only available option is **Power ON Server**.

Click **Perform Action**.

14 Return to the Flex Appliance Shell and wait for the system to turn on. When the splash screen appears, immediately press **F6** to enter the **boot** menu.

Note: You only get a window of a few seconds to perform this task. If you miss the window, the operating system loads, and you cannot access the **boot** menu.

15 When the **boot** menu appears, scroll down to **Virtual CDROM** and press **Enter**.

16 The system begins to start from the ISO image you selected earlier. It then presents you with the following options:

- **Boot from local drive**
- **Install Veritas Optimised OS**
- **Rescue a Red Hat Enterprise Linux system**

Select **Install Veritas Optimised OS** and press **Enter**.

Note: The remote management ISO installation is sensitive to the quality of the network connection. If an installation failure occurs, try the installation again. If the problem persists, try to improve the quality of the remote management network connection. You can also burn the ISO image onto a DVD and install it with a USB DVD-ROM drive that you physically connect to the appliance.

17 When the installation of the new appliance package is complete, you receive a **Welcome** message in the Flex Appliance Shell. The **hostadmin** user password resets to the default password (**P@ssw0rd**), so use the default password to log back in to the Flex Appliance Shell. Then run the following command to change the password:

```
set user password
```

18 Restart the node with the `system restart` command.

19 Proceed to the next steps that are listed at the end of this topic.

Next steps for a single-node appliance

After the reimage is complete, do one of the following:

- If you want to delete the existing storage data, perform a storage reset and then perform the initial configuration again to reconfigure your settings.
  This option is not available if your appliance is in lockdown mode.
  See "Performing a storage reset" on page 124.
  See "Performing the initial configuration" on page 28.
- If you do not want to delete the storage data, you can recover the appliance with the existing storage data.
  See "Recovering storage data after a factory reset or a reimage" on page 122.
- If the node was never configured with the `configure-console` command, proceed with the initial configuration.
  See "Performing the initial configuration" on page 28.

Next steps for a multi-node appliance

After the reimage is complete, do one of the following:

- If you reimaged only one of the nodes, remove the node from the appliance and then add it back to the appliance. If the node was previously updated, reinstall the update after you add it back.
  See "Removing a node" on page 125.
  See "Adding a node" on page 31.
  See "Updating Flex Appliance" on page 87.

- If you reimaged both nodes and want to delete the existing storage data, perform a storage reset and then perform the initial configuration again to reconfigure your settings.
  This option is not available if your appliance is in lockdown mode.
  See "Performing a storage reset" on page 124.
  See "Performing the initial configuration" on page 28.
- If you reimaged both nodes and do not want to delete the storage data, you can recover the appliance with the existing storage data.
  See "Recovering storage data after a factory reset or a reimage" on page 122.

Recovering storage data after a factory reset or a reimage

If you performed a factory reset or a reimage and want to keep the existing storage data, use the following procedure to recover the appliance.

Note: If you have a multi-node appliance, you only need to use this procedure if you performed a factory reset or a reimage on both nodes. If you only reset or reimaged one of the nodes, add that node back to the appliance. See "Adding a node" on page 31.

To recover the appliance

1. Make sure that no new storage has been attached to the appliance that was not added to the appliance before the factory reset or the reimage.
2. Log in to the Flex Appliance Shell. If you have a multi-node appliance and performed a factory reset on both nodes, log in to the node that you did not remove from the appliance. If you reimaged both nodes, select one of the nodes to perform this procedure on and log in to that node.
3. Run the following command to reconfigure the network:

   ```
   setup configure-network
   ```

   Follow the prompts to enter the host network information.

   Note: Make sure that you enter the same settings that were configured before the factory reset or the reimage.

   ---

4 Run the following command:

```
system appliance-recover
```

Warning: If you have a multi-node appliance, do not run the `system appliance-recover` command from both nodes.

5 Follow the prompts to recover the appliance.

Note: If the recovery fails, you must restart the node before you retry the recovery.

6 If you have a Veritas 5150 Appliance or a Veritas 52xx Appliance, add the applications that you have instances of and the add-ons that are installed on them to the repository before you start the instances. See “Adding files to the repository” on page 70.

7 If you have a multi-node appliance, add the node that you did not recover back to the recovered appliance. See “Adding a node” on page 31.

8 If your appliance previously had security patches installed, reinstall them. See “Updating Flex Appliance” on page 87.

Note: If the Flex Appliance Console was open before the appliance reset and recovery, open a new session after appliance recovery.

Features that must be reconfigured after an appliance recovery

If any of the following features were previously configured on the appliance, note that the settings cannot be saved during a recovery. Make sure that you reconfigure them after the recovery.

- Call Home
  See “Configuring Call Home” on page 101.
- Email alerts
  See “Configuring email alerts” on page 102.
- API access tokens

Note: The previous access tokens still appear after the recovery, but they are shown as **Inactive**. Delete all inactive tokens and generate new ones.

See “Revoking access for external monitoring” on page 112.
See “Providing access for external monitoring” on page 111.

- The appliance metadata for single sign-on (SSO)
  After a recovery, the appliance metadata file changes. Copy or download the new file and upload it to your identity provider (IDP).
  See the section called “Adding an IDP” on page 60.
- AMS registration
  You can reregister the appliance from the **Settings** > **Management server** page of the Flex Appliance Console. See the *Appliance Management Guide* for more information.

Performing a storage reset

The purpose of a storage reset is to remove existing data and instances. In most cases, you should perform a storage reset after a factory reset or a reimage. Make sure that the factory reset or the reimage completed successfully on all appliance nodes before you begin a storage reset.

Storage reset is not available if your appliance is in lockdown mode.

Warning: If you have a multi-node appliance, resetting the storage from one node removes the data for both nodes.

To perform a storage reset

1. Log in to the Flex Appliance Shell. If you have a multi-node appliance and performed a factory reset on both nodes, log in to the node that you did not remove from the appliance. If you reimaged both nodes, select one of the nodes to perform this procedure on and log in to that node.
2. Run the following command:

   ```
   system storage-reset
   ```

3. Enter **yes** to continue, and then enter **DELETE DATA** to confirm.

   Note: Do not perform any other tasks on the appliance until the `storage-reset` operation is complete.

   ---

4. Perform the initial configuration again to reconfigure the appliance.

Removing a node

Use the following procedure to remove a node from a multi-node Flex appliance.

Note: If your appliance is in lockdown mode, removing a node also removes the lockdown mode on that node. This change does not go into effect until you physically disconnect the removed node from the shared storage shelves.

To remove a node

1. From the Flex Appliance Console, make sure that there are no instances running on the node that you want to remove. Use the **System topology** page to view all of the running instances and relocate them as necessary.
2. Log in to the Flex Appliance Shell on the node that you want to keep in the appliance. Run the following commands and check which node the `infra_svc` service is running on:

   ```
   support shell
   ```

   ```
   hastatus -sum
   ```

3. If the `infra_svc` service is running on the node that you want to remove, run the following command to move it to the other node:

   ```
   system ha-service migrate service=infra_svc node=<node hostname>
   ```

   Where *<node hostname>* is the hostname of the node that you do not want to remove.

   You can check the status of the migration with the following commands:

   ```
   support shell
   ```

   ```
   hagrp -state
   ```

4. Once you have verified that the `infra_svc` is not running on the node that you want to remove, run the following command to remove it:

   ```
   setup remove-node
   ```

   Follow the prompts to remove the node.

   Note: Do not perform any other tasks on the appliance until the `remove-node` operation is complete.

   ---

5 When the `remove-node` operation is complete, disconnect the removed node from the shared storage shelves.

6 If you plan to add this node back to the original appliance or use it in another Flex multi-node appliance, you must first perform a factory reset. See "Performing a factory reset" on page 114.

Viewing or resetting the storage shelf order on a Veritas 52xx Appliance

The appliance hardware monitoring assigns IDs to the storage shelves to make sure that each one can be uniquely identified. If you remove or replace a storage shelf on a 52xx appliance, you need to reset the storage shelf order for proper monitoring. Use the following procedure to view or reset the shelf order.

To view or reset the storage shelf order

1 Log in to the Flex Appliance Shell.

2 Run one of the following commands:

- To view the storage shelf order: `support show-shelf-order`
- To reset the storage shelf order: `support reset-shelf-order`

Chapter 10

Troubleshooting guidelines

This chapter includes the following topics:

General troubleshooting steps

If you experience any issues with Flex Appliance, use the following steps as a guide to help you resolve the problem.

Table 10-1 Steps for troubleshooting Flex Appliance problems

Step	Action	Description
Step 1	Note the error message	Error messages are usually the vehicle for telling you something went wrong. If you receive an error message, first follow any troubleshooting steps that are listed in the message. Some error messages begin with a Unique Message Identifier (UMI) code. UMI codes consist of the letter V followed by a string of numbers in the following format: V-123-456-789. To find additional troubleshooting information for specific error messages, perform a search for the message or the UMI code on the Veritas Support website.

Table 10-1 Steps for troubleshooting Flex Appliance problems *(continued)*

Step	Action	Description
Step 2	Check the appliance monitoring information	If you cannot resolve the issue based on the error message, or if you don't see an error message in an interface but still suspect a problem, you can: ■ Use the hardware monitoring information to check for hardware errors. See "Viewing the hardware status" on page 105. ■ Run an appliance self-test. See "Viewing system data" on page 109. ■ Use the `support shell` command to access additional read-only information on the appliance.
Step 3	Gather information for Technical Support	If you cannot resolve the issue on your own, you may need to contact Technical Support for assistance. Before you contact Support, gather the following information: ■ Relevant error messages Record or take screen shots of any error messages you received, including the UMI code if applicable. ■ Data Collect logs Generate a Data Collect log package from the Flex Appliance Console. See "Gathering logs" on page 129. ■ Appliance serial number Locate and record the serial number of the appliance node. If you have a multi-node appliance, record the serial number of both nodes. For more information on locating serial numbers, see the *Product Description* guide for your particular appliance hardware. Also make sure that Call Home is enabled for maximum supportability.
Step 4	Contact Technical Support	Contact Veritas Technical Support from the Veritas Support website.
Step 5	If your appliance is in lockdown mode, you may need to unlock access for support	If your appliance is in lockdown mode, you may need to generate a One-Time Password (OTP) to allow Veritas Technical Support greater access to troubleshoot the issue. The OTP has a two-hour expiration period, so make sure that your support representative is ready for the password before you generate it. See "Generating a One-Time Password and unlocking access in lockdown mode" on page 128.

Generating a One-Time Password and unlocking access in lockdown mode

If your appliance is in lockdown mode and you need assistance from Veritas Technical Support, you may need to generate a One-Time Password (OTP) to allow your representative greater access to troubleshoot the issue. The OTP has a

two-hour expiration period, so make sure that your support representative is ready for the password before you generate it.

To generate an OTP and unlock access to the appliance

1. Log in to the Flex Appliance Shell and run the command `support generate-otp`. A 6-digit number displays, as in the following example. This number is the OTP.

```
[flex-2.0] n8-h72 > support generate-otp
>> Enter hostadmin's password:
   One-time password: 749264
Operation completed successfully
```

2. Send the OTP to your support representative. If you forget the OTP, you can use the command `support show-otp` to view it again.
3. When your representative asks you to, enter the command `support unlock`. You are prompted for a security key, which your representative must generate using the OTP. Enter the security key to unlock the appliance.
4. When your support representative is done troubleshooting the issue, enter the command `support lock` to close access to the appliance. Alternatively, it closes automatically after 12 hours.

Gathering logs

Logs provide support personnel detailed information about your appliance. You can share these logs with the Veritas Support team to resolve issues.

The following log packages are available on a Flex appliance:

- Appliance OS
  This log package includes the Flex Appliance software, high availability, and OS static logs.
- Data Collect
  This log package includes debugging information for the system. It provides a more complete view of the overall system status, which is helpful for technical support representatives.
  As part of a Data Collect package, you can also choose to include the following:
  - Application instance logs
  - Advanced logs
    These logs are helpful for storage and hardware failures.
- Performance

This log package includes performance and configuration data from the appliance and the application instances.

To generate and download an Appliance OS or Data Collect log package

1. From the Flex Appliance Console, click the question mark icon in the upper-right corner of the page, then select **Diagnostics**.
2. Click **Generate log package**.
3. Select the node or nodes that you want to view logs for and the log type, then click **Generate**. Note that the Data Collect logs may take a long time to generate. When the operation is done, the generated log package appears in a table on the **Diagnostics** page.

   Note: The logs that are generated from the Flex Appliance Console mask user information such as hostnames, IP addresses, usernames, etc. The masking process may take some time to complete. It is not currently possible to disable the masking option from the console. If you need to view the user information or want to speed up the log collection, generate the logs from the Flex Appliance Shell with the following commands:

   ```
   support data-collect advanced mask=off

   support data-collect advanced-and-appdata mask=off

   support data-collect appliance-os mask=off
   ```

   ---

4. To download the log package, select it in the table and click **Download**. A pop-up window appears that lets you limit the download bandwidth. Select this option if needed, then click **Download** to confirm.

To generate and download a Performance log package

1. Log in to the Flex Appliance Shell and run one of the following commands:
   - To generate the log package immediately:

     ```
     support data-collect performance at=now
     ```

   - To generate the log package later:

     ```
     support data-collect performance at=<yyyy-MM-dd-HH:mm>
     ```

     Where *<yyyy-MM-dd-HH:mm>* is the year, month, day, hour, and minute when you want to generate the log package.
     For example, to collect the logs on August 3, 2023 at 6:30 P.M., run the following command:

     ```
     support data-collect performance at=2023-08-03-18:30
     ```

Note: You can only run or schedule one log generation at a time. To check if any log generations are already scheduled, use the `support data-collect list-job` command.

2 Depending on your environment, the logs take approximately one hour to generate. When they are ready, they appear in the table on the **Diagnostics** page of the Flex Appliance Console. To access this page from the console, click the question mark in the upper-right corner and select **Diagnostics**.

3 To download the log package, select it in the table and click **Download**. A pop-up window appears that lets you limit the download bandwidth. Select this option if needed, then click **Download** to confirm.

To delete a log package

1 From the Flex Appliance Console, click the question mark icon in the upper-right corner of the page, then select **Diagnostics**.

2 Select the log package that you want to delete and click **Delete**. When the confirmation window appears, click **Delete** to confirm.