Veritas Flex Appliance Getting Started and Administration Guide

Release 2.0

VERITAS™

Veritas Flex Appliance Getting Started and Administration Guide

Last updated: 2021-03-05

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 master server
  You can also configure a BMR master 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)
  - AdvancedDisk
  - Cloud Catalyst

Note: You cannot use both MSDP and Cloud Catalyst storage in the same application instance.

- NetBackup WORM storage

For a full list of supported applications and versions, 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 5340 Appliance, supporting PCIe-based I/O configurations A, G, and H.
- An additional 5340 compute node for high availability (HA).

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

- 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 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 upgrades and 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.
Flex Appliance upgrade	A Flex Appliance release that removes and replaces the currently running version. An upgrade release contains new features, enhancements, and fixes.
Flex Appliance update	A Flex Appliance release that modifies the currently running version but does not replace it. An update release is primarily comprised of fixes, though it may also include enhancements.

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 5340 Appliance Hardware Installation Guide*

- The *Veritas 5340 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.

Flex Appliance 2.0 new features, enhancements, and changes

The following list describes the new features, enhancements, and changes in the Flex Appliance 2.0 release:

- Some of the content that used to be in this manual has been moved to new *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.
- This release supports VMware and Tape out backups over Fibre Channel on the Veritas 5340 Appliance. As part of this enhancement, Flex Appliance now supports the 5340 appliance PCIe-based I/O configurations A, G, and H.
  See “Managing the appliance Fibre Channel ports” on page 37.
- This release introduces 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 72.
- Starting with this release, password changes are enforced during initial configuration to make sure that the default password does not remain active on the system.
- You can now change the password policy for local Flex Appliance Console users and the **hostadmin** user in the Flex Appliance Shell. You also have the option to use the Security Technical Implementation Guides (STIGs) for validation of the policy.

See “Changing the password policy” on page 42.

- You can now expire the password of a local Flex Appliance Console user. Expiring a user password forces that user to change their password the next time that they sign in.
  See “Expiring a user password in the Flex Appliance Console” on page 49.
- This release also includes security enhancements related to user sessions and password protection, as well as OS hardening.
  See “Security overview” on page 71.
- The appliance hardware monitoring now sends alerts for high disk usage. The default threshold is 80%, or you can change the threshold from the Flex Appliance Shell.
  See “Configuring Call Home settings” on page 79.
- You can now gather logs from the Flex Appliance Console.
  See “Gathering logs” on page 100.
- OpenStorage (OST) plug-ins are now supported on all versions of NetBackup media server instances.
  See “Managing application add-ons on instances” on page 60.
- The `show instance performance` command has been replaced with the `support shell` > `ctop` commands.
  See “Viewing instance performance metrics” on page 62.

Supported upgrade paths to this release

The following describes the supported direct upgrade paths and two-step upgrade paths for Flex Appliance version 2.0:

- Direct upgrade path
  You can upgrade directly from version 1.2, 1.3, or 1.3.1 to version 2.0.
- Two-step upgrade path
  Any appliance running version 1.1 must first be upgraded to version 1.2. If you have a multi-node appliance, upgrade both nodes to version 1.2 before you upgrade to version 2.0.

Operational notes

This topic explains important aspects of Flex Appliance 2.0 operations that may not be documented elsewhere in the documentation.

Software operational notes

The following list contains the notes and the known issues that apply for the Flex Appliance 2.0 software:

- The upgrade to version 2.0 requires at least 100 GB of free storage space. Before you begin, check your storage allocations and resize your instance storage if necessary to make sure you have enough space.
- If you select and then deselect an instance in the **Application instances** section, the instance operation buttons remain enabled. If you click on any of these operations when no instance is selected, the operation runs on the most recently selected instance.
- When you add a file to the repository, the memory usage of the appliance infrastructure service increases from 100 MB to 10 GB. If your appliance has high memory usage, you can restart the infrastructure service instance to reset the memory usage to 100 MB. Use the following steps:
  - If you have a multi-node appliance, run the `show appliance status` command and locate the `infra_svc` service in the output. Note the hostname of the node that the instance is running on.
  - Run the following commands to stop and start the `infra_svc` service:

    `set appliance offline service_group=infra_svc node_name=<node hostname>`

    `set appliance online service_group=infra_svc node_name=<node hostname>`
- VMware SAN backups over Fibre Channel may fail when the datastore is on an LSI storage array that is configured in active/passive (A/P) mode. The backup jobs that use SAN transport mode fail with the following error:
  “Error opening the snapshot disks using given transport mode: Status 23”
  If you see this error, configure the LSI storage in Asymmetric Logical Access Unit (ALUA) mode by following the procedure from the storage vendor. The procedure may involve upgrading the storage array firmware to a version that supports ALUA mode, and unmapping and remapping the LSI storage LUNs to the Flex 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. Then retry the VMware SAN backup.
  If you need assistance with this issue, contact Veritas Technical Support and ask your representative to reference article 100048704.
- During a rollback after an instance upgrade, the Activity Monitor may erroneously show **Clear state** tasks with the following error message:
  "Failed to clear the fault on <*instance_ID*>_<*version*>_appVols on <*node_name*>. Check /log/nodeworker/worker.log and VCS logs for more details."

If you see this error during a rollback, it can be safely ignored. Continue to monitor the task to make sure that the rollback completes successfully.

- 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 **Apply 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.
- Depending on the current activity of your application instances, the **System topology** page may take up to a few minutes to load completely. If your application instances do not display when you sign in, wait a few minutes and check again.
- After a warning message displays to let you know that your password is about to expire, you can no longer sign out of the Flex Appliance Console because an “invalid token” error occurs. In addition, if you refresh the page, you are redirected to the sign-in page. To avoid this issue, change your password as soon as the warning message displays.
- If you upgrade an application instance that has an OpenStorage (OST) plug-in installed on it, you must reinstall the plug-in after the upgrade is committed successfully.
- In certain scenarios, the **Fibre Channel** page may briefly appear in the Flex Appliance Console on the Veritas 5150 Appliance. Fibre Channel is not currently supported on the 5150 appliance. If you see the page appear and it does not go away on its own, clear cookies on your browser, then sign out and sign back in.
- When you power cycle or restart a Veritas 5150 Appliance, the Flex Appliance Shell becomes available when the restart is complete. The Flex Appliance Console requires an additional three minutes before you can try to sign in.
- After you upgrade an appliance to this release or configure a new appliance with this release, the `system hardware-errors` command may show that the **RAID Information** and the **Disk Information** are **Not Found**. If you experience this issue, wait more than 24 hours and try again. The information should display correctly.
- If Fibre Channel devices are connected to the appliance but you do not have any application instances, “Abort command” messages display in the `/var/log/messages` log. The messages are similar to the following:
  Oct 8 11:13:56 <*hostname*> kernel: qla2xxx [0000:af:00.0]-8804:9: Abort command mbx success cmd=ffff890ecc0a47c0.

If you see these messages, they can be ignored. After you create an application instance and assign the Fibre Channel ports, they should no longer display.

- When you add a file to the repository on the Flex Appliance Console, a delay occurs after the progress bar completes before you are redirected to the Activity Monitor. Wait to be redirected, and then you can monitor the status of the task.
- When you add a large file to the repository, the following issues can occur:
  - If the upload takes longer than 15 minutes due to slow internet speeds, the upload may fail. If you experience this issue, improve your network connection and try again. If the issue persists, you can contact Veritas Technical Support to have a representative manually copy the file to the appliance repository. Ask your representative to reference article 100048789.
  - A “Failed to unmarshal JSON” error message may appear when you sign in to the Flex Appliance Console after the upload. If you experience this issue, close the current tab and open the console in a new window or tab.
- If you upgrade both nodes of a multi-node appliance and then roll back one of them, the Flex Appliance Console still shows the upgraded version on both nodes. The console does not show the correct version until you roll back the second node.
- 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 18. 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 have a tenant whose name or location contains special characters when you upgrade to this release, tenant operations fail after the upgrade. To resolve this issue, edit the tenant name and location so that they do not have special characters.
- If you change the timezone from the Flex Appliance Shell, 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.

- If an appliance node is powered off unexpectedly and then turned back on, an issue can occur that causes the Flex Appliance Console and all application instances to stop working. The Flex Appliance Shell displays the following error when you attempt to log in:

  ```
  Installation status: failed
  ```

  If you encounter this issue, contact Veritas Technical Support for assistance. Ask your representative to reference article 100046737.

- If you upgrade an instance that supports rollback, the 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 65.

- The following error message may display in the Flex Appliance Shell during an upgrade or a factory reset:

  ```
  dracut:Failed to install module bnx2
  ```

  This message displays in error and can be safely disregarded.

- If you attempt to upgrade Flex Appliance to this release when an instance operation is in progress or pending, the upgrade precheck fails with the following incorrect error message:
  "Error: VUF failed to install package."
  If you see this message, check the status of all instance operations and wait until they are complete before you try again. If an instance upgrade is pending, you must commit or roll back that upgrade before you can upgrade the appliance.

- If you upgrade a node and elect not to restart it when prompted, the node must be restarted with the 'restart' command to complete the upgrade. If the node is restarted incorrectly due to a power outage, pressing the power button, or a similar scenario, the remaining upgrade steps fail.
  If you encounter this issue, roll back the node to the previous version and then re-run the upgrade.

- If you have a multi-node appliance and one of the nodes is turned off for any reason, do not restart the other node until they are both online. If a node is restarted while the other node is off, the Flex Appliance Console fails to load.

If you encounter this scenario, contact Veritas Technical Support and ask your representative to reference article 100046118.

- When you create an instance, if you enter the IP address before you select a network interface, the **IP address** field displays the following error message: "IP address does not belong to the selected network's netmask."
  This message still displays after you select the network interface that corresponds to the IP address. To clear the message, click inside the **IP address** field and then click or tab outside of it.
- After some operations in the Flex Appliance Shell, an "Operation successfully" message may display even if a failure occurred. Read all of the messages that display at the end of each task to make sure that no further action is required.
- If you use the `set alerts email-hardware` or `set alerts email-software` command to add an email address for Call Home, you may see an error message similar to the following:

  ```
  [Error] The appliance was able to connect to your SMTP server, but
  either we were not able to authenticate properly, or your SMTP
  server is preventing us from sending emails through it. Please
  check your SMTP server for details.
  V-475-2-1006 : Added email example@veritas.com not usable with
  SMTP server.
  ```

  However, the messages also states that the address was added successfully, as follows:

  ```
  Email address(es) added successfully 1. example@veritas.com
  ```

  If you encounter this message, the email address was added to the appliance successfully, but the test email did not go through. Verify the email address, Sender ID, and SMTP password that you entered on the appliance. If they are all correct, check the settings on your SMTP server.
- It is not currently possible to edit a network bond after it has been created. If you need to edit a bond, you must delete it and then create a new bond with the new settings.
  See "Deleting a network bond" on page 36.
  See "Creating a network bond" on page 34.
- If the VLAN tags do not match between the nodes of a multi-node appliance, the following error appears when you attempt to relocate an instance:
  Failed to clear the fault on <network_interface> on <node_hostname>. Check /log/hostagent.log and VCS logs for more details.
  However, these logs do not include any additional details. If you encounter this issue, check the VLAN tags on the appliance from the **Settings > Network** page. Verify that all of the VLAN tags have been added on both nodes.

- If you run any of the `system hardware-health` commands in the Flex Appliance Shell immediately after starting or restarting the appliance, you may see the following error message:

  ```
  Unable to retrieve hardware information.
  ```

  If you see this error, wait a few minutes and try again. This issue also applies during initial configuration, after you run the `setup configure-network` command.

Flex Appliance 2.0 release content

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

- The Flex Appliance Shell let you log in using the IP address that you set for the Flex Appliance Console even though logging in to the shell with the console IP address is not supported.
- If you created a bond with a bond name that was all numbers, you could no longer create any additional bonds on the appliance.
- If you edited the MTU value of a network interface, the change was not preserved if the node restarted.
- If you removed a node from a multi-node appliance and then performed a factory reset on the node that you removed, the factory reset failed with the following error:

  ```
  Installing VxOS (Note - May take up to 15 minutes) [FAILED]

  Task Name: Generating boot configuration
  Error:
  "AnsibleUndefinedVariable: 'kernel_map' is undefined"
  ```

- If Call Home was enabled but was unable to communicate with the AutoSupport server due to a firewall, the `set alerts email-smtp` and `delete alerts email-smtp` commands took more than a minute to complete.
- If more than one user edited the network of an instance from the Flex Appliance Console at the same time, the second user's changes overwrote the first user's changes.

Chapter 2

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 2-1 Flex Appliance configuration guidelines and checklist

Parameter	Description
Network cabling for the Veritas 5340 Appliance	The following Veritas 5340 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, 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 5340 nodes. ■ privnic1 and privnic0 (multi-node appliances only) Used for communication between nodes. **Note:** These ports are labeled ETH2 and ETH3 on the 5340 nodes. ■ One to ten 10Gb NICs per node Used for the application instances. See the *Veritas 5340 Appliance Hardware Installation Guide* or the *Veritas 5340 Appliance Product Description* for more details.
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. ■ One or two 10Gb NICs Used for the application instances. See the *Veritas 5150 Appliance Hardware Installation Guide* or the *Veritas 5150 Appliance Product Description* for more details.

Table 2-1 Flex Appliance configuration guidelines and checklist *(continued)*

Parameter	Description
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

Required names and addresses	Before the configuration, gather the following information:
	■ (5340 appliance only) IP address for the Flex Appliance Console
	■ (5340 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
	■ Netmask
	■ (Optional) DNS server IP address
	■ DNS domain
	■ (Optional) Search domain
	Note: 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**

Table 2-1 Flex Appliance configuration guidelines and checklist *(continued)*

Parameter	Description
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.
(5340 appliance only) Memory requirements for expanded MSDP storage configurations	For all storage configurations with an aggregate total of all MSDP pools equaling 960TB or larger, Veritas strongly recommends upgrading the memory capacity to 1536GB. For complete details on the supported expanded storage configurations, see the *NetBackup 5340 Appliance Product Description Guide* and refer to the topic "Available appliance storage options".

Performing the initial configuration

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

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 18.

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 57 or higher
     - Mozilla Firefox version 52 or higher
   - 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**

A welcome message appears in the Flex Appliance Shell with the available commands `setup` and `system`.

See "Accessing and using the Flex Appliance Shell" on page 27.

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.

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, use the following steps to add the hostname resolution information to the appliance `Hosts` file:

- Enter the following command:

  ```
  system add-host
  ```

- One at a time, enter the required information for the node and 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 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.

---

8 (Optional) Use the `set date` commands to set the date and time for the appliance. See “Setting the date and time for appliance nodes” on page 32.

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 24.

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 87.

See “Performing a storage reset” on page 95.

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 29.
- Configure at least one network interface. You can configure a physical interface, add a VLAN tag, or create a bond.
  See “Configuring a network interface” on page 36.
  See “Creating a network bond” on page 34.
- Add the applications that you want to use to the repository.
  See “Managing the repository” on page 51.
- Add at least one tenant.
  See “Adding a tenant” on page 44.
- 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.
  See “Registering an appliance” on page 75.

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 5340 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 upgrade version of Flex Appliance, but they can have different update versions. For example, if your existing node has the 1.3.1 update installed on it, you can add a node that is running version 1.3. However, you cannot add a node that is running version 1.2.

   If the existing node is at a lower version that does not meet these requirements, upgrade 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. Contact Veritas Technical Support for assistance and ask your representative to reference article 100044669.

   Veritas also recommends that you install any missing updates after you add the node so that both nodes are running the same version.

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

   - IP address
   - Hostname

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

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

3. If the node that you want to add has existing Fibre Channel connections, disable all Fibre Channel ports that are connected to the storage array.

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 57 or higher
     - Mozilla Firefox version 52 or higher

- 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**

A welcome message appears in the Flex Appliance Shell with the available commands `setup` and `system`.

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.

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

   `setup add-node with-response new_node=<hostname>`, where <*hostname*> is the hostname of the node that you want to add.

   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.

3. 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.
4. 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 38.
5. 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 21.

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, open an SSH session to the appliance node and log in with the username **hostadmin** and the password that you set during

initial configuration. If you have not completed the initial configuration yet or do not want to use an SSH session, you can also access the shell through the Veritas Remote Management Interface. Refer to the initial configuration procedure for instructions.

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

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 21.

Navigating the Flex Appliance Shell

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 monitor the appliance hardware or access privileged operations, including security settings, upgrades, and factory reset
- `show`
  Includes the commands you can use to show the current appliance settings
- `set`
  Includes the commands you can use to modify the appliance settings
- `delete`
  Includes the commands you can use to remove appliance settings

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**.
- You can press **Alt** + **s** at any time to view a list of shell shortcuts and additional features.
- 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 33.

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 57 or higher
   - Mozilla Firefox version 52 or higher

   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 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 5340 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 43.

Navigating the Flex Appliance Console

Use the left-side navigation bar to navigate the Flex Appliance Console. The navigation bar uses icons to indicate the various pages. To see the page names, 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 shows a small overview of the system topology and a getting-started flow for first-time users. 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.

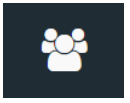
Repository

The **Repository** page lets you manage the applications and upgrade 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.

See “Common tasks in Flex Appliance” on page 33.

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 ntp_servers=<IP address or hostname>
   ```

2. Press **Enter**.
3. 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**.
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 2-2

Task	Quick links
Configuring Flex Appliance	See "Performing the initial configuration" on page 21. See "Adding a node" on page 24.
Managing tenants and users	See "Managing Flex Appliance Console users and tenants" on page 43.
Modifying settings	See "Configuring a network interface" on page 36. See "Creating a network bond" on page 34. See "Setting the date and time for appliance nodes" on page 32.
Configuring Call Home	See "About AutoSupport and Call Home" on page 75. See "Viewing Call Home information" on page 78. See "Configuring Call Home settings" on page 79. See "Deleting and disabling Call Home settings" on page 81.
Monitoring the appliance	See "Monitoring the hardware from the Flex Appliance Shell" on page 82. See "Viewing hardware faults" on page 85. See "Viewing system data" on page 86.
Adding files to the repository	See "Managing the repository" on page 51.
Creating instances	See "Creating application instances" on page 54. See "Managing application instances from Flex Appliance" on page 55.

Chapter 3

Managing network settings

This chapter includes the following topics:

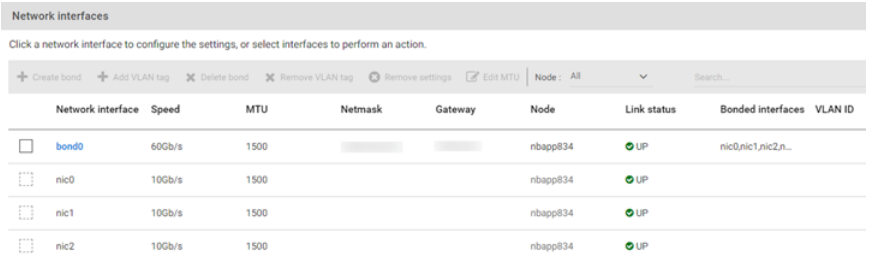
Creating a network bond

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

- balance-tlb - This bond mode is not supported due to a known issue in Red Hat. However, Veritas does not block this bond mode. If you want to use this bond mode, see the following article from Red hat before you proceed: https://access.redhat.com/solutions/67546
- balance-alb - This bond mode is not supported due to a known issue in Red Hat. However, Veritas does not block this bond mode. If you want to use this bond mode, see the following article from Red hat before you proceed: https://access.redhat.com/solutions/67546

4 Click **Create**.

5 Configure the new bond.

See “Configuring a network interface” on page 36.

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 57.

3 Navigate to the **Network interfaces** page and select the bond that you want to delete.

4 Click **Remove settings**.

5 Click **Delete bond**.

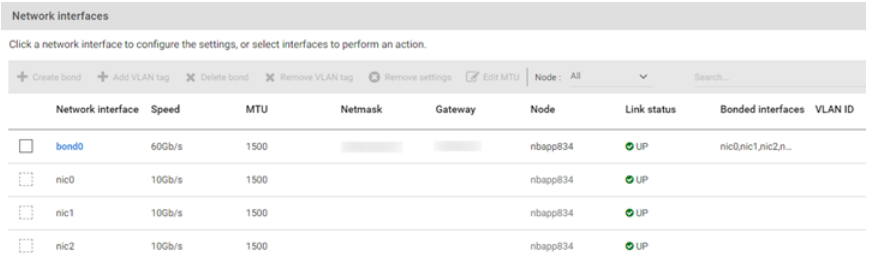
Configuring a network interface

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 a network interface

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 Do one of the following to enter network information:

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

- 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, netmask, and default gateway. Use CIDR format for the netmask and gateway. For example, 172.16.86.0/24.

  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 the netmask and gateway in CIDR format. For example, 172.16.86.0/24.

3 Click **OK**.

See "Creating a network bond" on page 34.

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 38.

Note: The number of Fibre Channel ports on the appliance depends on your hardware configuration. See the *Veritas 5340 Appliance Product Description* for more information.

This release supports VMware and Tape out backups over Fibre Channel.

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 58.

See "Unassigning Fibre Channel ports from an instance" on page 59.

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.

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:

   ```
   system set-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 39.

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 4

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.
- 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 and upgrades, 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.

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**.

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 44.

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 46.
- Active Directory users
  See “Importing an Active Directory user or user group to the Flex Appliance Console” on page 47.

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 all operations except for the following:
  - Enable or disable lockdown mode on the appliance.
  - Edit the password policy.
  - Expire the **admin** user's password, or all users' passwords.

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

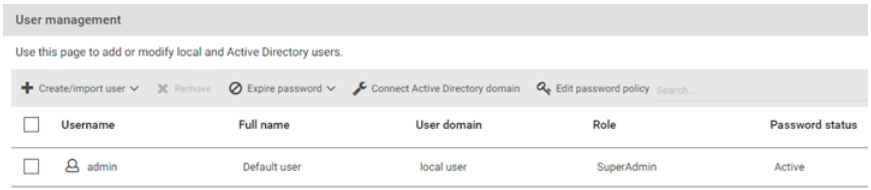
1. On the Flex Appliance Console, click the **Tenants** icon in the left-side navigation bar.
2. Select the tenant that you want to remove, then click **Remove**.

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.



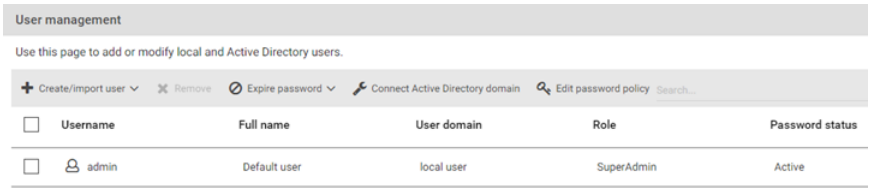
2. Click **Create/import user** > **Add local user**.
3. Enter a username, the user's full name, and a password.
4. Click **Save**.

Connecting an Active Directory domain to the Flex Appliance Console

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

To connect an AD 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 Active Directory domain**.
3. Fill in the required parameters and click **Save**.

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

See "Importing an Active Directory user or user group to the Flex Appliance Console" on page 47.

Importing an Active Directory user or user group to the Flex Appliance Console

Follow these steps to import an Active Directory (AD) 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 AD 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 AD domain that the user or the user group belongs to.

   See "Connecting an Active Directory domain to the Flex Appliance Console" on page 46.
3. Click **Create/import user** > **Import Active Directory 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 AD server to manage the users within a group.

Editing an Active Directory domain in the Flex Appliance Console

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

To edit an AD domain

1. From the **Home** page of the Flex Appliance Console, click the **User management** icon in the left-side navigation bar.
2. Click **Update Active directory domain**.
3. Modify the parameter fields as necessary and click **Save**.

Note: Changing the server name or IP address overwrites the existing AD domain with a new domain. Any imported users or user groups that are not part of the new domain are then unable to log 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 a user from the Flex Appliance Console" on page 49.

Changing a user password in the Flex Appliance Console

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

Note: Active Directory 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 42.
5. Click **Save**.

Expiring a user password 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 a local user or the default **admin**user.

To expire a user password

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 if you are signed in as the **admin** user, click **Expire password** > **Expire all users**.

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

Removing a user from the Flex Appliance Console

Follow these steps to remove a user.

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

To remove a user

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

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 42.

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 5

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 upgrade 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 upgrades and updates**

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

Use the Repository tabs to do the following:

- Add files to the repository
  See "Adding files to the repository" on page 52.
- Remove the current Flex Appliance upgrade or update package from the repository
  See "Removing the current appliance upgrade or update package from the repository" on page 53.
- Update Flex Appliance
  See "Updating Flex Appliance" on page 69.

Adding files to the repository

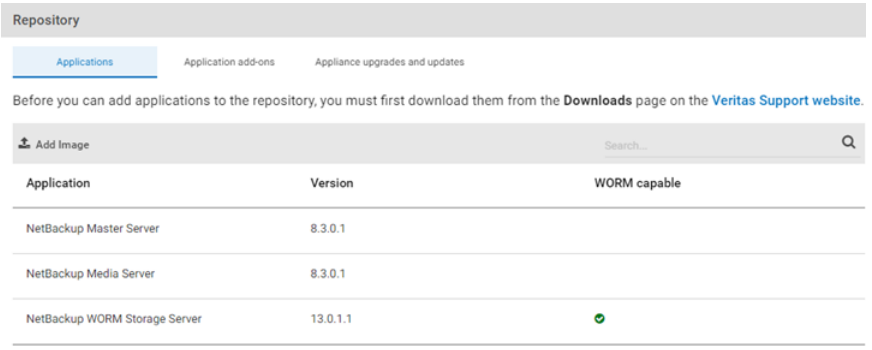
Use the following procedure to download and add files to the Flex Appliance repository.

Guidelines for adding files to the repository:

- Only add files that have been downloaded from or provided by Veritas.
- Do not change or modify 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 upgrades and updates** tab, depending on the type of file that you want to add.
4. Click **Add Image** 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 upgrade or update package, a progress banner appears at the top of the screen. When the task is complete, the new file should appear 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 the current appliance upgrade or update package from the repository

The Flex Appliance repository can only hold one appliance upgrade or update package at a time. Use the following procedure to remove the current package.

To remove an appliance upgrade or update package 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 **Appliance upgrades and updates** tab.
3. 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 master server
  You can also configure a BMR master 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)
  - AdvancedDisk
  - Cloud Catalyst

  Note: You cannot use both MSDP and Cloud Catalyst storage in the same application instance.

- NetBackup WORM storage server

For a full list of supported applications and versions, 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

See “Managing application instances from Flex Appliance” on page 55.

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.

Note that the following NetBackup features are not supported on application instances:

- Bare Metal Restore boot servers
- IPv6

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 54.
- 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 57.
  - Use the **Manage** drop-down to upgrade it.
    See “Upgrading application instances” on page 63.
- Click on an existing instance to perform the following tasks:
  - View the instance details.
  - Edit the network settings, including IP address and interface pairs.
    See “Editing instance network settings” on page 57.
  - Manage add-ons.
    See “Managing application add-ons on instances” on page 60.
  - Manage the assigned Fibre Channel ports
    See “Assigning Fibre Channel ports to an instance” on page 58.
    See “Unassigning Fibre Channel ports from an instance” on page 59.

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 62.

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.

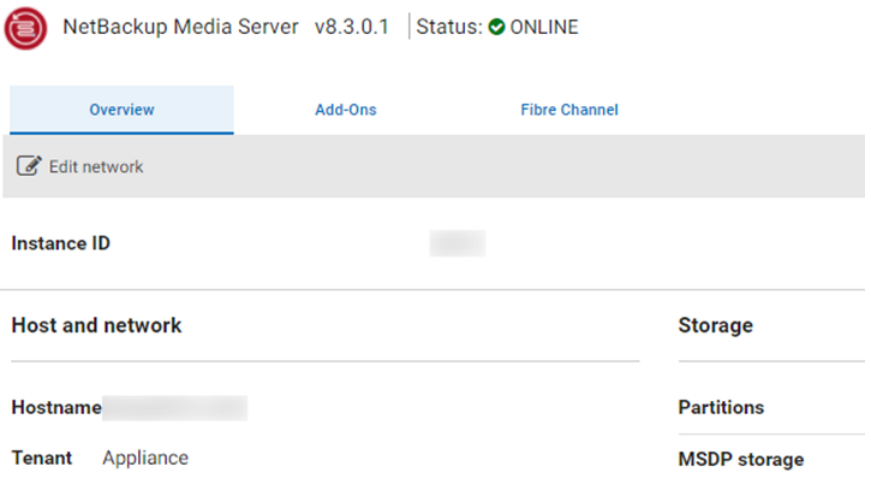
   When the resize is complete, you can view the new storage allocations by clicking on the instance name under **System topology** > **Application instances**.

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 it is running, select it and click **Stop**.
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. If you want to add or remove IP address and interface pairs, click **Manage pairs**.
6. When you are done, click **Save**.

Assigning Fibre Channel ports to an instance

This release supports VMware and Tape out backups over Fibre Channel. To perform backups over Fibre Channel, you must assign ports to your application instances.

Note the following information about port sharing and multipathing:

- Port sharing: You can assign the same port to multiple instances if the instances belong to the same tenant. You can also use the same port for both VMware and Tape out backups.
- Multipathing: The supported configurations depend on the use case, as follows:

- If multiple ports are connected to the same devices and are used for VMware only, those ports can be assigned to a single or to multiple application instances in any combination.
- If the ports are used for Tape out or for both Tape out and VMware, those 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.

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.

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.

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.

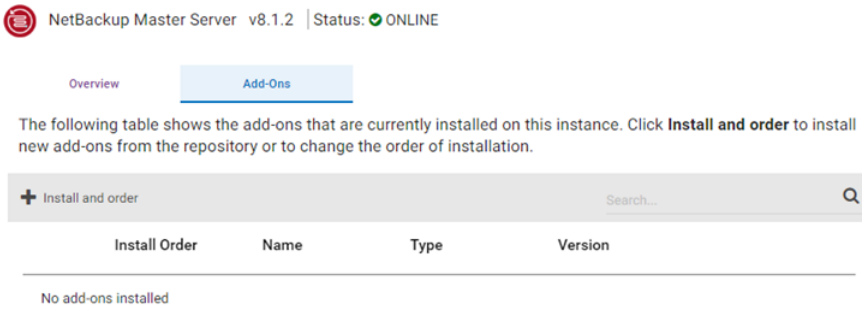
4 Select the port or ports that you want to unassign and click **Unassign ports**.

Managing application add-ons on instances

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

- NetBackup emergency engineering binaries (EEBs)
- 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 60.

See “Uninstalling application add-ons” on page 61.

See “Changing the application add-on installation order” on page 62.

Installing application add-ons

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

To install an add-on

1. Make sure that the add-on you want to install is located in the repository. See "Managing the repository" on page 51.
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-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.
4. Select the instance, then click **Manage** > **Install and order add-ons**. Alternatively, click on the instance name, navigate to the **Add-ons** tab, and click **Install and order**.
5. Select the appropriate add-on from the repository list that appears. If you want to install multiple add-ons, you can select more than one in this step. 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, the one that is installed last takes precedence.

   Note: Changing the add-on installation order is only supported for NetBackup 8.2 and later instances. Although the Flex Appliance Console allows changing the order on an earlier instance, any changes you make do not go into effect.

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. If any of the add-ons have conflicting changes, the one that is installed last takes precedence.

Note: Changing the add-on installation order is only supported for NetBackup 8.2 and later instances. Although the Flex Appliance Console allows changing the order on an earlier instance, any changes you make do not go into effect.

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 and order 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 Enter the following commands:

- `support shell`
- `ctop`

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 51.
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.

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 65.

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 master server instance, check the versions of all media servers and clients that are used with it. The version of the master 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.

See "Upgrading Flex Appliance" on page 67.

Warnings and considerations for instance rollbacks

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

- Instances with Cloud Catalyst storage do not support rollback. Also starting with NetBackup version 8.3.0.1, 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 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 or Cloud Catalyst storage, OST storage, or tape storage. When a rollback of the master 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 master 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 master server and the storage.

    If any backups were deleted after the upgrade and before the rollback, those backups come back as storage leak.

About Flex Appliance upgrades and updates

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

- Upgrades
  An upgrade release contains new features, enhancements, and fixes. An upgrade installs a new version of the Flex Appliance software, including the operating system and the appliance interfaces.
  The version number for an upgrade release includes a single decimal point. For example, 2.0.
- Updates
  An update release is primarily comprised of fixes, though it may also include enhancements. An update modifies the existing version of Flex Appliance by making changes to the operating system, the appliance interfaces, or both.
  The version number for an update release includes the version number of the release it modifies, followed by another decimal point and the update number. For example, 2.0.1 would be an update for release 2.0.

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

See “Upgrading Flex Appliance” on page 67.

See “Updating Flex Appliance” on page 69.

Upgrading Flex Appliance

Use the following procedure to upgrade the Flex Appliance software from version 2.0 to a later release.

To upgrade Flex Appliance

1. On the Flex Appliance Console, click the **Repository** icon in the left-side navigation bar and navigate to the **Appliance upgrades and updates** tab.
2. Make sure that the upgrade package you want to use is located in the repository. See “Managing the repository” on page 51.
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 upgrade first and relocate all of its instances to the other node.

5 On the node that you want to upgrade, use the Veritas Remote Management Interface to log in to the Flex Appliance Shell. If you have a multi-node appliance and chose to relocate instances, log in to the node that has no running instances.

Note: Veritas recommends that you log in from the Veritas Remote Management Interface instead of an SSH session to perform an upgrade. To access the Veritas Remote Management Interface, refer to the initial configuration procedure. See "Performing the initial configuration" on page 21.

---

6 Enter the following command:

```
system upgrade
```

Follow the prompts to enter the file name of the upgrade package and start the upgrade.

Note that the percent complete that shows for the upgrade progress can pause for approximately 15 minutes. This behavior is normal.

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

---

7 After the upgrade processes run, a prompt appears to restart the node. Confirm the restart to complete the upgrade, or you can restart it at a later time with the `system restart apply-upgrade` command.

Warning: If you have a multi-node appliance, do not restart both nodes at the same time.

---

8 If you have a multi-node appliance, refresh your browser cache and sign back in to the Flex Appliance Console to stop or relocate all instances on the other node.

Then repeat the upgrade on the other node.

9 Once the upgrade has completed on all nodes, 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 must upgrade both nodes and complete the rest of this procedure to restore full functionality.

Do one of the following:

- To commit the new version, run the following command.

  ```
  system upgrade-commit
  ```

  If you have a multi-node appliance, you only need to run this command on one of the nodes.

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

  ```
  system rollback
  ```

  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 upgrade. Complete the rollback and restart on the first node before proceeding with the next node.

---

10 The upgrade is now complete. Refresh your browser cache before you sign back in to the Flex Appliance Console.

See "Upgrading application instances" on page 63.

Updating Flex Appliance

Use the following procedure to update the Flex Appliance software from version 2.0 to a later update release.

To update Flex Appliance

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

2 Make sure that the update package you want to use is located in the repository. See "Managing the repository" on page 51.

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

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 21.

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

6 If you have a multi-node appliance, wait for the update process to complete on the selected node, then repeat this procedure on the other node.

7 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 must upgrade both nodes and complete the rest of this procedure to restore full functionality.

Log in to the appliance shell and do one of the following:

- To commit the new version, run the following command.

  ```
  system upgrade-commit
  ```

  If you have a multi-node appliance, you only need to run this command on one of the nodes.

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

  ```
  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 proceeding with the next node.

Chapter 6

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 *Flex Appliances with NetBackup 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 42.
- 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 72.
- Session timeouts that automatically sign users out of the Flex Appliance Console and the Flex Appliance Shell after 10 minutes of inactivity

- 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 5340 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, if smt is disabled, backup performance drops by up to 60%. 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 data. You can use lockdown mode 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 expire all data on the WORM storage instances, and then delete the instances.

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

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 74.

For more information on creating and managing WORM storage instances, see the *NetBackup Application Guide for Flex Appliance*, release 8.3.0.1 or later.

Changing the lockdown mode

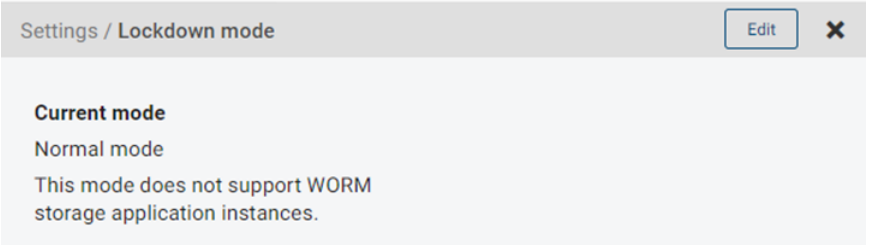
You can use the Flex Appliance Console to change the lockdown mode on a Flex appliance. Note the following restrictions:

- 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**.

Chapter 7

Monitoring the appliance

This chapter includes the following topics:

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.

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.

Call Home provides information regarding appliance component states and status. Call Home is enabled by default. This chapter explains how to view information, configure Call Home, and delete or disable Call Home settings.

More information about AutoSupport and Call Home is available in the *Veritas Appliance AutoSupport 2.0 Reference Guide* at the following site:

Appliance documentation

Registering an appliance

The appliance registration is centralized to the MyAppliance portal.

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.

Registration also provides access to additional reporting capabilities for your appliances, such as:

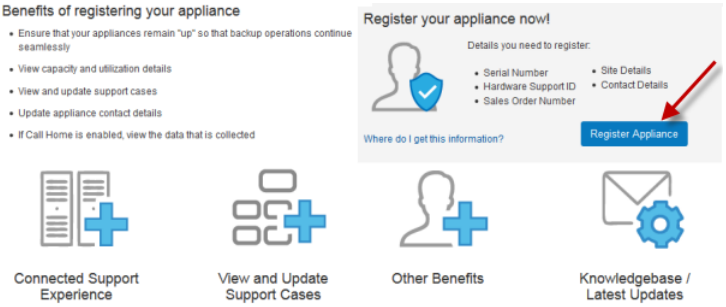
- An overview of all registered appliances
- Capacity and utilization details
- The ability to update contact and site information

Registration also ensures that you are alerted to product updates and other important information about your appliance.

If your appliance has access either directly or through a proxy to the Internet, the registration details populate automatically. If the appliance is not provisioned, the message to verify and update the appliance registration information is displayed.

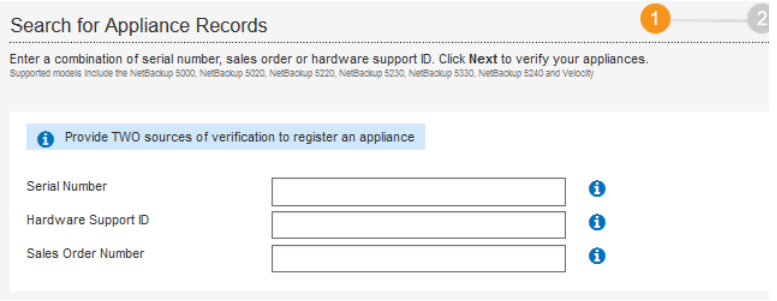
To register an appliance from the MyAppliance portal

1. Log on to the MyAppliance portal and start the registration process with one of the following methods:
   - If it is your first visit to the portal, an information page appears. Click on **Register Appliance**.



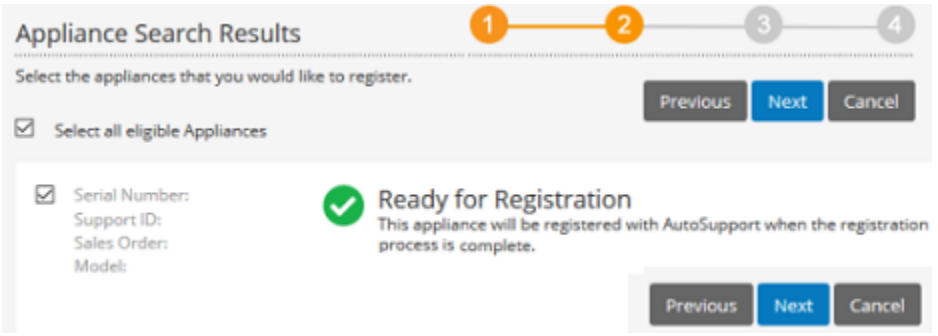
   - If you have previously registered appliances on your account, navigate to **Appliances > My Appliances** page and click on **Register Appliance**.

2 Input the sources of verification. Only two sources are required to register an appliance.



3 Click **Next** to initiate a search.

4 Choose the appliance you want to register.



5 Click **Next** to enter the **Register a New Appliance** page.

Note: Any field highlighted with an asterisk is compulsory for registration. Move to the next step only after you have entered the required information.

---

6 In the basic information column, input your company name.

7 In the **Appliance Location** column, click the **Add New Site** button to create a new site.

8 In the pop-up dialog box, input the site name, site address and other information.

9 In the **Select Site** filed, choose the site you created .

10 In the **Contact Information** column, click the **Add New Contact** button to create a new primary contact person.

11 In the pop-up dialog box, input contact name, email address, phone number and other information. You can add a total of twenty contacts per appliance.

12 In the **Select Contact** field, choose the contact person you created.

Note: The **Receive Call Home transmission failure alert** option is checked by default to enable alerts in the event that Veritas has not received a valid Call Home data transmission for over 28 hours. The alert will repeat every 24 hours until a valid data transmission is received.

If you have spam filtering enabled, configure your filtering settings to allow emails from this sender ID: appliance.veritas.com.

Uncheck the option if you no longer want to receive an alert from Veritas for Call Home transmission failure.

---

13 Verify the information and click **Submit**.

A notification informs you that your appliance is registered successfully.

Viewing Call Home information

An appliance has the ability to send an email to a local administrator when a hardware failure is detected. You can configure the email address that you want to use for hardware failure notifications from the Flex Appliance Shell. The contents of the email identifies the type of hardware failure that occurred and the status of the failure.

This section provides the information that is specific to the settings and configuration for the Call Home feature.

The available information is provided in the following table.

Table 7-1 Call Home information

Command	Description
`callhome`	Shows the current Call Home settings
`callhome-registration node-name=<node_name>`	Shows Call Home registration information based on the node hostname

Table 7-1 Call Home information *(continued)*

Command	Description
`callhome-test`	Sends a test to verify that Call Home is functional
`diskspace-threshold`	Shows the threshold for high disk usage alerts
`email`	Shows the email and the SMTP settings
`email-test`	Tests SMTP and sends an email about hardware data

To view information about Call Home

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

   ```
   show alerts callhome

   show alerts callhome-registration node-name=<node_name>

   show alerts callhome-test

   show alerts diskspace-threshold

   show alerts email

   show alerts email-test
   ```

2. Press **Enter** after each string to display the information.

Configuring Call Home settings

Call Home is enabled by default. This section provides the specific information for the settings and configuration for the Call Home feature.

The available options are provided in the following table.

Table 7-2 Call Home options

Command	Description
`callhome`	Enable the Call Home feature
`callhome-proxy`	Enable the Call Home proxy server
`callhome-proxy-server`	Enter the Call Home proxy server settings
`callhome-proxy-tunnel`	Enable the Call Home proxy tunneling
`diskspace-threshold`	Set the threshold for high disk usage alerts

Table 7-2 Call Home options *(continued)*

Command	Description
`email-smtp smtp_account=<smtp_account>`	(Optional) Enter the name of the account that is used for authentication to the SMTP server
`email-smtp smtp_password=<smtp_password>`	(Optional) Enter the password for authentication to the SMTP server
`email-smtp smtp_server=<smtp_server>`	Enter the SMTP server that is used to send email
`email-notification-interval interval=<interval>`	Enter the time (in minutes from 1 to 44640) between alert emails that are sent to the administrator. The default value is 1440 minutes.
`email-sender-id email_address=<email_address>`	Enter an email ID or account for emails that are received from the appliance
`email-hardware email_address=<email_address>`	Add hardware administrator email accounts

To configure Call Home settings

1. Log in to the Flex Appliance Shell, and type the following as needed. Press **Enter** after each string to display the information.
2. Enable Call Home.

   ```
   set alerts callhome
   ```

3. Set the Call Home proxy, proxy server, and proxy tunnel.

   ```
   set alerts callhome-proxy
   ```

   ```
   set alerts callhome-proxy-server
   ```

   ```
   set alerts callhome-proxy-tunnel
   ```

4. Set the SMTP server.

   ```
   set alerts email-smtp smtp_server=<smtp_server>
   ```

5. (Optional) Set the SMTP account and password.

   ```
   set alerts email-smtp smtp_account=<smtp_account>
   ```

   ```
   set alerts email-smtp smtp_password=<smtp_password>
   ```

6. Set the interval in minutes between email notifications.

   ```
   set alerts email-notification-interval interval=<interval>
   ```

7 (Optional) Set the threshold for high disk usage alerts. The default threshold is 80%.

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

Where <*value*> is an integer between 1 and 93. If you enter 0, all disk usage alerts are disabled.

Note: Critical disk usage alerts are sent when disk usage exceeds 94%. This threshold cannot be changed.

8 Set the sender and hardware administrator email addresses.

```
set alerts email-sender-id email_address=<email_address>
```

```
set alerts email-hardware email_address=<email_address>
```

You can enter multiple hardware administrator email addresses using a comma-separated list or by running the command once for each email address.

Deleting and disabling Call Home settings

Call Home is enabled by default. You can delete or disable Call Home settings as needed. Call Home is not required, but it serves as a critical step to proactive customer support and incident response for failures.

This section provides the information that is specific to the settings and configuration for the Call Home feature.

The available options are provided in the following table.

Table 7-3 Call Home disable and delete options

Command	Description
`callhome`	Disable the Call Home feature
`callhome-proxy`	Disable the Call Home proxy server
`callhome-proxy-tunnel`	Disable Call Home proxy tunneling
`diskspace-threshold`	Disable high disk usage alerts
`email-sender-id`	Delete the email ID for emails that are received from the appliance
`email-smtp`	Delete the SMTP server that is used by the appliance

Table 7-3 Call Home disable and delete options *(continued)*

Command	Description
`email-hardware email_address=<email_address>`	Delete hardware administrator email accounts

To delete Call Home settings

1. Log in to the Flex shell, and type any of the following as needed. Press **Enter** after each string to display the information.
2. Disable the Call Home feature.

   ```
   delete alerts callhome
   ```

3. Disable the Call Home proxy settings.

   ```
   delete alerts callhome-proxy
   ```

   ```
   delete alerts callhome-proxy-tunnel
   ```

4. Disable high disk usage alerts.

   ```
   set alerts diskspace-threshold threshold=0
   ```

5. Delete the appliance sender ID and the SMTP settings.

   ```
   delete alerts email-sender-id
   ```

   ```
   delete alerts email-smtp
   ```

6. Delete the hardware administrator email address.

   ```
   delete alerts email-hardware email_address=<email-hardware>
   ```

Monitoring the hardware from the Flex Appliance Shell

Use the Flex Appliance Shell to obtain information about hardware components. This interface provides tab-completed items to monitor your Flex appliance.

Before you configure the appliance and your network the `system` command is available to provide hardware monitoring information.

The following section describes the additional commands that are available after configuration is complete.

See “Accessing and using the Flex Appliance Shell” on page 27.

To view the hardware monitoring information

1. Log in to the Flex Appliance Shell.
2. Enter `system` and press **tab** to obtain further options.
3. Use one of the following strings. Enter `all` or a specific component where indicated.
   - `system hardware-health node node_component=<component>`
   - (Veritas 5340 Appliance only) `system hardware-health primaryshelf primaryshelf_component=<component>`
     The parameter `primaryshelf_component` is required.
   - (Veritas 5340 Appliance only) `system hardware-health expansionshelf expansionshelf_component=<component> shelf_id=<shelf number, starting from 1>`
     The parameter `shelf_id` is required.
   - `system hardware-errors`

Refer to the following sections for monitoring information about compute node and storage shelf components.

See "Viewing node information" on page 83.

See "Viewing Primary Storage Shelf information on a Veritas 5340 Appliance" on page 84.

See "Viewing Expansion Storage Shelf information on a Veritas 5340 Appliance" on page 85.

Viewing node information

You can view data about the following compute node components from the shell. Details are provided as needed.

- All (components)
- Connection (Veritas 5340 Appliance only - between the appliance and the Primary Storage Shelf)
- CPU
- DIMM
- Disk
- Fan
- Fibrechannel (Veritas 5340 Appliance only)

- Firmware
- Network
- PCI
- Power
- Product
- RAID
- SSD (Veritas 5150 Appliance only)
- StorageStatus (Veritas 5340 Appliance only)
- Temperature

To view node component health

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

   ```
   system hardware-health node node_component=<component>
   ```

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

Viewing Primary Storage Shelf information on a Veritas 5340 Appliance

You can view data about the following Primary Storage Shelf components from the shell. Details are provided as needed.

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

To view Primary Storage Shelf component status

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

   ```
   system hardware-health primaryshelf
   primaryshelf_component=<component>
   ```

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

Viewing Expansion Storage Shelf information on a Veritas 5340 Appliance

You can view data about the following Expansion Storage Shelf components from the shell. Details are provided as needed.

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

To view Expansion Storage Shelf status

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

  ```
  system hardware-health expansionshelf
  expansionshelf_component=<component>
  ```

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.

   ```
   system 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 7-4 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.
`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 100.

Chapter 8

Reconfiguring the appliance

This chapter includes the following topics:

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.

Note: If you have a multi-node appliance, a factory reset only affects the node that you run this procedure from. If you want to reset both nodes, repeat the procedure on the other node.

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.

To perform a factory reset

1. Log in to the Flex Appliance Shell from the node that you want to reset, and then type the following:

   ```
   system factory-reset
   ```

2. Press **Enter**.

3. 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.

4. 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
     ```

5. 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
   ```

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 95.
  See "Performing the initial configuration" on page 21.
- 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 94.
- If the node was never configured with the `configure-console` command, proceed with the initial configuration.
  See "Performing the initial configuration" on page 21.

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, remove the node from the appliance and then add it back to the appliance.
  See "Removing a node" on page 96.
  See "Adding a node" on page 24.
- 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 95.
  See "Performing the initial configuration" on page 21.
- 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 94.

Performing a reimage on a Veritas 5150 Appliance

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 can only be run on a Veritas 5150 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 a 5150 appliance.

Reimaging from the USB drive

To reimage a 5150 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 57 or higher
     - Mozilla Firefox version 52 or higher
   - 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 Optimized Operation System (Thunder Cloud)**
- **Rescue a Red Hat Enterprise Linux system**

Select **Install Veritas Optimized Operating System (Thunder Cloud)** 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 a 5150 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 57 or higher.
     - Mozilla Firefox version 52 or higher. 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 Optimized Operation System (Thunder Cloud)**
- **Rescue a Red Hat Enterprise Linux system**

Select **Install Veritas Optimized Operating System (Thunder Cloud)** 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

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.
  See "Performing a storage reset" on page 95.
  See "Performing the initial configuration" on page 21.
- 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 94.
- If the node was never configured with the `configure-console` command, proceed with the initial configuration.
  See "Performing the initial configuration" on page 21.

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 on both nodes. If you only reset one of the nodes, add that node back to the appliance. See "Adding a node" on page 24.

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, 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. Make sure that you enter the same settings that were configured before 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.
6. If you have a Veritas 5150 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 52.
7. If your appliance was previously configured for Call Home and email alerts, you must reconfigure the Call Home settings with the `set alerts` commands. See "Configuring Call Home settings" on page 79.
8. 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 24.

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 and run the following command:

   ```
   system storage-reset
   ```

2. 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.

3. 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 command and check which node the `infra_svc` service is running on:

   ```
   show appliance status
   ```

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:

   ```
   set appliance migrate
   ```

   You can check the status of the migration with the `show appliance status service_groups` command.

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 with-response remove_node=<hostname>`, where *<hostname>* is the hostname of the node that you want to remove.

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 87.

Chapter 9

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 9-1 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 9-1 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 "Monitoring the hardware from the Flex Appliance Shell" on page 82. ■ Run an appliance self-test. See "Viewing system data" on page 86. ■ 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 100. ■ 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 99.

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.

To generate and download log packages

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.
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.