Veritas Flex Appliance Getting Started and Administration Guide

Release 4.x

VERITAS™

Veritas Flex Appliance Getting Started and Administration Guide

Last updated: 2024-07-23

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

https://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:

https://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

Product overview

This chapter includes the following topics:

Introduction to Veritas Flex Appliance

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

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

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

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

Flex Appliance supported applications and usage information

Flex Appliance is currently available in English only.

This release is compatible with the following hardware:

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

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

- The Veritas 5260 Appliance, supporting all PCIe-based I/O configurations.
- The Veritas 5250 Appliance, supporting all PCIe-based I/O configurations.
- The Veritas 5150 Appliance, supporting all PCIe-based I/O configurations.

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

Flex Appliance terminology

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

Table 1-1 Common terms

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

Table 1-1 Common terms *(continued)*

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

About the Flex Appliance documentation

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

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

The following documents contain information about the appliance hardware:

- The *Hardware Installation Guide* for your particular model
- The *Product Description* for your particular model
- The *Veritas Appliance Safety and Maintenance Guide*

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

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

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

Chapter 2

Release notes

This chapter includes the following topics:

Flex Appliance 4.0 new features, enhancements, and changes

The following list describes the new features, enhancements, and changes in the Flex Appliance 4.0 release:

- This release of Flex Appliance introduces NetBackup primary server resilience across any two Flex appliances with remote replication. Remote replication saves easy-to-manage replicas of your primary server application instances on another appliance. You can use remote replication to minimize downtime during planned maintenance or troubleshooting activities and as additional protection from a disaster scenario. You can also use remote replication to easily migrate your data from one Flex appliance to another.
  See “About remote replication” on page 92.

- A security administrator user role has been added in this release. A user with the security administrator role can manage users and oversee the security management of the appliance.
  See "Managing Flex Appliance Console users and tenants" on page 46.
- Deleting an application instance now requires multiperson authorization for the following versions:
  - NetBackup primary or media server instances on version 10.3.0.1 or later
  - NetBackup WORM storage server instances on version 19.0.1 or later
  - NetBackup WORM storage server instances on version 19.0 in the following scenarios:
    - The appliance is in compliance lockdown mode.
    - The appliance is in enterprise lockdown mode, and you do not have the security administrator role.

  With multiperson authorization, the application administrator must unlock the deletion option before you can delete the instance. For details, see the topics "Authorizing a primary or a media server instance for deletion" and "Authorizing a WORM storage server for deletion" in the *NetBackup Application Guide*.
- Multifactor authentication is now supported for the Flex Appliance Console and the Flex Appliance Shell. Each user can configure multifactor authentication individually, or a security administrator can enforce multifactor authentication for all console users.
  See "Managing multifactor authentication" on page 61.
- The majority of the actions that you can perform from the **Application instances** section of the **System topology** page have moved from the table header to the Actions menu to the right of each instance. Click the three vertical dots to access the Actions menu.
  See "Managing application instances from Flex Appliance" on page 71.
- You can now reconfigure the appliance network after initial configuration.
  See "Reconfiguring the appliance network" on page 125.
- You can now choose whether or not to mask user data in the log packages that you generate from the Flex Appliance Console.
  See "Gathering logs" on page 144.
- This release introduces the `support storage-shelf shutdown` command to safely shut down the storage shelves on a 53xx appliance. Veritas recommends that you run this command before you physically turn off the storage shelves.
  See "Shutting down the appliance" on page 127.

- The One-Time Password that was previously required to unlock access in lockdown mode has been replaced with an access key. Veritas Support can generate the access key on their own, or you can generate it from System Health Insights.
  See "Unlocking access in lockdown mode" on page 143.
- This release introduces the `show serial-number` command to view the serial number of the node.
- Flex appliances are no longer supported on the Appliance Management Server (AMS).
- The critical alert threshold for disk usage alerts has been changed from 94% to 90%.

Flex Appliance 4.1 new features, enhancements, and changes

The following list describes the new features, enhancements, and changes in the Flex Appliance 4.1 release:

- Starting with this release, Flex Appliance Console user accounts with multifactor authentication become locked for 15 minutes after three sign-in attempts with incorrect codes.

Flex Appliance 4.2 new features, enhancements, and changes

The Flex Appliance 4.2 release includes a variety of fixes. It does not include any new features.

Supported update paths to this release

The following describes the supported update paths to Flex Appliance version 4.x:

- Direct update path
  You can update directly from version 2.1 or later to version 4.x.
- Multi-step update path
  Any appliance running an earlier version must first be updated to version 2.1. If you have a multi-node appliance, update both nodes to version 2.1 before you update to version 4.x.

Operational notes

This topic explains important aspects of Flex Appliance 4.x operations that may not be documented elsewhere in the documentation.

The following list contains the notes and the known issues that apply for the Flex Appliance 4.x software:

- After a new installation or an upgrade to version 4.x, SAN client (Fibre Transport Media Server) backups do not work on NetBackup application instances earlier than version 10.3. To use SAN client on an earlier supported version, you must install an EEB. Versions earlier than 10.0.0.1 must be upgraded before you can install the EEB.
  You can find the EEBs at the following locations:
  - Version 10.0.0.1
  - Version 10.1.1
  - Version 10.2.0.1

  Note: Update the appliance before you upgrade the instance or install the EEB.

- If you have a multi-node appliance with remote replication configured, and a replication error occurs, you may receive a separate alert for the same issue on each node. In addition, if the system is down on one of the nodes when the issue is resolved, you may not receive an email to notify you of the fix until that node is back online.
- When you restart the appliance, the network interfaces temporarily go down and then come back up. Due to this behavior, a failed "Clear state" task sometimes displays in the Activity Monitor, indicating that the network interface is down. If you see this failed task, check the **Network interfaces** page. If the interface shows as **UP**, you can ignore the failed task.
- To use universal shares on NetBackup 10.1 or 10.0.0.1, you must install an EEB on the instance.
  You can find the EEBs at the following locations:
  - Version 10.1
  - Version 10.0.0.1
- For this release, the **Performance** graphs on the Flex Appliance Console **Home** page show data only in the UTC time zone.
- On a multi-node appliance, an issue can occur if you remove a node while that node is powered off. If the node comes back online before you have restarted

the appliance, the removed node is added back to the appliance. If you experience this issue, remove the node again and then immediately restart the appliance.

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

  The messages look similar to the following:

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

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

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

- If the host0 or host1 port is not connected to the appliance node during initial configuration, the following error message appears that does not provide complete information:
  “Network card for *<interface name>* is missing. Make sure that all network interfaces are connected to the appliance.”
  If you encounter this message, verify that all ports are connected according to the initial configuration guidelines. See “Initial configuration guidelines and checklist” on page 19. 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 **Deleted** while the creation is in progress. The **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.
- For this release, the audit log may include incorrect username or group name values for user identifiers (for example, UID and GUID). The log shows the values for the user IDs or group IDs on the appliance instead of the user IDs or group IDs on the application instance.
- When the `rsyslogs` service starts, messages that include the text `avc: denied` and `comm="(rsyslogd)"` may appear in the logs at `/var/log/audit/audit.log`. The `rsyslog` service starts when the appliance starts up or when another service that uses it restarts.
  The messages look similar to the following:
  ```
  node=localhost.localdomain type=AVC msg=audit(1700916265.786:623):
  avc: denied { mounton } for pid=57833 comm="(rsyslogd)"
  ```
  These messages can be ignored.
- If you generate a Data Collect log package and stay on the **Activity Monitor** page for more than 15 minutes, you may see a new task appear on the monitor page. The new task stops immediately with the following message:
  “A Data Collect operation is already in progress. Retry after the task is completed.”
  This issue is fixed in version 4.2.
  On earlier versions, this task displays in error and can be ignored. It has no impact on the generation of the log package.
- When you create an instance, if you change the unit for a volume in the **Storage** section but do not enter a new size, the unit does not update.
  This issue is fixed in version 4.2.
  To work around this issue on an earlier version, you must also enter a new size. Once the unit has updated, you can change the size back to the previous value if needed.

- If you change the threshold for high disk usage alerts, the Flex Appliance Shell lets you set the warning threshold up to 93%. However, the critical threshold that cannot be changed is 90%.
  This issue is fixed in version 4.1.
  On version 4.0, do not set the warning threshold above 89%.
- If a remote replication alert is not resolved before you forget the paired appliance, the alert remains in the alert summary.
  This issue is fixed in version 4.1.
  To clear the alert on version 4.0, refer to the following article: How to clear an unresolved remote replication alert after forgetting an appliance
- If you try to create a replica instance, but the appliance with the active instance does not have enough storage space, the replica creation fails but does not include the reason for the failure.
  This issue is fixed in version 4.1.
  If you experience an undefined failure when you try to create a replica on version 4.0, you can check the logs for more information. To do so, run the `support shell` command in the Flex Appliance Shell and then run the following commands:
  `vi /var/log/nodeworker/inframodule.log`
  `vi /var/log/nodeworker/worker.log`
  Check the logs for the following message:
  V-492-101-102: Not enough space; request size of <*requested space*> MiB is greater than remaining space of <*available space*> MiB. The log volume and the internal data volumes are included in space calculations.

Flex Appliance 4.0 release content

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

- The Linux lspci utility showed an incorrect model number for the SAS storage controller.
- The **Alt** + **s** shortcut in the Flex Appliance Shell was not enabled.
- When you added a node to the appliance either during initial configuration or after, the `system self-test` command failed on the new node if you ran it before you ran `setup add-node`. The following error appeared:
  "Hostagent must not be active on unconfigured appliance"

Flex Appliance 4.1 release content

The following list contains the known issues that were fixed and that are included in the Flex Appliance 4.1 release:

- If you tried to create a replica instance, but the appliance with the active instance did not have enough storage space, the replica creation failed but id not include the reason for the failure.
- If a remote replication alert was not resolved before you forgot the paired appliance, the alert remained in the alert summary.
- If you changed the threshold for high disk usage alerts, the Flex Appliance Shell let you set the warning threshold up to 93%. However, the critical threshold that cannot be changed is 90%.

Flex Appliance 4.2 release content

The following list contains the known issues that were fixed and that are included in the Flex Appliance 4.2 release:

- When you created an instance, if you changed the unit for a volume in the **Storage** section but did not enter a new size, the unit did not update.
- If you generated a Data Collect log package and stayed on the **Activity Monitor** page for more than 15 minutes, you may have seen a new task appear in error on the monitor page. The new task stopped immediately with the following message:
  “A Data Collect operation is already in progress. Retry after the task is completed.”

Chapter 3

Getting started

This chapter includes the following topics:

Initial configuration guidelines and checklist

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

Table 3-1 Flex Appliance configuration guidelines and checklist

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

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

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

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

Parameter	Description

Required names and addresses	Before the configuration, gather the following information:
	■ (53xx appliance only) IP address for the Flex Appliance Console
	■ (53xx appliance only) Hostname for the Flex Appliance Console
	The Fully Qualified Domain Name (FQDN) can be a maximum of 45 characters.
	■ IP address for each node in the appliance
	■ Hostname for each node in the appliance
	The Fully Qualified Domain Name (FQDN) can be a maximum of 45 characters.
	■ Default gateway
	■ (Optional) DNS server IP address
	■ DNS domain
	■ (Optional) Search domain
	Note: You can use IPv4 or IPv6 addresses for the appliance, but a dual-stack network is not supported. The IPv4 and IPv6 protocols are disabled until you complete the initial configuration. After configuration, the protocol that you did not configure remains disabled.
	The following subnets are also reserved for internal use and cannot be used for the appliance network:
	192.168.227.0/24 and fdf8:192:168:227::/120
	192.168.228.0/24 and fdf8:192:168:228::/120
	192.168.229.0/24 and fdf8:192:168:229::/120
	192.168.230.0/24 and fdf8:192:168:230::/120
	If you plan to use DNS, make sure that forward and reverse DNS lookups are configured properly in your environment. If a forward or a reverse DNS lookup returns multiple records, the initial configuration may fail. You can check the DNS configuration with the following commands for each node. Each command should return only one entry.
	Linux:
	`dig +short @<DNS server IP address> a <node FQDN>`
	`dig +short @<DNS server IP address> -x <node IP address>`
	Windows:
	`nslookup <node IP address>`
	`nslookup <node hostname>`

Default username and password	New appliances are shipped with the following default login credentials: ■ Username: **hostadmin** ■ Password: **P@ssw0rd**

Table 3-1 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.

Performing the initial configuration

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

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

See "Managing the appliance Fibre Channel ports" on page 42.

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 19.

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

- Open a supported web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:
  - Google Chrome version 94 or later recommended (minimum version 80 or later)
  - Mozilla Firefox version 93 or later recommended (minimum version 80 or later)
- Enter the IP address that is assigned to the remote management (IPMI) port of the appliance node. If you have a multi-node appliance, select one of the nodes to use to begin the initial configuration.
- Log in to the Veritas Remote Management Interface with the following default credentials:

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

- Change the **sysadmin** password from the known default password as follows:
  - Navigate to **Configuration** > **Users** and select the **sysadmin** user.
  - Click **Modify User**.
  - Select the **Change Password** check box and enter a new password.
- Do one of the following to launch the Flex Appliance Shell:
  - Navigate to **Remote Control** > **Console Redirection** and click **Launch Console**.
  - If available, navigate to **Remote Control** > **iKVM over HTML5** and click **Launch Console over HTML5**.

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

---

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

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

See "Accessing and using the Flex Appliance Shell" on page 30.

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

```
set user password
```

5 Enter the following command to configure the host network:

```
setup configure-network
```

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

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

- Enter the following command:

```
system add-host
```

- One at a time, enter the required hostname information for the following:
  - The node
  - The Flex Appliance Console if the `setup configure-network` prompts asked for it

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

7 Use the `set date` commands to set the date and time. See "Setting the date and time for appliance nodes" on page 35.

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

```
setup configure-console
```

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

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

---

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

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

See "Adding a node" on page 26.

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 128.

See "Performing a storage reset" on page 139.

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 32.

- Configure at least one network interface. You can configure a physical interface, add a VLAN tag, or create a bond.
  See "Configuring or editing a network interface" on page 41.
  See "Creating a network bond" on page 38.
- Add the applications that you want to use to the repository.
  See "Managing the repository" on page 67.
- Add at least one tenant.
  See "Adding a tenant" on page 47.
- Veritas also recommends that you register your appliance to ensure that you receive maximum support in the event of a failure. Registration helps Veritas to contact the right person and to dispatch field services to the correct location for repairs.

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

Adding a node

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

A multi-node appliance provides the following benefits:

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

Adding a second node consists of the following tasks:

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

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

Tasks for adding a node

To perform the host network configuration on the new node

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

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

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

   - IP address
   - Hostname

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
set user password
```

7 Enter the following command to configure the host network:

```
setup configure-network
```

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

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

```
system add-host
```

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

9 Use the `set date` commands to set the date and time. Make sure that the settings are in sync with the other node. See "Setting the date and time for appliance nodes" on page 35.

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
```

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 44.

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 23.

Accessing and using the Flex Appliance Shell

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

Accessing the Flex Appliance Shell

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

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

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

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

- Restarting the node
- Factory resets
- Reimaging

Note: When you access the Flex Appliance Shell through the Veritas Remote Management Interface, do not enter **alt+PrtScn** while a command is running. If you do, the command fails, and it still may not work when you try to rerun it.

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

- Ciphers:
  - aes256-ctr
  - aes192-ctr
  - aes128-ctr
- MACs:
  - hmac-sha2-512
  - hmac-sha2-256

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

Navigating the Flex Appliance Shell

Note: When you log in for the first time, the available commands are limited to those that you can run on an unconfigured appliance. Complete the initial configuration to gain access to the rest of the command options. See "Performing the initial configuration" on page 23.

The Flex Appliance Shell includes the following command views:

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

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

- You can press the **?** key at any time to display more information about the commands or sub-views. If you press **?** after you enter a command, the format and usage of the parameters for that command is displayed.
- To type a **?** without displaying the help, first press **Ctrl** + **v**.
- 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 36.

Accessing and using the Flex Appliance Console

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

Accessing the Flex Appliance Console

To access the Flex Appliance Console

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

   Note: These browsers may display a **Privacy error** or **Insecure Connection** page when you access the Flex Appliance Console. Use the **Advanced** option on the page to proceed.
2. Navigate to **https://*console.domain***, where *console.domain* is one of the following:
   - If you have a Veritas 52xx or 5150 Appliance, *console.domain* is the fully qualified domain name (FQDN) or the IP address that you entered during initial configuration.
   - If you have a Veritas 53xx Appliance, *console.domain* is the fully qualified domain name (FQDN) or the IP address that you entered for the Flex Appliance Console during initial configuration.
3. When you sign in for the first time, use the following default credentials:

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

After you have signed in, you can create other users from the **User management** page. See "Managing Flex Appliance Console users and tenants" on page 46.

Navigating the Flex Appliance Console

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

The Flex Appliance Console includes the following pages:

Home

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

System topology

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

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

Activity Monitor

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

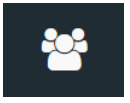
Repository

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

Tenants

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

User management



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

Network interfaces

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

Fibre Channel interfaces

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

Remote replication

The **Remote replication** page lets you configure and manage remote replication with a paired appliance. To access this page, click the **Remote replication** icon in the left-side navigation bar.

Settings

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

See “Common tasks in Flex Appliance” on page 36.

Setting the date and time for appliance nodes

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

Note: NTP is required for multifactor authentication.

To set the date and time using NTP

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

   ```
   set date ntp
   ```

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

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

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

   ```
   set date manual-date
   ```

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

To set the time zone

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

   ```
   set date timezone
   ```

2. Press **Enter**.
3. Type the number that corresponds to your continent or ocean, and then press **Enter**.
4. Type the number that corresponds to your country, and then press **Enter**.
5. Type the number that corresponds to your time zone, and then press **Enter**.
6. Type **1** to verify that the time zone is correct, and then press **Enter**.
7. If you have a multi-node appliance, repeat this procedure on the other node.

Common tasks in Flex Appliance

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

Table 3-2

Task	Quick links
Configuring Flex Appliance	See "Performing the initial configuration" on page 23. See "Adding a node" on page 26.
Managing tenants and users	See "Managing Flex Appliance Console users and tenants" on page 46.
Modifying settings	See "Configuring or editing a network interface" on page 41. See "Creating a network bond" on page 38. See "Setting the date and time for appliance nodes" on page 35.

Table 3-2 *(continued)*

Task	Quick links
Configuring Call Home	See "About AutoSupport and Call Home" on page 113.
Monitoring the appliance	See "Viewing the hardware status" on page 117. See "Viewing hardware faults" on page 121. See "Viewing system data" on page 121.
Adding files to the repository	See "Managing the repository" on page 67.
Creating instances	See "Creating application instances" on page 70. See "Managing application instances from Flex Appliance" on page 71.

Chapter 4

Managing network settings for instances

This chapter includes the following topics:

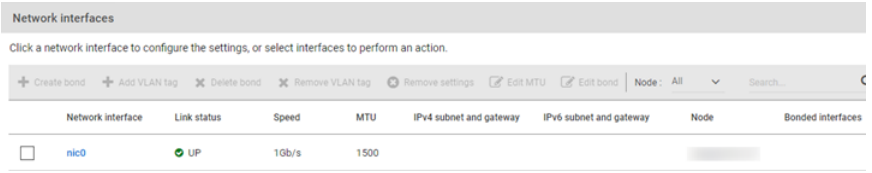
Creating a network bond

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

To create a network bond

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

   It may take a few minutes to load.



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

   The following bond modes are available:

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

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

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

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

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

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

   See “Configuring or editing a network interface” on page 41.

Editing a network bond

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

To edit a network bond

1. From the **System topology** page on the Flex Appliance Console, click on each of your application instances and verify that the bond is not listed in the **IP address and interface pairs** field. If the bond is listed for one or more instances, edit the network of each instance to remove the bond. See "Editing instance network settings" on page 74.

   You may need to add a different IP address and interface pair if the bond that you want to edit is the only interface that is assigned to the instance. If you do not have another available configured interface, configure an interface with placeholder values that you can use until you complete the edits. See "Configuring or editing a network interface" on page 41.

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

Deleting a network bond

Follow these steps to delete a network bond.

To delete a network bond

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

   See "Editing instance network settings" on page 74.

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

Configuring or editing a network interface

The information that you enter when you configure an interface is used to populate the network information fields when you perform operations on the Flex Appliance Console.

To configure or edit a network interface

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

   - Navigate to the **Paired appliances** section of the **Remote replication** page. Verify that the interface is not listed under **Local appliance network interface**.

     If the interface displays in this field, edit the replication network to use a different interface. See "Editing the replication network" on page 97.

   - Navigate to the **Application instances** section of the **System topology** page. Click on each of your application instances and verify that the interface is not listed in the **IP address and interface pairs** field.

     If the interface is listed for one or more instances, edit the network of each instance to remove the interface. You may need to add a different IP address and interface pair if the interface that you want to edit is the only interface that is assigned to the instance. See "Editing instance network settings" on page 74.

   For both of these settings, if you do not have another available configured interface, use this procedure to configure an interface with placeholder values that you can use until you complete the edits.

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

   It may take a few minutes to load.

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

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

   - If you want to use VLAN tagging, select the network interface and click **Add VLAN Tag**. Then enter a VLAN ID between 1 and 4,094 and at least one subnet and gateway pair. Use CIDR notation for the subnet and gateway. For example, 1.1.1.0/24.

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

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

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

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

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

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

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

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

4 Click **OK**.

See "Creating a network bond" on page 38.

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 44.

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

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

- VMware SAN transport (initiator)
- Tape out (initiator)
- SAN client (Fibre Transport target)

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 75.

See "Unassigning Fibre Channel ports from an instance" on page 77.

Fibre Channel best practices

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

- Flex Appliance 4.x has been tested for up to 6,000 storage devices or paths in the case of multipathing. If you zone more than the tested number of devices or paths, you may have to take additional steps to perform the following operations and avoid the associated issues:
  - Initial configuration and Flex Appliance updates
    These operations may take a long time or fail.
  - Factory reset
    During a factory reset, the Veritas Remote Management Interface may go blank and may not accept input.

  You should consult with Veritas Technical Support before you implement a Fibre Channel configuration of that size.
- VMware SAN transport mode only works with VMware Virtual Machine File System (VMFS) datastores version 6.0 or later. Other devices such as the raw device-mapping (RDM) format are not supported. Make sure that only VMFS devices are zoned to the appliance to avoid backup failures.
  Refer to the NetBackup Software Compatibility List to confirm the supported VDDK versions.
- Veritas recommends that you do not allocate more than four ports to the same device unless the storage array requires it.
- If you run VMware SAN backups to LSI storage, the LSI storage should be configured in Asymmetric Logical Access Unit (ALUA) mode by following the procedure from the storage vendor. The procedure may involve updating the storage array firmware to a version that supports ALUA mode. If the storage was connected before it was configured in ALUA mode, you also need to unmap and remap the LSI storage LUNs to the appliance. After the LSI storage LUNs have been remapped, rescan the associated Fibre Channel ports from the **Fibre Channel interfaces** page on the Flex Appliance Console.
- After an appliance restart or an instance relocation, monitor the **Fibre Channel interfaces** page and wait for the link state of the ports to be up before you run any backups. The ports may take up to 10 minutes to become active.

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.

A rescan is also required if a SAN configuration change occurs, including device restarts or disconnections.

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

To rescan or clean Fibre Channel ports

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

Chapter 5

Managing users

This chapter includes the following topics:

Overview of the Flex Appliance default users

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

The following list describes the default users and their functions:

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

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

Managing Flex Appliance Console users and tenants

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

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

See "Adding a tenant" on page 47.

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 49.
- Active Directory and LDAP users
  See "Connecting a remote user domain to the Flex Appliance Console" on page 49.
- Single sign-on (SSO) users
  See "Managing single sign-on (SSO)" on page 51.

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, which includes both the security administrator role and the administrator role. The **admin** user has access to all areas of the Flex Appliance Console and can perform all operations.
- Security administrator

A user with the security administrator role can manage users and oversee the security management of the appliance.

The **admin** user or another security administrator can assign the security administrator role when they add a new local user. They can also edit the role of an existing user from the **User management** page. Select the user and click **Edit roles**.

- Administrator

  A user with the administrator role can perform all but the security operations on the Flex Appliance Console.

  All users have the administrator role, and it cannot be removed.

Adding a tenant

Follow these steps to add a tenant.

To add a tenant

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

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

4 Complete the following network configuration settings:

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

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

5 Click **Save**.

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

Editing a tenant

Follow these steps to change the settings for a tenant.

To edit a tenant

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

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

3 Change the appropriate settings.

4 Click **Save**.

Removing a tenant

Follow these steps to remove a tenant.

To remove a tenant

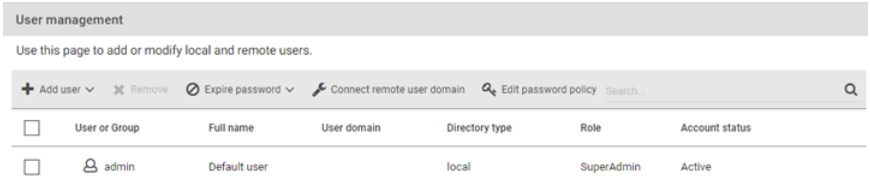
1. On the Flex Appliance Console, click the **Tenants** icon in the left-side navigation bar.
2. Select the tenant that you want to remove, then click **Remove**.

Adding a local user to the Flex Appliance Console

Follow these steps to add a local user.

To add a local user

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



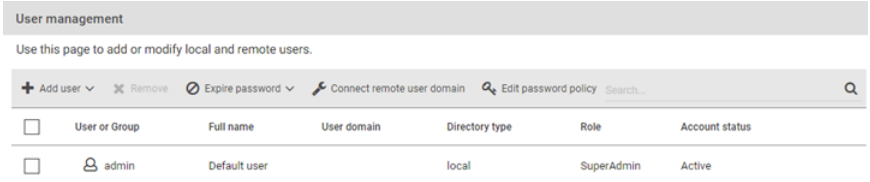
2. Click **Add user** > **Add local user**.
3. Enter the requested information and click **Save**.

Connecting a remote user domain to the Flex Appliance Console

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

To connect a remote user domain

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



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

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

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

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

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

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

See "Importing a remote user or user group to the Flex Appliance Console" on page 50.

Editing a remote user domain in the Flex Appliance Console

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

To edit a remote user domain

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

2 Click **Edit remote user domain**.

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

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

See "Removing users from the Flex Appliance Console" on page 59.

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

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

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

To import a remote user or user group

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

   See "Connecting a remote user domain to the Flex Appliance Console" on page 49.
3. Click **Add user** > **Import remote users**.
4. Select **User** or **User group**.
5. Depending on your selection, enter the username or the group name. Do not include the domain name.
6. Click **Import**.

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

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

Managing single sign-on (SSO)

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

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

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

Configuring SSO

Perform the following steps to configure SSO.

To configure SSO

1. Add the SSO identity provider (IDP).

   See the section called “Adding an IDP” on page 53.

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

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

   See “Importing a remote user or user group to the Flex Appliance Console” on page 50.

Enabling or disabling SSO

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

To disable or enable SSO

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

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

Managing identity providers (IDPs)

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

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

Use the following procedures to manage your IDPs.

Adding an IDP

To add an IDP

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
2. Under **Appliance service provider URL**, copy or download the appliance metadata file. Upload that file to your IDP and add the appliance as a service provider. For more specific instructions, see the following articles on the Veritas Support website:
   - Active Directory Federation Services (ADFS)
   - IBM
   - Microsoft Azure Active Directory
   - Okta
   - Ping Federate
   - Shibboleth
3. From the IDP, download and save the IDP metadata XML file.
4. Gather the following information for the IDP:
   - Name: A name of your choosing to identify the IDP.
   - User field: The SAML attribute name that is mapped to the user attribute of the remote user domain. For example, **userPrincipalName**, **displayName**, **identifier**, **uid**, etc.
   - Group field: The SAML attribute name that is mapped to the group attribute of the remote user domain. For example, **memberOf**, **role**, etc.
5. From the **Single sign-on** page on the Flex Appliance Console, click **Add**.
6. Upload the IDP metadata file. Once the file has uploaded successfully, click **View details** and verify the certificate subject values and SHA-256 fingerprints.
7. Fill in the other required fields, then click **Save**.
8. If you have added only one IDP, enable SSO to start using it. See the section called “Enabling or disabling SSO” on page 52.

   If you have added more than one IDP, the first IDP is used by default. Switch to the new IDP if necessary. See the section called “Switching to a different IDP” on page 54.

Editing an IDP

To edit an IDP

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

Switching to a different IDP

To switch to a different IDP

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
2. If you have not done so already, add the IDP that you want to use. See the section called “Adding an IDP” on page 53.
3. Make sure that SSO is enabled. Then select the IDP that you want to use and click **Use**.

Removing an IDP

To remove an IDP

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

Note: If you have more than one IDP, you cannot remove the one that is in use unless you remove the others first. If you have only one IDP or have already removed the others, you must disable SSO before you can remove it. See the section called “Enabling or disabling SSO” on page 52.

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

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

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

To import an SSO user or user group

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

   See "Managing identity providers (IDPs)" on page 52.

   See "Managing single sign-on (SSO)" on page 51.
3. Click **Add user** > **Import single sign-on (SSO) users**.
4. Select **User** or **User group**.
5. Depending on your selection, enter the username or the group name in the format ***<user or group>@<domain>***. Note that the parameters are case sensitive. For example, **User@example.com** or **group@example.com**.

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

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

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

Managing user authentication with smart cards or digital certificates

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

Note: Smart card authentication does not apply for users who have configured multifactor authentication.

Prerequisites

Note the following prerequisites for smart card authentication:

- DNS must be configured on the appliance.
  See "Changing DNS or Hosts file settings" on page 126.

- The remote users who are associated with the smart cards or digital certificates must be imported to the appliance.
  See "Importing a remote user or user group to the Flex Appliance Console" on page 50.
- Veritas recommends that the appliance date and time are set using NTP.
  See "Setting the date and time for appliance nodes" on page 35.

Configuring or editing smart card authentication

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

To configure or edit smart card authentication

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

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

   Note: If you use Mozilla Firefox, you must also remove the certificate from the browser's certificate manager. See the browser documentation for instructions.
5. Click **Save**.
6. Open a new session to the Flex Appliance Console. The sign-in page should now display an option to sign in with a certificate or smart card.

7 Before a user can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager. See the browser documentation for instructions.

8 Once a user inserts a smart card or uploads a certificate, they are prompted to select and authenticate the certificate when they open a new session to the Flex Appliance Console. Once they do so, they can use the certificate to sign in.

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

Disabling or enabling smart card authentication

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

To disable or enable smart card authentication

1 Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Smart card authentication**.

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

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

Changing a local user password in the Flex Appliance Console

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

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

To change a user password

1 Sign in to the Flex Appliance Console from the user account that you want to change the password for.

2 In the top-right corner of the screen, click the black circle icon that includes the user's initials. For example, if the user's full name is Default User, the icon includes the initials DU.

3 Click **Change password**.

4 Fill in the required fields. The password must adhere to the current password policy.

See "Changing the password policy" on page 60.

5 Click **Save**.

Expiring local user passwords in the Flex Appliance Console

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

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

To expire user passwords

1 Sign in to the Flex Appliance Console. If you want to expire the **admin** user password or all user passwords, you must sign in as a security administrator.

2 Click the **User management** icon in the left-side navigation bar to open the **User management** page.

3 Do one of the following:

- To expire the password for a specific user or users, select the user or users and click **Expire password** > **Expire selected users**.
- To expire the password for all users, click **Expire password** > **Expire all users**.

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

Unlocking a user account in the Flex Appliance Console

The Flex Appliance Console is protected with the following account locks:

- Local user accounts become locked after three sign-in attempts with incorrect passwords. If a security administrator account becomes locked, it is unlocked automatically after 30 minutes. If a different local user account becomes locked, that user and a security administrator must work together to unlock it.

- Accounts with multifactor authentication become locked after three sign-in attempts with incorrect codes. The account unlocks automatically after 15 minutes.

Use the following procedures to unlock a locked user account. You can use these procedures for situations where the account unlocks automatically, but note that once you start the manual unlock, the automatic unlock is canceled.

Steps for the security administrator

The security administrator must generate a secure unlock code for the locked user.

To generate a secure unlock code

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

Steps for the locked user

Once the security administrator has sent the secure unlock code, the locked user can unlock their account.

To unlock a user account

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

Removing users from the Flex Appliance Console

Follow these steps to remove users.

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

To remove users

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

Changing the password policy

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

The default password policy is as follows:

Password complexity:

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

Password age:

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

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

To edit the password policy

1. Sign in to the Flex Appliance Console as a security administrator.
2. Click the **User management** icon in the left-side navigation bar to open the **User management** page.
3. Click **Edit password policy**.

4 If you want your password policy to adhere to the Security Technical Implementation Guides (STIGs), select the **Use STIG for validation** toggle. You can click **Reset to STIG default** to fill in the default values for all fields.

5 Fill in or adjust the required parameters as needed, then click **Save**.

Changing the hostadmin user password in the Flex Appliance Shell

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

To change a hostadmin user password

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

```
set user password
```

2 Press **Enter**.

3 Type a new password.

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

See “Changing the password policy” on page 60.

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.

Managing multifactor authentication

Flex Appliance supports multifactor authentication for local, Active Directory (AD), and LDAP users in the Flex Appliance Console and the **hostadmin** user in the Flex Appliance Shell. Multifactor authentication uses time-based one-time passwords to provide secure authentication. Each user can configure multifactor authentication

individually, or a security administrator can enforce multifactor authentication for all console users.

Multifactor authentication does not apply for users who have configured smart card authentication or for SSO users. For SSO users, Veritas recommends that you configure multifactor authentication through the SSO identity provider (IDP).

Note: AD and LDAP user groups are not supported for multifactor authentication. You can add these users individually so they can configure multifactor authentication, or you can configure authentication with smart cards or digital certificates instead.

See "Configuring or reconfiguring multifactor authentication" on page 62.

See "Enforcing multifactor authentication" on page 64.

Configuring or reconfiguring multifactor authentication

Flex Appliance supports multifactor authentication for local, Active Directory (AD), and LDAP users in the Flex Appliance Console and the **hostadmin** user in the Flex Appliance Shell.

The following authenticator apps are supported:

- Microsoft Authenticator version 6.5.12 and later
- Google Authenticator
- Okta Verify
  Note that when you scan the QR code with this app, the authentication process could take up to a minute.
- Symantec VIP Access 4.3.3 and later

Note: Multifactor authentication may affect integrations like APIs, automation, and third-party Privileged Access Management (PAM) solutions.

Configuring or reconfiguring multifactor authentication for the Flex Appliance Console

Before you can configure multifactor authentication for a user in the Flex Appliance Console, the following prerequisites must be met:

- The appliance date and time must be set with NTP.
- At least one user must have the security administrator role. If you are the user with the security administrator role, at least one additional user must also have the security administrator role.

- You must have a supported authenticator app installed on your mobile device.

To configure or reconfigure multifactor authentication for the Flex Appliance Console

1. From the Flex Appliance Console, click your user icon in the top-right corner and click **Configure multifactor authentication**.
2. On the **Configure multifactor authentication** page, click **Configure** or **Reconfigure**.

   Note: The **Reconfigure** option is only available if multifactor authentication is enforced, and the start date has passed. For other scenarios, click **Disable** and then click **Configure**.

   ---

3. Follow the prompts to add your Flex Appliance account to the authenticator app.

   If you have already configured multifactor authentication for another appliance and want to use the same authenticator account to sign in to this appliance, select the option **Use a custom key**. Enter the key from the appliance that is already configured.

   You can also create and enter your own key with the custom key option. If you create your own key, note that some authenticator apps may not support pad characters. Confirm compatibility with your app if you want to use them.

Configuring or reconfiguring multifactor authentication for the Flex Appliance Shell

Before you can configure multifactor authentication for the **hostadmin** user in the Flex Appliance Shell, the following prerequisites must be met:

- The appliance date and time must be set with NTP.
- You must have a supported authenticator app installed on your mobile device.

To configure or reconfigure multifactor authentication for the Flex Appliance Shell

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

   ```
   set user mfa
   ```

2. Follow the prompts to add the **hostadmin** account to your authenticator app.

   If you have already configured multifactor authentication for another appliance and want to use the same authenticator account to sign in to this appliance, respond **yes** to the question **Do you want to specify an existing key?** Enter the key from the appliance that is already configured. You can view the key on the other appliance with the `show user mfa key` command.

   You can also create and enter your own key with the existing key option. If you create your own key, note that some authenticator apps may not support pad characters. Confirm compatibility with your app if you want to use them.

3. Share the QR code or the key with anyone else who requires access to the Flex Appliance Shell so that they can also add the **hostadmin** account to their authenticator app. You can view the QR code and the key at any time with the following command:

   ```
   show user mfa key
   ```

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

Enforcing multifactor authentication

You can enforce multifactor authentication for users in the Flex Appliance Console, so that they must configure it by the date that you select.

Note: Remote AD and LDAP user groups are not supported when multifactor authentication is enforced. Once you enforce it, users in these groups can no longer sign in.

You cannot enforce multifactor authentication for the **hostadmin** user in the Flex Appliance Shell.

Before you can enforce multifactor authentication, the following prerequisites must be met:

- The appliance date and time must be set with NTP.
- You and at least one other user must have the security administrator role. At least one of the users with the security administrator role must be a local user.
- You must have multifactor authentication configured on your account.

To enforce multifactor authentication

1. Sign in to the Flex Appliance Console as a security administrator. Click the **Settings** icon in the top-right corner of the page and then click **Enforce multifactor authentication**.
2. On the **Multifactor authentication enforcement** page, click **Enforce**.
3. Select a start date within the next 90 days.

   Caution: Once you enforce multifactor authentication, you can't cancel the enforcement or extend the start date past 90 days.

4. Click **Enforce**.

If you need to change the start date, return to the **Multifactor authentication enforcement** page and click **Edit enforcement**.

Resetting multifactor authentication

If a user with multifactor authentication changes or loses access to their mobile device and cannot sign in, use one of the following procedures to reset multifactor authentication for that user. After a reset, the user is forced to reconfigure multifactor authentication the next time that they sign in.

Resetting multifactor authentication for a Flex Appliance Console user

To reset multifactor authentication for a Flex Appliance Console user

1. Sign in to the Flex Appliance Console as a security administrator and navigate to the **User management** page.
2. Click the Actions menu to the right of the user that you need to reset and click **Reset multifactor authentication**.

Resetting multifactor authentication for the hostadmin user in the Flex Appliance Shell

If multifactor authentication for the **hostadmin** user is configured on more than one mobile device, you may not need to reset multifactor authentication if you lose access. Instead, ask someone who still has access to share the QR code or the key and use them to add the account back to your authenticator app.

The other user can view the QR code and the key with the following command in the Flex Appliance Shell:

```
show user mfa key
```

If no other devices have access, use the following procedure to reset multifactor authentication for the **hostadmin** user.

To reset multifactor authentication for the hostadmin user in the Flex Appliance Shell

1. Sign in to the Flex Appliance Console as a security administrator.
2. Click the **Help and support** icon in the top-right corner of the page. Under **Reset multifactor authentication**, click the **hostadmin** user for the node that you need to reset.

Disabling multifactor authentication

Use the following procedures to disable multifactor authentication after it has been configured.

Note: If multifactor authentication is enforced, Flex Appliance Console users cannot disable it after the start date.

To disable multifactor authentication for the Flex Appliance Console

1. From the Flex Appliance Console, click your user icon in the top-right corner and click **Configure multifactor authentication**.
2. On the **Configure multifactor authentication** page, click **Disable**.

To disable multifactor authentication for the Flex Appliance Shell

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

```
delete user mfa
```

Chapter 6

Using Flex Appliance

This chapter includes the following topics:

Managing the repository

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

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

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

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

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

Use the Repository tabs to do the following:

- Add files to the repository
  See "Adding files to the repository" on page 68.
- Remove files from the repository
  See "Removing files from the repository" on page 69.
- Update Flex Appliance
  See "Updating Flex Appliance" on page 88.

Adding files to the repository

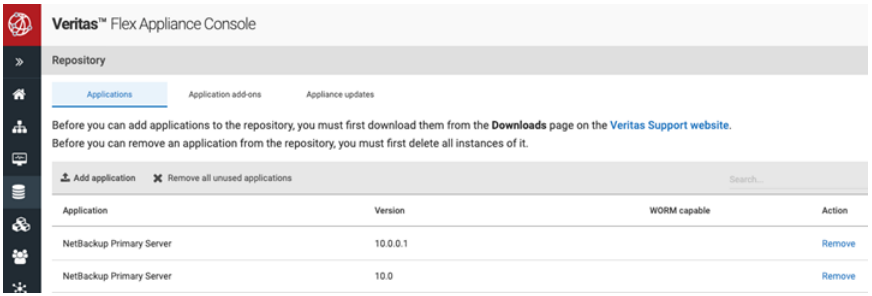
Use the following procedure to download and add files to the Flex Appliance repository.

Guidelines for adding files to the repository:

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

To download and add files to the repository

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



3. On the **Repository** page, navigate to the **Applications**, **Application add-ons**, or **Appliance updates** tab, depending on the type of file that you want to add.
4. Click **Add application**, **Add add-on**, or **Add package**.
5. In the dialog box that appears, do the following:
   - At the top of the dialog box, click on the drop-down and navigate to the location where you downloaded the file from Veritas.
   - Select the downloaded file from the list of items that appears, then click **Open**.

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

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

Removing files from the repository

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

To remove files from the repository

1. Sign in to the Flex Appliance Console and click the **Repository** icon in the left-side navigation bar.
2. On the **Repository** page, navigate to the tab for the type of file that you want to remove.
3. Do one of the following:
   - To remove an application, locate the row of the application that you want to remove and click **Remove**. You can also click **Remove all unused applications** to remove all of the applications that are not currently in use. You can also remove the unused add-ons that correspond to the application. To do so, select **Remove corresponding unused add-ons** in the confirmation window that appears. Then click **Remove**.
   - To remove an add-on, locate the row of the add-on that you want to remove and click **Remove**. You can also click **Remove all unused add-ons** to remove all of the add-ons that are not currently installed on application instances.
   - To remove an update package, click **Remove package**.

Creating application instances

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

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

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

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

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

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

Flex Appliance supported applications and usage information

Managing application instances from Flex Appliance and NetBackup

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

Instance operations that you can perform from Flex Appliance

Use Flex Appliance to do the following:

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

See "Managing application instances from Flex Appliance" on page 71.

Instance operations that you can perform from NetBackup

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

Managing application instances from Flex Appliance

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

Under **Application instances**, you can perform the following tasks, depending on the features that you have configured:

- Create a new instance.
  See "Creating application instances" on page 70.
- Create a replica.
  See "Creating a replica" on page 94.
- Use the Actions menu to the right of an 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.

- Delete it.
  See "Deleting an application instance" on page 82.
- Resize the storage.
  See "Resizing instance storage" on page 73.
- Upgrade it.
  See "Upgrading application instances" on page 83.
- Install add-ons.
  See "Installing application add-ons" on page 78.
- Clear a configuration error status.
  See "Clearing a configuration error status on an application instance" on page 82.
- Pause or resume replication.
  See "Pausing and resuming replication" on page 98.
- Change the replication role.
  See "Changing the replication role of an instance" on page 100.
- Unlink it from its active or replica instance.
  See "Unlinking active and replica instances" on page 101.

- Click on an existing instance to:
  - View the instance details.
  - Edit the network settings, including IP address and interface pairs.
    See "Editing instance network settings" on page 74.
  - Manage add-ons.
    See "Managing application add-ons on instances" on page 77.
  - Manage the assigned Fibre Channel ports.
    See "Assigning Fibre Channel ports to an instance" on page 75.
    See "Unassigning Fibre Channel ports from an instance" on page 77.

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 81.

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.

Note: If you have configured remote replication, you can only resize the active instance. The replica instance is automatically resized to match when you resume replication after the resize. Make sure that the paired appliance has enough available storage to resize the replica. If it does not, you cannot resume replication until you have freed up or added the required storage.

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, click **Actions** > **Stop**.
3. If the instance has a replica, check the data status from the **Remote replication** page and make sure that it shows a status of **Consistent**. If it does not, wait for it to become consistent and then return to the **Application instances** section of the **System topology** page.
4. Click **Actions** > **Resize storage**.
5. Follow the prompts to enter new storage allocations for each volume, then click **Resize**.

6 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**.

7 If the instance has a replica, resume replication.

Editing instance network settings

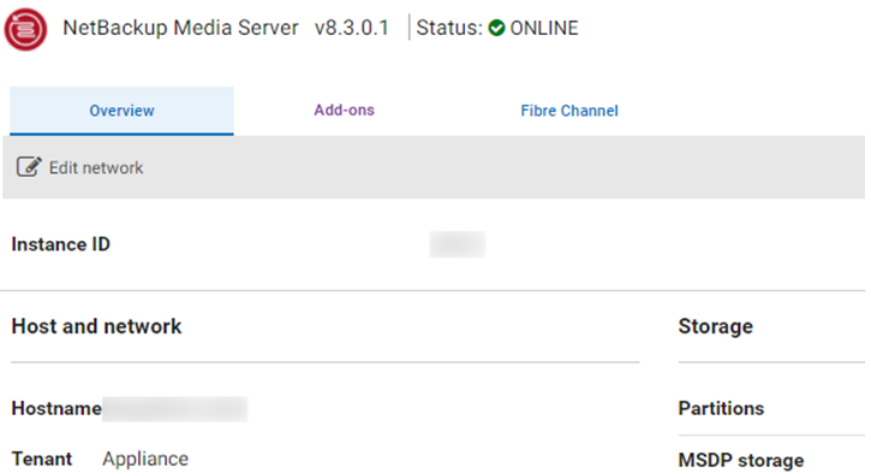
Use the following procedure to edit the network settings of an existing application instance in Flex Appliance.

To edit the instance network settings

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

2 Locate the instance that you want to edit. If you want to edit the IP address and interface pairs or the default gateway, click **Actions** > **Stop**. You do not need to stop the instance to edit the other settings.

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



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

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

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

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

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

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

Assigning Fibre Channel ports to an instance

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

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

- VMware SAN transport (initiator)
- Tape out (initiator)
- SAN client (Fibre Transport target)

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, click **Actions** > **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.
3. Click on the instance name to open the instance details page, then navigate to the **Fibre Channel** tab.
4. Click **Assign ports** and follow the prompts to assign available ports. If you assign a port as an initiator that was previously used as a target, you are prompted to rescan the port before you can continue.

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

Port sharing and multipathing support

Note the following information:

- You can assign an initiator port to multiple instances if the instances belong to the same tenant. You cannot assign a target port to multiple instances.
- You can use the same port for both VMware and Tape out backups.
- You can assign multiple ports to the same application instance or instances as long as they meet the following guidelines:
  - Used for VMware SAN transport:
    Multiple ports can be assigned to a single or to multiple application instances in any combination.
  - Used for Tape out or for both Tape out and VMware SAN transport:
    Multiple ports can be assigned to a single or to multiple application instances. However, the ports that are connected to the same tape devices must also be connected to the same application instances. The same tape devices cannot be assigned to different instances using different ports.
  - Used for SAN client:
    Multiple ports can be assigned to a single or to multiple application instances in any combination. Once you have assigned the ports, you cannot assign them to additional application instances or use them for another use case unless you unassign the existing instances.

  - Assigned to load balancing servers:
    If you have configured multiple media server instances as load balancing servers and want to use Fibre Channel for VMware SAN transport, you must assign the same ports to all of the load balancing media server instances.

- A Fibre Transport (FT) target port can handle data streams from multiple SAN client initiator ports concurrently. However, if you want it to handle streams from more than two SAN client initiator ports, consider changing the following NetBackup primary server setting:

  ```
  nbftconfig -setconfig -ncp4
  ```

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

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

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

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

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

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

Unassigning Fibre Channel ports from an instance

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

To unassign Fibre Channel ports from an instance

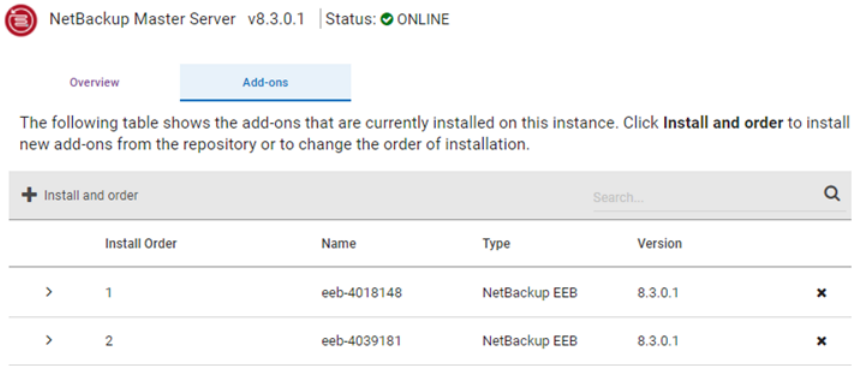
1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance that you want to unassign ports from. If it is running, click **Actions** > **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts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

Managing application add-ons on instances

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

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

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



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

See “Installing application add-ons” on page 78.

See “Uninstalling application add-ons” on page 79.

See “Changing the application add-on installation order” on page 80.

Installing application add-ons

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

To install add-ons

1. Make sure that the add-ons you want to install are located in the repository. See “Managing the repository” on page 67.
2. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
3. Locate the instance on which you want to install the add-ons. If it is running, click **Actions** > **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.

4. Click **Actions** > **Install add-ons**. Alternatively, click on the instance name, navigate to the **Add-ons** tab, and click **Install and order**.
5. Select the appropriate add-ons from the repository list that appears. When you are done, click **Next**.
6. On the following page, you have the option to change the add-on installation order. In most cases, the install order does not affect operation, and you can skip this step. However, if recommended by Veritas Support or otherwise required, you can use the up and down arrows to change the order.

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

   Otherwise, resolve the conflicts manually as follows:

   - If a conflict exists between new add-ons, the add-on that is listed last takes precedence. You can use the up and down arrows to change the order and prioritize a different add-on.
   - If a conflict exists between a new add-on and an installed add-on, the new add-on is not installed. If you want to install the new-add-on, click **Cancel** to back out of the procedure. Then remove the installed add-on and try again.
   - If a conflict exists between installed add-ons, you must remove one of the add-ons before you can continue. Click **Cancel** to back out of the procedure.
   - If all of the add-ons are required or if you are unsure which add-ons should be installed, contact Veritas Support for assistance. Before you do so, navigate to the **Conflict report** and click **Copy**. Share this report with your representative.
7. Click **Install**.

Note: If the instance that you installed the add-ons on has a replica, make sure that the remote administrator also installs them on the replica. Alternatively, you can make sure the add-ons are in the repository on the remote appliance and then pause and resume replication.

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, click **Actions** > **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.
3. Click on the instance name to open the instance details page.
4. At the top of the details page, navigate to the **Add-ons** tab.
5. Click the **X** icon next to the add-on that you want to uninstall.

Changing the application add-on installation order

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

To change the add-on install order

1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance that you want to modify. If it is running, click **Actions** > **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.
3. Click **Actions** > **Install add-ons**. Alternatively, click on the instance name, navigate to the **Add-ons** tab, and click **Install and order**.
4. In the wizard that appears, click **Next** to skip the add-on installation step.
5. Use the up and down arrows to change the add-on install order as needed.
6. Click **Install**.

Updating an application add-on to a newer revision

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

For example, the file `VRTSflex-nb_EEB_ET4070421-10.0-9.x86_64.rpm` indicates that the version is 10.0, and the revision number is 9.

You can view the revision numbers of your add-ons on the **Application add-ons** page of the **Repository**.

Use the following procedure to update an application add-on to a newer revision.

To update an add-on to a newer revision

1 Add the new revision of the add-on to the repository.

Note: If the instance that has the add-on installed has a replica, make sure that the new revision is also in the repository on the remote appliance.

See "Adding files to the repository" on page 68.

2 Restart the instance that has the add-on installed.

Note: If you have more than one instance that has the add-on installed, they all get updated to the newer revision the next time they are restarted or if you change the replication role for remote replication.

Viewing instance performance metrics

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

To view instance performance metrics

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

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

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

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

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

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

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

- PIDS: The total number of processes that are running on the instance

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

Clearing a configuration error status on an application instance

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

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

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

To clear a configuration error status:

1 Before you can clear the error status, you must resolve the underlying configuration error or errors. Hover over the **Configuration Failed** status to see more specific information, and refer to the error messages that display in the Activity Monitor. Then log in to the instance and resolve all errors.

2 When you are sure that all errors have been resolved, navigate to the **System topology** > **Application instances** section.

3 Locate the instance and click **Actions** > **Clear status**, then refresh the page to see the change.

Deleting an application instance

Use the following procedure to delete an application instance.

To delete an application instance

1 Deleting an application instance requires multiperson authorization for the following versions:

- NetBackup primary or media server instances on version 10.3.0.1 or later
- NetBackup WORM storage server instances on version 19.0.1 or later
- NetBackup WORM storage server instances on version 19.0 in the following scenarios:
  - The appliance is in compliance lockdown mode.
  - The appliance is in enterprise lockdown mode, and you do not have the security administrator role.

With multiperson authorization, the application administrator must unlock the deletion option before you can delete the instance. Ask them to refer to the

topics “Authorizing a primary or a media server instance for deletion” and “Authorizing a WORM storage server for deletion” in the *NetBackup Application Guide*.

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 delete and click **Actions** > **Delete**.

Note: Depending on the application type and version and the lockdown mode of the appliance, the instance may need to be running before you can delete it. If the instance is stopped, and you don’t see the **Delete** option, start it and try again.

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 67.

Note: If the instance that you want to upgrade has a replica, make sure that the new version of the application is also located in the repository on the paired appliance.

---

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, click **Actions** > **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, click **Actions** > **Upgrade instance**.

6 Select the version that you want to upgrade to and click **Precheck**.

7 If the precheck passes, click **Next** to continue. If the application needs any additional configuration parameters, you are prompted to enter them. Enter the parameters and click **Next**. Then verify the selection summary and click **Upgrade** to begin the upgrade process.

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

If the upgrade fails for any reason, the instance automatically rolls back to the previous version. You can find more detailed information on the failure in the Activity Monitor. Resolve any issues before restarting the upgrade procedure.

8 If your application does not support rollback, the upgrade is now complete.

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

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

See "Warnings and considerations for instance rollbacks" on page 85.

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, locate the instance and click **Actions** > **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 locate the instance and click **Actions** > **Upgrade instance** > **Roll back**. You can also click on the instance name to open the instance details page, then click **Roll back** at the top of the screen.

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

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

Warnings and considerations for instance rollbacks

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

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

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

  - Incremental or transaction log-based database backups:

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

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

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

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

- Backup expiration catalog and storage inconsistency:
  If backup images expire and cleanup begins after the upgrade and before the rollback, backup data may be removed from storage units external to the instance. For example, this behavior can happen with an MSDP media server, cloud storage, OST storage, or tape storage. When a rollback of the primary server catalog occurs, the catalog indicates that there is a valid backup even though the data was removed from storage. This inconsistency results in backup data that cannot be restored, duplicated, or replicated. It may also affect scheduling of subsequent backups (delaying backups or performing incrementals instead of fulls).
- Orphaned backups on storage:
  If backup images are created on external storage after the upgrade and before the rollback of the primary server, the backup images exist on storage but not in the NetBackup catalog. This discrepancy results in situations where the backups are never removed from storage (data leakage).
  To resolve this issue, import the images from storage or use the consistency check tools.
- Backup considerations if the instance is a media server:
  - The backups between the upgrade and rollback are not restorable even though NetBackup has them in the catalog.
  - Unfinished SLP jobs fail, causing inconsistencies between the NetBackup primary server and the storage.
    If any backups were deleted after the upgrade and before the rollback, those backups come back as storage leak.

Updating an application instance to a newer revision

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

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

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

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

```
support shell
```

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

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

To update an instance to a newer revision

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

Note: If the instance that you are updating has a replica, make sure that the new revision is also in the repository on the remote appliance.

See "Adding files to the repository" on page 68.

2 Restart the instance.

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

About Flex Appliance updates

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

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

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

See "Updating Flex Appliance" on page 88.

Updating Flex Appliance

Use the following procedure to update the Flex Appliance software from version 4.x to a later release.

Note: To update to version 4.x, refer to the *Getting Started and Administration Guide* for the version that you are currently on.

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

See "Managing the appliance Fibre Channel ports" on page 42.

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 updates** tab.
2. Make sure that the update package you want to use is located in the repository. See "Managing the repository" on page 67.
3. Navigate to **System topology** > **Application instances** and do one of the following:
   - If you have a single-node appliance, stop all running instances.
   - If you have a multi-node appliance, stop all running instances or select the node that you want to update first and relocate all of its instances to the other node.
4. (Optional) If you want to check ahead of time if the appliance is ready for the update, run a precheck on each node. The precheck also runs as part of the update process, so you can skip this step if you prefer to wait for the system to run it.

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

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

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

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 23.

Warning: Do not make configuration changes, start application instances, or restart the appliance while the update is in progress.

---

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

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

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

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

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

Do one of the following:

- To commit the update, return to the **Appliance updates** tab on the **Repository** page and click **Commit**.
- To roll back to the previous version, stop all instances on the appliance and then run the following command from the Flex Appliance Shell:

  ```
  system rollback
  ```

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

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

  ---

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

10 After you complete the software update, also make sure that the appliance firmware is up to date. See "Updating the firmware" on page 90.

Updating the firmware

Use the following procedure to update the appliance firmware.

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

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

Use the Veritas Appliance firmware update tool to get the latest firmware update RPMs.

To update the firmware

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

2 Make sure that the update package you want to use is located in the repository. See "Managing the repository" on page 67.

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

4 Do one of the following:

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

5 Return to the **Appliance updates** tab on the **Repository** page. Select the node that you want to update and click one of the following:

- To install the firmware update for the first time, click **Update**.
- To install the firmware update again because of new hardware, click **Update again**.

If the update requires a restart, you can monitor the restart progress from the Veritas Remote Management Interface. However, the interface briefly becomes unavailable during the update. To access the Veritas Remote Management Interface, refer to the initial configuration procedure. See "Performing the initial configuration" on page 23.

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

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

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

Then repeat the update on the other node.

Chapter 7

Remote replication

This chapter includes the following topics:

About remote replication

Remote replication saves replicas of your primary server application instances on another appliance. You can use remote replication to minimize downtime during planned maintenance or troubleshooting activities and as additional protection from a disaster scenario. You can also use remote replication to easily migrate your data from one Flex appliance to another.

Note: Remote replication is not an alternative to the NetBackup catalog backup policy. You should still configure a NetBackup catalog backup policy on your primary server. See the topic "Mounting an NFS share on a NetBackup primary server instance" in the *NetBackup Application Guide* for details.

To configure remote replication, you need two Flex appliances. An administrator from each appliance must coordinate to pair the appliances, and then you can create replicas of your primary server instances.

See “Pairing appliances for remote replication” on page 93.

See “Creating a replica” on page 94.

Pairing appliances for remote replication

Use the following procedures to pair two appliances for remote replication. These steps require the coordination of an administrator from each appliance. You can start pairing from either appliance.

Prerequisites

Make sure that the following prerequisites are met before you begin.

- The node IP addresses of each appliance must be able to communicate with the console IP address of the other appliance.
- If you use network access control, make sure that each appliance's allowed list includes all node IP addresses of the other appliance.
- You must have a network interface configured to use for replication. Veritas recommends that you do not select a shared interface or an interface that is configured with the same subnet as the appliance node IP addresses.
- The following ports must be open in both directions between the two appliances:

  Between the replication IP addresses:

  - 4145 (TCP and UDP)
  - 8199 (TCP and UDP)
  - 8989 (TCP and UDP)

  Note: If you need to use the same subnet for replication and the node IP addresses, these ports must also be open between each appliance's replication IP address and the other appliance's node IP addresses.

  Between all of the node and the Flex Appliance Console IP addresses:

  - 443 (TCP)

Step 1: First appliance sends a fingerprint

To start the pairing process, the administrator of one of the appliances must send a client fingerprint to the second administrator. Use the following steps.

To send the fingerprint

1. From the Flex Appliance Console on your appliance, navigate to the **Remote replication** page.
2. Click **Copy fingerprint**.
3. Share this fingerprint securely with the administrator of the second appliance.

Step 2: Second appliance starts pairing

Once the second administrator has the fingerprint from the first appliance, they can start pairing. Use the following steps.

To start pairing

1. Obtain the fingerprint from the first appliance administrator.
2. From the Flex Appliance Console on your appliance, navigate to the **Remote replication** page.
3. Click **Start pairing**.
4. Follow the prompts to enter the fingerprint and configure the network for replication.

   If you select an interface that was configured with a dual stack IPv4-IPv6 network, you can only use one of the protocols for the replication IP address.
5. When the pairing key displays, copy the key and share it securely with the first administrator.

Step 3: First appliance finishes pairing

Once the first administrator has the pairing key, they can finish pairing. Use the following steps.

To finish pairing

1. Obtain the pairing key from the second appliance administrator.
2. From the Flex Appliance Console on your appliance, navigate to the **Remote replication** page.
3. Click **Finish pairing**.
4. Follow the prompts to enter the pairing key and configure the network for replication.

   When you are done, you can monitor the progress in the Activity Monitor on both appliances. Once the pairing has completed successfully, the **Paired appliances** section of the **Remote replication** page shows the **Management connection status** and the **Replication connection status** as **Connected**.

Creating a replica

Once you have paired two appliances, you can create replicas of your primary server application instances on either appliance.

Note: The appliance where you create the replica must have enough available storage to accommodate the size of the instance. Both appliances also require up to an extra 20% of the size of the instance to be reserved for replication logging.

Use the following procedure to create a replica.

To create a replica

1. Sign in to the Flex Appliance Console on the appliance that you want to create the replica on.
2. Click the **Remote replication** icon in the left-side navigation bar, then click **Create replica**.

   Alternatively, you can navigate to the **Application instances** section of the **System topology** page and click **Create** > **Create replica**.
3. Locate the instance that you want to create a replica of.

   If any prerequisites are not met for that instance, it is greyed out, and the **Status** column shows **Missing prerequisites**. Click **Missing prerequisites** to see the list of issues. You must resolve them before you can continue.
4. Select the instance and click **Next**.
5. Follow the prompts to create the replica. When you are done, the replica appears on the **Remote replication** page with a status of **Configuring**. You can view the progress in the Activity Monitor.

   Once the replica has been created, the **Remote replication** page on the remote appliance updates as well. The instance that you created the replica of displays on this page as an active instance.

   Note: The instance widgets on the **Remote replication** page have different available actions, depending on whether they are for the active or the replica instance.

Managing remote replication

Once you have paired two appliances, you can manage the pairing and your replicas from the following locations:

- The **Remote replication** page

  From this page, you can edit the replication network, create and manage replicas, and monitor your configuration.
- The **Home** page

This page includes a **Remote replication** widget that alerts you to any issues with the replication network, the management network, or your replicas.

- The **System topology** page
  From this page, you can use the **Application instances** section to create and manage replicas.

Remote replication best practices

When you configure remote replication, Veritas recommends that you adhere to the following best practices:

- When you configure remote replication for the first time, start with one replica per appliance. Then monitor the replication performance. Based on the results, you can consider creating additional replicas.
- Use a dedicated network for replication.
- If you configure remote replication on a Veritas 52xx appliance without storage shelves, use that appliance for primary server instances only. If you want to add media and WORM instances, add storage shelves with enough storage capacity to handle them.
- Configure email alerts to make sure that you are notified of any issues with the replication.

Monitoring remote replication

You can monitor remote replication from the **Remote replication** page. This page provides information about the network between your paired appliances, and individual widgets display the status of all active and replica instances on the appliance.

If an issue occurs with replication, the Flex Appliance Console may alert you in the following ways:

- An alert message appears in the **Remote replication** widget on the **Home** page.
- An alert icon appears next to the **Remote replication** icon in the left-side navigation bar.
- The connection status changes in the **Paired appliances** section of the **Remote replication** page. It turns yellow if the connection is degraded or changes to **Disconnected** if the connection is lost.
- If you have email alerts configured, an email alert is sent.

Editing the replication network

Use the following procedure to edit the replication network between two paired appliances. The replication connection status must be **Connected** to edit the network, and the old and the new IP addresses must have a network connection to each other.

Note: You cannot change the protocol (IPv4 or IPv6) of the network.

Use the following procedure to edit the replication network.

To edit the replication network

1. From the Flex Appliance Console on the appliance that you want to edit the network of, pause replication. See “Pausing and resuming replication” on page 98.
2. Navigate to the **Remote replication** page. Under **Paired appliances**, click **Edit network interface**.
3. Change the network details as needed and click **Save**.
4. Resume replication.

Repairing a lost connection between paired appliances

If your paired appliances become disconnected, first check if either of the appliances is under maintenance (for example, an appliance update or a factory reset). If so, wait for the maintenance to complete and recheck the status. In some scenarios, the connection repairs itself after the maintenance is complete.

If neither appliance is under maintenance or if the maintenance is complete, but the connection status still shows as **Disconnected** with a **Repair connection** option, use the following procedures to repair the connection. These steps require the coordination of an administrator from each appliance.

Steps for the administrator on the first appliance

The administrator of one of the appliances must start the repairing process.

To start repairing

1. Obtain the fingerprint of the second appliance from the second appliance administrator. To locate the fingerprint, the second administrator can navigate to the **Remote replication** page and click **Repair connection**. The fingerprint displays at the bottom of the window that appears. Make sure that they share it with you in a secure manner.
2. From the Flex Appliance Console on your appliance, navigate to the **Remote replication** page.
3. Click **Repair connection** > **Start repairing**.
4. Enter the fingerprint. When the repairing key displays, copy the key and share it securely with the second administrator.

Steps for the administrator on the second appliance

The administrator of the second appliance must finish the repairing process.

To finish repairing

1. Obtain the repairing key from the first administrator.
2. From the Flex Appliance Console on your appliance, navigate to the **Remote replication** page.
3. Click **Repair connection** > **Finish repairing**.
4. Enter the repairing key and click **Save and close**. Note that the repair can take up to 15 minutes to complete.

Pausing and resuming replication

Use the following procedures to pause or resume replication between an active and a replica instance. The replication connection status must be **Connected** to pause or resume replication.

Warning: If you pause replication, the data between the active and the replica instances becomes out of sync. The longer that replication is paused, the longer it takes for the data to sync again when you resume. Only pause replication when it is specifically required for maintenance activities on the instances or the appliances.

To pause replication

1. Sign in to the Flex Appliance Console on either appliance.
2. Navigate to the **Remote replication** page and locate the instance that you want to pause. Under **Replication status**, click **Pause**.

   Alternatively, you can navigate to the **Application instances** section of the **System topology** page. Locate the instance that you want to pause and click **Actions** > **Pause**.

To resume replication

1. Sign in to the Flex Appliance Console on the appliance where the active instance is located.
2. Navigate to the **Remote replication** page and locate the instance that you want to resume. Under **Replication status**, click **Resume replication**.

   Alternatively, you can navigate to the **Application instances** section of the **System topology** page. Locate the instance that you want to resume and click **Actions** > **Resume replication**.

   You are redirected to the Activity Monitor to view the progress.

Note: As part of the resume operation, the appliance checks for the following configuration changes on the active instance: an instance upgrade or update, add-on installations or updates, and storage resizes. It attempts to make the same changes on the replica. Once those changes have been made on the replica, replication resumes.

Resolving discrepancies between an active and a replica instance

An active instance and its replica instance should always have the same configuration. However, discrepancies can occur between them in the following scenarios:

- You upgrade or update the active instance, but the newer version or revision is not in the repository on the appliance where the replica is located.
- You install a new add-on on the active instance but do not install it on the replica instance.
- You update an add-on on the active instance, but the newer revision is not in the repository on the appliance where the replica is located.
- You update the replica instance to a newer revision.
- You install or update an add-on on the replica instance

To avoid these scenarios, adhere to the following best practices:

- Always make sure that the required application and add-ons are available in the repositories on both appliances.
- If you install an add-on on the active instance, also install it on the replica instance. Alternatively, you can make sure the add-on is in the repository on the appliance where the replica is located and then pause and resume replication.
- Do not perform operations on the replica instance unless they are required to match the configuration of the active instance.

You can verify the configurations of the active and the replica instances from the **Remote replication** page. Locate the instance that you want to check and click **Compare configurations**. The window that appears displays discrepancies if any exist, along with instructions on how to resolve them.

Changing the replication role of an instance

You can change the replication role of an instance so that the active instance becomes the replica, and the replica becomes the active instance. You can use this option during planned downtimes on the appliance with the active instance so that the primary server can continue to run.

Use the following procedure to change the replication role. The replication network must be connected, and the data status between the instances must be consistent before you begin.

To change the replication role

1. Sign in to the Flex Appliance Console on the appliance where the active instance is located.
2. Navigate to the **Application instances** section of the **System topology** page and locate the instance that you want to change the replication role of. If it is running, click **Actions** > **Stop**.
3. Click **Actions** > **Change replication role**.

   Alternatively, you can navigate to the **Remote replication** page, locate the instance, and click **Change replication role**.

   You are redirected to the Activity Monitor to view the progress.
4. If you use DNS, and the server is different on the other appliance, update your media servers and clients with the new settings.
5. Ask the other appliance administrator to start the instance.

Unlinking active and replica instances

In the event of a disaster scenario or after a migration, you can unlink the active and the replica instances. The replica instance becomes a separate, standalone instance. Once the instances have been unlinked, you cannot link them again, and you must choose one to use as your primary server going forward.

Use the following procedure to unlink an active and a replica instance.

To unlink an active and a replica instance

1. Sign in to the Flex Appliance Console on either appliance.
2. Navigate to the **Remote replication** page. Locate the instance that you want to unlink. Under **Replication status**, click **Unlink from replica** or **Unlink from active instance**.

   Alternatively, you can navigate to the **Application instances** section of the **System topology** page. Click **Actions** > **Unlink from replica** or **Unlink from active instance**.

   Note: If you unlink from the active instance, the instance must be stopped.

   You are redirected to the Activity Monitor to view the progress.
3. When possible, the replication settings are removed from both appliances as part of the unlink operation. However, in some cases, the settings may remain on the paired appliance. If the settings remain, perform the unlink operation again from that appliance.
4. If you use DNS and want to use the instance that was previously the replica, update your media servers and clients as needed with its settings.
5. Start the instance that you want to use. Do not start both of the unlinked instances.

Forgetting a paired appliance

Use the following procedure to forget a paired appliance. All pairing information is removed from both of the appliances.

To forget a paired appliance

1. Sign in to the Flex Appliance Console on either appliance. If you haven't already, unlink all active and replica instances.

   See "Unlinking active and replica instances" on page 101.
2. Navigate to the **Remote replication** page. In the **Paired appliances** section, click **Forget this appliance**.

3. In the confirmation window that appears, click **Forget this appliance**. You are redirected to the Activity Monitor to view the progress.
4. When the operation completes, the appliance that you started the operation from attempts to notify the other appliance of the change. In some scenarios, the notification may not be possible. If the paired appliance information remains on the **Remote replication** page of the other appliance, repeat these steps on the other appliance.

Chapter 8

Appliance security

This chapter includes the following topics:

Security overview

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

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

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

- OS security hardening, including Security-Enhanced Linux (SELinux).
- Forced password changes during initial configuration to make sure that the default password does not remain active on the system.
- The ability to set your own password policy, including the option to use STIG for validation.
  See “Changing the password policy” on page 60.

- 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 105.
- The ability to add a sign-in banner that appears before a user signs in to the Flex Appliance Console and the Flex Appliance Shell.
  See “Using a sign-in banner” on page 108.
- Support for external certificates.
  See “Using an external certificate” on page 108.
- Support for multifactor authentication, including the ability to enforce it for all Flex Appliance Console users.
  See “Managing multifactor authentication” on page 61.
- Session timeouts that automatically sign users out of the Flex Appliance Console and the Flex Appliance Shell after 10 minutes of inactivity.
- Conformance to the Federal Information Processing Standards (FIPS) 140-2.
- Password protection in the Flex Appliance Console that locks local user accounts after three sign-in attempts with incorrect passwords. If a security administrator account becomes locked, it is unlocked automatically after 30 minutes. If a different local user account becomes locked, that user and a security administrator must work together to unlock it.
- (Version 4.1 and later) Sign-in protection in the Flex Appliance Console that locks user accounts with multifactor authentication for 15 minutes after three sign-in attempts with incorrect codes.
- Password protection in the Flex Appliance Shell that locks the **hostadmin** account for 15 minutes after three login attempts with incorrect passwords.
- Password protection that restricts access to the **GRUB** menu except with assistance from Veritas Technical Support. If you need to edit GRUB, contact Technical Support and ask your representative to reference article 100048098.

Also note the following information regarding the appliance security:

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

- CVE-2019-11091

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

About lockdown mode

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

Lockdown mode provides the following benefits:

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

Flex Appliance includes the following lockdown modes:

- Normal mode
  This mode is the default mode of the appliance. Normal mode does not support WORM storage.
- Enterprise mode
  This mode adds additional access restrictions but retains a level of flexibility. In this mode:
  - You can create WORM storage instances.

- If needed, the application administrator can disable the retention lock on backup images so that they can be expired before the specified retention date.
- Users with the administrator role can delete the instances only if no data is present. If the instance is on WORM storage server version 19.0 or later, the application administrator must approve the deletion beforehand.
- If the instance is on WORM storage server version 19.0.1 or later, security administrators can delete the instances only if no data is present. The application administrator must approve the deletion beforehand.
- If the instance is on WORM storage server version 19.0 or earlier, security administrators can delete the instance if data is present. The application administrator does not need to approve the deletion beforehand.
- 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.
  - The retention lock on backup images cannot be disabled before the specified retention date.
  - You can delete the instances only if no data is present. If the instance is on WORM storage server version 19.0 or later, the application administrator must approve the deletion beforehand.
  - To change from compliance mode to enterprise mode or normal mode, you must first wait for all data on the WORM storage instances to expire and then delete the instances.

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

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

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

The appliance must be in lockdown mode before you can create WORM storage instances. See “Changing the lockdown mode” on page 107.

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

Changing the lockdown mode

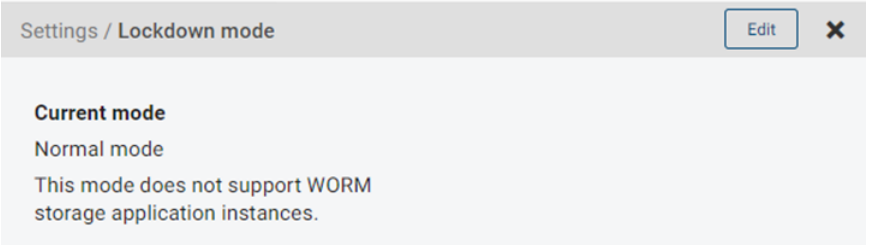
You can use the Flex Appliance Console to change the lockdown mode on a Flex appliance. Note the following restrictions:

- Lockdown mode does not block access to the remote management (IPMI) port. Veritas recommends that you set up your network to restrict access and only allow security administrators or the users that manage the physical hardware to use the port.
- Only a security administrator 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 a security administrator and click the gear icon in the upper-right corner of the page, then click **Lockdown mode**.



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

Using a sign-in banner

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

To add or edit a sign-in banner

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

To remove a sign-in banner

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

Using an external certificate

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

Importing an external certificate

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

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

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

- All certificate files must have a suffix of .pem or .cer and include `-----BEGIN CERTIFICATE-----` at the beginning of the certificate.
- All certificate files must contain the Flex Appliance Console FQDN in the common name or the subject alternative name (SAN) field of the certificate.
- The subject name and common name fields must not be left empty.

- Only ASCII 7 characters can be used in the subject and SAN fields of the certificate.
- The private key must be in the PKCS #8 PEM format, and it must begin with a header line of `-----BEGIN ENCRYPTED PRIVATE KEY-----`, `-----BEGIN PRIVATE KEY-----`, or `-----BEGIN RSA PRIVATE KEY-----`.
- Flex Appliance's web service uses the PKCS #12 standard and requires certificate files to be in the X.509 (.pem) format. If you obtained the certificate and private key in any other format you must first convert them to the X.509 (.pem) format.

To import an external certificate

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

Removing an external certificate

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

To remove an external certificate

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

Using network access control

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

To configure or edit network access control

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

   Note the following information:

   - The IP protocol of the addresses in the allowed list must match the protocol of the appliance.
   - Subnets must be entered in CIDR notation. For example, 1.1.1.0/24.
   - If you use the Dynamic Host Configuration Protocol (DHCP), add subnets instead of IP addresses.
   - For HTTPS access control, you must include your current IP address in the allowed list. It can be entered by itself or as part of a subnet.
   - For SSH access control, you can leave the allowed list empty to block all SSH access.

To disable or enable network access control

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

Changing the SSH port

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

To change the SSH port

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

Chapter 9

Monitoring the appliance

This chapter includes the following topics:

Registering an appliance

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

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

Configuring alerts

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

- Call Home
  Send notifications to Veritas and the NetInsights Console. Call Home is enabled by default.
  See "About AutoSupport and Call Home" on page 113.
  See "Configuring Call Home" on page 113.
- Email alerts
  Send notifications to an email address.
  See "Configuring email alerts" on page 114.
- SNMP alerts
  Send notifications to an SNMP manager.
  See "Configuring SNMP alerts" on page 115.

About AutoSupport and Call Home

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

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

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

Appliance documentation

Configuring Call Home

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

Use the following procedures to manage the Call Home configuration.

To configure or edit Call Home

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

To disable or enable Call Home

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

Configuring email alerts

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

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

Use the following procedures to manage email alerts.

To configure or edit email alerts

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

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

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

Enter the server IPv6 address instead of the hostname.

After alert configuration, add the server IPv6 address to the appliance Hosts file. See "Changing DNS or Hosts file settings" on page 126.

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

---

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

To disable or enable email alerts

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

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

Configuring SNMP alerts

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

Use the following procedures to manage SNMP alerts.

To configure or edit SNMP alerts

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

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

Note: If you use SNMPv3, the appliance engine ID may be required by your SNMP manager. See the following article for the steps to calculate the engine ID: How to calculate the appliance engine ID for SNMPv3

---

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

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

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

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

Enter the server IPv6 address instead of the hostname.

After alert configuration, add the server IPv6 address to the appliance Hosts file. See "Changing DNS or Hosts file settings" on page 126.

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

---

5 To verify the connection, check your SNMP manager.

To disable or enable SNMP alerts

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

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

Setting the threshold values for disk usage alerts

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

Note: Critical `diskspace` alerts are sent when disk usage exceeds 90%. This threshold cannot be changed. In some cases, backup jobs may fail before you reach the 90% threshold, so Veritas recommends that you add storage or otherwise address the issue as soon as you see an alert.

To set the threshold value

1 Log in to the Flex Appliance Shell.

2 Run the following command:

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

Where <*value*> is an integer between 0 and 89. If you enter 0, disk usage alerts are disabled. Veritas recommends that you do not set this value higher than 85.

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

To view the threshold value

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

```
show alerts diskspace-threshold
```

Monitoring the appliance from the System Health Insights portal

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

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

Viewing the hardware status

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

See "Viewing node information" on page 117.

See "Viewing storage shelf information on a Veritas 52xx Appliance" on page 120.

Viewing node information

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

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

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

To view node component health

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

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

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

Viewing storage shelf information on a Veritas 53xx Appliance

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

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

- All (components)
- BBU (battery backup unit)
- Controller
- Disk

- Fan
- Firmware
- Power
- Product
- Temperature
- Volume
- VolumeGroup

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

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

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

- configuration
- controllers
- disk-affinity
- disk-group-statistics
- disk-groups
- disk-statistics
- disks
- enclosures
- events
- pools

- ports
- sensor-status
- system
- volumes

To view storage shelf component status

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

Viewing storage shelf information on a Veritas 52xx Appliance

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

- All (components)
- Disk
- Fan
- Power
- Product
- Temperature

To view the storage shelf status

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

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

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

Viewing hardware faults

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

To view hardware faults

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

   ```
   show hardware-errors
   ```

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

Viewing system data

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

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

Table 9-1 Self-test data

Command	Description
`disk`	Shows the current status of the storage array.
`software`	Shows the current status of the various appliance software components.
`hardware`	Shows the current status of the various appliance hardware components.
`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 144.

Clearing the hardware status

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

To clear the hardware status

1 Log in to the Flex Appliance Shell.

2 Run the following command:

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

3 Follow the prompts to confirm.

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

Forwarding logs

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

Flex Appliance supports the following:

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

To configure or edit log forwarding:

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

To stop forwarding logs

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

Providing access for external monitoring

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

The following token types are available:

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

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

To generate an API access token

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **API access token**.
2. Click **Generate**.
3. Select the token type and enter the required details. When you are finished, click **Generate**.

4 A pop-up window appears with the token.

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

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

Revoking access for external monitoring

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

To delete an API access token

1 Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **API access token**.

2 Select the token that you want to delete and click **Delete**.

Chapter 10

Reconfiguring the appliance

This chapter includes the following topics:

Reconfiguring the appliance network

Use the following procedure to reconfigure the appliance network after initial configuration.

Note: You cannot change the hostnames of the nodes or the Flex Appliance Console.

To reconfigure the network

1. Stop all application instances.
2. Log in to the Flex Appliance Shell from the Veritas Remote Management Interface. If you have a multi-node appliance, you can log in to either node.
3. If DNS is not configured for the current configuration, you must update the hostname resolution information in the appliance `Hosts` file before you reconfigure the network. Update the required information for the node and the Flex Appliance Console.

   See "Changing DNS or Hosts file settings" on page 126.
4. Run the following command:

   ```
   setup configure-network
   ```
5. Follow the prompts to enter the host network information. You can enter up to three DNS server IP addresses with a comma-separated list. If you need to add more, you can use the `set network dns` command after the reconfiguration.

Note: You can use IPv4 or IPv6 addresses for the appliance, but a dual-stack network is not supported. If you change the protocol, the protocol that was originally configured becomes disabled.

Changing DNS or Hosts file settings

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

Changing DNS settings

To change the DNS server IP address or search domain

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

   ```
   set network dns
   ```
2. Follow the prompts to change the DNS settings as follows:
   - To replace the existing settings with new parameters, enter the new information in the appropriate fields. You can enter multiple DNS server IP addresses or search domains using a comma-separated list.
   - To remove the DNS settings, leave the fields blank.

Warning: If you remove existing DNS settings, you must add the hostname resolution information to the appliance `Hosts` file. See the section called "Changing Hosts file settings" on page 127.

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.

Shutting down the appliance

Use the following procedure to shut down your appliance.

To shut down an appliance

1. Stop all instances from the Flex Appliance Console.
2. Log in to the Flex Appliance Shell.
3. Do one of the following:
   - If you have a 5150 or a 52xx appliance, or if you have a 53xx appliance and do not want to turn off the storage shelves, run the following command:

     ```
     system shutdown
     ```

- If you have a 53xx appliance and want to turn off the storage shelves, Veritas recommends that you shut them down first.

  Warning: Shutting down the storage shelves is not mandatory, but if you do shut them down, you must also use the power button to turn them off. Only shut down the shelves if you are prepared to do so.

  To shut down the storage shelves, run the following command:

  ```
  support storage-shelf shutdown
  ```

  This command also shuts down the appliance nodes.

4. If you shut down the storage shelves, use the power button to turn off the primary shelf. Wait until the fans have stopped spinning, all noises have stopped, and all lights on the front panel are off. Then do the same for the expansion shelves, in order from the one that is closest to the nodes to the one that is farthest from the nodes.

   If you also need to physically turn off the appliance nodes, unplug the power cables.

   Note: When you turn the appliance and the shelves back on, you must do so in the reverse order that you turned them off. Follow the instructions in the *Hardware Installation Guide* for your appliance.

Performing a factory reset

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

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

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

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

See "Managing the appliance Fibre Channel ports" on page 42.

To perform a factory reset

1. If you have a multi-node appliance, remove the node that you want to reset from the appliance. If you want to reset both nodes, choose a node to begin the procedure with and remove that node. See "Removing a node" on page 140.
2. Log in to the Flex Appliance Shell from the node that you want to reset.

   Note: Veritas recommends that you log in from the Veritas Remote Management Interface instead of an SSH session to perform a factory reset. To access the Veritas Remote Management Interface, refer to the initial configuration procedure. See "Performing the initial configuration" on page 23.

3. Enter the following command:

   ```
   system factory-reset
   ```

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

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

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

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

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

```
set user password
```

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

Next steps for a single-node appliance

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

- If you want to delete the existing storage data, perform a storage reset and then perform the initial configuration again to reconfigure your settings.
  This option is not available if your appliance is in lockdown mode.
  See "Performing a storage reset" on page 139.
  See "Performing the initial configuration" on page 23.
- 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 137.
- If the node was never configured with the `configure-console` command, proceed with the initial configuration.
  See "Performing the initial configuration" on page 23.

Next steps for a multi-node appliance

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

- If you performed the factory reset on only one of the nodes, add it back to the appliance. If the node was previously updated, reinstall the update after you add it back.
  See "Adding a node" on page 26.
  See "Updating Flex Appliance" on page 88.
- 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 139.
  See "Performing the initial configuration" on page 23.
- 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 137.

Performing a reimage

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

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

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

Use one of the following procedures to reimage an appliance.

Reimaging from the USB drive

To reimage an appliance from the USB drive

1. Before you begin the reimage process, Veritas recommends that you record the configuration information that you entered when you performed the initial configuration.
2. Create the USB drive. See the following article for instructions: How to create a Flex Appliance USB flash drive
3. 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
4. Insert the USB drive into a USB port on the node that you want to reimage.
5. Use the following steps to access the Veritas Remote Management Interface:
   - Open a supported web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:
     - Google Chrome version 94 or later recommended (minimum version 80 or later)
     - Mozilla Firefox version 93 or later recommended (minimum version 80 or later)
   - Enter the IP address that is assigned to the remote management port of the node that you want to reimage.

- Log in to the Veritas Remote Management Interface. If you have not previously logged in, use the following default credentials:
  - **User Name**: **sysadmin**
  - **Password**: **P@ssw0rd**

6 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.

7 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.

---

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

9 On that page, do the following:

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

10 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.

---

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

12 The system begins to start from the USB drive. It then presents you with multiple options.

If you have a Veritas 5240 or 5x50 appliance, select **Install Veritas Optimised OS** and press **Enter**.

If you have a Veritas 5x60 appliance, perform the following steps:

- Select **Install Vertias Optimised OS (RA Appliances Only!)** and press **e**.
- On the following screen, locate the following line:

```
nst.ks=cdrom:/ks.cfg
inst.xdriver=vesamodprobe.blacklist\t=qla2xxx,lpfc,ocs..fc..scst,ahci,isci,ast
pcie_aspm=off
```

- Replace this line with the following text:

```
inst.stage2=hd:LABEL=VxOS inst.ks=hd:LABEL=VxOS:/ks.cfg
inst.repo=hd:LABEL=VxOS:/
```

- Enter **Ctrl +X**.

13 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
```

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

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

Reimaging from an ISO file

To reimage an appliance from an ISO file

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 file from the Download Center on the Veritas Support website.

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

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

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

- When the shell launches, click on the **Device** drop-down menu on the console and select **Redirect ISO**.
- From the **Open** pop-up window that appears, choose the ISO file 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 file 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** or **UEFI USB Device** and press **Enter**.

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

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

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

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

---

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

```
set user password
```

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

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

Next steps for a single-node appliance

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

- If you want to delete the existing storage data, perform a storage reset and then perform the initial configuration again to reconfigure your settings.
  This option is not available if your appliance is in lockdown mode.
  See "Performing a storage reset" on page 139.
  See "Performing the initial configuration" on page 23.
- 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 137.
- If the node was never configured with the `configure-console` command, proceed with the initial configuration.
  See "Performing the initial configuration" on page 23.

Next steps for a multi-node appliance

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

- If you reimaged only one of the nodes, remove the node from the appliance and then add it back to the appliance. If the node was previously updated, reinstall the update after you add it back.
  See "Removing a node" on page 140.
  See "Adding a node" on page 26.

See “Updating Flex Appliance” on page 88.

- If you reimaged both nodes and want to delete the existing storage data, perform a storage reset and then perform the initial configuration again to reconfigure your settings.
  This option is not available if your appliance is in lockdown mode.
  See “Performing a storage reset” on page 139.
  See “Performing the initial configuration” on page 23.
- If you reimaged both nodes and do not want to delete the storage data, you can recover the appliance with the existing storage data.
  See “Recovering storage data after a factory reset or a reimage” on page 137.

Recovering storage data after a factory reset or a reimage

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

Note: If you have a multi-node appliance, you only need to use this procedure if you performed a factory reset or a reimage on both nodes. If you only reset or reimaged one of the nodes, add that node back to the appliance. See “Adding a node” on page 26.

To recover the appliance

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

   ```
   setup configure-network
   ```

   Follow the prompts to enter the host network information.

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

   ---

4 Run the following command:

```
system appliance-recover
```

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

5 Follow the prompts to recover the appliance.

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

6 If you have a Veritas 5150 Appliance or a Veritas 52xx Appliance, add the applications that you have instances of and the add-ons that are installed on them to the repository before you start the instances. See “Adding files to the repository” on page 68.

7 If you have a multi-node appliance, add the node that you did not recover back to the recovered appliance. See “Adding a node” on page 26.

8 If your appliance previously had security patches installed, reinstall them. See “Updating Flex Appliance” on page 88.

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

Features that must be reconfigured after an appliance recovery

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

- Call Home
  See “Configuring Call Home” on page 113.
- Email alerts
  See “Configuring email alerts” on page 114.
- API access tokens

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

See “Revoking access for external monitoring” on page 124.
See “Providing access for external monitoring” on page 123.

- The appliance metadata for single sign-on (SSO)
  After a recovery, the appliance metadata file changes. Copy or download the new file and upload it to your identity provider (IDP).
  See the section called “Adding an IDP” on page 53.
- Multifactor authentication for the shell
  If multifactor authentication was previously configured, you are forced to reconfigure it the next time you log in to the shell.
- Remote replication with self-signed certificates
  If you have paired appliances that use self-signed certificates for communication, you must repair the connection after a recovery.
  See “Repairing a lost connection between paired appliances” on page 97.

Performing a storage reset

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

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

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

To perform a storage reset

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

   ```
   system storage-reset
   ```

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

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

4 Perform the initial configuration again to reconfigure the appliance.

Removing a node

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

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

To remove a node

1 From the Flex Appliance Console, make sure that there are no instances running on the node that you want to remove. Use the **System topology** page to view all of the running instances and relocate them as necessary.

2 Log in to the Flex Appliance Shell on the node that you want to keep in the appliance. Run the following commands and check which node the `infra_svc` service is running on:

```
support shell

hastatus -sum
```

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

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

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

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

```
support shell

hagrp -state
```

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

`setup remove-node`

Follow the prompts to remove the node.

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

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

6 If you plan to add this node back to the original appliance or use it in another Flex multi-node appliance, you must first perform a factory reset. See "Performing a factory reset" on page 128.

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

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

To view or reset the storage shelf order

1 Log in to the Flex Appliance Shell.

2 Run one of the following commands:

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

Chapter 11

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 11-1 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 11-1 Steps for troubleshooting Flex Appliance problems *(continued)*

Step	Action	Description
Step 2	Check the appliance monitoring information	If you cannot resolve the issue based on the error message, or if you don't see an error message in an interface but still suspect a problem, you can: ■ Use the hardware monitoring information to check for hardware errors. See "Viewing the hardware status" on page 117. ■ Run an appliance self-test. See "Viewing system data" on page 121. ■ 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 144. ■ 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, your representative may need an access key to unlock greater access to troubleshoot the issue. Support can generate this access key on their own, but if you prefer, you can also generate it from System Health Insights. The access key has a two-hour expiration period, so make sure that your support representative is ready to assist before you generate it. See "Unlocking access in lockdown mode" on page 143.

Unlocking access in lockdown mode

If your appliance is in lockdown mode and you need assistance from Veritas Technical Support, your representative may need an access key to unlock greater access to troubleshoot the issue. Support can generate this access key on their own, but if you prefer, you can also generate it from System Health Insights.

Warning: Improper use of the access key may result in rendering the node or the entire appliance unusable. The key should only be used for designated troubleshooting and system configuration changes under Veritas Support guidance.

Any unauthorized use is at your own risk, and you assume any liability for failures, defects, loss of data or security, or other issues that may result from such usage.

The node serial number is required to generate an access key. Use the following procedure to locate the serial number of the node that you need to unlock. Then refer to the *System Health Insights User Guide* for the procedure to generate the access key.

To locate the serial number

1. From the **System topology** page of the Flex Appliance Console, navigate to **Head nodes**. The serial number is listed in this widget.

   You can also run the following command in the Flex Appliance Shell:

   ```
   show serial-number
   ```

2. Use the serial number to generate an access key from System Health Insights. The access key has a two-hour expiration period, so make sure that your support representative is ready to assist before you generate it.

   For instructions on how to generate the access key, see the topic "Access Key" in the *System Health Insights User Guide*.

Gathering logs

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

Note: You can only generate one log package at a time.

The following log packages are available on a Flex appliance:

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

- Application instance logs
- Advanced logs
  These logs are helpful for storage and hardware failures.

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

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

1. From the Flex Appliance Console, click the question mark icon in the upper-right corner of the page, then select **Diagnostics**.
2. Click **Generate log package**.
3. By default, the logs mask user information such as hostnames, IP addresses, usernames, etc. The masking process adds additional time to the log collection. If you need to view the user information or want to speed up the log collection, deselect the **Enable data masking** option.
4. 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.
5. To download the log package, select it in the table and click **Download**. A pop-up window appears that lets you limit the download bandwidth. Select this option if needed, then click **Download** to confirm.

To generate and download a Performance log package

1. Log in to the Flex Appliance Shell and run one of the following commands:
   - To generate the log package immediately:
     ```
     support data-collect performance at=now
     ```
   - To generate the log package later:
     ```
     support data-collect performance at=<yyyy-MM-dd-HH:mm>
     ```
     Where *<yyyy-MM-dd-HH:mm>* is the year, month, day, hour, and minute when you want to generate the log package.
     For example, to collect the logs on August 3, 2023 at 6:30 P.M., run the following command:
     ```
     support data-collect performance at=2023-08-03-18:30
     ```

Note: You can only run or schedule one log generation at a time. To check if any log generations are already scheduled, use the `support data-collect list-job` command.

2 Depending on your environment, the logs take approximately one hour to generate. When they are ready, they appear in the table on the **Diagnostics** page of the Flex Appliance Console. To access this page from the console, click the question mark in the upper-right corner and select **Diagnostics**.

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

To delete a log package

1 From the Flex Appliance Console, click the question mark icon in the upper-right corner of the page, then select **Diagnostics**.

2 Select the log package that you want to delete and click **Delete**. When the confirmation window appears, click **Delete** to confirm.