NetBackup™ Flex Scale Installation and Configuration Guide

3.5.100

May 2026

VERITAS
now part of Cohesity

NetBackup Flex Scale Installation and Configuration Guide

Last updated: 2026-05-18

Legal Notice

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1

Preparing for NetBackup Flex Scale deployment

This chapter includes the following topics:

Deployment overview

At a high level, deploying Veritas NetBackup Flex Scale involves the following stages:

- **Stage 1 - Verify the deployment requirements**
  Carefully evaluate all the software and hardware requirements for NetBackup Flex Scale. The requirements cover high level areas such as power and cooling needs, networking infrastructure, and rack sizing, to more specific needs such as system requirements, IP addresses, storage, and security.
  It is critical that your IT environment meets all the required infrastructure needs so as to ensure a smoother deployment and operational experience.
  For HPE 5551 model, use the https://www.veritas.com/content/support/en_US/article.100053580 link to refer to the *NetBackup Flex Scale Hardware Cabling* poster.
  For HPE 5561 model, use the https://www.veritas.com/support/en_US/article.100065998 link to refer to the *NetBackup Flex Scale Hardware Cabling* poster.
- **Stage 2 - Assemble the nodes and install the software**
  Assemble the supported hardware and mount the nodes on to a rack in your datacenter. Connect all the power and network cables as per the instructions provided.

After setting up the target systems, procure the installation media and install the Veritas NetBackup Flex Scale software on all the nodes.

Note: Your appliance by default comes pre-installed with the NetBackup Flex Scale software. You do not need to install anything on the appliance out of the box. The installation instructions are provided only as a reference, in case you wish to wipe the appliance clean and start a fresh deployment.

See "About NetBackup Flex Scale software installation" on page 132.

- **Stage 3 - Ensure that the required Emergency Engineering Binaries (EEBs) are installed on the nodes**
  The required EEBs are available on the Download Center on the Veritas Support site (https://www.veritas.com/support/en_US). You must download and install these EEBs before you begin the configuration.
  See "Downloading EEBs" on page 120.
  See "Installing EEBs using GUI" on page 121.
- **Verifying the firmware version**
  Hardware vendors periodically release new firmware version for the appliance node components. Ensure that you install the firmware packages that are released by the vendors so the appliance nodes have the latest firmware version installed on them.
  See "About firmware upgrades" on page 95.
- **Stage 4 - Configure the cluster**
  From a web browser, connect to one of the nodes using a public IP address and run the cluster configuration workflow to configure all the nodes into a cluster.
  During the cluster configuration, you will configure the infrastructure components as well as the core NetBackup services.
- **Stage 5 - Sign in and start protecting workloads**
  Once the configuration is successful, you simply sign in to the NetBackup Flex Scale web UI and create protection plans and start protecting desired workloads.
  You can also sign in to the Veritas NetBackup Flex Scale infrastructure management UI to monitor the infrastructure components and the general health of all the configured services.
  Refer to the *NetBackup Flex Scale Administrator's Guide* for more information.

Deployment options

The following options are supported for deploying the NetBackup Flex Scale cluster:

- Deploy the cluster as a new NetBackup domain with both NetBackup primary and media servers

  In this scenario, the nodes are configured as media servers and a NetBackup primary server is configured to run on one of the cluster nodes. The media services run on all the nodes and the primary service runs on the node where the primary server is configured.

- Deploy the cluster as a scale-out media server for an existing NetBackup domain

  In this scenario, all the nodes in the cluster are configured as media servers. In a media server only deployment, the primary server is not configured as a part of the cluster. The cluster connects to an external NetBackup primary server that is already set up in a NetBackup domain. Configuring all the cluster nodes as media servers provides increased storage for backup if you already have an existing NetBackup domain configured.

Chapter 2

Configuring NetBackup Flex Scale

This chapter includes the following topics:

Assigning public IP address to a management network interface

Before you start configuring the NetBackup Flex Scale cluster, you must first assign a public IP address to management network adapter on one of the nodes. You can assign the public address to eth1, bonded eth1 and eth2, VLAN on eth1, or VLAN on bonded eth1 and eth2. If you configure the IP address on all or multiple nodes, ensure that you configure it on the same interface on all nodes. You can then connect to that node using the assigned IP address and start the NetBackup Flex Scale cluster configuration.

To assign an IP address to the eth1 management network interface on one of the nodes:

See "Assigning a public IP address to network adapter eth1 or to a VLAN on eth1 of a node" on page 11.

To configure a bond on eth1 and eth2 management network interfaces and assign an IP address to the bonded device:

See "Configuring a bond device and assigning an IP address to the bonded device or to a VLAN on the bonded device" on page 13.

Assigning a public IP address to network adapter eth1 or to a VLAN on eth1 of a node

Before you start configuring the NetBackup Flex Scale cluster, you must first assign a public IP address to network adapter eth1 on one of the nodes. eth1 is one of the network adapters on the nodes and is the designated interface for public network connections. Pick any of the nodes where NetBackup Flex Scale is installed. You need to assign an IP to the node so that it is accessible on the network. You can then connect to that node using the assigned IP address and start the NetBackup Flex Scale cluster configuration.

The node to which you assign the IP address and from where you start the cluster configuration is called the driver node.

Note: Perform these steps on one of the nodes only. You do not have to do this on all the nodes. You will require physical access to the system console.

Note: The `fd00:200/120` network is reserved and used internally by NetBackup Flex Scale, and it should not be used anywhere.

To assign a public IP to eth1 adapter or to a VLAN on eth1 on a node

1. From the system console, log on to one of the nodes using the default admin user account.

   Enter the following user credentials at the command prompt:

   - User: `admin`
   - Password: `P@ssw0rd`

   Note: The admin user account is used prior to the cluster configuration only. This account is blocked after the cluster is configured successfully.

   ---

2. Run the `set network` command to assign a public IP address to network adapter eth1 on the node.

   Type `set network` and press `Tab` to view the next available parameters.

   If the network is configured to use VLAN, use the `set network vlan gateway ip netmask vlanid` command.

- Use the following syntax on the command prompt:
  `set network interface gateway ip netmask` or `set network vlan gateway ip netmask vlanid`

Parameter	Description
ip	A public IP address that is to be assigned to the node.
netmask	The subnet mask of the network to which the public IP address belongs.
gateway	The IP address of the gateway server in your network.
vlanid	VLAN ID

  Example:
  set network interface gateway=10.100.10.1 ip=10.100.10.100 netmask=255.255.0.10
  set network vlan gateway=10.100.10.1 ip=10.100.10.100 netmask=255.255.0.10 vlanid=999

- Press **Enter**.
  The system starts making the required network changes based on the provided inputs. Messages similar to the following appear on the command prompt:

  ```
  INFO: Validating Inputs
  INFO: Setting the IP/Netmask
  INFO: Persisting the changes
  INFO: Applying the changes
  ```

3. Ensure that the following confirmation message is displayed on the command prompt:

   ```
   SUCCESS: Device configured successfully!
   ```

   When you see this message, it indicates that the IP has been assigned to the node successfully.

   You can now log out of the node.

4. Verify that the node is reachable and that you are able to access the node using the assigned IP address.

   You can now proceed to the cluster configuration workflow.

Configuring a bond device and assigning an IP address to the bonded device or to a VLAN on the bonded device

For greater resiliency, you can bond the management interfaces eth1 and eth2 and assign an IP address to the bonded device.

Before you configure bonding, ensure that both eth1 and eth2 are physically connected to the switch and the gateway for your network is reachable from eth1 and eth2 network interfaces.

Pick any of the nodes to create a bond and assign an IP to the bonded device so that it is accessible on the network. You can then connect to that node using the assigned IP address and start the NetBackup Flex Scale cluster configuration.

The node to which you assign the IP address and from where you start the cluster configuration is called the driver node.

Note: Perform these steps on one of the nodes only. You do not have to do this on all the nodes. You require physical access to the system console.

To configure bonding for eth1 and eth2 and assigning a public IP to the bonded device or to a VLAN on bonded device on a node:

1. From the system console, log on to one of the nodes using the default admin user account. Enter the following user credentials at the command prompt:

   - User: `admin`
   - Password: `P@ssw0rd`

   Note: The admin user account is used prior to the cluster configuration only. This account is blocked after the cluster is configured successfully.

   ---

2. Run the `set network bond` command to assign a public IP address to the bonded interface.

   Type `set network bond` and press `Tab` to view the next available parameters.

   If the network is configured to use VLAN, use the `set network bond gateway ip netmask mode bond_vlanid` command.

   - Use the following syntax on the command prompt:
     `set network bond gateway ip netmask mode xmit` or `set network bond gateway ip netmask mode bond_vlanid`

Parameter	Description
ip	A public IP address that is to be assigned to the node.
netmask	The subnet mask of the network to which the public IP address belongs.
gateway	The IP address of the gateway server in your network.
mode	The mode to be used for bonding.
xmit	The transmission hash policy for the bonding mode. This parameter is optional. If this option is not specified the default policy is used for each bonding mode.
bond_vlanid	The VLAN ID if you configure VLAN on the bonded interface.

Example:

```
set network bond gateway=10.100.10.1 ip=10.100.10.100
netmask=255.255.0.10 mode=802.3ad xmit=layer3+4
set network bond gateway=10.100.10.1 ip=10.100.10.100
netmask=255.255.0.10 mode=802.3ad xmit=layer3+4 bond_vlanid=999
```

Note: Both eth1 and eth2 must be physically connected and the specified gateway in the above command should be reachable from both the interfaces eth1 and eth2. If any of the devices is not connected or can't reach the gateway from that device, the `set network bond` command fails.

- Press **Enter**.
  The system starts making the required network changes based on the provided inputs. Messages similar to the following appear on the command prompt:

```
INFO: Validating Inputs
INFO: Setting the IP/Netmask
INFO: Persisting the changes
INFO: Applying the changes
```

3 Ensure that the following confirmation message is displayed on the command prompt:

```
SUCCESS: Device configured successfully!
```

When you see this message, it indicates that the IP has been assigned to the node successfully.

You can now log out of the node.

4 Verify that the node is reachable and that you can access the node using the assigned IP address.

You can now proceed to the cluster configuration workflow.

NetBackup Flex Scale configuration methods

To configure the NetBackup Flex Scale cluster, you can use a YML-based template or type the configuration details manually in the setup wizard.

See "YML configuration file" on page 52.

Configuring NetBackup Flex Scale using the setup wizard

Before you proceed, ensure that you do the following:

- Verify that you have all the prerequisites necessary for the cluster configuration. See the *NetBackup™ Flex Scale Best Practices and Troubleshooting Guide*.
- Verify that you have assigned a public IP to a node. You will use that node to start the configuration process.
  See "Assigning public IP address to a management network interface" on page 10.

To configure the NetBackup Flex Scale cluster

1 Open a web browser and connect to the NetBackup Flex Scale node to which you had assigned a public IP address earlier.

Enter the following URL in the address bar:

`https://`*`nodepublicIP`*`:8443`

If you are using IPv6 addresses, use the following URL syntax:

`https://[`*`nodepublicIP`*`]:8443`

Here, *nodepublicIP* is the public IP address that you assigned to the eth1 management interface or bonded interface of the node earlier.

Note: You can use this URL to connect to the node and launch the cluster configuration wizard only until the time the node is not part of the cluster. After the cluster is configured, the node is no longer accessible using this URL.

---

2 Sign in to the node using the root user account.

Do the following on the sign in page:

- Enter the following user credentials:
  User: `root`
  Password: `P@ssw0rd`

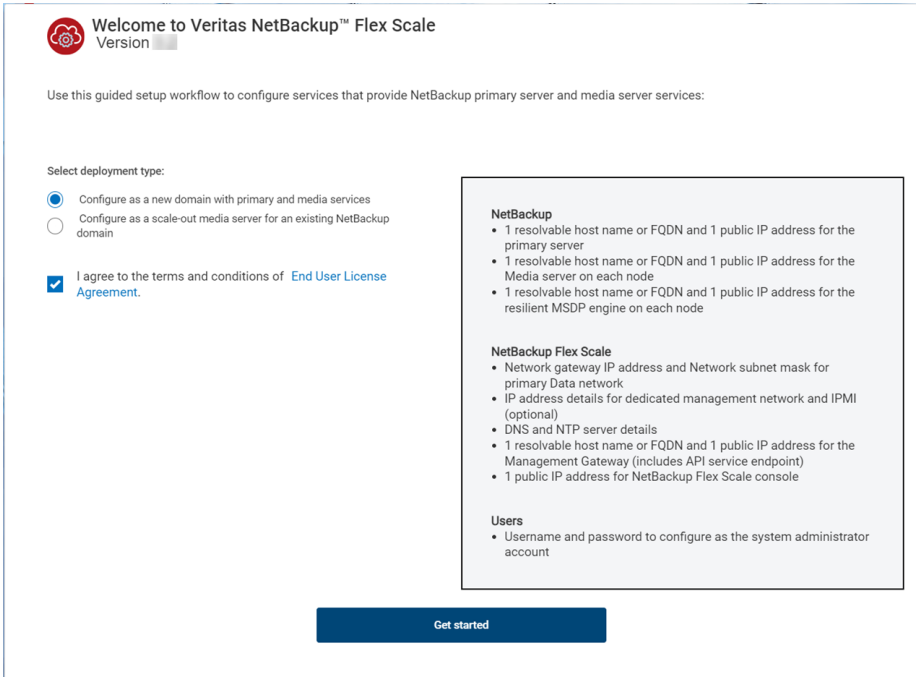
  Note: The root user account is used only during the cluster configuration. This account is blocked after the cluster is configured successfully.

  While viewing the cluster configuration status, if your session is terminated and you cannot login using the root and P@ssw0rd credentials, this mostly means the cluster configuration is successful. You can confirm by accessing the management infrastructure GUI using `https://`*`managmentConsoleIP`*`:14161`. If configuration has failed or is in progress, you will be able to log in to the configuration GUI using the root and P@ssw0rd credentials.

- Click **Sign in**.


Veritas NetBackup™ Flex Scale
Username *
root
Password *
Sign in

3 On the Welcome screen, select the deployment option. To configure both a NetBackup primary server and media servers in the cluster, select the **Configure as a new domain with primary and media services** option. To configure only media servers in the cluster, select the **Configure as a scale-out media server for an existing NetBackup domain** option. Review the information displayed on the Welcome screen, select **I agree to the terms and conditions of End User License Agreement**, and then click **Get started**.



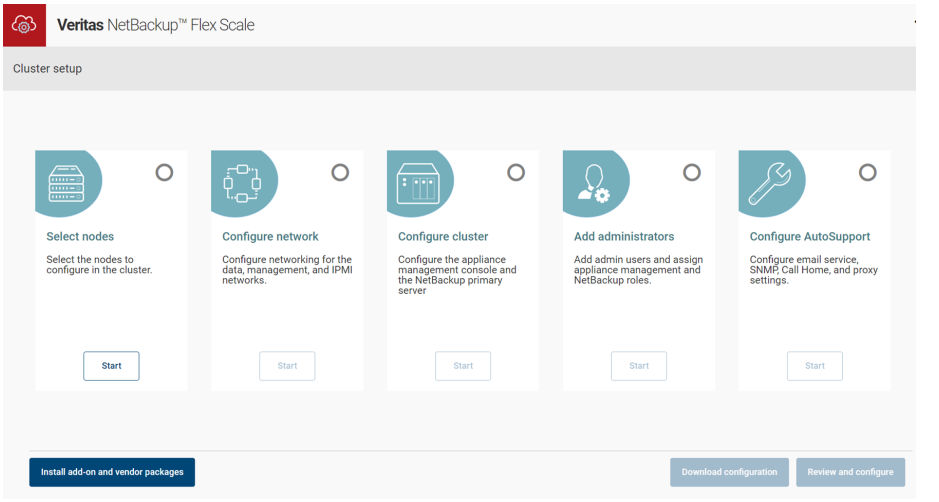
4 On the Cluster Setup panel, you are presented with a set of configuration options. To configure the cluster, you can either click through each of these options and provide the required configuration details manually in the setup wizard or you can import a YML configuration file. The YML file contains the configuration settings in form of name-value pairs, which correspond to all the parameters that are displayed in the setup wizard.

As a part of the cluster configuration, you can choose to install Emergency Engineering Binaries (EEBs), which provide critical fixes that are not included as part of the ISO image that is pre-installed on the NetBackup Flex Scale node. Ensure that all the required EEBs are installed before the cluster configuration. To install EEBs:

- On the Cluster Setup panel, click **Install add-ons and vendor packages**.

- Select and upload the EEBs that you want to install. On the **Install add-ons** tab, click **Choose add-ons**, select the EEBs, and then click **Upload file**.
  The uploaded EEBs are displayed and their status is shown as **Available**. The EEBs are installed in the order in which they are displayed. If the EEBs are required to be installed in a specific sequence, click the arrows in the **Reorder** column to change the installation sequence. If you want to delete the uploaded EEBs, select the EEBs and click **Remove**. You cannot delete EEBs after they are installed.
- Install the EEBs. Select the EEBs and click **Install**.
  The selected EEBs are installed on all the nodes. If the EEBs are installed successfully on all the nodes, a notifications is displayed on the top of the page and the status is shown as **Installed**. If the installation fails on one of the nodes, the EEB is rolled back on all the nodes and the EEB status is shown as **Available**. If one of the selected EEBs fails to install and multiple EEBs are selected, the successive EEBs are not installed. You can continue with cluster configuration irrespective of the failure.

To provide configuration inputs and begin with the cluster configuration, in the Select nodes box, click **Start**.



5 If you want to use a configuration file for providing the configuration details, on the Select Nodes panel click **Import configuration file**, select the YML configuration file, and then click **Save**. To continue with the cluster configuration go to step 11.

If you want to provide the configuration details manually in the setup wizard, go to step 6.

6 On the Select Nodes panel, review the cluster settings and the names of the nodes that you want to configure in the cluster.

Cluster settings:

- Click **Edit names** and on the Edit name dialog box, specify the required parameters:

Parameter	Description
Cluster name	Specify a name for the NetBackup Flex Scale cluster. The following criteria apply: ■ The cluster name can contain the following characters: a-z, 0-9, - ■ The cluster name must start with a lowercase letter. ■ The cluster name must not contain uppercase letters. ■ The cluster name must include a minimum of 3 characters and can contain a maximum of 63 characters.
Domain name	Specify the name of the domain that the nodes will be a part of. The name must be a fully qualified name. For example, `mycompany.mydomain.com`.

The cluster name serves as a prefix for the node names. The serial number of the nodes is displayed, which helps you to identify the nodes and assign the node names accordingly. You can modify the node names if required. The following conditions are applicable:
Which host name is assigned to which node

- In the node name, the hostname can contain a maximum of 63 characters.
- The host names need not be resolvable.
- The Fully Qualified Domain Name (FQDN) of the node can contain a maximum of 253 characters, including all the dots used in the name. Node name FQDN (253 characters) = hostname (63 characters) + domain name (190 characters, including dots)
- Ensure that the FQDN corresponding to the node names are unique in the domain. Node names can be the same as management interface name of that node but it can't be same as the hostname of any other FQDN.

- Click **Confirm**.

Nodes:

A minimum of 4 healthy nodes are required to form a cluster. You can deploy a maximum of 16 nodes. The available nodes are discovered automatically. To rediscover the nodes, click **Rescan**.

Note: Ensure that you click **Rescan** before you proceed.

The panel displays the following details about each node:

Label	Description
Node name	Displays the auto-generated name for the node. The names are numerically sequenced based on the specified cluster name and domain.
Status	Displays the current status of the node. A healthy status indicates that the node is ready to be part of the cluster. **Note:** You cannot add unhealthy nodes to the cluster.
Size	Displays the maximum storage capacity available on the node.
Model	Displays the appliance model number.
Revision	Displays the model revision number.
Serial number	Displays the unique serial number of the node.
Primary Data(eth5)	Displays the MAC address of network interface eth5 on the node. This interface is used for the data network traffic.
Management(eth1)	Displays the MAC address of network interface eth1 on the node. This interface is used for the cluster management network traffic.

Download configuration file template or export configuration:

- Click **Generate configuration template** if you want to download the default YML configuration file template (`config.yml`).

  The wizard prompts you whether you wish to specify an IP range for the required IP addresses.

  - Click **Yes** if you want NetBackup Flex Scale to automatically assign IP addresses based on the IP range that you specify.
  - Click **No** if you wish to manually specify all the required IP addresses.

Based on your response, the YML configuration file that gets generated includes the IP address parameter in the appropriate syntax.
You can manually edit the `config.yml` template file to add the necessary cluster parameter values, and then import that YML file again.

- Click **Export inventory CSV** if you want to save the displayed node details as a comma separate values (csv) file for reference.

Click **Save** to confirm the cluster and node settings.

Note: Ensure that you select at least 4 healthy nodes. The driver node from where you launched the cluster configuration workflow is selected by default. You cannot select unhealthy nodes to be a part of the cluster as these are disabled for selection.

---

7 Configure the network settings for the data network, the management network, and the IPMI network for the cluster.

To begin, in the Configure network box, click **Start** and then specify the following details:

Data Network

Specify the networking details for the data network. All the NetBackup operational data traffic, including communications with external hosts and services, is routed on this network. A data network is required to set up the cluster.

Note: If you configure a DNS for the cluster, ensure that you use the same FQDN or the short name for the IP addresses for which there are entries in the DNS. The IP address and FQDNs which do not have an entry in DNS can still be used for configuration.

- Routing settings
  Specify the network routing settings for the data network.

Parameter	Description
IPv4 | IPv6	Click **IPv4** or **IPv6** depending on the IP addressing that you wish to configure in the cluster.
Subnet Mask	If using IPv4 public addresses, specify the subnet mask of the data network.

Parameter	Description
Gateway	If using IPv4 public addresses, specify the IP address of the gateway server in your network.
Prefix Length	If using IPv6 public addresses, specify the IPv6 prefix length.
Router	If using IPv6 public addresses, specify the router address.

Note: If you switch from IPv4 to IPv6 (or vice versa) after specifying the parameter inputs, then all the inputs entered until that point will be lost and you will have to enter them again.

- Domain Name System (DNS)
  To specify the DNS server settings for the data network, select **Enable DNS** and specify the following details.

Parameter	Description
Domain name	Displays the domain name you specified in the cluster settings panel earlier. To modify this parameter, save and close this dialog box and go back to the Select nodes panel to edit the domain name.
DNS server	Specify the IP address of the DNS server for the management and the data network.
Search Domains	Specify the search domains for resolving host names and IP addresses. Use commas to separate multiple values.

- Advanced network options

Parameter	Description
Interface Bonding	If you wish to use NIC bonding for high availability of the network interfaces, select Interface Bonding and then choose the bonding type from the drop-down list. Refer to the *NetBackup Flex Scale Administrator's Guide* for more details about NIC bonding support.
VLAN ID	If you wish to use a pre-configured virtual LAN, specify the VLAN ID. The ID can be any value between 1 and 4095.

- Media servers

Specify a public IP address and either a Fully Qualified Domain Name (FQDN) or a short host name for the media server service for each node.

Note: The name and the serial number is displayed for each node, so you can identify the nodes to which the media server IP addresses will be assigned.

Parameter	Description
Automatic | Custom	Choose how you wish to assign IP addresses to the media server service on each node. ■ Click **Automatic** if you want NetBackup Flex Scale to automatically assign IP addresses from the IP range that you specify. FQDN is automatically resolved with DNS lookup if the **Automatic** option is selected. ■ Click **Custom** if you want to specify the IP addresses manually.
IP address	If using the Automatic option, specify an IP address range. Ensure that the IP range includes a sufficient number of IP addresses to assign, depending on the number of nodes. ■ You can specify the IP address range separated by a dash. For example, `10.xx.xxx.192-10.xx.xxx.208`. ■ You can specify the IP address range in the CIDR format. For example, `10.xx.xxx.192/30`. If you don't have an IP address range but want to avoid specifying FQDNs, you can specify comma-separated individual IP addresses. For example, 10.100.10.101,10.100.10.143,10.100.10.201,10.100.10.212
FQDN | Short host Name	If using the Custom option, specify the FQDN or the short host name for the media server service on each node. The FQDN or the short host name that you specify can contain a maximum of 64 characters. The FQDN must resolve to a single IP address.
IPv4 address	If using the Custom option, specify the IP address for the media server service on each node.

Note: If you switch between **Automatic** and **Custom** after specifying the parameter inputs, then all the inputs entered until that point will be lost and you will have to enter them again.

- MSDP engines
  Specify a public IP address and either a FQDN or a short host name for the MSDP engine service for each node.

Note: The name and the serial number is displayed for each node, so you can identify the nodes to which the msdp engine IP addresses will be assigned.

Parameter	Description
Automatic | Custom	Choose how you wish to assign IP addresses to the MSDP engine service on each node. ■ Click **Automatic** if you want NetBackup Flex Scale to automatically assign IP addresses from the IP range that you specify. FQDN is automatically resolved with DNS lookup if the **Automatic** option is selected. ■ Click **Custom** if you want to specify the IP addresses manually.
IP address	If using the **Automatic** option, specify an IP address range. Ensure that the IP range includes a sufficient number of IP addresses to assign, depending on the number of nodes. ■ You can specify the IP address range separated by a dash. For example, `10.xx.xxx.192-10.xx.xxx.208`. ■ You can specify the IP address range in the CIDR format. For example, `10.xx.xxx.192/30`. If you don't have an IP address range but want to avoid specifying FQDNs, you can specify comma-separated individual IP addresses. For example, 10.100.10.101,10.100.10.143,10.100.10.201,10.100.10.212
FQDN | Short host name	If using the Custom option, specify the FQDN or the short host name for the MSDP engine service on each node. The FQDN or the short host name that you specify can contain a maximum of 64 characters. The FQDN must resolve to a single IP address.
IPv4 address	If using the **Custom** option, specify the IP address for the MSDP engine service on each node.

Note: If you switch between **Automatic** and **Custom** after specifying the parameter inputs, then all the inputs entered until that point will be lost and you will have to enter them again.

- Click **Next**.

Management Network

Specify the networking details for the management network.

- Routing settings
  Select **Configure a separate management network** and then specify the network routing settings for the management network.
  Configuring a separate network for the management traffic is optional. If you skip this step, all the cluster management traffic is automatically routed over the data network.

Parameter	Description
IPv4 | IPv6	Click **IPv4** or **IPv6** depending on the IP addressing that you wish to configure in the cluster.
Subnet Mask	If using IPv4 public addresses, specify the subnet mask of the management network.
Gateway	If using IPv4 public addresses, specify the IP address of the gateway server in your network.
Prefix length	If using IPv6 public addresses, specify the IPv6 prefix length.
Router	If using IPv6 public addresses, specify the router address.

- Domain Name System (DNS)
  To specify the DNS server settings for the management network, select **Enable DNS** and specify the following details:

Parameter	Description
Domain name	Displays the domain name you specified in the cluster settings panel earlier. To modify this parameter, save and close this dialog box and go back to the Select nodes panel to edit the domain name.
DNS server	Specify the IP address of the DNS server for the management network.
Search Domains	Specify the search domains for resolving host names and IP addresses. Use commas to separate multiple values.

- Advanced network options

Parameter	Description
Interface Bonding	If you wish to use NIC bonding for high availability of the management network interfaces (eth1 and eth2), select **Interface Bonding** and then choose the bonding type from the drop-down list.
VLAN ID	If you wish to use a pre-configured virtual LAN, specify the VLAN ID. The ID can be any value between 1 and 4095.

- Management Interfaces

  Specify the public IP address to be assigned to the designated management network interface on each node.

  The node names are displayed automatically.

Note: The name and the serial number is displayed for each node, so you can identify the nodes to which the management interface IP addresses will be assigned.

Parameter	Description
Automatic | Custom	Choose how you wish to assign IP addresses to the management interfaces on each node. ■ Click **Automatic** if you want NetBackup Flex Scale to automatically assign IP addresses from the IP range that you specify. ■ Click **Custom** if you want to specify the IP addresses manually.
IP address	If using the Automatic option, specify an IP address range. Ensure that the IP range includes a sufficient number of IP addresses to assign, depending on the number of nodes. ■ You can specify the IP address range separated by a dash. For example, `10.xx.xxx.192-10.xx.xxx.208`. ■ You can specify the IP address range in the CIDR format. For example, `10.xx.xxx.192/30`. If you don't have an IP address range but want to avoid specifying FQDNs, you can specify comma-separated individual IP addresses. For example, 10.100.10.101,10.100.10.143,10.100.10.201,10.100.10.212
FQDN	If using the Custom option, specify the FQDN for the management interface on each node. The FQDN must resolve to a single IP address.

Parameter	Description
IPv4 address	If using the Custom option, specify the IP address for the management interface on each node.

- Click **Next**.

IPMI Network

Specify network details for the IPMI network. An IPMI network is used for system monitoring and management by directly connecting to the system hardware. It is independent of the host CPU, firmware, and operating system.

This is an optional step. You can configure the IPMI network at any time after the cluster configuration.

Select **Configure a separate IPMI network** and then specify the following details:

- IPMI interfaces
  Specify a public IP address to be assigned to the designated IPMI network interface on each node.

Parameter	Description
Automatic | Custom	Choose how you wish to assign IP addresses to the IPMI interfaces on each node. ■ Click **Automatic** if you want NetBackup Flex Scale to automatically assign IP addresses from the IP range that you specify. ■ Click **Custom** if you want to specify the IP addresses manually.
IP address	If using the Automatic option, specify an IP address range. Ensure that the IP range includes a sufficient number of IP addresses to assign, depending on the number of nodes. ■ You can specify the IP address range separated by a dash. For example, `10.xx.xxx.192-10.xx.xxx.208`. ■ You can specify the IP address range in the CIDR format. For example, `10.xx.xxx.192/30`.
IPv4 address | IPv6 address	If using the Custom option, specify the IP address for the IPMI interface on each node.

- Routing settings
  Specify the network routing settings for the IPMI network.

Parameter	Description
IPv4 | IPv6	Click **IPv4** or **IPv6** depending on the IP addressing that you wish to configure for the IPMI network.
Subnet mask	If using IPv4 public addresses, specify the subnet mask of the IPMI network.
Gateway	If using IPv4 public addresses, specify the IP address of the gateway server in your network.
Prefix length	If using IPv6 public addresses, specify the IPv6 prefix length.
Router	If using IPv6 public addresses, specify the router address.

- Click **Next**.

Custom hosts

Configure a custom hosts file to map host names and domain to IP addresses so that it helps the system to resolve addresses quickly without querying the DNS.

This is an optional step. You can create a custom hosts file at any time after the cluster configuration.

- Select **Configure a custom hosts file** and then review the list of the host and IP mapping entries that are auto-generated based on the configuration inputs that you have provided so far.
- You can add any additional host names as required.
  To add an entry, specify the IP address and FQDN in the respective fields and then click the plus icon that appears on the right side of the panel.
  You can specify both IPv4 and IPv6 addresses for the additional host entries.
- Click **Next**.

Summary

- Review the network configuration settings that you have specified so far. To modify any settings, click the **Edit** button.
- Click **Save** to confirm the network configuration settings.

8 Specify the network settings for the NetBackup Flex Scale infrastructure management UI, the NetBackup primary server, and the management server.

To begin, in the Configure Cluster box, click **Start** and then specify the following details:

Network

- **Infrastructure Management**

Parameter	Description
Cluster name	Displays the cluster name you specified in the cluster settings panel earlier. To modify this parameter, save and close this dialog box and go back to the Select nodes panel to edit the cluster name.
Console IPv4 | Console IPv6	Specify a public IP address for the NetBackup Flex Scale infrastructure management UI. The type of IP address, whether IPv4 or IPv6, depends on the IP addressing you specified for the management network's routing settings. This IP is used to access the NetBackup Flex Scale infrastructure management UI.
Console FQDN	Specify the FQDN which corresponds to the console IP. This is not a mandatory field. You can add this post configuration.
Management Server FQDN	If you chose to deploy both the NetBackup primary server and media servers, specify a resolvable short host name or FQDN for the NetBackup Flex Scale management and API server. If the cluster is deployed with only media servers, NetBackup Flex Scale management and API server is not supported and the console IPv4 or IPv6 address is used to access the UI. The short host name or the FQDN that you specify can contain a maximum of 64 characters. **Note:** This is the internal management server of the NetBackup Flex Scale cluster. Do not specify the name of your public network gateway server here.
Management Server IPv4 | Management Server IPv6	If you chose to deploy both the NetBackup primary server and media servers, specify a public IP address for the NetBackup Flex Scale management server. The type of IP address, whether IPv4 or IPv6, depends on the IP addressing you specified for the management network's routing settings. **Note:** This is the internal management gateway of the NetBackup Flex Scale cluster. Do not specify the IP address of your public network gateway server here. If a media server only cluster is deployed, the NetBackup Flex Scale management server is not supported and the console IPv4 or IPv6 address is used to access the UI.

- **NetBackup Primary Settings**

  Specify the settings described in the table below if you opted for new NetBackup domain with both primary and media server deployment:

Parameter	Description
Host Name	Specify a resolvable short host name or FQDN for the NetBackup primary server service. The primary server service is configured as a highly available failover service and runs on any one of the cluster nodes. The short host name or the FQDN that you specify can contain a maximum of 64 characters. The FQDN for the primary server must belong to the same domain as that of the cluster nodes and the FQDN for the media server and MSDP engine services that you specified earlier.
IPv4 | IPv6	Specify a public IP address for the NetBackup primary server service. The type of IP address, whether IPv4 or IPv6, depends on the IP addressing you specified for the data network's routing settings.

  Specify the following details if you opted for the media server only deployment option:

Parameter	Description
Primary server host name	Specify the FQDN or the short name of the NetBackup primary server that the cluster will connect to. The primary server is external to the cluster and must be already configured in an existing NetBackup domain. The FQDN can contain a maximum of 253 characters and the short host name can contain a maximum of 64 characters. The FQDN for the primary server must belong to the same domain as that of the cluster nodes and the FQDN for the media server and MSDP engine services that you specified earlier.

Parameter	Description
API key	Specify the NetBackup API key, which is a pre-authenticated token that identifies a NetBackup user to NetBackup RESTful APIs. The user can use the API key in an API request header when a NetBackup API requires authentication. API keys can be created for authenticated NetBackup users. A specific API key is only created one time and cannot be recreated. Each API key has a unique key value and API key tag. **Note:** Only one API key can be associated with a specific user at a time. If you create a new key for a user that already has an API key, the existing key becomes invalid, leading to issues in cases where the key was used previously for configuring a cluster or used by users for accessing APIs.
Media server gateway name	Specify a name that the primary server can use to identify all the media servers in the cluster. This name is used by the primary server to map and access all the media servers in the cluster.

- **Private IP Settings**

Parameter	Description
Private IPv4	If using IPv4 addresses, specify a private subnet IP to be used for internal communication between the cluster nodes. For example, you can specify the IP as 172.16.0.1.
Subnet Mask	Specify the subnet mask for the IP address that you specified earlier. The default supported private network subnet mask is 255.255.224.0. You must use a subnet that is equal or larger than 255.255.224.0.
Private IPv6	If using IPv6 addresses, specify a private subnet IP to be used for internal communication between the cluster nodes.
Prefix Length	If using IPv6 addresses, specify the IPv6 prefix length. The prefix length must be greater than or equal to 115.

Note: The private network supports IPv4 and IPv6 addresses. You can specify both IPv4 and IPv6 addresses simultaneously.

- Click **Next**.

Cluster setting

- **MSDP engine account**
  Specify a user account that can be used to access the MSDP engine containers. This account will have the permissions to manage all the storage on the NetBackup Flex Scale cluster nodes. This account is also used to set up NetBackup Auto Image Replication (AIR).

Parameter	Description
Username	Specify the name for the user account that can be used to access the NetBackup MSDP engine containers.
Password	Specify the password for the user account that you specified earlier.
Confirm password	Confirm the password for the user account that you specified earlier.

  The following are the rules for the credentials:

  - The user name and the password can be up to 62 characters in length. The user name and the password cannot be empty and cannot contain spaces and tabs.
  - You can use characters in the printable ASCII range (0x20-0x7E) except for the following characters:
    - Asterisk (*)
    - Forward slash (/)
    - Ampersand (&)
    - Dollar sign ($)
    - Percent sign (%)
    - Caret sign (^)
    - Angular brackets (<>)
    - Quotation mark (")
    - Comma (,)

- Parentheses (())
- Square brackets ([])
- Single quotation mark (')
- Curly brackets ({})
- backtick or grave accent (`)

- **Region Settings**

Parameter	Description
Timezone	From the drop-down list, select a time zone that you want to apply to the cluster nodes.
NTP server	Specify an NTP server that you want to use to set and synchronize the system clocks on the cluster nodes. You can specify an IP address or an FQDN. The type of IP address depends on the data network routing settings that you specified earlier. If the data network is configured to use IPv4 addresses, the NTP server IP address must be an IPv4 address. Conversely, if the data network uses IPv6 addresses, the NTP server IP must be an IPv6 address. For example, `time.google.com`.

- **Disaster recovery**
  Specify the settings described in the table below if you opted to deploy both NetBackup primary and media servers:

Parameter	Description
Passphrase	Enter the disaster recovery passphrase for the cluster.
Confirm passphrase	Enter the passphrase again to confirm it.

- Click **Next**.

Security settings

Lockdown modes provide additional levels of security for your data. With lockdown mode, you can create Write Once Read Many (WORM) storage and protect WORM data from being modified or deleted. You can also specify a retention period, which specifies the duration for which you want to protect the data.

- **Select lockdown mode**
  You can choose from the following lockdown modes:
  - Normal: This mode is the default mode of the cluster. Normal mode does not support WORM storage and data retention capabilities.
  - Enterprise: In this mode, you can create WORM storage and define the duration for which you want to retain the data. In this mode, a user with Appliance administrator role can remove the retention lock and expire data but cannot reduce the retention period. Retention lock can be removed using only the MSDP Restrict Shell. A user with NetBackup administrator role can increase the retention period.
  - Compliance: In this mode, you can create WORM storage and define the duration for which you want to retain the data. However, you cannot expire data before the defined retention period. A user with NetBackup administrator role can increase the retention period.

  Note: After the initial configuration is complete, you have the option to change the lockdown mode. You can change the lockdown mode from normal to enterprise or compliance mode, or from enterprise to compliance mode.

  If you select enterprise or compliance mode, you can restrict remote access to the node by selecting the **Restrict remote management access** checkbox. This option is not available for normal lockdown mode. Restricting remote management access to nodes provides an additional level of data security and limits the privileges and operations that you can perform. You can view and perform limited operations in the IPMI web GUI but cannot open the remote console. Physical access to the system is required to log on to the console.
  After you enable this restriction, an IPMI Administrator user on an HPE platform has only **Login** and **Virtual Power and Reset** privileges. With these privileges, the user can only view settings in iLO and perform power-related operations.

  Note: After you enable restricted remote access, you can disable this option if the appliance is in enterprise lockdown mode. If the lockdown mode is set to compliance, you cannot disable the remote access restriction. You can also choose to enable or disable remote access after the initial configuration is complete.

- **Storage settings**

Set the minimum and maximum retention time in hours, days, months, or years. The minimum retention time specifies the minimum duration for which the data cannot be modified or deleted if the cluster is in enterprise or compliance mode. Minimum retention period is one hour. The maximum retention time specifies the maximum duration for which data must be retained before it can modified or deleted.

The maximum retention time is 30 years.

- **STIG**

  The Security Technical Implementation Guide (STIG) provides technical guidance for increasing the security of information systems and software to help prevent malicious computer attacks. Select the **Enable STIG** option to enable STIG.

  STIG is enabled at the cluster level. If the STIG option is enabled, the STIG rules are enforced on all the nodes in a cluster.

- Click **Next**.

Licenses

Add the desired storage and NetBackup licenses to the cluster. You can add both the NetBackup and the storage license during the initial configuration.

This step is optional. If you do not add a license at this stage, the cluster is automatically configured with a trial license. However, to maintain a working cluster, after the cluster configuration is complete, you must add a valid storage license using the NetBackup Flex Scale infrastructure management UI. To add a NetBackup license post cluster configuration, you must use the NetBackup Java Console UI.

Parameter	Description
Storage licenses	Click **Add license** to add one or more storage licenses to the cluster configuration. A valid storage license is required to maintain a working cluster.

Parameter	Description
NetBackup licenses	Click **Add a license** to add a NetBackup license to the cluster configuration. A valid license is necessary to maintain a working cluster. NetBackup license is not required for cluster configuration if you opted for the media server only deployment option. **Note:** You can use the NetBackup Java Console UI to manage the NetBackup licenses that are added to the cluster.

Summary

- Review the network, cluster, security, and licensing settings that you have specified so far. To modify any settings, click the **Edit** button.
- Click **Save** to confirm all the settings.

9 Add administrative user accounts to the cluster.

If you opted to deploy the cluster with both NetBackup primary and media servers, assign NetBackup Flex Scale cluster management and NetBackup roles. If you opted to deploy the cluster with only media servers, assign NetBackup Flex Scale cluster management role.

To begin, in the Add administrators box, click **Start** and specify the following details:

Add users

If you opted to deploy the cluster with both NetBackup primary and media servers, you must add at least one administrator account with the Appliance administrator and NetBackup administrator role to manage the NetBackup Flex Scale cluster system and NetBackup. If you opted to deploy the cluster with only media servers, you must add at least one administrator account with the Appliance administrator role to manage the NetBackup Flex Scale cluster system. You cannot assign the NetBackup administrator role to the account.

Ensure that you do not add any of the default users that already exist such as the maintenance user, and do not specify a dictionary word as the password.

Do the following:

- Click **Add Appliance and NetBackup Administrator**.
- On the Add default administrator dialog, specify the required parameters:

Parameter	Description
Username	Specify the name for the admin user account.
Password	Specify the password for the admin user account.
Confirm password	Confirm the password for the admin user account. The password must be at least 8 characters long and must fulfill the following requirements: ■ Must contain at least one lowercase letter, one uppercase character, and a numeric digit ■ Must contain one of the following special characters: !@#$%^&~ ■ Must not be a dictionary word
Appliance Administrator	Select this option to assign the NetBackup Flex Scale cluster administrator role to this user account. The cluster admin user account has the permissions to manage all the infrastructure components in the cluster such as the cluster nodes, cluster settings, and the cluster operations.
NetBackup Administrator	Select this option to assign the NetBackup administrator role to this user account. This role has the permissions to manage the NetBackup services and operations in the cluster. **Note:** This role is applicable only if the cluster is deployed with both NetBackup primary and media servers.

- Click **Add** to add the specified user account.
  Repeat this process to add additional user accounts as required. You can add up to 10 admin users.
  To edit or remove an existing user account, in the table row, click the action button that appears on the right and then select **Edit** or **Remove**.

Change default passwords

For increased security, password changes are enforced to ensure that known default passwords do not exist on the system. You must change the default password for the maintenance user before you configure the cluster. The maintenance user account with Maintenance User role is a default account that is present on all the nodes. To change the password for the maintenance accounts, click **Set password**. Specify the password and click **Save**.

The password for the maintenance user must be at least eight characters in length and must include at least one uppercase, lowercase, numeric, and special character. The permitted special characters are: !@#$%^&~

Dictionary words are not allowed.

The password for the Administrator user can be a maximum of 16 characters and cannot include white spaces and the special characters backslash (\) and exclamation point (!).

Summary

- Review the admin user accounts that you have added so far. To modify any settings, click the **Edit** button.
- Click **Save** to confirm the user accounts.

10 Configure the Veritas Autosupport service.

The AutoSupport service allows for proactive monitoring, management, and support of the cluster's health and performance. It identifies the probable risks and issues in the environment and provides alerts to admin users and service engineers. This mechanism allows you to manage such issues before they have an adverse effect on your production environment.

Note: Veritas recommends that you configure AutoSupport for improved customer support experience and reduced downtime in case of failures.

This step is optional. You can configure the Autosupport service at any time after the cluster configuration.

To begin, in the Configure Autosupport box, click **Start** and then provide the following details:

- **Email service configuration**
  Configure an SMTP email server to enable email-based alerts and notifications.
  Specify the following parameters:

Parameter	Description
Notification interval	Specify the notification interval, in minutes, for email-based alerts. Enter a value in multiples of 15 minutes.
SMTP server	Enter the FQDN or the IP address (IPv4 or IPv6) of the SMTP server.

Parameter	Description
Server port	Specify the port number to use for communicating with the SMTP server.
Software administrator email	Specify the email address of the admin users who will be the recipients of software-related email alerts. Use commas to separate multiple entries.
Hardware administrator email	Specify the email address of the admin users who will be the recipients of hardware-related email alerts. Use commas to separate multiple entries.
Sender email	Specify the sender email address. The sender email is used as a source address for sending all email-based communications.
SMTP account	Enter the SMTP server user account.
Password	Enter the password of the SMTP server user account specified earlier.
Encryption enabled	Select this option to enable encrypted communication.

- **SNMP service configuration**
  Configure the SNMP service if you want to remotely monitor the cluster nodes using the SNMP protocol.
  - Click to expand the SNMP service configuration section and then click **Enable SNMP** to enable it.
  - Specify the following parameters:
    NetBackup Flex Scale supports SNMP-v2 and SNMP-v3 prototcols. If you select SNMP-v2, specify the following details:

Parameter	Description
SNMP server	Enter the FQDN or IP address (IPv4 or IPv6) of the SNMP server in your network.
SNMP port	Specify the SNMP port. For example, 161.
Community	Enter the community string to be used to authenticate the SNMP requests.

    If you select SNMP-v3 specify the following details:

Parameter	Description
SNMP server	Host name or the IP address of the SNMP server. The IP address can be an IPv4 or an IPv6 address. Alert notifications that are generated by the appliance are sent to this server.
SNMP port	Port number of the SNMP server. The default port is 162. **Note:** Your firewall must allow access from the appliance to the SNMP server through the configured port.
SNMP username	SNMP user name
Authentication protocol	Specify the authentication protocol. It provides authentication based on the HMAC-SHA algorithms. Choose one of the following options: ■ None ■ SHA256 ■ SHA512 This is a mandatory field.
SNMP password	Enter the password.
Encryption protocol	Specify the encryption protocol. If provides DES 56-bit encryption in addition to authentication based on the AES standard. ■ None ■ AES128 ■ AES192 ■ AES256 ■ AES512 This is a mandatory field.
Encryption passphrase	Enter the passphrase that you want to use for encryption.

- **Call home and proxy settings**
  Configure the Call Home and proxy settings to enable communication with the Veritas Call Home server for uploading system software and hardware diagnostics information.
  - Click **Enable Call Home transmission** to enable the option.

- Click **Enable proxy server** to enable proxy server communication option and then specify the following parameters:

Parameter	Description
Proxy server	Enter the IP address or the FQDN of the proxy server in your network. If you use an IPv6 cluster, ensure that you specify an IP address for the proxy server.
Proxy Port	Specify the port number to use for communicating with the proxy server.

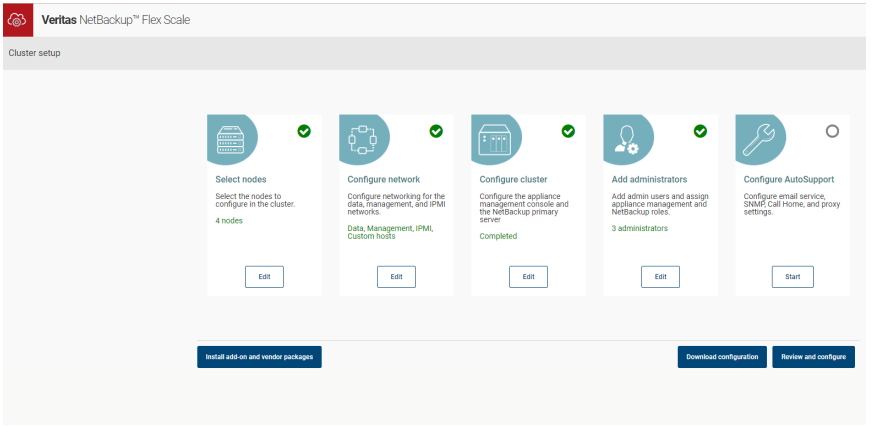
- Click **Enable proxy tunneling** to enable a secure communication channel with the Veritas Call Home server.
- Select **Authenticate proxy server** and then specify the following parameters:

Parameter	Description
Proxy username	Specify the user account to use for authenticating communication requests to the proxy server.
Proxy password	Enter the password of the user account specified earlier.

- Click **Save** to confirm the specified settings.

11 The Cluster Setup panel is displayed. A green tick mark in the configuration options box indicates that all the required parameters have been specified.

If you had opted to use the configuration file, the configuration settings that you specified in the configuration file as name-value pairs are displayed in the corresponding parameters in the setup wizard.



To proceed, do the following:

- Click **Download Configuration** if you want to save all the specified cluster configuration settings locally in a YML file. The YML file serves as a reference and can be used to import the settings if you want to reconfigure the cluster.
- Click **Review and configure**. A summary page is displayed, which shows a summary of the all specified details for all the options.

  To validate the specified configuration details before you start with the cluster configuration, click **Run precheck**. This step is optional. However, running cluster configuration precheck helps you to identify issues earlier in the cycle. You can fix these issues before you start the configuration, which can help reduce the deployment time.

When you click **Run precheck**, a list of tasks is displayed, which shows the type of checks that are performed. The page also displays the total number of errors and warnings, if any. If any of the tasks fail, click the task to view details about the error. After the precheck is complete, you can go back to the **Cluster configuration summary** page by clicking **Back to summary** or you can download the logs for further analysis by clicking **Download logs**. On the **Cluster configuration summary** page, click **Edit** and make the required changes to fix the issues. To view the result of the previous precheck, click **View precheck results**. To run the precheck again after fixing the issues, click **View precheck results > Run precheck again**.

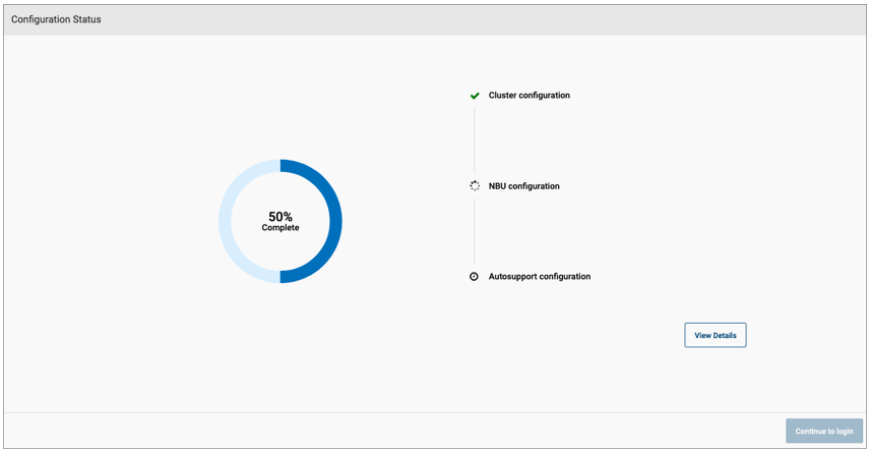
If you opt not to run the precheck, you can also review the details by clicking **Edit** for each of the options on the **Cluster configuration summary** page.

To start the NetBackup Flex Scale cluster configuration process click **Configure**.

If you choose not to run the precheck and click **Configure**, a message mentioning that you are configuring the cluster without running the precheck is displayed. If the precheck fails and you still continue with the cluster configuration, a message specifying that you are continuing with configuration while there are precheck errors is displayed.

The Configuration Status page displays the progress of the cluster configuration.

The following figure shows the Configuration Status page that is displayed when both the NetBackup primary and media servers are configured in the cluster:



The setup wizard performs the following tasks:

- Prepares all the cluster nodes and configures the cluster services.

- Configures the data, management, and IPMI networks and sets up the infrastructure management console.
- Configures all the components and services including the NetBackup primary server, media server, and MSDP engine services if both the NetBackup primary and media servers are deployed.
  Configures all the components and services including the media server and MSDP engine services if only media servers are deployed.
- Changes the known default passwords for maintenance user accounts.
- Configures AutoSupport services and performs basic validation tests.
- Starts all the cluster and NetBackup services.

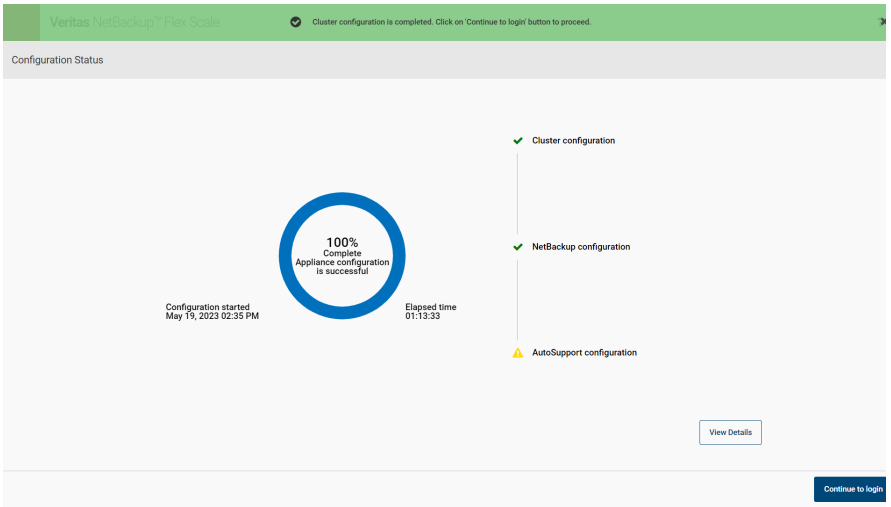
Click **View Details** if you want to see the detailed list of tasks performed and their status.

Note: If the NTP server was not set before the initial configuration then the timestamp of the tasks may not be consistent.

---

12 Wait for the Configuration Status page to confirm that the cluster is configured successfully. A confirmation message indicates that the cluster configuration process is complete.

The following figure is an example of the status that is displayed after the cluster is configured successfully:

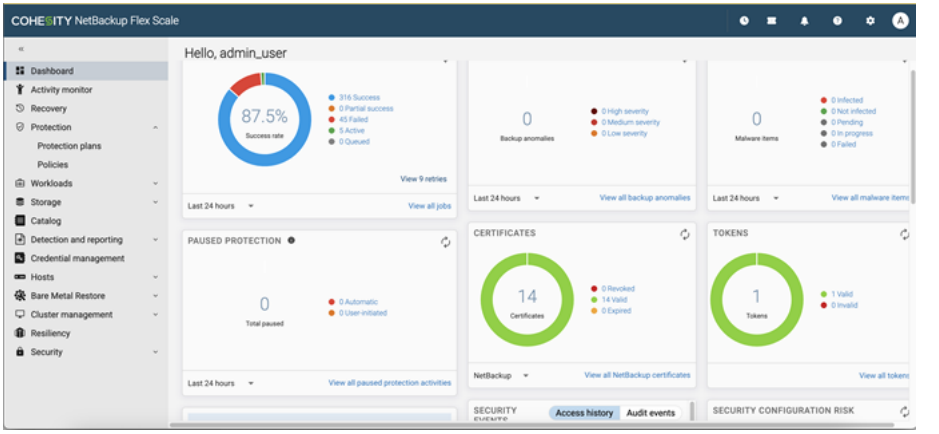


If the configuration fails during the initial phase of preparing the nodes and configuring the cluster services, an error message is displayed and you are prompted to reconfigure the cluster. To restart the configuration process, on the Configuration Status page click **Reconfigure**. You are taken back to the Welcome screen where you can restart the cluster configuration process.

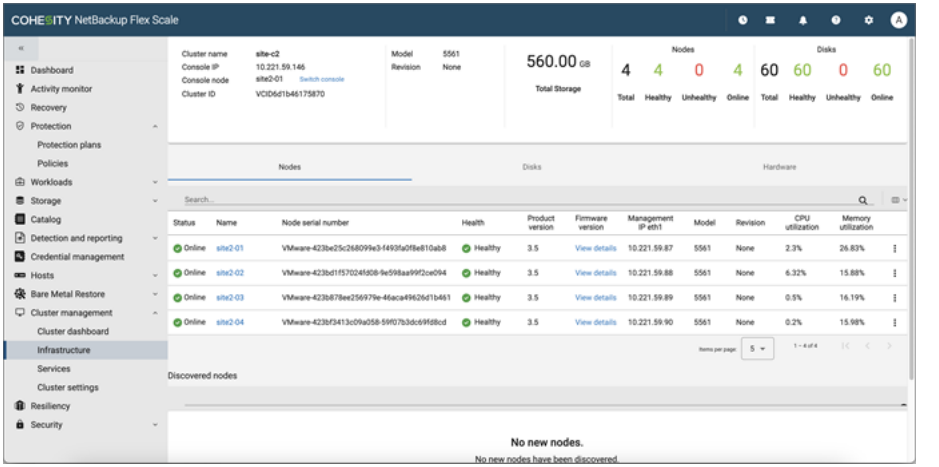
If the configuration fails in a later phase while configuring NetBackup services, you are required to factory reset the nodes and then restart the configuration process. At this stage, on the Configuration Status page, you can click **Download Logs** to download the logs for analyzing the issues. To reset all the nodes to their default factory settings, click **Factory reset**. After the factory reset is complete, you are redirected to the `https://`*`nodepublicIP`*`:8433` URL where you need to sign in with root and P@ssw0rd credentials to start the configuration process again.

13 If both primary and media servers are configured in the cluster, you can now proceed to the NetBackup Flex Scale web UI to configure protection plans and start protecting workloads. You can use the NetBackup Flex Scale web UI to manage both NetBackup and NetBackup Flex Scale infrastructure. On the Configuration Status page, click **Continue to login** to launch the NetBackup Flex Scale in a new browser window. On the sign in page, specify the user account that has both the Appliance administrator and the NetBackup Administrator role, which you created during the cluster configuration (refer to step 9 earlier), enter the password for the user account, and then click **Sign in**. Note that the URL to access the NetBackup Flex Scale is the IP address or the FQDN of the NetBackup Flex Scale management server that you specified during the cluster configuration (refer to step 8 earlier).

`https://`*`ManagementServerIPorFQDN`*`/webui`



To view the cluster infrastructure, click **Cluster Management > Infrastructure**.



At this stage, you can also sign in to the NetBackup Flex Scale infrastructure management UI to view all the details about the cluster, nodes, storage, and services.

Open a web browser and type the following URL in the address bar:

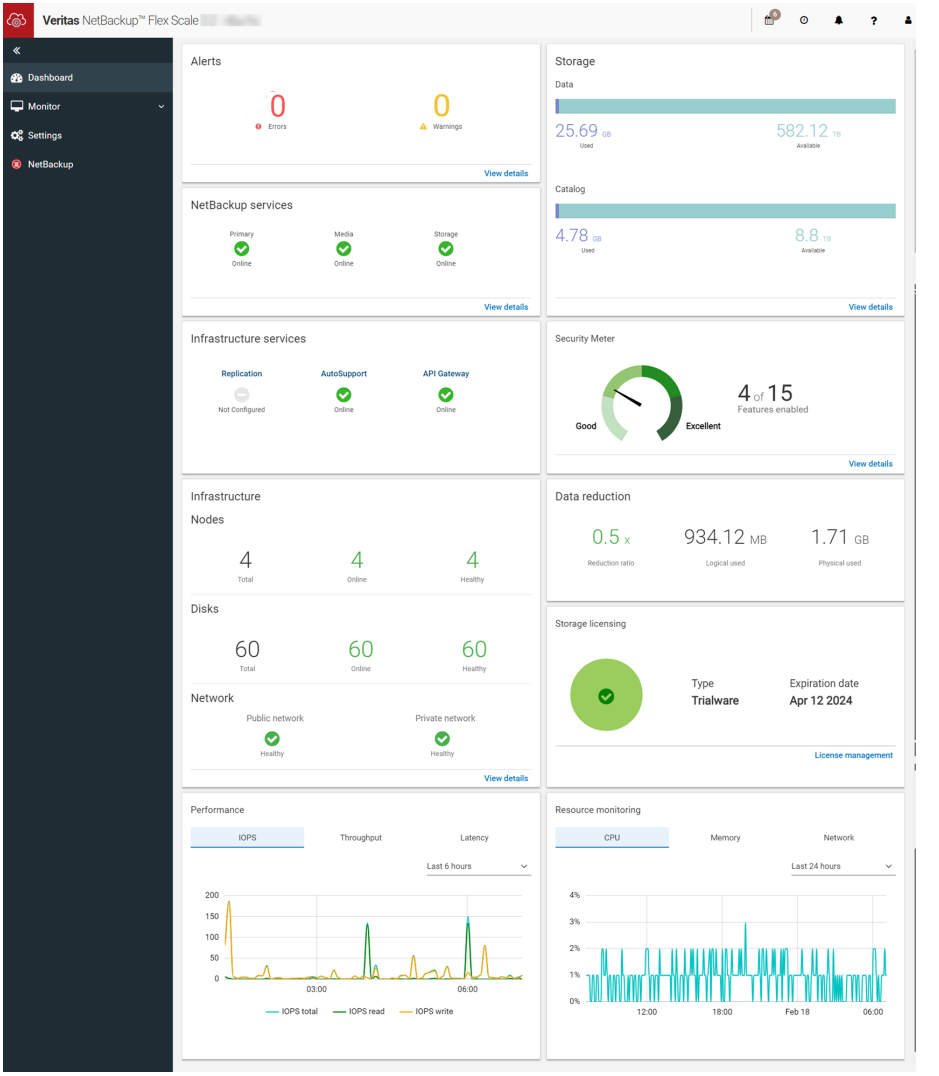
`https://`*`ManagementServerIPorFQDN`*`:14161`

If you are using IPv6 addresses, use the following URL syntax:

`https://[`*`ManagementServerIP`*`]:14161`

Here, *ManagementServerIPorFQDN* is the public IP address or FQDN that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration.

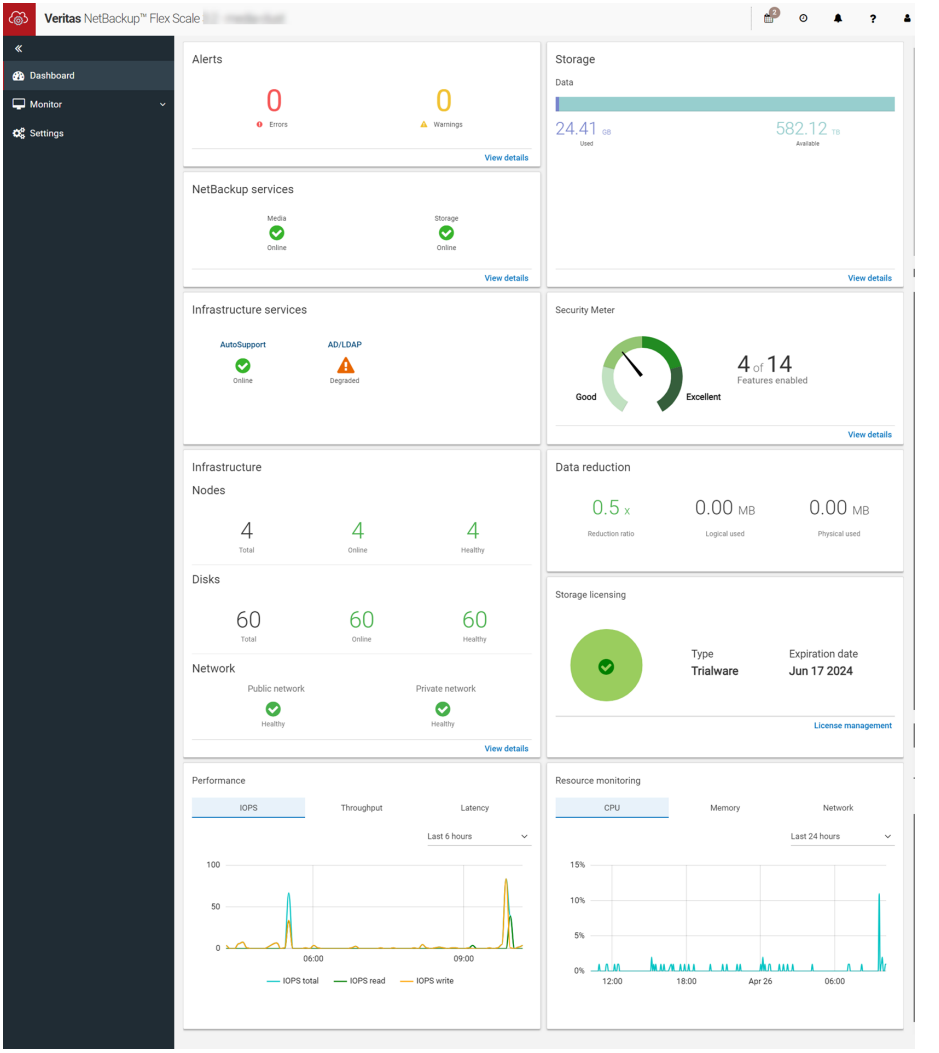
On the sign in page, specify the NetBackup Flex Scale administrator user account with the Appliance administrator role that you created during the cluster configuration, enter the password for the user account, and then click **Sign in**.


Veritas NetBackup™ Flex Scale
Dashboard
Monitor
Settings
NetBackup
Alerts
0
Errors
0
Warnings
View details
NetBackup services
Primary
Online
Media
Online
Storage
Online
View details
Infrastructure services
Replication
Not Configured
AutoSupport
Online
API Gateway
Online
Infrastructure
Nodes
4
Total
4
Online
4
Healthy
Disks
60
Total
60
Online
60
Healthy
Network
Public network
Healthy
Private network
Healthy
View details
Performance
IOPS
Throughput
Latency
Last 6 hours
200
150
100
50
0
03:00
06:00
IOPS total
IOPS read
IOPS write
Storage
Data
25.69 GB
Used
582.12 TB
Available
Catalog
4.78 GB
Used
8.8 TB
Available
View details
Security Meter
Good
Excellent
4 of 15
Features enabled
View details
Data reduction
0.5 x
Reduction ratio
934.12 MB
Logical used
1.71 GB
Physical used
Storage licensing
Type
Trialware
Expiration date
Apr 12 2024
License management
Resource monitoring
CPU
Memory
Network
Last 24 hours
4%
3%
2%
1%
0%
12:00
18:00
Feb 18
06:00

For more information on the NetBackup Flex Scale web UI and how to use it to manage your NetBackup Flex Scale cluster, refer to the *Veritas NetBackup Flex Scale Administrator's Guide* .

14 If only media servers are configured in the cluster, you can sign in to the NetBackup Flex Scale infrastructure management UI to view all the details about the cluster, nodes, storage, and services. On the Configuration Status page, click **Continue to login** to launch the NetBackup Flex Scale infrastructure management UI using `https://consoleIP:14161`where *consoleIP* is the public IP address that you specified for the infrastructure management UI during the cluster configuration.

On the sign in page, specify the NetBackup Flex Scale administrator user account and password that you created during the cluster configuration (refer to step 9 earlier) and then click **Sign in**.



For more information on the NetBackup Flex Scale infrastructure management UI and how to use it to manage your NetBackup Flex Scale cluster, refer to the *Veritas NetBackup Flex Scale Administrator's Guide* .

YML configuration file

The YML-based configuration file contains the NetBackup Flex Scale cluster configuration settings as name-value pairs. When you import the configuration file,

the configuration settings that you specify in the YML file are displayed in the corresponding parameters in the setup wizard.

Your Veritas Sales Engineer can generate the configuration file using the Appliance Deployment Planner (ADP) tool or you can download the default configuration template from the setup wizard and update the configuration settings as per your setup environment.

The configuration file contains the following sections:

- **cluster_setting**
- **common_network_setting**
- **nodes_setting**
- **external_primary_server_setting** (**Only for media server only deployment**)

The following table describes the parameters in the YML configuration file:

cluster_setting

Settings that are common to the cluster, such as the cluster name, NetBackup primary server settings, NTP settings, user details, and AutoSupport configuration details.

Under the **additional_fqdn_entries** section specify the following details:

Table 2-1

Parameter	Description
ip_address	IPv4 or IPv6 addresses that must be added to the `/etc/hosts` file so that the IP addresses are resolved.
name	Domain name

Under the **autosupport_setting** section specify the following details:

Table 2-2

Parameter	Description
call_home	
enable_call_home	Specify whether you want to enable Call Home. If you enable Call Home, you can upload the appliance health information to the Veritas AutoSupport server. Set to **true** to enable Call Home. Set to **false** to disable Call home.

Table 2-2 *(continued)*

Parameter	Description
enable_proxy_server	Specify if the appliance connects to the AutoSupport server through a proxy server. Set to **true** to enable proxy server. Set to **false** if a proxy server is not used.
enable_proxy_tunel	Specify if the proxy server supports SSL tunneling. Set to **true** to enable secure communication. Set to **false** if the proxy server does not support secure communication.
password	Password to authenticate the user name that is used to log in to the proxy server.
port	Port number to use for communicating with the proxy server.
server	Name of the proxy server.(Required if you enable the proxy server) .
username	User account to use for authenticating communication requests to the proxy server.
smtp	
account	User name to access the SMTP account.
emailServer	FQDN or the IP address of the SMTP server.
encryption_enabled	Specify whether to use a secure connection and to encrypt communication with the SMTP server.
hardware	Email address of the admin users who will be the recipients of hardware-related email alerts.
notificationInterval	Notification interval, in minutes, for email-based alerts. Enter a value in multiples of 15 minutes.
password	Password for the user name if authentication is required to access the SMTP account.

Table 2-2 *(continued)*

Parameter	Description
senderEmail	Source email address that is used to send email alerts.
serverPort	Port number to use for communicating with the SMTP server. The default port is 25.
software	Email address of the admin users who will be the recipients of software-related email alerts.
snmp	
server	FQDN or the IP address (IPv4 or IPv6) of the SNMP server in your network Alert notifications that are generated by the appliance are sent to this server.
port	Port number of the SNMP server.
community	Community to which the alerts are sent.
enable_snmp	Specify whether you want to enable the SNMP service to remotely monitor the cluster nodes using the SNMP protocol. Set to **true** to enable the SNMP service. Set to **false** if you do not want to configure the SNMP service.
version	Specify the SNMP version. NetBackup Flex Scale supports SNMP-v2 and SNMP-v3 prototcols
username	Specify the SNMP user name.
authenticationProtocol	Specify the authentication protocol. It provides authentication based on the HMAC-SHA algorithms. Choose one of the following options: ■ None ■ SHA256 ■ SHA512
authenticationPassword	Enter the password.

Table 2-2 *(continued)*

Parameter	Description
encryptionProtocol	Specify the encryption protocol. If provides DES 56-bit encryption in addition to authentication based on the AES standard. ■ None ■ AES128 ■ AES192 ■ AES256 ■ AES512
encryptionPassphrase	Enter the passphrase that you want to use for encryption.

Table 2-3

Parameter	Description
console_ip_ipv4	Public IPv4 address for the NetBackup Flex Scale infrastructure management UI. The type of IP address, whether IPv4 or IPv6 depends on the IP addressing you specified for the management network's routing settings.
console_ip_ipv6	Public IPv6 address for the NetBackup Flex Scale infrastructure management UI. The type of IP address, whether IPv4 or IPv6 depends on the IP addressing you specified for the management network's routing settings.
console_fqdn	FQDN which corresponds to the console IP. This is not a mandatory field. You can add this post configuration.
dr_passphrase	Passphrase for the disaster recovery package that is created for the NetBackup catalog backup. This passphrase is required when installing NetBackup in a disaster recovery mode. (**Only for a new NetBackup domain with both primary and media server deployment**)

Table 2-3 *(continued)*

Parameter	Description
NBU_licenses	A `.slf` license file for NetBackup. If not specified, the default trialware NetBackup license is installed. (**Only for a new NetBackup domain with both primary and media server deployment**)
storage_licenses	Storage license. You can specify multiple storage licenses during the initial configuration.
management_server_fqdn	Resolvable host name or FQDN for the NetBackup Flex Scale management and API server. The FQDN can contain a maximum of 64 characters.
management_server_ip_ipv4	Public IP address for the NetBackup Flex Scale management server. The type of IP address, whether IPv4 or IPv6 depends on the IP addressing you specified for the management network's routing settings.
name	Cluster name. ■ The cluster name can contain a-z, 0-9, - characters. ■ The cluster name must start with a lowercase letter. ■ The cluster name must not contain uppercase letters. ■ The cluster name must include a minimum of 3 characters and can contain a maximum of 63 characters.

Under the **netbackup_master** section, specify the following details:

(**Only for a new NetBackup domain with both primary and media server deployment**)

Table 2-4

Parameter	Description
ipv4_address	Public IPv4 address for the NetBackup primary server service. **Note:** You can specify either an IPv4 or an IPv6 address based on the data network settings.
ipv6_address	Public IPv6 address for the NetBackup primary server service. **Note:** You can specify either an IPv4 or an IPv6 address based on the data network settings.
name	Resolvable host name or FQDN for the NetBackup primary server service.

Under the **ntp_setting** section, specify the following details:

Table 2-5

Parameter	Description
server	NTP server that you want to use to set and synchronize the system clocks on the cluster nodes. You can specify an IP address or an FQDN. The type of IP address depends on the data network routing settings that you specified earlier. If the data network is configured to use IPv4 addresses, the NTP server IP address must be an IPv4 address. Conversely, if the data network uses IPv6 addresses, the NTP server IP must be an IPv6 address.
timezone	Time zone of the nodes.

Under the **lockdown_mode** section, specify the following details:

Table 2-6

Parameter	Description
mode	Lockdown mode that provides different levels of security and data retention capabilities to protect data. You can use lockdown mode to create WORM storage that prevents your data from being encrypted, modified, or deleted. Each mode provides different levels of protection and data retention capabilities. NetBackup Flex Scale supports the following lockdown modes: ■ Normal: Default mode that does not support WORM storage and data retention. ■ Enterprise: In this mode, you can create WORM storage and specify the expiration time for data. In this mode, a user with an Appliance administrator role can remove the retention lock and delete data before the specified expiration duration. A user with NetBackup administrator role can increase the retention period. ■ Compliance: In this mode you can create WORM storage and specify the expiration time for data. However, you cannot remove the retention lock and delete the data before the specified expiration duration. A user with NetBackup administrator role can increase the retention period.
retention	
min	Minimum duration for which data cannot be modified or deleted when the cluster is in enterprise or compliance mode.
max	Maximum duration for which data cannot be modified or deleted when the cluster is in enterprise or compliance mode.
unit	Retention period in terms of hours, days, months, or years. Minimum data retention time is one hour and maximum retention time is 30 years.

Table 2-6 *(continued)*

Parameter	Description
ipmiRestricted	Restrict remote management access to the node when the lockdown mode is set to enterprise or compliance. Specify **yes** to restrict remote access and **no** to disable the restriction. This option is not available for normal lockdown mode. Restricting remote access to nodes provides an additional level of data security and limits the privileges and operations that you can perform. You can view and perform limited operations in the IPMI web GUI but cannot open the remote console. Physical access to the system is required to log on to the console. After you enable this restriction, an IPMI Administrator user on an HPE platform has only **Login** and **Virtual Power and Reset** privileges. With these privileges, the user can only view settings in iLO and perform power-related operations. **Note:** After you enable restricted remote access, you can disable this option if the appliance is in enterprise lockdown mode. If the lockdown mode is set to compliance, you cannot disable the remote access restriction. You can also choose to enable or disable remote access after the initial configuration is complete.

Under the **private_network** section, specify the following details. Specify both the IPv4 and IPv6 addresses irrespective of the data network settings.

Table 2-7

Parameter	Description
ipv4	
ip	Specify a private subnet IP to be used for internal communication between the cluster nodes.

Table 2-7 *(continued)*

Parameter	Description
subnet	Subnet mask for the specified IP address.
ipv6	
ip	Specify a private subnet IP to be used for internal communication between the cluster nodes.
prefix_length	If using IPv6 addresses, specify the IPv6 prefix length. The prefix length must be greater than or equal to 115.

Under **user_management**, specify the following details:

Table 2-8

Parameter	Description
msdp_engine	
password	Password for the user account that can access the MSDP engine containers.
user_name	Name for the user account that can be used to access the MSDP engine containers. This account has the permissions to manage all the storage on the NetBackup Flex Scale cluster nodes.

Table 2-8 *(continued)*

Parameter	Description
The following are the rules for the credentials: ■ The user name and the password can be up to 62 characters in length. The user name and the password cannot be empty and cannot contain spaces and tabs. ■ You can use characters in the printable ASCII range (0x20-0x7E) except for the following characters: ■ Asterisk (*) ■ Forward slash (/) ■ Ampersand (&) ■ Dollar sign ($) ■ Percent sign (%) ■ Caret sign (^) ■ Angular brackets (<>) ■ Quotation mark (") ■ Comma (,) ■ Parentheses () ■ Square brackets ([]) ■ Curly brackets ({}) ■ Single quotation mark (') ■ Backtick or grave accent (`)	
users	
password	Password for the administrator account.
roles	Role to assign to the administrator account. The Appliance administrator role has permissions to manage all the infrastructure components in the cluster such as the cluster nodes, cluster settings, and the cluster operations. The NetBackup administrator role has the permissions to manage the NetBackup services and operations in the cluster. You can assign both the roles to a single administrator account.
user_name	Name for the administrator account.
additional_users	

Table 2-8 *(continued)*

Parameter	Description
user_name	Maintenance user account for which you want to change the known default password. Specify maintenance.
password	The new password that you want to set for the maintenance user account. The known default password of the user account, which is specified in the **user_name** parameter is set to this new password. The password for the maintenance user must be at least eight characters in length and must include at least one uppercase, lowercase, numeric, and special character. The permitted special characters are !@#$%^&~ Dictionary words are not allowed.

Under the **enable_stig** section, specify whether STIG should be enabled during initial configuration.

Table 2-9

Parameter	Description
enable_stig : true	Enables STIG during initial configuration
enable_stig : false	Does not enable STIG during initial configuration. If required, user can enable STIG after cluster configuration.

common_network_settings

Network settings for the cluster, such as network boding, DNS, and gateway details.

dns

Table 2-10

Parameter	Description
dns_domain	Domain that the nodes will be a part of. The name must be a fully qualified name.

data

Table 2-11

Parameter	Description
bond	
enable	Specify if you want to use NIC bonding for eth5 and eth7 for high availability of the network interfaces.
mode	Specify the bonding mode: ■ **balance-rr** ■ **active-backup** ■ **balance-xor** ■ **broadcast** ■ **802.3ad** ■ **balance-tlb** ■ **balance-alb**
option	Sub-type **layer2**, **layer2+3** , and **layer3+4** for bonding mode **802.3ad** and **balance-xorbond** types.
ipv4	
gateway_ip	If using IPv4 public addresses, specify the IP address of the gateway server in your network.
subnet_mask	If using IPv4 public addresses, specify the subnet mask of the data network.
ipv6	
prefix_length	If using IPv6 public addresses, specify the IPv6 prefix length.
router_ip	If using IPv6 public addresses, specify the router address.

Table 2-12

Parameter	Description
vlan_id	VLAN ID of a pre-configured virtual LAN. The ID can be any value between 1 and 4095.

dns

Table 2-13

Parameter	Description
dns_server	IP address of the DNS server in your network. Specify an IPv4 or an IPv6 address based on the data network settings. For details about the supported options for DNS configuration, see the *Veritas NetBackup™ Flex Scale Best Practices and Troubleshooting Guide*.
search_domain	Search domains for resolving host names and IP addresses.

ipmi

Table 2-14

Parameter	Description
ipv4	
gateway_ip	If using IPv4 public addresses, specify the IP address of the gateway server in your network.
subnet_mask	If using IPv4 public addresses, specify the subnet mask of the IPMI network.
ipv6	
prefix_length	If using IPv6 public addresses, specify the IPv6 prefix length.
router_ip	If using IPv6 public addresses, specify the router address.

management

Table 2-15

Parameter	Description
ipv4	
gateway_ip	If using IPv4 public addresses, specify the IP address of the gateway server in your network.

Table 2-15 *(continued)*

Parameter	Description
subnet_mask	If using IPv4 public addresses, specify the subnet mask of the management network.
ipv6	
prefix_length	If using IPv6 public addresses, specify the IPv6 prefix length.
router_ip	If using IPv6 public addresses, specify the router address.

dns

Table 2-16

Parameter	Description
dns_server	IP address of the DNS server in your network. Specify an IPv4 or an IPv6 address based on the management network settings. For details about the supported options for DNS configuration, see the *Veritas NetBackup™ Flex Scale Best Practices and Troubleshooting Guide*.
search_domain	Search domains for resolving host names and IP addresses.

Table 2-17

Parameter	Description
bond	
enable	Specify true if you want to use NIC bonding for eth1 and eth2 for high availability of management network interfaces. By default, the value is set to false.

Table 2-17 *(continued)*

Parameter	Description
mode	Specify the bonding mode: ■ **balance-rr** ■ **active-backup** ■ **balance-xor** ■ **broadcast** ■ **802.3ad** ■ **balance-tlb** ■ **balance-alb**
option	Sub-type **layer2**, **layer2+3** , and **layer3+4** for bonding mode **802.3ad** and **balance-xorbond** types.

nodes_setting

Node name and details of media server, MSDP engine, and management server for each node:

Table 2-18

Parameter	Description
hostnames	Name of the nodes, can contain a maximum of 63 characters.
serial_number	Serial number of the node. You can specify the serial number to assign the media, storage, and management interface IP to the specific node for which the serial number is specified. If you do not specify the serial number, these are assigned randomly. Specifying a serial number is optional. If you specify the serial number, ensure that you specify it for all the nodes. You can find the serial number on the pull tab present on the server. The pull tab is double-sided, one side shows the server serial number and the other side shows the default iLO account information.

Table 2-18 *(continued)*

Parameter	Description
media_server_ip	Public IP address range for the media server service on each node. ■ You can specify the IP address range separated by a hyphen. For example,10.xx.xxx.192-10.xx.xxx.208 ■ You can specify the IP address range in the CIDR format. For example,10.xx.xxx.192/30 ■ If you don't have an IP address range but want to avoid specifying FQDNs, you can specify comma-separated individual IP addresses. For example, 10.100.10.101,10.100.10.143,10.100.10.201,10.100.10.212 The FQDN is automatically resolved with DNS lookup.
msdp_engine_ip	Public IP address range for the MSDP engine service on each node ■ You can specify the IP address range separated by a hyphen. For example,10.xx.xxx.192-10.xx.xxx.208 ■ You can specify the IP address range in the CIDR format. For example,10.xx.xxx.192/30 The FQDN is automatically resolved with DNS lookup.
management_interface_ip	Public IP address to be assigned to the designated management network interface (eth1) on each node. You can specify: ■ A single IP range ■ Multiple IP ranges separated by a comma ■ Comma-separated individual IP addresses ■ A combination of individual IP addresses and IP ranges separated by a comma ■ IP addresses in CIDR format

Table 2-18 *(continued)*

Parameter	Description
ipmi_interface	Public IP address to be assigned to the designated IPMI interface on each node. ■ You can specify the IP address range separated by a dash. For example,10.xx.xxx.192-10.xx.xxx.208 ■ You can specify the IP address range in the CIDR format. For example,10.xx.xxx.192/30 The FQDN is automatically resolved with DNS lookup.

external_primary_server_setting

Details of the external NetBackup primary server that the cluster connects to.

(**Only for media server only deployment**)

Table 2-19

Parameter	Description
name	Resolvable host name or FQDN of the NetBackup primary server that is external to the cluster. The primary server must be already configured in an existing NetBackup domain. The media servers configured in the cluster communicate with this external primary server for NetBackup primary server services. The FQDN can contain a maximum of 253 characters.
ipv4_address	IPv4 address of the external primary server. The type of IP address, whether IPv4 or IPv6 depends on your network settings.
ipv6_address	IPv6 address of the external primary server. The type of IP address, whether IPv4 or IPv6 depends on your network settings.

Table 2-19 *(continued)*

Parameter	Description
api_key	NetBackup API key, which is a pre-authenticated token that identifies a NetBackup user to NetBackup RESTful APIs. The user can use the API key in an API request header when a NetBackup API requires authentication. API keys can be created for authenticated NetBackup users. A specific API key is only created one time and cannot be recreated. Each API key has a unique key value and API key tag. Ensure that the provided API key corresponds to a NetBackup user who has the administrator role.

Table 2-19 *(continued)*

Parameter	Description

media_server_gateway	Name that the primary server can use to identify all the media servers in the cluster. The primary server uses this name as an alias to map and access all the media servers in the cluster.
	This alias is not automatically updated in the bp.conf file. For backups jobs to be successful, on the NetBackup client, edit the `/usr/openv/netbackup/bp.conf` file and add a **SERVER** entry that corresponds to the name specified by the media_server_gateway parameter.
	For example, for the following settings:
	`external_primary_server_setting:`
	`  name: "sclhypscontainer3vm06p3.xxx.yyy.com"`
	`  ipv4_address: '192.168.2.241'`
	`  ipv6_address: ''`
	`  api_key: "A0sBjVxO5S8hwfa5cp_QvSqs0AmY1Fsy6qzGIK8z2S5ayBfPnOKV6jXOI-cLtXrd"`
	`  media_server_gateway: "nbfsclus001"`
	Add the `SERVER` entry as follows in the `bp.conf` file:
	`SERVER=nbfsclus001`

Sample YML file for primary and media server deployment

The following example shows a sample YML configuration file where a separate DNS is configured for the management and the data network and bonding is configured for the eth1 and eth2 management interfaces:

```
# deployment_yaml_version: V3.5

cluster_setting:
  name: meteor
  storage:
    format_disks: true
```

```
  tag_disks: true
autosupport_setting:
  smtp:
    notificationInterval: ''
    emailServer: ''
    serverPort: ''
    account: ''
    password: ''
    encryption_enabled: false
    hardware: ''
    software: ''
    senderEmail: ''
  snmp:
    enable_snmp: true
    version : 'v3'
    server: xx.xx.xx.xx
    port: 162
    community: ''
    username: 'v3user1'
    authenticationProtocol: "SHA256"
    authenticationPassword: xxxxxxxxxxxxx
    encryptionProtocol: "AES256"
    encryptionPassphrase: xxxxxxxxxxxxx
  call_home:
    enable_call_home: true
    enable_proxy_server: false
    proxy:
      enable_proxy_tunel: false
      server: ''
      port: ''
      username: ''
      password: ''
console_ip_ipv6: ''
console_ip_ipv4: xx.xx.xx.xx
console_fqdn: ' '
management_server_ip_ipv4: xx.xx.xx.xx
management_server_ip_ipv6: ''
ntp_setting:
  timezone: Pacific
  server:
    - xx.xx.xx.xx
dr_passphrase: xxxxxxxxxxxxx
NBU_licenses: ''
```

```
storage_licenses: []
netbackup_master:
  name: netbackup-master.xxx.yyy.com
  ipv4_address: xx.xx.xx.xx
  ipv6_address: ''
user_management:
  users:
    - user_name: admin_user
      password: xxxxxxxxxxxxx
      roles:
        - appliance_admin
        - backup_admin
    - user_name: app_admin_user
      password: xxxxxxxxxxxxx
      roles:
        - appliance_admin
    - user_name: nbu_admin_user
      password: xxxxxxxxxxxxx
      roles:
        - backup_admin
  msdp_engine:
    - password: xxxxxxxxxxxxx
      user_name: root
  additional_users:
    - user_name: maintenance
      password: xxxxxxxxxxxxx
enable_stig: false
private_network:
  ipv4:
    ip: xx.xx.xx.xx
    subnet: yy.yy.yy.yy
  ipv6:
    ip: 'fd00::2'
    prefix_length: '115'
additional_fqdn_entries:
  - ip_address: ''
    name: []
lockdown_mode:
  mode: Normal
  ipmiRestricted: 'no'
  retention:
    min: 'null'
    max: 'null'
```

```
      unit: null
  management_server_fqdn: management-server.xxx.yyy.com
common_network_setting:
  dns:
    dns_domain: xxx.yyy.com
  data:
    dns:
      dns_server: xx.xx.xx.xx
      search_domain:
        - xxx.yyy.com
    bond:
      enable: false
      mode: ''
      option: ''
    vlan_id: ''
    ipv4:
      gateway_ip: xx.xx.xx.xx
      subnet_mask: yy.yy.yy.yy
    ipv6:
      prefix_length: ''
      router_ip: ''
  management:
    dns:
      dns_server: xx.xx.xx.xx
      search_domain:
        - xxx.yyy.com
    bond:
      enable: false
      mode: ''
      option: ''
    vlan_id: ''
    ipv4:
      gateway_ip: xx.xx.xx.xx
      subnet_mask: yy.yy.yy.yy
    ipv6:
      prefix_length: ''
      router_ip: ''
  ipmi:
    ipv4:
      gateway_ip: ''
      subnet_mask: ''
    ipv6:
      prefix_length: ''
```

```
      router_ip: ''
nodes_setting:
  - host_name: host01
    ipmi_interface:
      ipv4_address: ''
      ipv6_address: ''
    management_interface:
      name: management01.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    media_server:
      name: media01.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    msdp_engine:
      name: engine01.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    serial_number: ''
  - host_name: host02
    ipmi_interface:
      ipv4_address: ''
      ipv6_address: ''
    management_interface:
      name: management02.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    media_server:
      name: media02.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    msdp_engine:
      name: engine02.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    serial_number: ''
  - host_name: host03
    ipmi_interface:
      ipv4_address: ''
      ipv6_address: ''
    management_interface:
      name: management03.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
```

```
      ipv6_address: ''
    media_server:
      name: media03.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    msdp_engine:
      name: engine03.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    serial_number: ''
  - host_name: host04
    ipmi_interface:
      ipv4_address: ''
      ipv6_address: ''
    management_interface:
      name: management04.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    media_server:
      name: media04.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    msdp_engine:
      name: engine04.xxx.yyy.com
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    serial_number: ''
```

Sample YML file for media server only deployment

The following example shows a sample YML configuration file with different DNS servers for the data and the management network, management bonding configured for eth1 and eth2 interfaces, and lockdown mode set to enterprise with restricted remote management access:

```
# deployment_yaml_version: V3.5

cluster_setting:
  name: meteor
  storage:
    format_disks: true
    tag_disks: true
  autosupport_setting:
    smtp:
```

```
    notificationInterval: ''
    emailServer: ''
    serverPort: ''
    account: ''
    password: ''
    encryption_enabled: false
    hardware: ''
    software: ''
    senderEmail: ''
  snmp:
    enable_snmp: true
    version: v3
    server: xx.xx.xx.xx
    port: 162
    community: ''
    username: v3user1
    authenticationProtocol: SHA256
    authenticationPassword: xxxxxxxx
    encryptionProtocol: AES256
    encryptionPassphrase: xxxxxxxx
  call_home:
    enable_call_home: true
    enable_proxy_server: false
    proxy:
      enable_proxy_tunel: false
      server: ''
      port: ''
      username: ''
      password: ''
console_ip_ipv6: ''
console_ip_ipv4: xx.xx.xx.xx
console_fqdn: ' '
enable_stig: false
management_server_ip_ipv4: xx.xx.xx.xx
management_server_ip_ipv6: ''
ntp_setting:
  timezone: Pacific
  server:
    - xx.xx.xx.xx
dr_passphrase: xxxxxxxxxxxxx
NBU_licenses: ''
storage_licenses: []
user_management:
```

```
    users:
      - user_name: admin_user
        password: xxxxxxxxxxxx
        roles:
          - appliance_admin
      - user_name: app_admin_user
        password: xxxxxxxxxxxx
        roles:
          - appliance_admin
    msdp_engine:
      - password: xxxxxxxxxxxx
        user_name: root
    additional_users:
      - user_name: maintenance
        password: xxxxxxxxxxxx
  private_network:
    ipv4:
      ip: xx.xx.xx.xx
      subnet: yy.yy.yy.yy
    ipv6:
      ip: fd00::2
      prefix_length: '115'
  additional_fqdn_entries:
    - ip_address: ''
      name: []
  lockdown_mode:
    mode: Normal
    ipmiRestricted: 'no'
    retention:
      min: 'null'
      max: 'null'
      unit: null
  management_server_fqdn: management-server.xxx.yyy.com
common_network_setting:
  dns:
    dns_domain: vxindia.veritas.com
  data:
    dns:
      dns_server: xx.xx.xx.xx
      search_domain:
        - vxindia.veritas.com
    bond:
      enable: false
```

```
      mode: ''
      option: ''
    vlan_id: ''
    ipv4:
      gateway_ip: xx.xx.xx.xx
      subnet_mask: yy.yy.yy.yy
    ipv6:
      prefix_length: ''
      router_ip: ''
  management:
    dns:
      dns_server: xx.xx.xx.xx
      search_domain:
        - vxindia.veritas.com
    bond:
      enable: false
      mode: ''
      option: ''
    vlan_id: ''
    ipv4:
      gateway_ip: xx.xx.xx.xx
      subnet_mask: yy.yy.yy.yy
    ipv6:
      prefix_length: ''
      router_ip: ''
  ipmi:
    ipv4:
      gateway_ip: ''
      subnet_mask: ''
    ipv6:
      prefix_length: ''
      router_ip: ''
nodes_setting:
  - host_name: pbnso01.xxx.yyy.com
    ipmi_interface:
      ipv4_address: ''
      ipv6_address: ''
    management_interface:
      name: 'management01.xxx.yyy.com'
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    media_server:
      name: 'media01.xxx.yyy.com'
```

```
    ipv4_address: xx.xx.xx.xx
    ipv6_address: ''
  msdp_engine:
    name: 'engine01.xxx.yyy.com'
    ipv4_address: xx.xx.xx.xx
    ipv6_address: ''
  serial_number: FSVSMH3
- host_name: pbnso02.xxx.yyy.com
  ipmi_interface:
    ipv4_address: ''
    ipv6_address: ''
  management_interface:
    name: 'management02.xxx.yyy.com'
    ipv4_address: xx.xx.xx.xx
    ipv6_address: ''
  media_server:
    name: 'media02.xxx.yyy.com'
    ipv4_address: xx.xx.xx.xx
    ipv6_address: ''
  msdp_engine:
    name: 'engine02.xxx.yyy.com'
    ipv4_address: xx.xx.xx.xx
    ipv6_address: ''
  serial_number: FSVQMH3
- host_name: pbnso03.xxx.yyy.com
  ipmi_interface:
    ipv4_address: ''
    ipv6_address: ''
  management_interface:
    name: 'management03.xxx.yyy.com'
    ipv4_address: xx.xx.xx.xx
    ipv6_address: ''
  media_server:
    name: 'media03.xxx.yyy.com'
    ipv4_address: xx.xx.xx.xx
    ipv6_address: ''
  msdp_engine:
    name: 'engine03.xxx.yyy.com'
    ipv4_address: xx.xx.xx.xx
    ipv6_address: ''
  serial_number: FSVTMH3
- host_name: pbnso04.xxx.yyy.com
  ipmi_interface:
```

```
      ipv4_address: ''
      ipv6_address: ''
    management_interface:
      name: 'management04.xxx.yyy.com'
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    media_server:
      name: 'media04.xxx.yyy.com'
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    msdp_engine:
      name: 'engine04.xxx.yyy.com'
      ipv4_address: xx.xx.xx.xx
      ipv6_address: ''
    serial_number: 'FSVUMH3'
external_primary_server_setting:
  name: abc.com
  ipv4_address: 'xx.xx.xx.xx'
  ipv6_address: ''
  api_key: "abcdefgh"
  media_server_gateway: "nbfsclus001"
```

Chapter 3

Upgrading NetBackup Flex Scale to 3.5.100

This chapter includes the following topics:

About NetBackup Flex Scale upgrades and EEBs

NetBackup Flex Scale supports software version upgrades. The upgrade operation is supported using both the GUI and RESTful APIs.

Open a web browser and type the following URL in the address bar to sign in to the NetBackup Flex Scale infrastructure management UI:

`https://`*`ManagementServerIPorFQDN`*`:14161`

If you are using IPv6 addresses, use the following URL syntax:

`https://[`*`ManagementServerIP`*`]:14161`

Here, *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration.

Note: If you access the NetBackup Flex Scale infrastructure management UI by using the short host name from a node, set the DNS settings (name server, domain name, and search domain) or ensure that the entry for mapping the short host name to an IP address exists in the hosts file of the node.

You can find the RESTful APIs at

`https://`*`ManagementServerIPorFQDN`*`:14161/swagger/infra/v1.0/`

If you are using IPv6 addresses, use the following URL syntax:

`https://[`*`ManagementServerIP`*`]:14161/swagger/infra/v1.0/`

The NetBackup Flex Scale upgrade consists of several steps. These steps and the overall upgrade progress can be seen in the GUI. In case the upgrade fails at a step from where automatic rollback is possible, NetBackup Flex Scale completes the rollback automatically. The progress and status for rollback can also be seen on the GUI.

The GUI supports the following operations:

- Check SORT for the availability of major upgrades, and patches. The **Check online for upgrade** option shows the details of packages available on SORT.
- You can download available major upgrades, and patches from SORT.
- You can upload major upgrades, patches, and EEBs from your local systems.
- The GUI displays the download package progress.
- The GUI displays the details of downloaded and installed major upgrades, patches, and EEBs.
- You can install major upgrades and patches when all nodes are healthy.
- You can install and roll back EEBs from the system if all the nodes are reachable.

  Note: Depending on the EEB, you might need to ensure that there are no jobs running before you install or roll back the EEB.

- You can delete major upgrades, and patches which are downloaded in the system through the GUI.
- You can delete downloaded EEBs which are not installed on the system.

Considerations about the upgrade workflow:

- If a node goes down during an upgrade, rollback will be triggered automatically. But if the nodes remains down, the rollback will fail and you must contact Veritas Support to resolve the issue.
- The GUI disables other operations when upgrade or rollback operations are in progress.
- Any operation that changes the configuration is not allowed during an upgrade.

Note: If disaster recovery is configured, make sure that you install the EEBs and patches on the secondary site.

You cannot perform the following operations if an upgrade is in progress:

- Add another node to the cluster.
- Replace an existing node in the cluster.
- Add or modify existing data networks.
- Create, edit, or delete a network bond.
- Create, edit, or delete a user.
- Factory reset a node.
- Start or stop containers
- Deploy external certificate

NetBackup Flex Scale upgrade overview

To upgrade NetBackup Flex Scale, refer to the following steps:

See “Supported upgrade paths” on page 84.

See “Performing pre-upgrade tasks” on page 85.

See “Downloading the upgrade file” on page 87.

See “Uploading the upgrade file and performing an upgrade precheck” on page 87.

See “Performing an upgrade using GUI” on page 88.

See “Performing post-upgrade tasks” on page 91.

See “Collecting logs for an upgrade precheck failure” on page 93.

Supported upgrade paths

NetBackup Flex Scale supports both rolling and parallel upgrade.

In a rolling upgrade, each node in the cluster is upgraded successively and restarted without shutting down the cluster. During a rolling upgrade, cluster services are not available for a very limited period. The nodes restart automatically as part of the upgrade process. Rolling upgrade minimizes the service and application downtime by limiting the downtime to the time it takes to stop and restart the NetBackup services on the cluster nodes.

In a parallel upgrade, all the nodes in the cluster are upgraded and restarted simultaneously and the services downtime is part of the overall upgrade duration. During a parallel upgrade, cluster services are not available after the cluster nodes are restarted. The nodes restart automatically as part of the upgrade process.

The following upgrade paths are supported forNetBackup Flex Scale:

- From version 3.2.100, and 3.5 to version 3.5.100

Performing pre-upgrade tasks

Before you begin the upgrade, ensure that you complete the following tasks:

Verify that the maintenance account password is not set to the default password

For increased security, password changes are enforced to ensure that known default passwords do not exist on the system. If the maintenance account password is set to the default password **P@ssw0rd**, you must change the password before you upgrade the cluster. To change the default password of the maintenance account:

To change the maintenance user account password

- Sign in to the NetBackup Flex Scale infrastructure management UI.

  Open a web browser and type the following URL in the address bar:

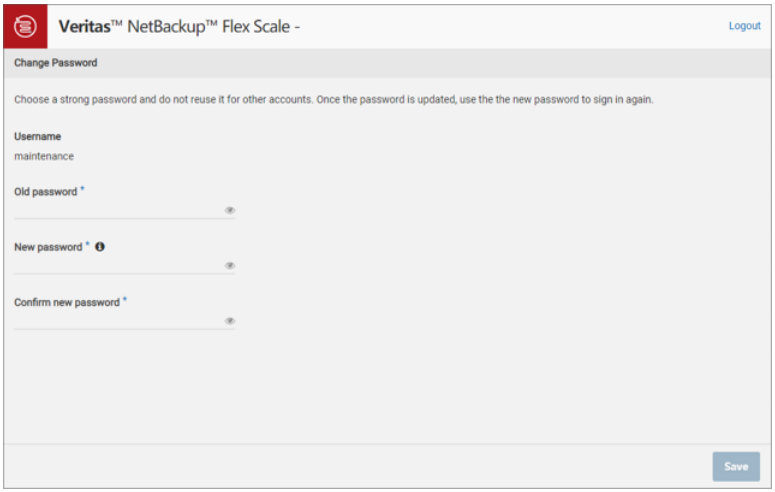
  `https://consoleIP:14161`

  Here, *consoleIP* is the public IP address that you specified for the infrastructure management UI during the cluster configuration.

  Use the following user account to sign in:

  - User name: *maintenance*
  - Password: *P@ssw0rd*

  After login, an option is given to change the password. Select **Change password** to update the password.



On the Change Password screen, enter the existing password (mentioned earlier), then set a new password for the user account, and then click **Save**.

Refer to the *Veritas NetBackup Flex Scale Administrator's Guide* for more information about NetBackup Flex Scale user management.

Considerations for upgrade when disaster recovery is configured

When disaster recovery is configured, both the primary and secondary sites are upgraded in parallel and you are required to start the upgrade from only one site.

Review the following guidelines before you upgrade:

- Upgrade can be performed only when both the primary and secondary sites are up and nodes are in healthy state.
- Download and upload the upgrade package to only one of the sites.
  After the upgrade package is uploaded, before you start the upgrade, navigate to **Settings > Software management** and click **Start pre-check**. This will sync the upgrade package to the secondary site and trigger pre-checks on both the sites automatically.
- Upgrade can be triggered from any cluster and both clusters are upgraded simultaneously.
- If the upgrade fails on any cluster for any reason, both the clusters are rolled back to the previous version.

Downloading the upgrade file

You can download the upgrade file from the Veritas Support site. You require Veritas account credentials to download the file.

To download the required upgrade file

1. Go to the Veritas Support website (https://www.veritas.com/support/en_US) and click **Downloads**, which redirects you to the Download Center.
2. In the Veritas Download Center, in the **Products** list, select **Appliances**, in the **Sub product** list select **NetBackup Flex Scale**. Select the version as and click **Explore**.

Uploading the upgrade file and performing an upgrade precheck

Upload the upgrade file to the cluster and run an upgrade pre-check. The upgrade precheck determines if the system is ready for an upgrade. The pre-check does not require a scheduled downtime.

Run the precheck at least 10 days prior to the upgrade so that you can identify any configuration issues that might prevent the upgrade from proceeding smoothly. The results will allow you to assess whether the upgrade is feasible and give you enough time to resolve any problems, ensuring that the upgrade can proceed on the planned date.

Run the precheck again a day before the upgrade to catch any last-minute changes or issues that might have arisen since the initial check to reduce the chances of upgrade failure and ensure minimal downtime.

If the precheck fails, the upgrade cannot proceed. You must resolve the issues before you upgrade the cluster.

To upload the upgrade file and run the precheck:

1. Sign in to the NetBackup Flex Scale web UI.
2. Click **Cluster Management > Cluster settings > Software management**.
3. On the Software management page click **Software update**.

4 To upload the upgrade file that you had downloaded earlier, click **Upload file**. Select the file and then click **Upload**. After uploading the package, it is displayed under **Downloaded package files**.

Note: Ensure that you do not navigate away or refresh the page while the upload operation is in progress.

5 To start the upgrade precheck, under **Downloaded package files** for the file, from the Actions menu (vertical ellipsis) click **Start pre-check**.

When prompted for confirmation click **Start pre-check**. A success or failure notification is displayed on the top of the page. To view detailed status, click **View details**.

6 If the precheck is successful continue to perform the preupgrade tasks. See "Performing pre-upgrade tasks" on page 85.

If the precheck fails, review the failures displayed in the GUI. You can also collect logs for further analysis. See "Collecting logs for an upgrade precheck failure" on page 93.

Performing an upgrade using GUI

Before you upgrade:

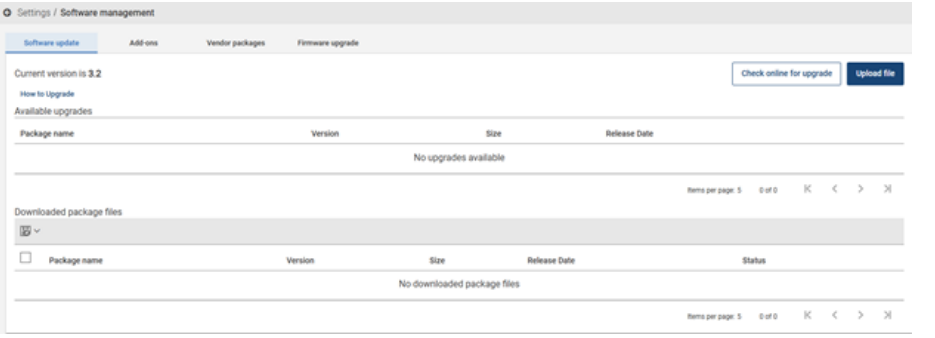
- Complete the tasks described in See "Performing pre-upgrade tasks" on page 85..
- If disaster recovery is configured for the cluster, review the guidelines specified in See "Considerations for upgrade when disaster recovery is configured" on page 86.

To perform an upgrade using the GUI

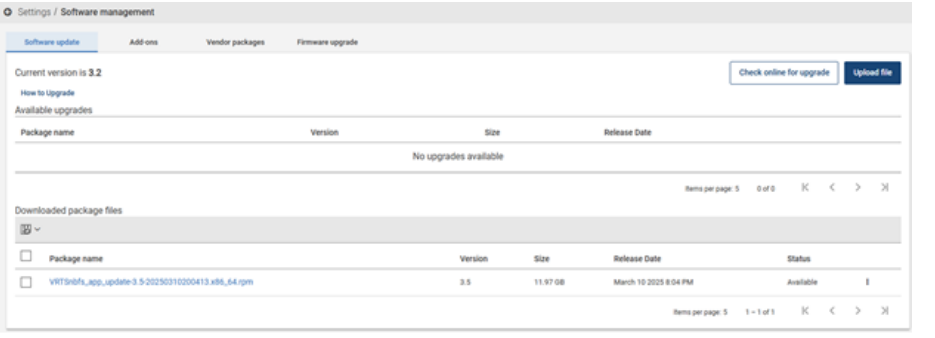
1 Sign in to the NetBackup Flex Scale web UI, if not already done so.

2 In the left pane click **Cluster Management > Cluster settings > Software management**

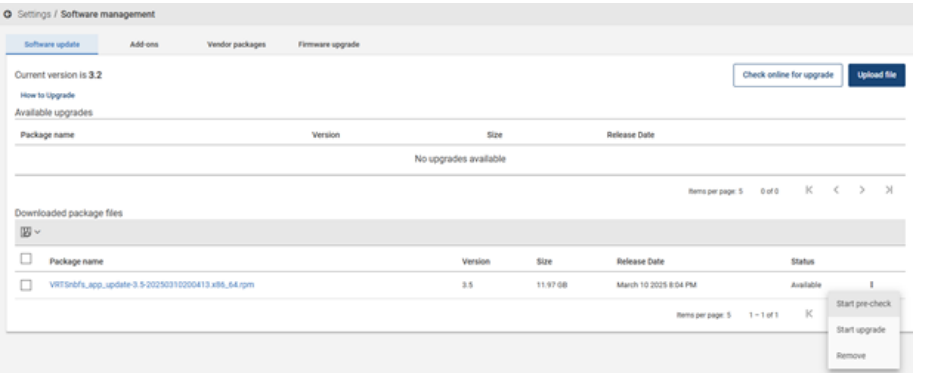
3 On the Software management page click **Software update**.



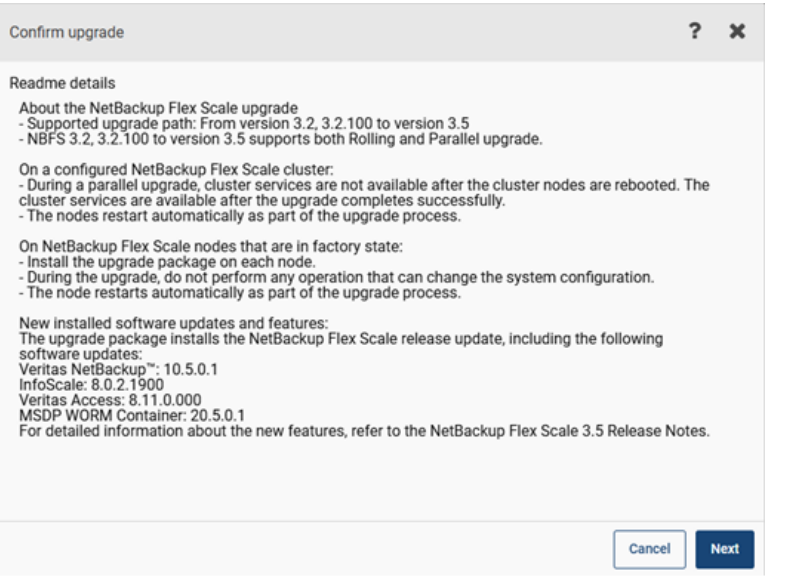
4 The upgrade file that is uploaded earlier is displayed under **Downloaded package files** and its status is displayed as **Available**. To view details about the upgrade file, click the file name.



5 To start the upgrade, under **Downloaded package files** for the upgrade file, from the Actions menu (vertical ellipsis) click **Start upgrade**.



6 Review the readme and click **Next**.



You can view the progress of the upgrade operation on the Software management page. To view detailed status, click **View details**.

7 After the upgrade is complete, a notification about successful upgrade is displayed on the top of the page. The version displayed on the page is updated to the newer version and the status of the package in the **Downloaded package files** changes to **Installed**.

8 If the upgrade fails on any one of the cluster nodes, message about successful rollback is displayed in the upgrade progress details and all the nodes in the cluster are automatically rolled back to the previous version. You can view the details about the failure by clicking **View details**. To troubleshoot any issues during an upgrade, you can download upgrade logs by going to **Settings > Diagnostics** and selecting the **Upgrade** component on the **Basic** tab.

Performing post-upgrade tasks

After the upgrade is complete, ensure that you complete the following tasks.

Downloading and installing the required EEBs

You are required to download and install the EEBs that are available on the Veritas Support website. You can install the EEBs in any order.

You can install the EEBs using the GUI or by using the REST APIs.

For details about downloading the EEBs:

See "Downloading EEBs" on page 120.

For details about installing the EEBs:

See "Installing EEBs using GUI" on page 121.

Verifying appliance firmware compatibility

Ensure that the firmware version of the appliance components is updated to the latest versions as listed on the https://sort.veritas.com/netbackup/acl website. After a product upgrade, the system must have the latest firmware version.

See "Determining if a firmware upgrade is required" on page 96.

See "Downloading the firmware package" on page 97.

See "Upgrading the firmware" on page 99.

Adding NetBackup license file

To download the license file for Veritas NetBackup, see https://support.cohesity.com/s/article/article-100058779

To view and add license keys using the command line, see https://www.veritas.com/content/support/en_US/article.100059061 :

Saving the default password of the HPE iLO Administrator user

The default password of the iLO user Administrator is printed on appliance pull tab. The following figure shows the default password printed on the pull tab:

Use the following command to save the default iLO password:

```
system store-default-BMC-credentials
```

If the default password is changed, provide the current administrator password using the following command:

```
system store-updated-admin-BMC-credentials
```

Collecting logs post upgrade

After the upgrade is completed successfully, collect logs for all the nodes.

To collect logs:

1. Sign in to the NetBackup Flex Scale web UI.
2. In the left pane, click **Cluster Management > Cluster settings > Diagnostics**.
3. Click **Generate log package**.
4. On the Generate log package page, on the **Basic** tab do the following:
   - Under **Log settings**, select the **Infrastructure** and **Upgrade** components.
   - Under **Historical logs** click **Archived logs**.

- Under **Package options**, specify a name for the log package and optionally the case number if provided by Veritas Support.
- Under **Nodes**, click **All nodes**.

5 Click **Generate**.

To view the progress of the operation, click **View details** on the **Diagnostics** page. If you had specified the case number, it is prefixed to the package name. The generated log package is displayed under **Packaged logs**. You can now download the package to your node.

Collecting logs for an upgrade precheck failure

If the precheck fails, the GUI shows the reasons for the failure. If further troubleshooting is required, collect the following logs from the console node. If disaster recovery is configured, logs from both the clusters are required even if the failure occurs on one site.

To identify the management console node, in the NetBackup Flex Scale web UI, navigate to **Cluster Management > Infrastructure**. On the Infrastructure page, **Console node** shows the management console node and the remaining nodes are the non-management console nodes.

To collect logs:

1 Sign in to the NetBackup Flex Scale infrastructure management UI.

2 Navigate to **Settings > Diagnostics** and click **Generate log package**.

3 On the **Advanced** tab, select the following files from the management console node:

If the log file is of zero size, expand **archived_logs** and select the specified file.

- Expand **infrastructure**, click **/log/VRTSnas/** and select the following files:
  - `isagui_upgrade_support.log`
  - `upgrade_nas_opr.log`
- Expand **upgrade**, click **log** and select the `preflight_check_report.json` file.
- If disaster recovery is configured, expand **common-logs**, click **/log/VRTSnas/** and select the `nso_replication.log` file.

4 Under **Package options**, specify a name for the log package and optionally the case number if provided by Veritas Support.

5 Click **Generate**.

To view the progress of the operation, click **View details** on the **Diagnostics** page. If you had specified the case number, it is prefixed to the package name. The generated log package is displayed under **Packaged logs**.

Chapter 4

Upgrading the firmware in NetBackup Flex Scale cluster

This chapter includes the following topics:

About firmware upgrades

The appliance nodes include multiple hardware components, which have firmware installed on them. Hardware vendors release new firmware versions periodically to fix issues or to improve the security and performance of the components. These updates are made available as firmware packages. You must upgrade the firmware on the appliance nodes when new firmware packages are made available.

Each node includes an `acl_info.json` appliance compatibility list (ACL) file that maintains a list of latest supported firmware versions for each of the components. If the firmware version of an appliance node component does not match the version that is listed in the ACL file, alerts are generated and the node is marked unhealthy.

Note: You can upgrade directly to the latest firmware version **(n)** if you are upgrading from the previous two firmware versions **(n-2)** or **(n-1)**.

However, if you are upgrading from an older firmware version directly to the latest available firmware version, some of the appliance components might not upgrade successfully. In such situations, you need to follow a multi-step path and upgrade to intermediate firmware versions **(n-2)** or **(n-1)**, and then upgrade to version **n** where **n** denotes the latest firmware version.

To upgrade the firmware, refer to the following steps:

See "Determining if a firmware upgrade is required" on page 96.

See "Downloading the firmware package" on page 97.

See "About the firmware upgrade options" on page 98.

See "Upgrading the firmware" on page 99.

(if required)

Determining if a firmware upgrade is required

Before you upgrade the firmware, check the current firmware version of the appliance components with the latest supported version. If there is a mismatch in the firmware version of any of the components, you must update the firmware on your nodes.

To check if a firmware upgrade is required using the CLI:

1. Check the current firmware version of the components. To check the current firmware version of the appliance components from the node-level CLI, use the following command:

   ```
   show hardware-health node component=firmware
   ```

   The current firmware version for the components is listed in the **Version** column of the output.

2. Note the **Status** column in the output. If the **Status** column shows **Update Available** or **Unsupported Version** you are required to upgrade the firmware.

To check if a firmware upgrade is required using the UI:

1. Check the current firmware version of the components. In the NetBackup Flex Scale web UI, navigate to **Cluster management > Infrastructure > Nodes**. In the **Firmware version** column, click **View details**.

   The components and their current firmware versions are displayed.

2. Check the latest supported firmware version. To check the latest supported firmware version, go to the SORT Appliance Compatibility List site (https://sort.veritas.com/netbackup/acl).

   On the Appliance Compatibility Page, do the following:

   - In the **Product** list, select NetBackup Flex Scale.
   - In the **Hardware** list, select the appliance model.
   - In the **Version** list, select the latest version. The naming convention is **Productversion (spp-yyyymm)**. Ignore the leading **Productversion** and select the latest version for the appliance model.
   - In the **Category** list, select **All**.
     The components and their latest supported firmware versions are displayed.

3. Compare the firmware version listed in the ACL file on SORT with the version installed on your node. If there is a mismatch in the firmware version for any of the components, you need to upgrade the firmware.

To check if you can upgrade directly to the latest firmware version or require a multi-path upgrade, first check the current firmware version of the iLO component that is installed on the appliance and compare the iLO component version on the appliance with the version included in the firmware packages on SORT. To check the current firmware version on the appliance, in the NetBackup Flex Scale web UI, navigate to **Cluster management > Infrastructure > Nodes** and in the **Firmware version** column, click **View details**. Note the firmware version of the iLO component, which shows the version and the release date. Go to the SORT Appliance Compatibility List site (https://sort.veritas.com/netbackup/acl) and check which firmware package includes the iLO component with the same version as that on the appliance.

See “Downloading the firmware package” on page 97.

Downloading the firmware package

The firmware package is available for download from the Download Center on the Veritas Support site. Download the firmware package to a Windows system that can access the Download Center and the cluster nodes. Installing the firmware packages that are downloaded from the Veritas website ensures that you only install

the firmware packages that are verified and tested by Veritas. Veritas recommends that you install the firmware packages that are downloaded from the Veritas website.

NetBackup Flex Scale appliances currently have two models: 5551 and 5561. The firmware package must be downloaded from the Download Center for the corresponding model. To identify the model of the appliance, go to the NetBackup Flex Scale web UI, navigate to **Cluster Management > Infrastructure > Nodes**, and check the **Model** field.

To download the firmware package from the Veritas Download Center:

1. Go to the Veritas Support website (https://www.veritas.com/support/en_US).

   Click **Downloads**, which redirects you to the Download Center.

2. In the Veritas Download Center, in the **Products** list, select **Appliances**, in the **Sub product** list select **NetBackup Flex Scale**. Select the version and click **Explore**.

3. Expand **Updates**. Sign in with your Veritas account credentials to download the firmware package.

See "About the firmware upgrade options" on page 98.

About the firmware upgrade options

You can upgrade the firmware by using the HPE iLO interface or from the NetBackup Flex Scale web UI.

- **HPE iLO-based interface**: Veritas recommends using the HPE Integrated Lights-Out (iLO) interface for upgrading the firmware. With the HPE iLO interface, you can use any of the following methods to upgrade the firmware:
  See "Updating the firmware in NetBackup Flex Scale clusters using HPE iLO" on page 99.
  - **Rolling method**: In a rolling firmware upgrade, firmware on each node is upgraded successively.
  - **Parallel method**: In a parallel firmware upgrade, firmware on all the nodes is upgraded simultaneously.
- **NetBackup Flex Scale web UI**: You can use the **Firmware upgrade** option in the UI to upgrade the firmware.
  You have an option to do the upgrade using rolling or parallel upgrade method.
  See "Updating the firmware in NetBackup Flex Scale clusters using the UI" on page 115.

Upgrading the firmware

This section describes the different procedures for upgrading the firmware.

To upgrade the firmware using HPE iLO:

See "Upgrading the firmware using the rolling method" on page 99.

See "Upgrading the firmware using the parallel method" on page 107.

To upgrade the firmware using the NetBackup Flex Scale web UI:

Updating the firmware in NetBackup Flex Scale clusters using HPE iLO

Before you begin the firmware upgrade process, ensure that all the nodes in the cluster are up. Veritas recommends that you install the firmware packages that are downloaded from the Veritas website. After the upgrade is complete, ensure that the firmware version of the appliance components is updated to the latest versions as listed as on the SORT Appliance Compatibility List website (https://sort.veritas.com/netbackup/acl).

During the firmware upgrade, the node is restarted using the media that contains the firmware update package and again after the upgrade is complete. All the infrastructure components in the cluster must have the same firmware version.

You can upgrade the firmware using the rolling or the parallel method. In a rolling firmware upgrade, firmware on each node is upgraded successively. During parallel upgrade, firmware on all the nodes is upgraded successively.

See "Upgrading the firmware using the rolling method" on page 99.

See "Upgrading the firmware using the parallel method" on page 107.

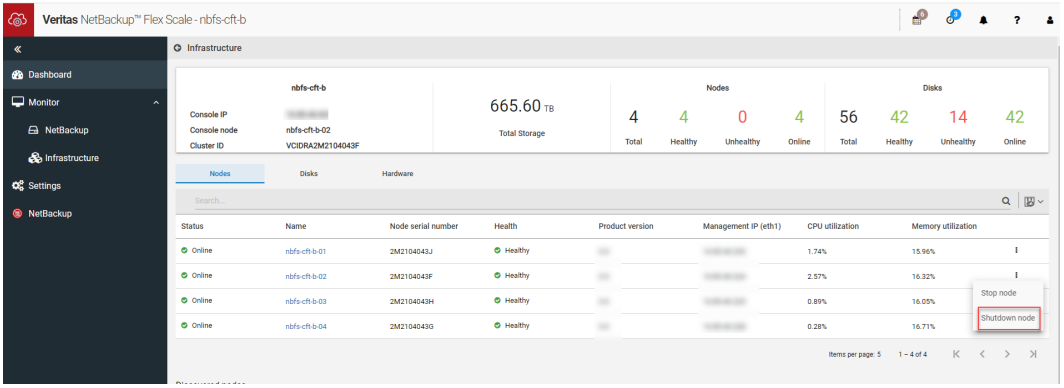
Upgrading the firmware using the rolling method

In a rolling firmware upgrade, firmware on each node is upgraded successively. When you upgrade the firmware, ensure that the node that you upgrade has joined the cluster and the data rebuild is complete.

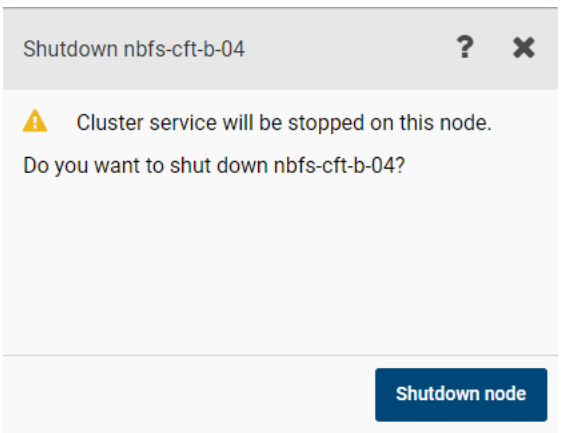
During a rolling upgrade, you must shut down the node on which you want to upgrade the firmware. After you upgrade the firmware, wait for the node to be resynced before upgrading the firmware on another node.

To upgrade the firmware using the rolling method:

1. Sign in to the NetBackup Flex Scale web UI and in the left pane click **Cluster Management > Infrastructure**.
2. Shut down the node for which you want to update the firmware. Click the Actions menu (vertical ellipsis) from the right side of the row in the UI and click **Shutdown node**.



3. When prompted for confirmation, click **Shutdown node**.



Wait for the shutdown process to complete.

The task is shown completed in **Recent activity**.

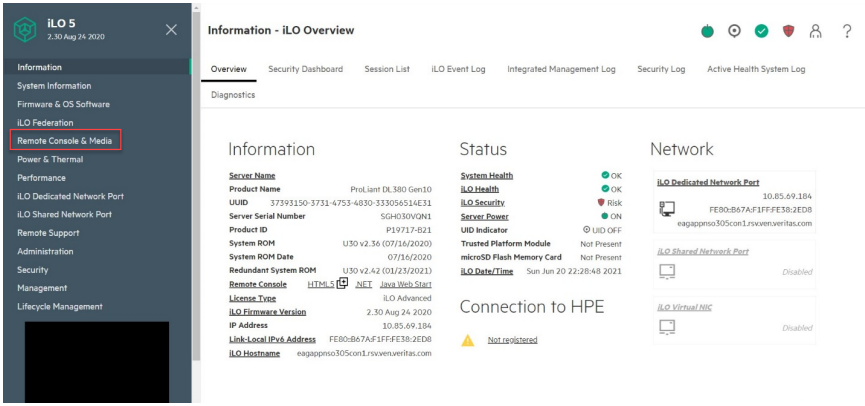
4 Verify that the node is shut down. A blank screen is displayed and the Power button turns yellow.

5 Log on to HPE-Integrated Lights-Out (iLO) remote console from a Windows system that can access the cluster nodes and on which the firmware package is downloaded from the Download Center.

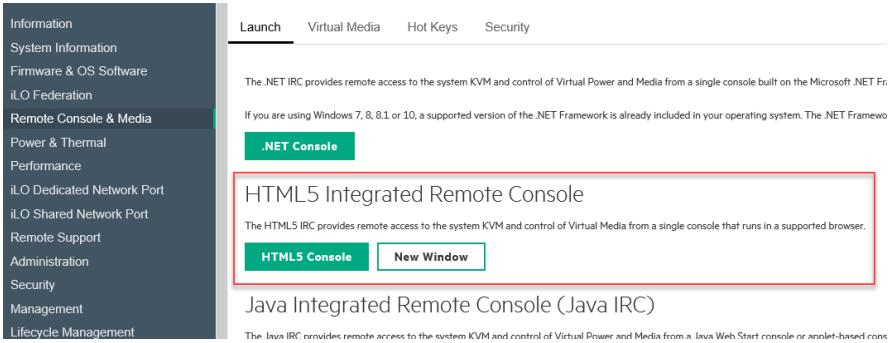
Note: The network connectivity between the jump server (Windows system) containing the firmware package and the NetBackup Flex Scale cluster nodes should be stable and reliable to ensure the firmware upgrade process progresses successfully.

---

6 In the left navigation pane click **Remote Console & Media**.

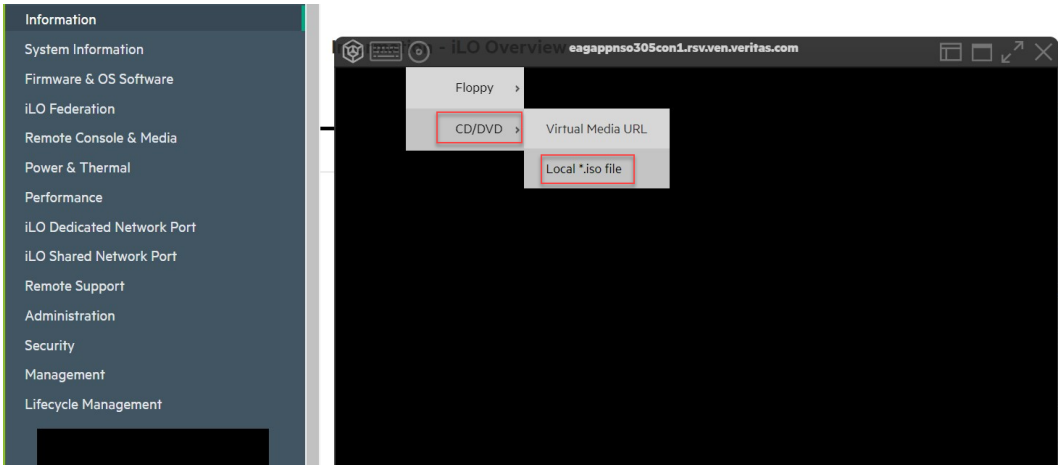


7 Click **HTML5 Integrated Remote Console**.

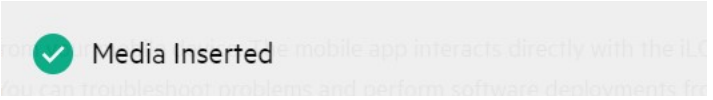


8 In the console, wait until no messages are displayed and the screen is blank. Set up **CD/DVD** drive option as a first boot option and then upload the firmware package and restart the node.

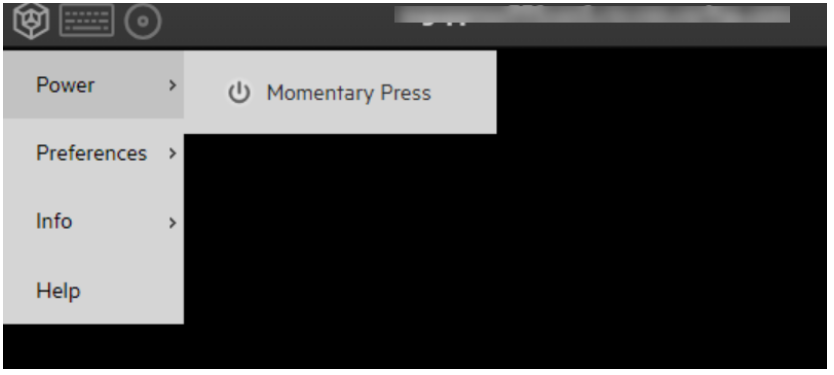
To upload the firmware package, click the **Disk** icon on the top of the screen, click **CD/DVD > Local *.iso file** and select the firmware package.



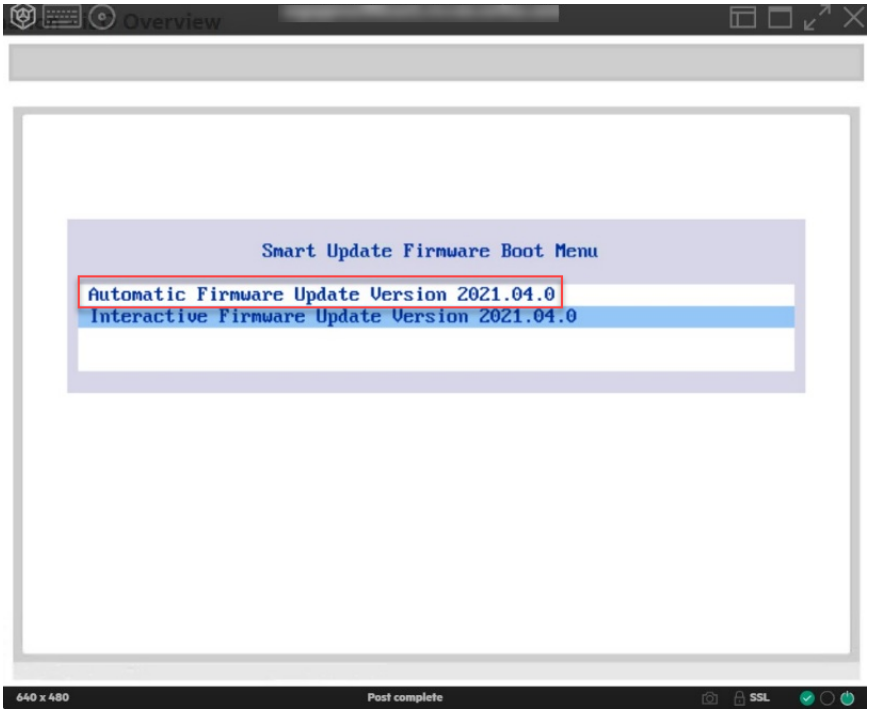
Ensure that the media is uploaded successfully.



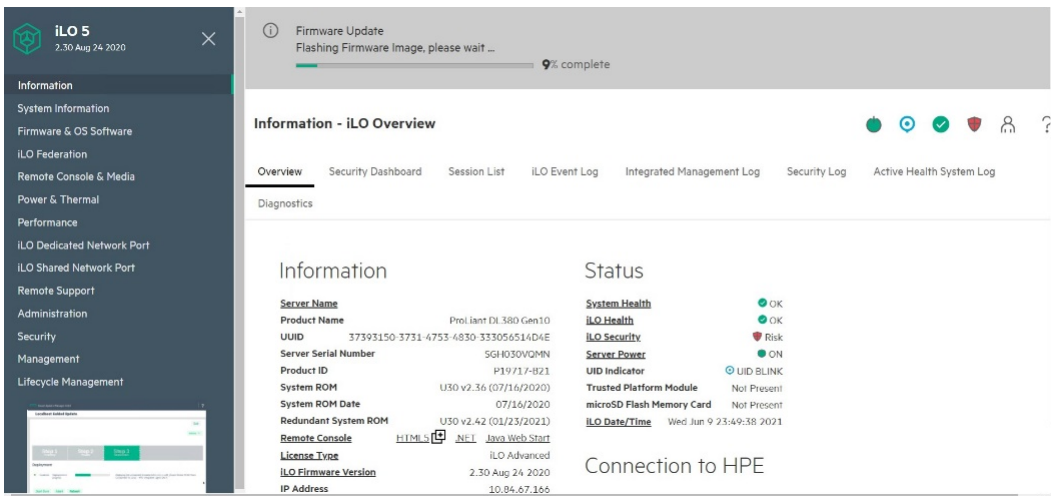
9 Restart the node. Click the iLO icon and click **Power > Momentary press**.



10 From the **Smart Update Firmware Boot Menu** utility, the **Automatic Firmware update mode** option is selected by default.

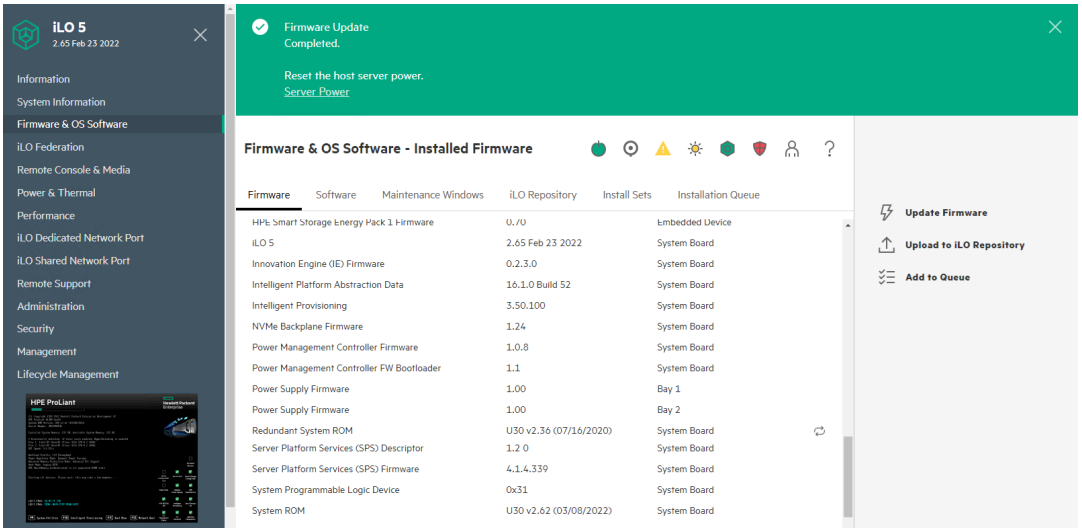


Note the flashing firmware image in the iLO.

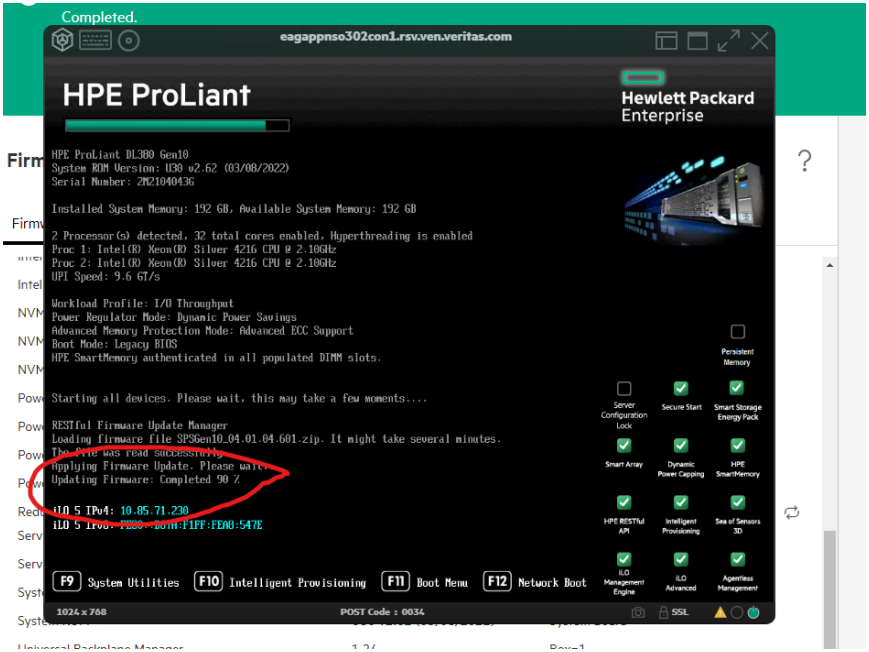


During the upgrade, several components are upgraded. Several times, the GUI reports that the firmware update is complete but wait till all components are upgraded. At one point the iLO firmware is upgraded and you are logged out and you need to log in to the iLO again.

You can monitor the progress in the remote console. Ignore the status in the main ILO screen. At a few points during the upgrade an option to reboot the node is shown. Do not reboot the node.

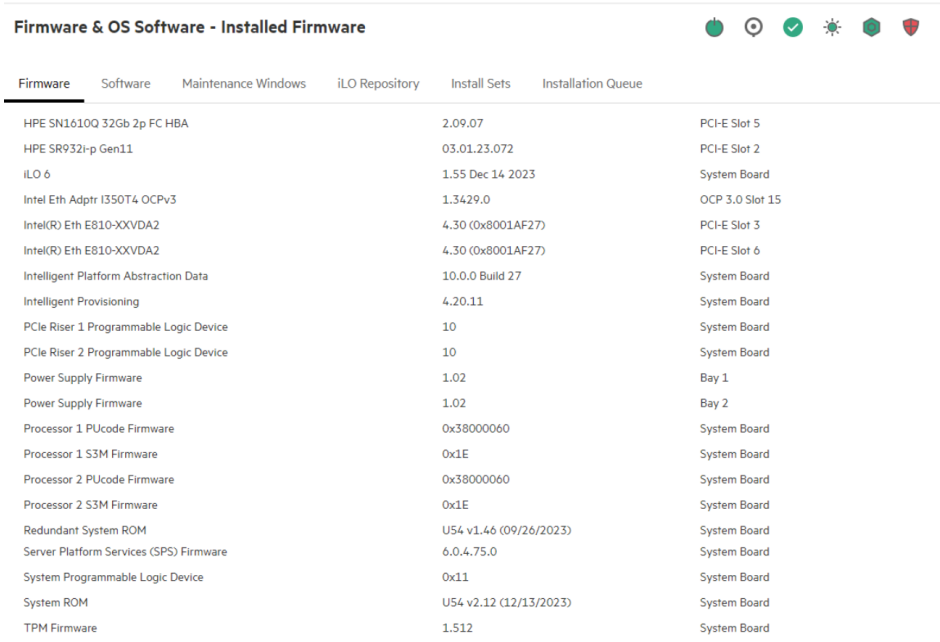


Continue to monitor the progress in the remote console.



It takes approximately 40 minutes to upgrade all the components. After the upgrade is complete, the remote console shows the logs momentarily before rebooting the node automatically. Wait until iLO returns to the login window. It will return to the login window automatically once the firmware upgrade is done.

11 Verify the firmware version of the components is updated as per the ACL file on SORT. Click **Firmware & OS Software tab > Firmware** and review the firmware version of the components.



Firmware & OS Software - Installed Firmware

Firmware | Software | Maintenance Windows | iLO Repository | Install Sets | Installation Queue

HPE SN1610Q 32Gb 2p FC HBA	2.09.07	PCI-E Slot 5
HPE SR932i-p Gen11	03.01.23.072	PCI-E Slot 2
iLO 6	1.55 Dec 14 2023	System Board
Intel Eth Adptr I350T4 OCPv3	1.3429.0	OCP 3.0 Slot 15
Intel(R) Eth E810-XXVDA2	4.30 (0x8001AF27)	PCI-E Slot 3
Intel(R) Eth E810-XXVDA2	4.30 (0x8001AF27)	PCI-E Slot 6
Intelligent Platform Abstraction Data	10.0.0 Build 27	System Board
Intelligent Provisioning	4.20.11	System Board
PCIe Riser 1 Programmable Logic Device	10	System Board
PCIe Riser 2 Programmable Logic Device	10	System Board
Power Supply Firmware	1.02	Bay 1
Power Supply Firmware	1.02	Bay 2
Processor 1 PUcode Firmware	0x38000060	System Board
Processor 1 S3M Firmware	0x1E	System Board
Processor 2 PUcode Firmware	0x38000060	System Board
Processor 2 S3M Firmware	0x1E	System Board
Redundant System ROM	U54 v1.46 (09/26/2023)	System Board
Server Platform Services (SPS) Firmware	6.0.4.75.0	System Board
System Programmable Logic Device	0x11	System Board
System ROM	U54 v2.12 (12/13/2023)	System Board
TPM Firmware	1.512	System Board

After the firmware upgrade is complete, the node restarts automatically and rejoins the cluster. Wait for the data rebuilding to complete before you upgrade the firmware of another node in the cluster. During data rebuilding, the node is shown as unhealthy on the GUI. You can view the disk resync status by navigating to **Infrastructure > Disks**. After the resync is complete, the node is marked as healthy.

12 Update the `acl_info.json` ACL file on the nodes.

See “ACL configuration” on page 118.

Upgrading the firmware using the parallel method

In a parallel firmware upgrade, firmware on all the nodes is upgraded simultaneously. During parallel upgrade, you must shut down the cluster. Ensure that all the nodes are shut down, and then upgrade the firmware on all the nodes simultaneously.

To upgrade the firmware using the parallel method:

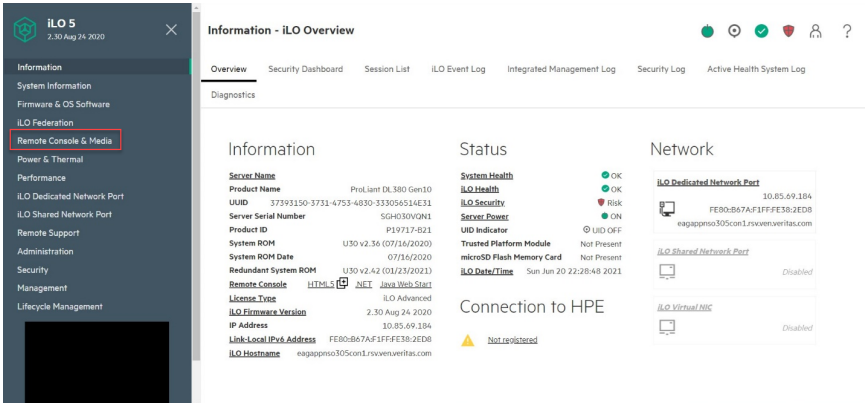
1. To shut down all the nodes, log in to the cluster-level CLI by logging into the system using the console IP address with your credentials, and then run the `cluster node shutdown nodename=all` command.
2. Verify that the node is shut down. A blank screen is displayed and the Power button turns yellow.

3. Log on to HPE-Integrated Lights-Out (iLO) remote console from a Windows system that can access the cluster nodes and on which the firmware package is downloaded from the Download Center.

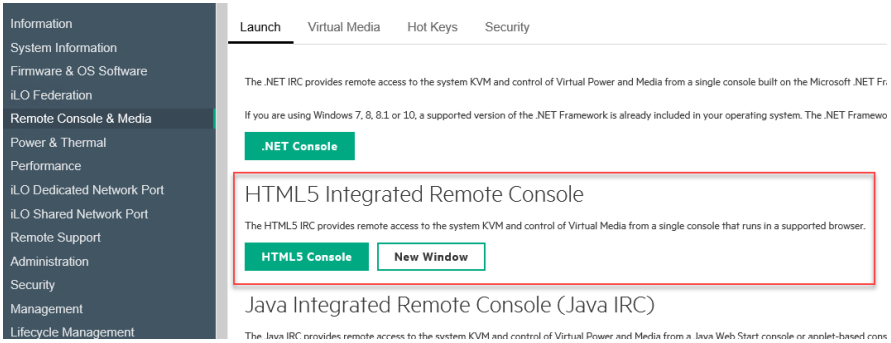
Note: The network connectivity between the jump server (Windows system) containing the firmware package and the NetBackup Flex Scale cluster nodes should be stable and reliable to ensure the firmware upgrade process progresses successfully.

---

4 In the left navigation pane click **Remote Console & Media**.



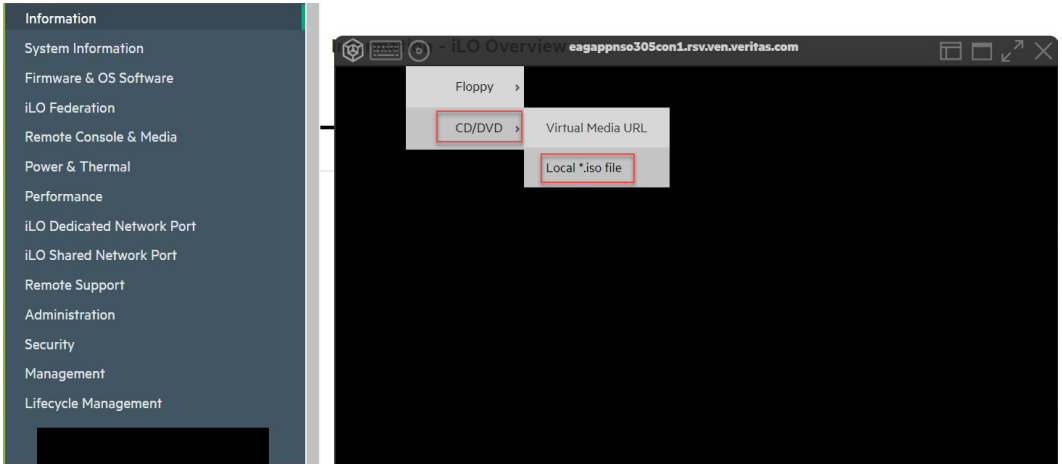
5 Click **HTML5 Integrated Remote Console**.



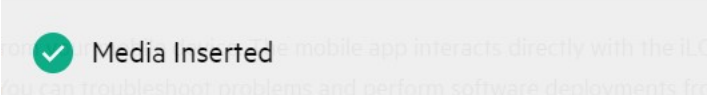
6 In the console, wait until no messages are displayed and the screen is blank. Set up **CD/DVD** drive option as a first boot option and then upload the firmware package and restart the node.

To upload the file, click the **Disk** icon on the top of the screen, click **CD/DVD > Local *.iso file** and select the ISO file.

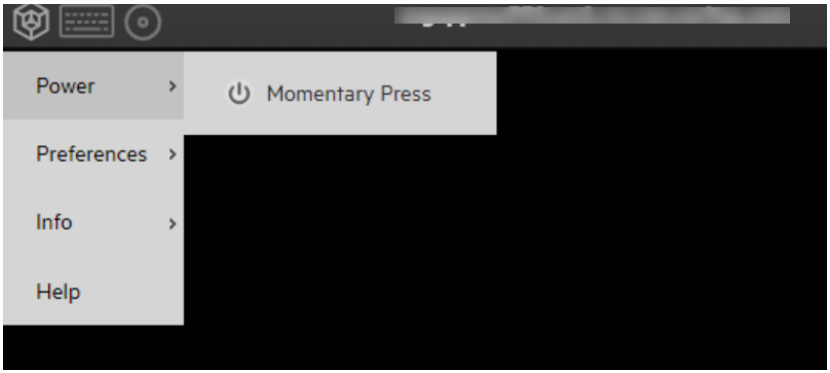
Note: A separate mount point for the firmware package is required for each node. For example, for a four-node cluster, create four different mount points and attach the firmware package separately.



Ensure that the media is uploaded successfully.



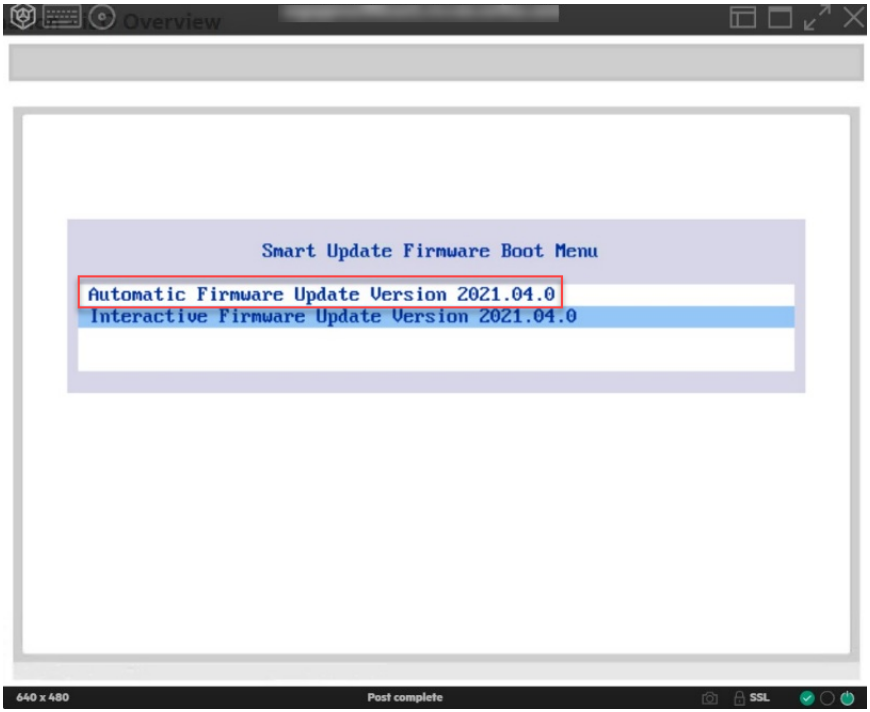
7 Restart all the nodes. Click the iLO icon and click **Power > Momentary press**.



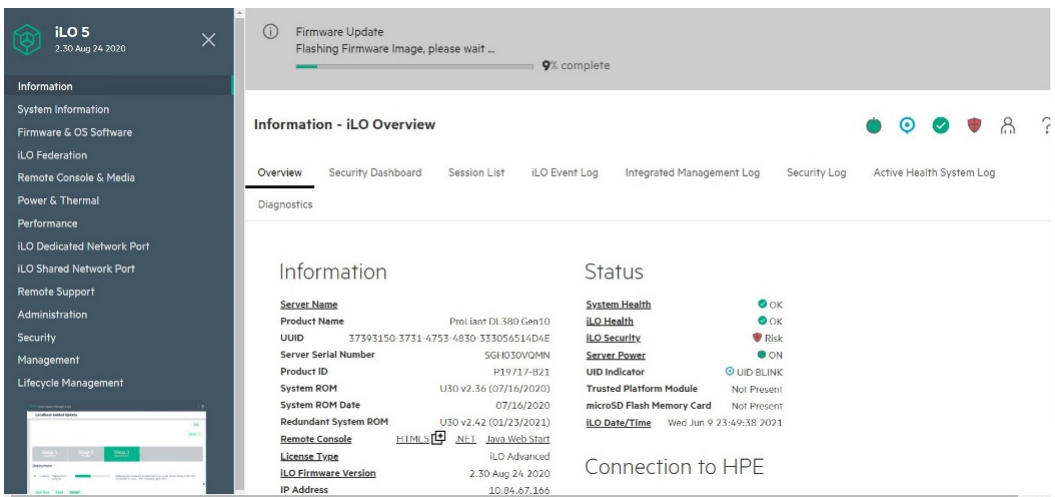
After the nodes are restarted, the nodes are expected to reboot from the mounted firmware package. Monitor the ILO console for all nodes, and if any node fails to boot from the firmware package and instead boots from the HDD containing the NetBackup Flex Scale software, perform the following steps on that node immediately:

- Reset the ILO.
- Unmount and remount the firmware package.
- Reset the node from the ILO.

8 From the **Smart Update Firmware Boot Menu** utility, the **Automatic Firmware update mode** option is selected by default.

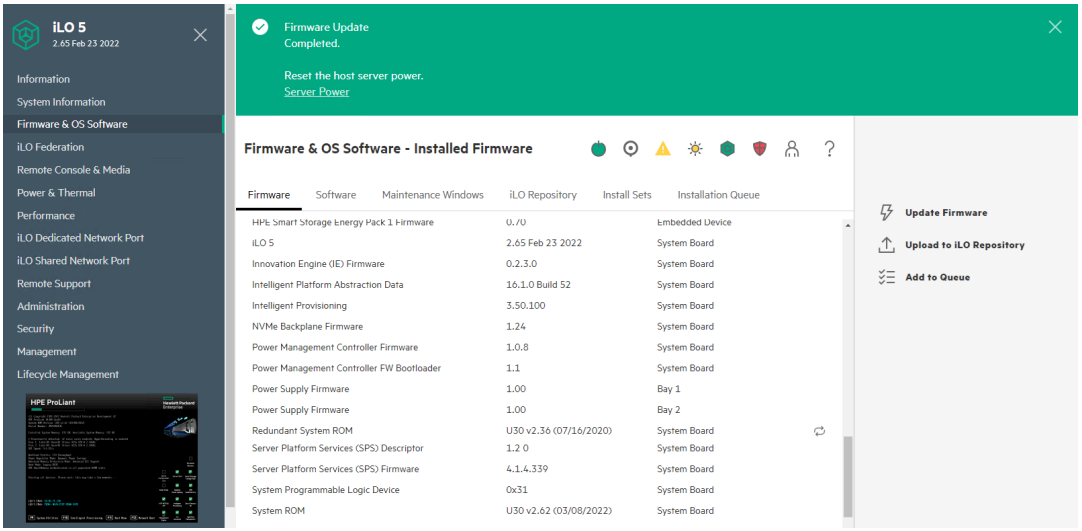


Note the flashing firmware image in the iLO.

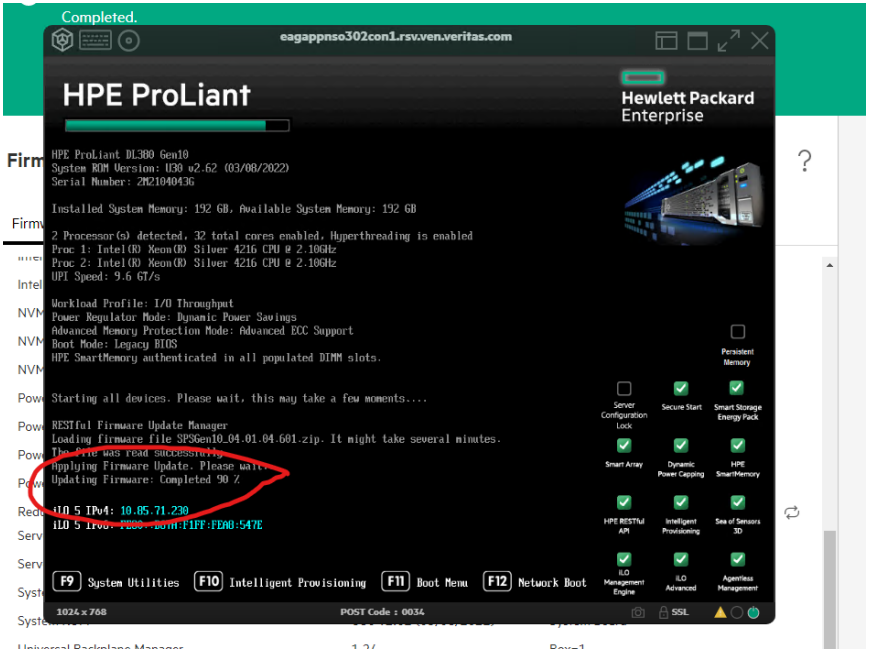


During the upgrade, several components are upgraded. Several times, the GUI reports that the firmware update is complete but wait till all components are upgraded. At one point the iLO firmware is upgraded and you are logged out and you need to log in to the iLO again.

You can monitor the progress in the remote console. Ignore the status in the main ILO screen. At a few points during the upgrade an option to reboot the node is shown. Do not reboot the node.

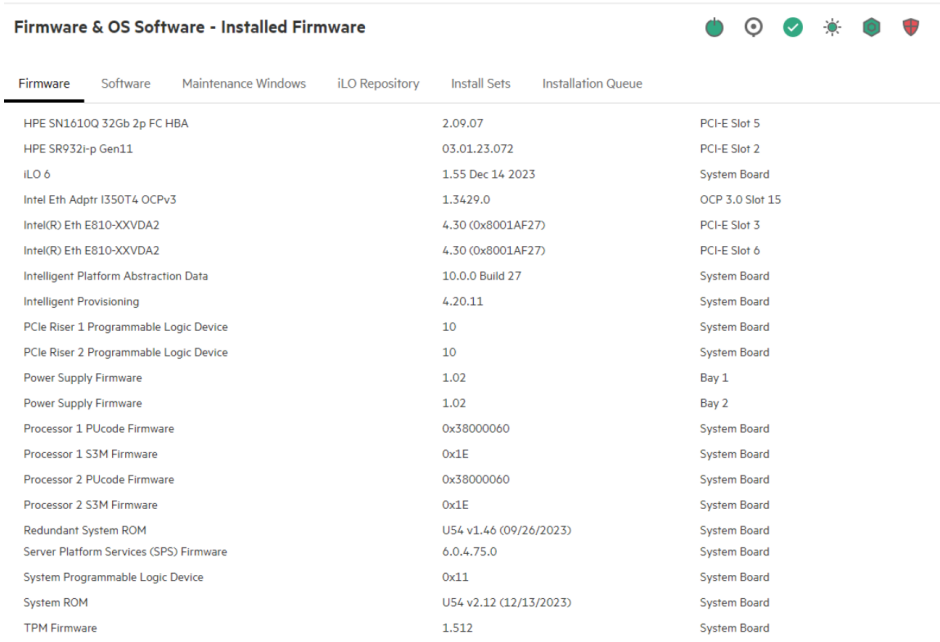


Continue to monitor the progress in the remote console.



It takes approximately 40 minutes to upgrade all the components. After the upgrade is complete, the remote console shows the logs momentarily before rebooting the node automatically. Wait until iLO returns to the login window. It returns to the login window automatically once the firmware upgrade is done.

9 Verify that the firmware version of the components is updated as per the ACL file on SORT. Click **Firmware & OS Software tab > Firmware** and review the firmware version of the components.



After the firmware upgrade is complete, the node restarts automatically and rejoins the cluster.

10 Update the `acl_info.json` ACL file on the nodes.

See “ACL configuration” on page 118.

Updating the firmware in NetBackup Flex Scale clusters using the UI

You can upgrade the firmware of the cluster nodes from the NetBackup Flex Scale GUI. Before you begin the firmware upgrade process, ensure that all the nodes in the cluster are up. You can install the firmware packages that are downloaded from the Download Center of the Veritas Support website to a Windows system that can access the Download Center and the cluster nodes. Installing firmware packages that are downloaded from the Veritas website ensures that you only install the firmware packages that are verified and tested by Veritas. You can choose to

download and install firmware packages from vendor sites. However, these packages are not validated by Veritas.

Ensure that the firmware version of the appliance components is updated to the latest versions as listed in the appliance compatibility list (ACL) on the Veritas website (https://sort.veritas.com/netbackup/acl). Alerts are raised if the firmware version of the components is not supported in the ACL. You can view the alerts in the **Alerts** area of the dashboard or by navigating to **Settings > Alerts management**.

To update the firmware on cluster nodes:

1. Sign in to the NetBackup Flex Scale web UI and in the left pane click **Cluster Management > Cluster settings > Software management > Firmware upgrade**.
2. To upload a firmware package from the Windows system where you had downloaded the firmware package earlier, click **Upload file**.

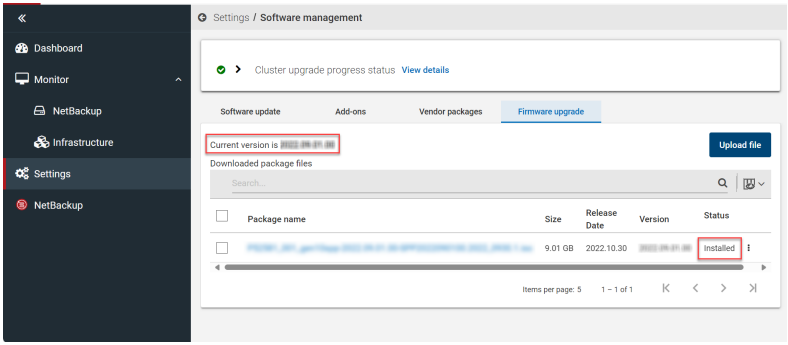
   Select the file and then click **Upload**.

   After uploading the package, it is displayed under **Downloaded package files**.
3. To install the firmware package, under **Downloaded package files** from the Actions menu (vertical ellipsis) click **Start update**. If the firmware package was downloaded from the vendor site, you are prompted to confirm if you want to proceed with the installation. If you want to proceed, click **Continue**.

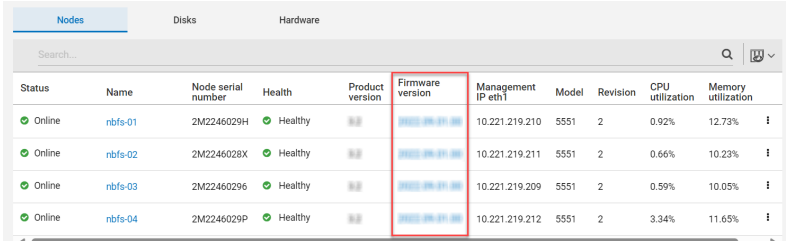
4 To upgrade the firmware on all the nodes simultaneously click **Parallel**. To upgrade the firmware on each of the nodes successively, click **Rolling**.

A success or failure notification is displayed on the top of the page. To view detailed status, click **View details.**

If the firmware upgrade is completed successfully, a notification about the successful upgrade is displayed on the top of the page. The current version displayed on the page is updated to the firmware package version and the status of the firmware package in the **Downloaded package files** changes to **Installed**.



On the **Infrastructure > Nodes** tab, the **Firmware version** column shows the firmware package version. You can click the version to view the firmware version of each of the components.



If the firmware upgrade fails, a notification about the failure is displayed on the top of the page and the status of the package in the **Downloaded package files** is set to **Available**. To view details about the failure, click **View details**.

5 Update the `acl_info.json` ACL file on the nodes.

See “ACL configuration” on page 118.

Deleting firmware packages using UI

You can delete the firmware packages from the cluster nodes that are uploaded from the NetBackup Flex Scale UI.

To delete a firmware package:

1. Sign in to the NetBackup Flex Scale web UI and in the left pane click **Cluster Management > Cluster settings > Software management > Firmware upgrade**.
2. To delete a firmware package, under **Downloaded package files**, from the Actions menu (vertical ellipsis) click **Remove**.

   A success or a failure notification is displayed on the top of the page. To view detailed status, click **View details**.

ACL configuration

The ACL Configuration page lets you manage Appliance Compatibility List (ACL) configuration files on the cluster. From this page, you can upload, apply, download, and remove ACL configuration files, as well as view their current status.

You can navigate to this page by going to **Settings > Software Management > ACL Configuration**. The ACL Configuration table lists all ACL configuration files available on the cluster and displays their current status:

- Available: The ACL configuration file is uploaded to the cluster but not applied.
- Installed: The ACL configuration file is currently applied on the cluster.

To upload a new ACL configuration file

1. Navigate to the **ACL Configuration** page. Click **Add**.
2. Select an ACL configuration file with the valid extension `.acl.json`. Upload the file to the cluster.

   Note: Uploaded files appear in the table with an `Available` status until applied.

To download an existing ACL configuration file

1. Navigate to the **ACL Configuration** page. .
2. Select an ACL configuration file. Click **Download** to save the selected ACL configuration file to your local system.

To apply or remove an ACL configuration file

1. Navigate to the **ACL Configuration** page. .
2. Use the kebab menu (vertical ellipsis) corresponding to an ACL configuration file to perform the following actions:
   - Apply:
     Applies the selected ACL configuration file to the cluster. Applying the ACL configuration also restarts the collector service.
   - Remove:
     Removes the selected ACL configuration file from the cluster. You can remove one or more ACL configuration files at a time.

Chapter 5

Managing EEBs

This chapter includes the following topics:

Downloading EEBs

To download the required EEBs:

1. Go to the Veritas Support website (https://www.veritas.com/support/en_US) and click **Downloads**, which redirects you to the Download Center.
2. In the Veritas Download Center, in the **Products** list, select Appliances, in the **Sub product** list select **NetBackup Flex Scale**. Select the required version and click **Explore**.
3. Expand **Updates**.

   Select the package specific to the version you are upgrading to.

   You can download the EEBs from the **Updates** section. You must sign in with your Veritas account credentials to download the EEB.

Installing EEBs using GUI

You can install Emergency Engineering Binaries (EEBs) from the GUI using the rolling or the parallel method. In the rolling method, EEBs are installed on each node successively. In the parallel method, EEBs are installed on all the nodes in parallel. Depending on the type of EEB that you choose to install, you have the following installation options:

- Data EEBs (including NetBackup EEBs): You can use only the rolling method to install the EEBs. In the rolling method, EEBs are installed on each node successively.
- Non-data EEBs (including non-data NetBackup EEBs and appliance EEBs): You can use the rolling or the parallel method to install the EEBs. In the rolling method, EEBs are installed on each node successively. In the parallel method, EEBs are installed on all the nodes in parallel.
- Both data and non-data EEBs: You can use only the rolling method to install the EEBs. In the rolling method, EEBs are installed on each node successively.

Note: The same restrictions apply when you roll back the installed EEBs.

In the GUI, the installed EEBs are listed in ascending order of the dates on which they are installed.

Note: If disaster recovery is configured, you must upload and install the EEBs separately on both the sites.

See "About NetBackup Flex Scale upgrades and EEBs" on page 82.

To install an EEB using the GUI:

1. Download the EEB on the local system.
2. Go to **Settings** > **Software management** > **Add-ons**.

   If you already have EEBs on your system, all the EEBs (available and installed) are displayed.
3. To upload EEBs:
   - If there are no EEBs on your system, click **Choose add-ons**, select the EEBs, and click **Upload file**.
   - If the EEB that you want to install is not in the displayed EEB list, click **Add**. In the **Upload EEBs** screen, click **Choose add-ons**, select the EEBs, and click **Add**.

You can upload multiple EEBs simultaneously.

4 On the **Add-ons** tab, select the EEBs that you want to install and click **Install**.

If only data EEBs are selected, you can perform only the rolling installation. If non-data EEBs are selected, when prompted, choose whether you want to use the rolling or the parallel option. Click **Install**.

EEB installation progress information is displayed on top of the page. To monitor the progress, click **View details**.

After the EEBs are installed, the status of the EEBs changes from **Available** to **Installed**.

Installing EEBs during upgrade

NetBackup Flex Scale upgrades to version 3.5.100 supports installation of Emergency Engineering Binaries (EEBs) during upgrade. It ensures that known vulnerabilities and bugs are addressed during upgrade.

You can upload the following EEBs before starting an upgrade:

- VRTSnbfsapp_EEB_ET4189567-3.5.0.0-4.x86_64.rpm
- VRTSnbfsapp_nb_EEB_ET4189143-10.5.0.1-7.x86_64.rpm
- VRTSnbfsapp_nb_EEB_ET4194051-10.5.0.1-1.x86_64.rpm
- VRTSnbfsapp_nb_EEB_ET4191929-10.5.0.1-1.x86_64.rpm

If External Certificate Authority (ECA) is configured on the setup, then it is recommended that the above EEBs should be installed during upgrade, otherwise upgrade to version 3.5.100 may not work.

The above mentioned EEBs should be uploaded on NetBackup Flex Scale web UI before upgrade to install the EEBs during upgrade.

To upload EEBs

1 Go to **Settings > Software management > Add-ons**.

2 If there are no EEBs on your system, click **Choose add-ons**, select the EEBs, and click **Upload file**.

3 If the EEB that you want to install is not in the displayed EEB list, click **Add**. In the **Upload EEBs** screen, click **Choose add-ons**, select the EEBs, and click **Add**.

You can upload multiple EEBs simultaneously

Note: After uploading the EEBs, if the management console fails over to some other node for any reason, then remove the EEBs from NetBackup Flex Scale web UI and re-upload them before upgrade.

To identify the management console node, go to the NetBackup Flex Scale web UI, navigate to **Cluster Management > Infrastructure**. On the **Infrastructure** page, the console node field shows the management console node. The remaining nodes are the non-management console nodes.

Removing EEBs using GUI

You can remove EEBs using the GUI.

To remove an EEB using the GUI

1. Go to **Settings > Software management > Add-ons**.
2. On the **Add-ons** tab, select the EEBs that you want to remove and click **Remove**.

   You can delete multiple EEBs at once by selecting them simultaneously.

Uninstalling EEBs using GUI

You can uninstall EEBs from the GUI using the rolling or the parallel method. In the rolling method, EEBs are uninstalled on each node successively. In the parallel method, EEBs are uninstalled on all the nodes in parallel.

To uninstall an EEB using the GUI

1. Go to **Settings > Software management > Add-ons**.
2. On the **Add-ons** tab, select the EEBs that you want to uninstall and click **Rollback**.
3. When prompted, select either the rolling or parallel option, then click **Rollback**.

   EEB uninstallation progress information is displayed at the top of the page. To monitor the progress, click **View details**. Once the EEBs are uninstalled, their status changes from *Installed* to *Available*.

Installing EEBs using REST APIs

You can perform an upgrade by installing EEBs using REST APIs.

To install EEBs using REST APIs

1. (Optional) Upload an EEB package file to the cluster. This also downloads the EEB directly.

   ```
   POST /api/appliance/v1.0/upgrade/upload
   ```

   Usually, the EEB RPM file upload takes around 2 minutes.

2. Find the list of all the available EEBs (downloaded/installed).

   ```
   GET /api/appliance/v1.0/upgrade/eebs
   ```

3. Find the summary of a specific EEB.

   ```
   GET /api/appliance/v1.0/upgrade/eebs/{eebName}
   ```

4. (Optional) Find the directory path where the EEB should be placed.

   ```
   GET /api/appliance/v1.0/upgrade/path
   ```

5. Install the EEB.

   ```
   PATCH /api/appliance/v1.0/upgrade/eebs/{eebName}
   ```

6. You can find the details of the progress of the EEB installation using the task ID.

   ```
   GET /api/appliance/v1.0/tasks/{taskId}
   ```

Chapter 6

Removing NetBackup Flex Scale

This chapter includes the following topics:

About disk erasure

Disk erasure destroys all data stored on the appliance disks by overwriting the disks with a digital pattern. The operation cannot be reverted and the erased data cannot be recovered. Ensure that the data has been backed up and verified, or that the data is no longer needed before you erase the disks. The data erasure process complies with the National Institute of Standards and Technology Special Publication 800-88 (NIST SP800-88).

Note: Veritas recommends that you erase the disks before you perform a factory reset.

Before erasing the disks on the node, note the following points:

- Disks cannot be erased when a node is a part of the cluster.
- Once a data erasure operation is running on a disk, no other storage operations can be performed on the disk. Data cannot be accessed from the node once disk erasure begins.
- Disk erasure can take up to days or weeks to complete depending on the size of the disk and the pass algorithm used.

Pass algorithm

To minimize the chance that the erased data is recoverable, the data erasure feature provides options for the pass algorithm that is used to overwrite all of the data on the disks. The following pass algorithms are supported:

- One-pass algorithm: Overwrites the disks with a randomly-selected digital pattern. This option takes the least amount of time.
- Three-pass algorithm: Overwrites the disks a total of three times. The first pass, it uses a pre-selected digital pattern. The second pass uses the binary complement of the previous pattern, and the last pass uses a randomly-selected digital pattern.
- Seven-pass algorithm: Overwrites the disks a total of seven times. In each pass, the data is overwritten with a randomly-selected digital pattern or with the binary complement of the previous pattern.

You can configure data erasure multiple times. You can only use one of the three pass algorithms each time you configure the data erasure.

Disk erasure operations

Data erasure is only supported from the NetBackup Flex Scale Appliance Shell Menu. The following command operations are available from the `system` view:

- `system storage erase-disks configure`: Specify the pass algorithm to use to erase the disks. The time required for disk erasure is determined by the size of the disks and the pass algorithm used.
- `system storage erase-disks show`: Shows the progress of the erasure operations and the erasure status for all the disks.
- `system storage erase-disks abort`: Stops the erasure operation, which is in progress.

Configuring data erasure

Use the shell menu to configure the data erasure.

To configure data erasure:

1. Log in to the NetBackup Flex Scale Appliance Shell Menu.
2. From the `system` view, run the following command:

   ```
   system storage erase-disks configure
   ```

   Enter **Yes** to continue.

   The options for the pass algorithm are displayed.

   Note: You can no longer use the data after you start erasing the disks.

3. Enter the pass algorithm to use.
4. A summary of the configuration and the estimated time for erasing each disk is displayed. Enter **Yes** to proceed.

   After you start the data erasure, you can use the `system storage erase-disks show` command to monitor the progress.

Viewing the data erasure status

You can monitor the tasks that are in progress and the data erasure history. The status shows detailed information for each storage disk.

Note: Ensure that you configure and monitor data erasure on the same node. The data erasure operation initialized from one node can only be seen from that node, and is not visible on the other nodes.

You can view the following details for the disk erasure tasks that are in progress:

- The disk name
- The pass algorithm used
- The time elapsed
- The remaining time
- The erasure progress in percentage

The disk erasure status shows the following details for each disk:

- The disk name
- The pass algorithm used
- The status or completion time of the last erasure operation

To view the disk erasure status:

1. Log on to the NetBackup Flex Scale Appliance Shell Menu.
2. From the `system` view, run the following command:

   ```
   system storage erase-disks show
   ```

Aborting data erasure

You can abort a running data erasure operation at any time. After you abort the operation, the data on the affected disks is corrupted. The **Last Erasure Status** for the affected disks shows **Aborted**. You must configure data erasure again for all the disks if you want to complete the erasure. The data erasure operation starts anew on all the disks the next time.

To abort the data erasure

1. Log on to the NetBackup Flex Scale Appliance Shell Menu.
2. From the `system` view, run the following command:

   ```
   system storage erase-disks abort
   ```

3. Enter **Yes** to abort the data erasure operation.

About NetBackup Flex Scale node factory reset

The purpose of a factory reset is to return a node to a clean unconfigured default factory state. A factory reset discards all the data from the node, including storage and networking configuration and reverts the node to the factory image. However, you can choose to retain the network configuration, if required, before you initiate a factory reset. Additionally, you can also choose whether or not to restart the node immediately after the reset completes. However, a node restart is required for the factory reset process changes to take effect on the node.

During the factory reset process, the following components are reset:

- Appliance software
- NetBackup software
- Storage configuration and backup data
- (optional) Networking configuration

You can perform a factory reset using the factory reset command from the system command prompt.

See “Performing a factory reset on a node” on page 129.

Note: You cannot factory reset a node if the node is in the cluster, disk erasure is in progress, or the lockdown mode is set to compliance or enterprise.

Performing a factory reset on a node

The following steps describe how to run a factory reset on a node that has either been removed from a cluster or a node that has not yet been added to a cluster.

Note: Veritas recommends that you erase the disks before you perform a factory reset.

To perform a factory reset on a node

1. Log in to the node on which you want to perform a factory reset with user account that has Appliance administrator role.
2. Enter the following command:

   ```
   system factory-reset
   ```

3. Specify whether you want to reset the network configuration on the node.

   The Factory Reset command displays the following prompt on the command line:

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

   Type **Yes** to include the network configuration in the factory reset process or type **No** to retain the network settings on the node.

   The default setting is yes, which means the network settings are included in the factory reset.

   Note: If you choose to reset the network configuration, you cannot access the node using its management IP. After the factory reset is complete, you can access the node either by physically accessing the node console directly or using the IPMI network.

4 Specify whether you want to automatically restart the node after the factory reset is complete.

The Factory Reset command displays the following prompt on the command line:

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

Type **Yes** to automatically restart the node after the factory reset is complete, or type **No** if you want to restart the node at a later time.

The default setting is no, which means the node is not restarted after the factory reset.

Note: Veritas recommends that you restart the node at the end of the factory reset process. A system restart is required for completing the factory reset process related changes to take effect.

---

5 Confirm whether you want to proceed with the factory reset process.

The Factory Reset command displays a summary of the configuration settings and the following prompt:

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

Type **Yes** if you want to proceed with the factory reset, or type **No** if you cancel the process or go back and change the factory reset options for the node.

The factory reset process starts and can take up to 20 minutes to complete. The command line displays several messages that indicate the progress.

The following messages are displayed after factory reset completes successfully:

```
- [Info] V-409-889-0009: Running factory reset. This process can
 take up to 20 minutes...

- [Info] The appliance is restarting...
```

Note: Once the factory reset is complete, you may have to install software release updates or EEB packages on the node before you add the node back into the cluster.

If you install hardware vendor packages prior to running factory reset on a node, the vendor packages are installed automatically on the node after the factory reset is complete.

Appendix A

Installing NetBackup Flex Scale using a downloaded ISO file

This appendix includes the following topics:

About NetBackup Flex Scale software installation

Your NetBackup Flex Scale appliance comes pre-installed with an operating system and the NetBackup Flex Scale software. You do not have to install anything on the raw nodes after you take them out of the box. Once you have assembled the nodes and placed the appliance in your data center environment, you verify the configuration prerequisites and begin with the cluster configuration.

The installation instructions provided here are intended to serve only as a reference.

Refer to the following:

See “Enabling remote IPMI connections” on page 133.

See “Setting up the RAID configuration on the nodes” on page 135.

See “Configuring the BIOS settings on the nodes” on page 142.

See “Downloading the product installer ISO” on page 149.

See “Mounting the ISO file on the nodes” on page 150.

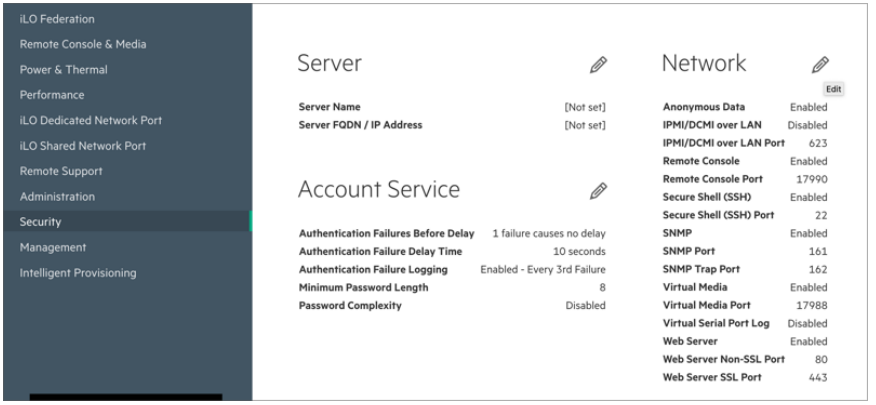
See “Installing NetBackup Flex Scale using the ISO” on page 151.

Enabling remote IPMI connections

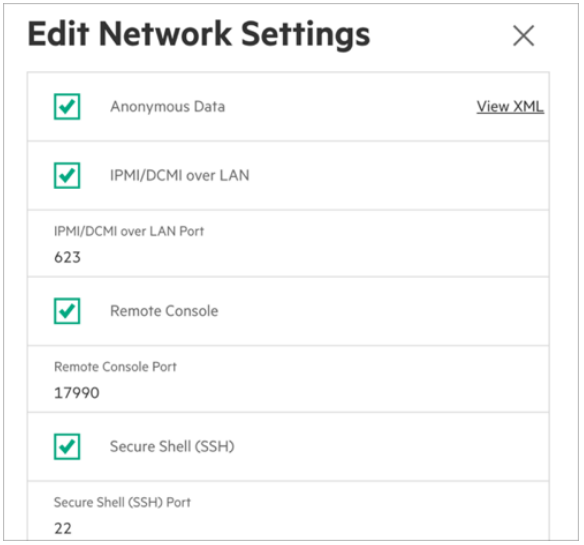
Use the HPE iLO Remote Console administration interface to enable remote IPMI connections over a Local Area Network (LAN).

To enable IPMI connections

1. Launch the HPE iLO Remote Console interface and from the menu on the left, click **Security**.
2. In the Network section on the right, click the pencil icon to edit the Network settings.



3. On the Edit Network Settings dialog, select the **IPMI/DCMI over LAN** option to enable the settings.



4. Click **OK** to save and exit.

Setting up the RAID configuration on the nodes

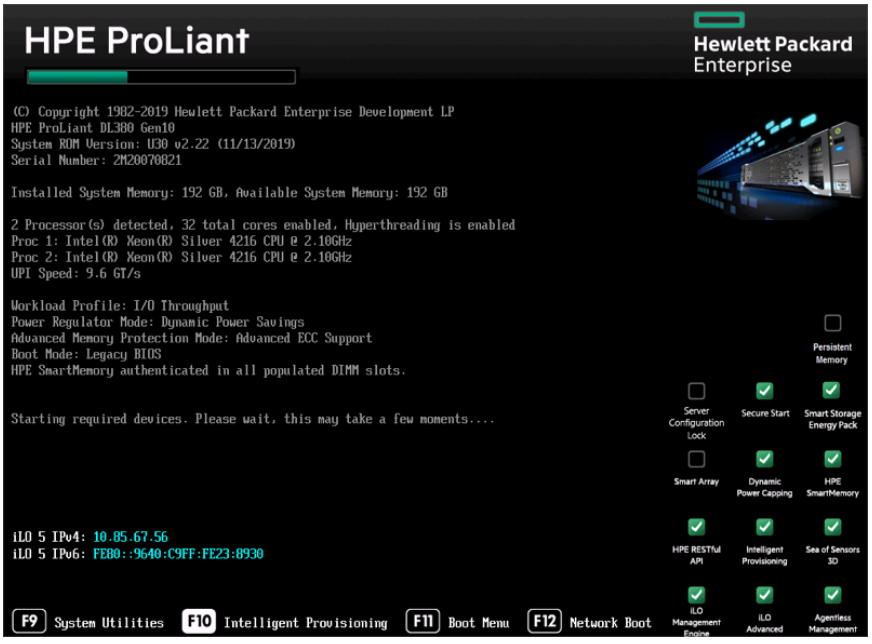
You must initialize and set up the RAID configuration on each node before you install the NetBackup Flex Scale software on the node. Set up a RAID 1 configuration and configure the two 1.92 TB SATA storage devices as the RAID volumes.

The following procedure provides a high level overview of the process. For detailed information, refer to the HPE ProLiant DL380 Gen10 Server documentation.

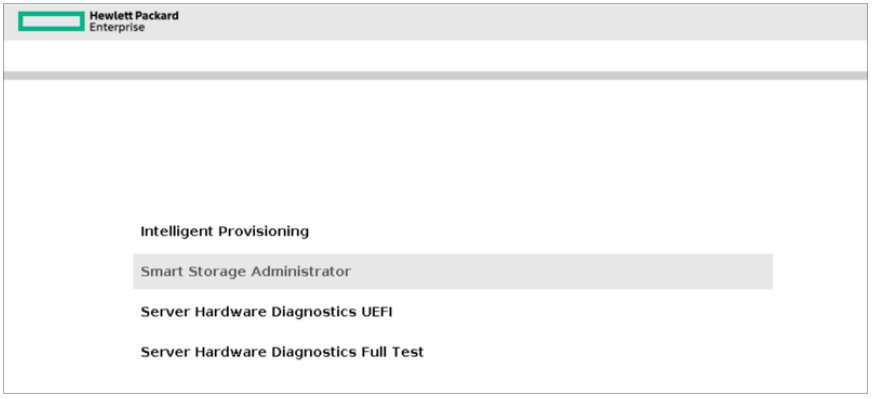
Note: The screenshots provided in this section are for Gen10 Server. For Gen11 Server, refer to the corresponding images.

To initialize RAID on the node

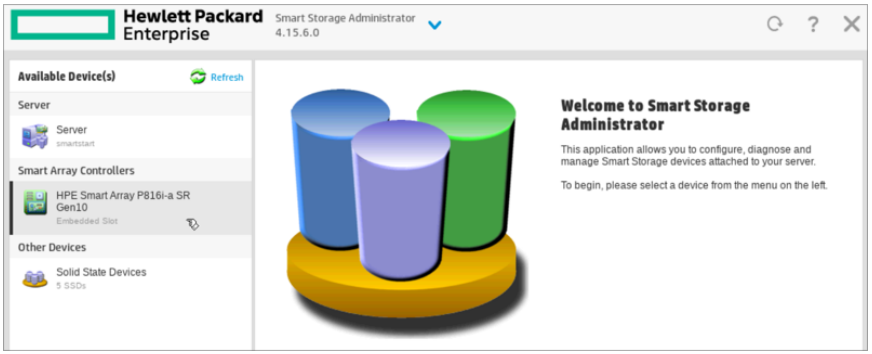
1 Power ON the node and press the **F10** key on the boot screen to launch the Intelligent Provisioning module.



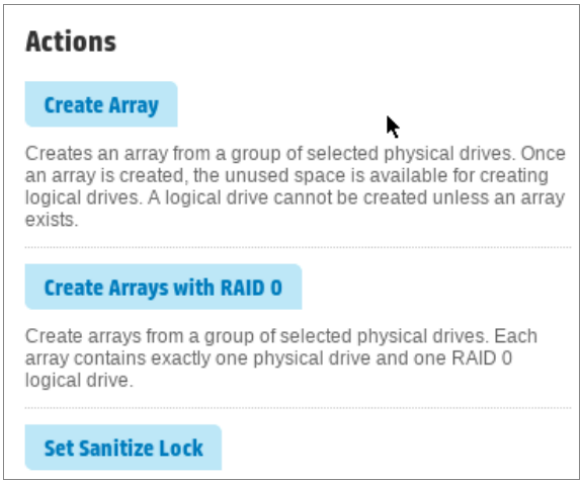
2 Click **Smart Storage Administrator** to begin the RAID configuration.



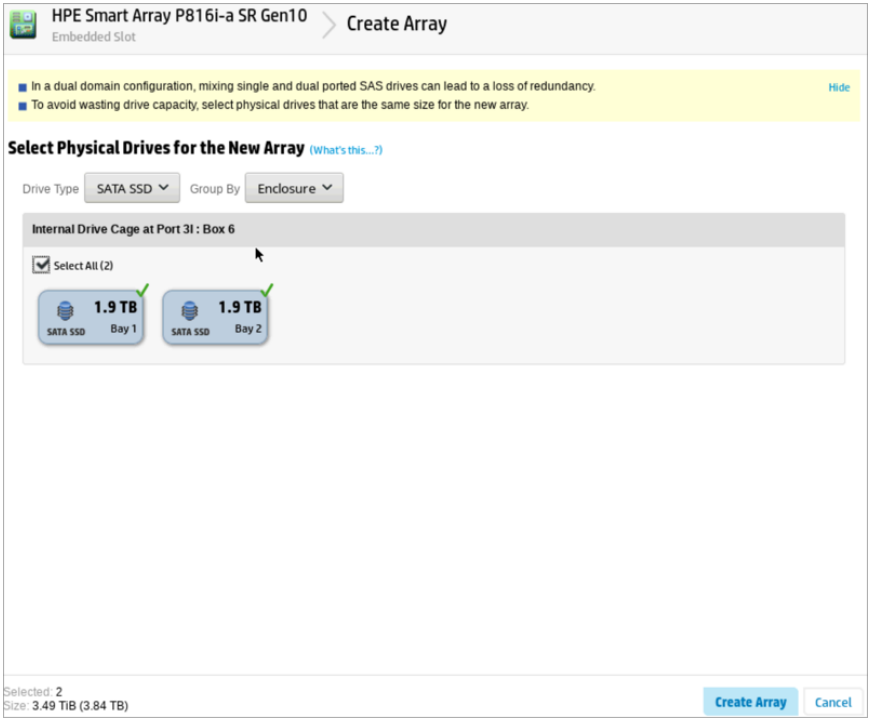
3 On the welcome page, from under the Available Devices displayed on the left, click **HPE Smart Array P816i-a SR Gen10**.



4 On the Actions dialog, click **Create Array**.



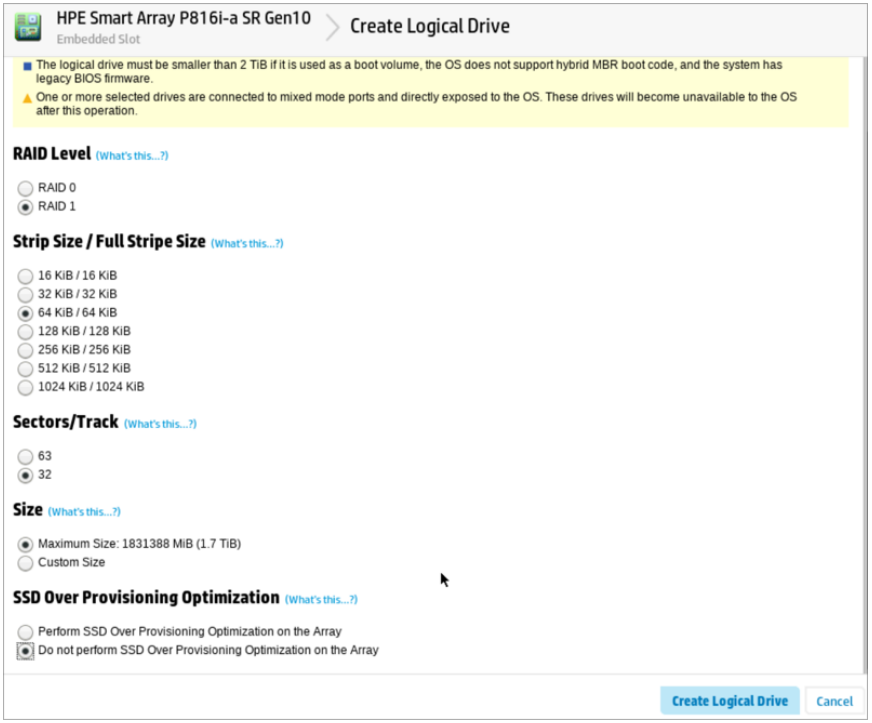
5 On the Create Array page, select the SSD storage devices to configure in the array.



Perform the following steps:

- From the Drive Type drop down menu, select **SATA SSD**.
- Then click **Select All** to select the two SSD storage devices that are displayed.
- Click **Create Array** and then click **Yes** to proceed to the RAID settings page.

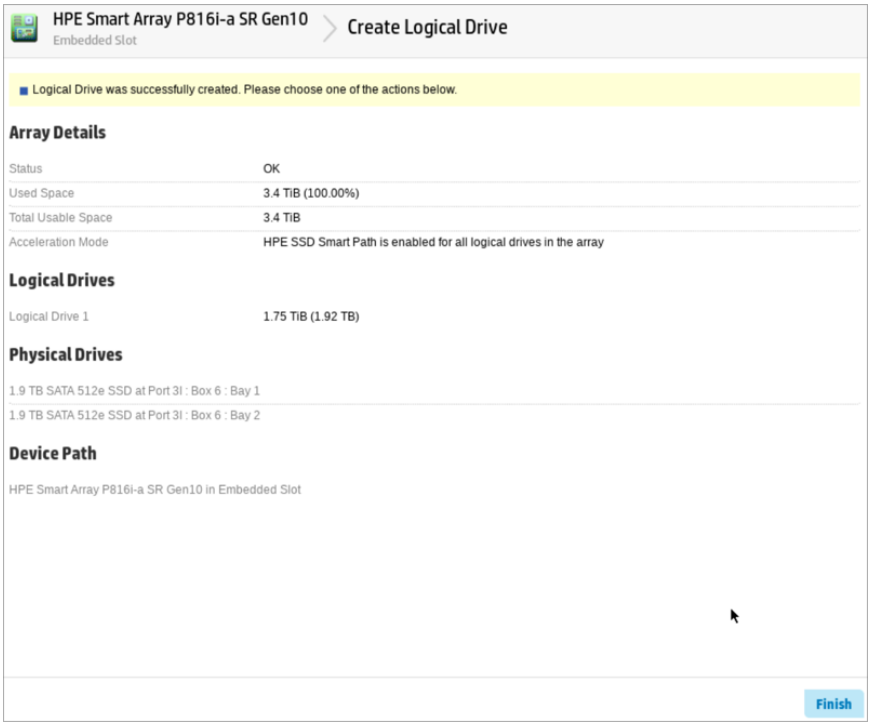
6 On the Create Logical Drive page, modify the RAID settings for the array.



Perform the following steps:

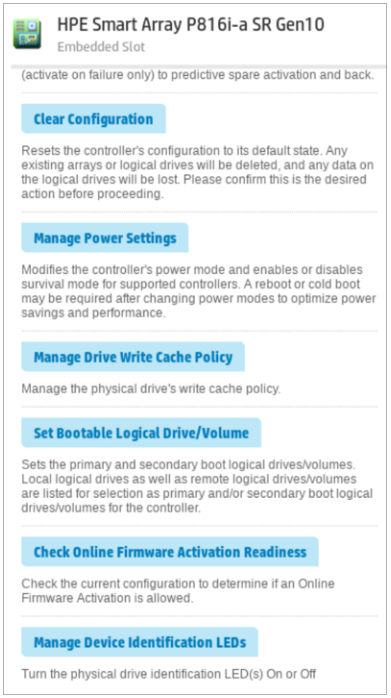
- Under Strip Size / Full Stripe Size, select **64 KiB / 64 KiB**.
- Under SSD Over Provisioning Optimization, select **Do not perform SSD over Provisioning Optimization on the Array**.
- Leave the other settings to their default values.
- Click **Create Logical Drive** to start the configuration.

7 On the confirmation page, make a note of the name listed under Logical Drives, and then click **Finish**.

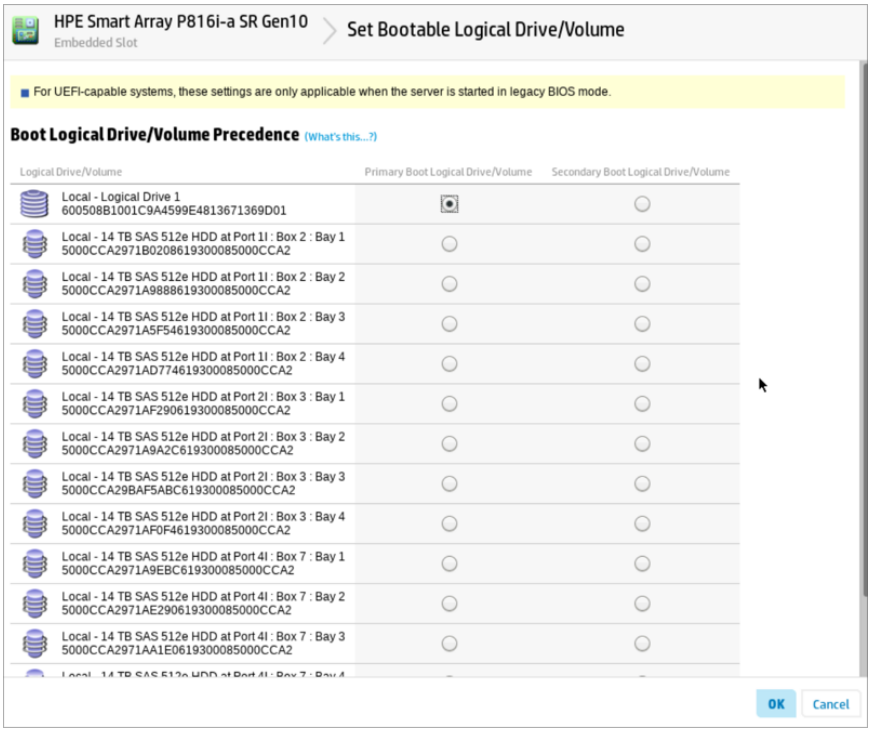


For example, here the name of the logical drive created appears as *Logical Drive 1*. You will use the name to identify the drive in the subsequent steps.

8 On the Actions dialog, click **Set Bootable Logical Drive/Volume**.



9 Under Boot Logical Drive/Volume Precedence, identify the logical drive based on the name that you noted in the earlier step and then select it as the Primary Boot Logical Drive/Volume.



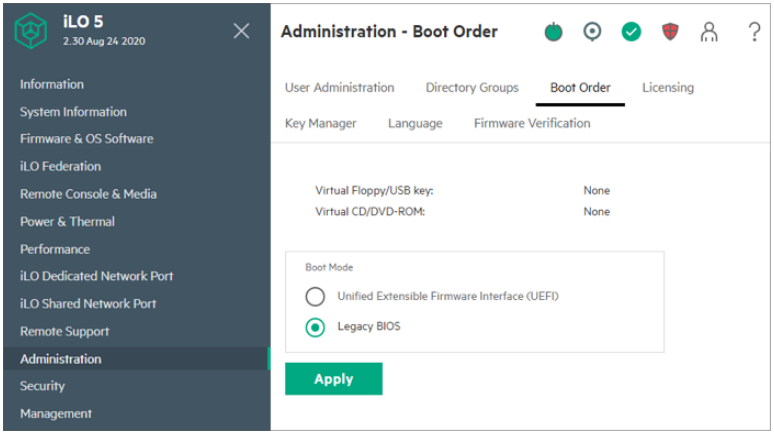
10 Click **OK** and then click **Finish** to complete the process and exit.

Configuring the BIOS settings on the nodes

Change the default boot order by modifying the BIOS settings of the node. The following procedure provides a high level overview of the process. For detailed information, refer to the HPE ProLiant DL380 Gen10 Server documentation.

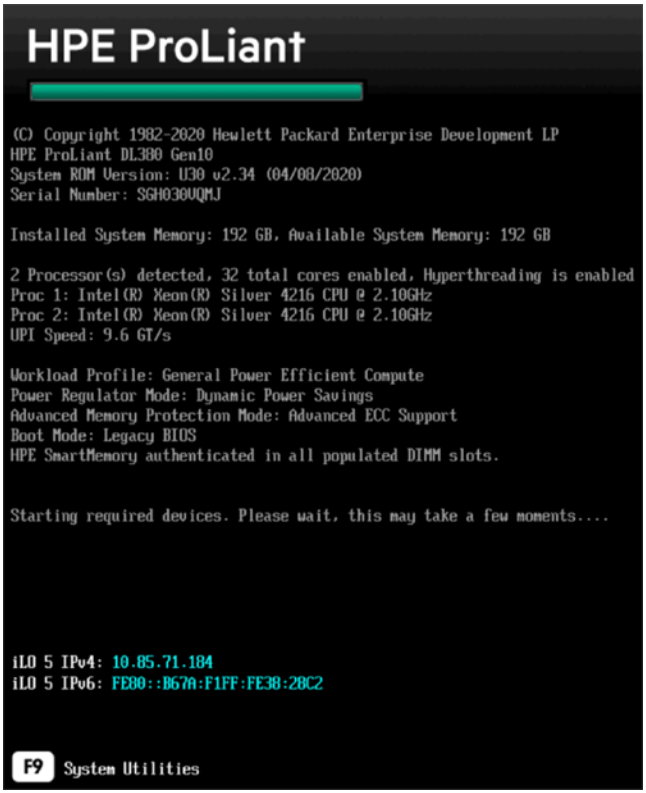
To modify the BIOS settings on the node

1. Launch the HPE iLO Remote Console interface and from the menu on the left, click **Administration**.
2. Click the **Boot Order** tab on the right, and from the Boot Mode options, select **Legacy BIOS**, and then click **Apply**.

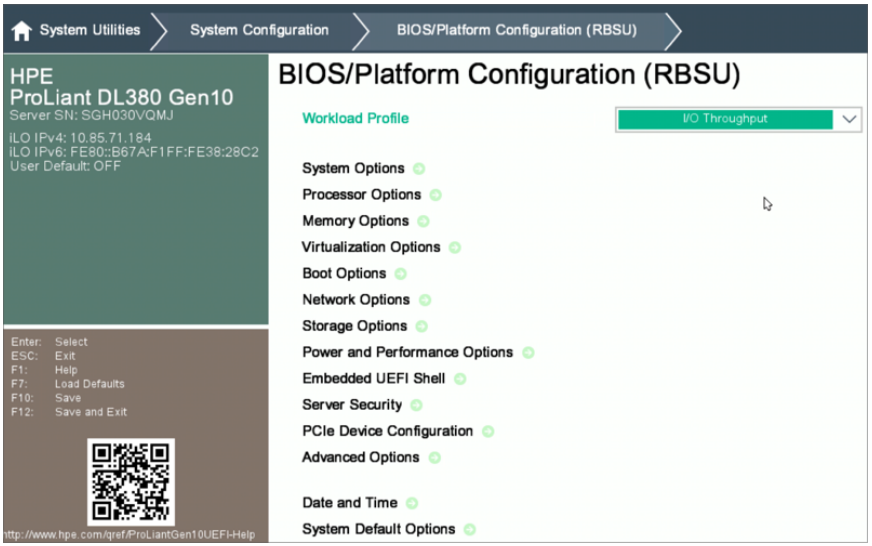


3. Reboot the node for the changes to take effect.

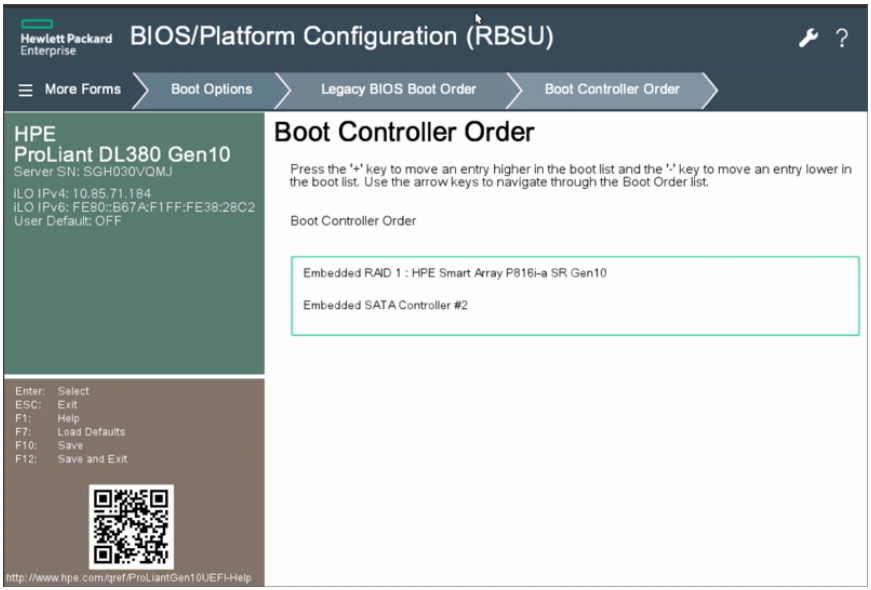
4 After the node restarts successfully, reboot it again and press the **F9** key on the boot screen to open the System Utilities.



5 Navigate through **System Configuration > BIOS/Platform Configuration (RBSU)** and change the Workload Profile field value to **I/O Throughput**.

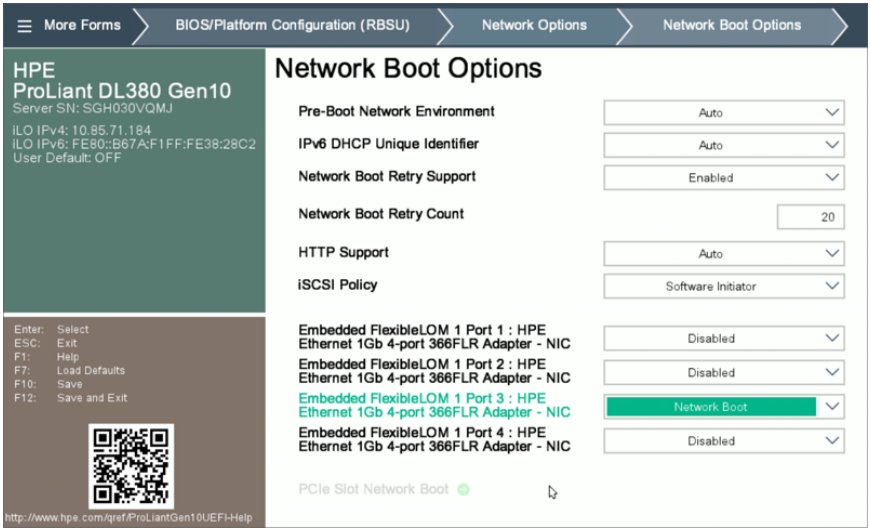


6 Navigate through **BIOS/Platform Configuration (RBSU) > Boot Options > Legacy BIOS Boot Order > Boot Controller Order** and move **Embedded RAID 1 : HPE Smart Array P816i-a SR Gen10** to the top of the list.



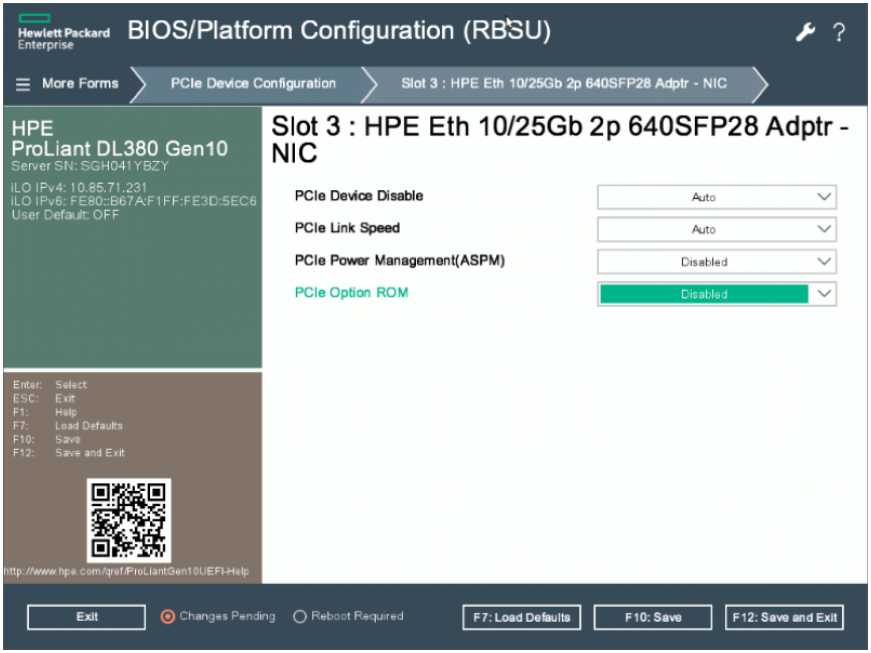
7 Navigate through **BIOS/Platform Configuration (RBSU) > Network Options > Network Boot Options** and do the following:

- Change Embedded FlexibleLOM 1 Port 1 setting to **Disabled**.
- Change the Embedded FlexibleLOM 1 Port 3 setting to **Network Boot**.
- Leave the other settings to their default values.



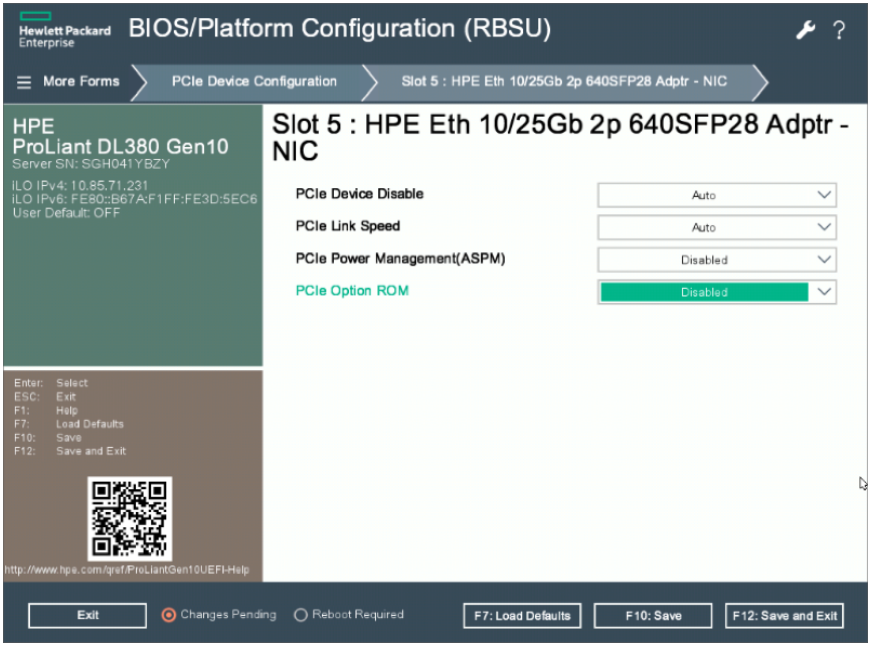
8 Navigate through **BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Slot 3 : HPE Eth 10/25Gb 2p 640SFP28 Adprt-NIC** and do the following:

- Change PCIe Option ROM setting to **Disabled**.
- Leave the other settings to their default values.



9 Navigate through **BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Slot 5 : HPE Eth 10/25Gb 2p 640SFP28 Adprt-NIC** and do the following:

- Change PCIe Option ROM setting to **Disabled**.
- Leave the other settings to their default values.



10 Press the **F12** key to save the changes and exit.

11 Power OFF the node.

12 Repeat these steps on each node in the appliance.

Downloading the product installer ISO

Veritas NetBackup Flex Scale software components are packaged in the form of an ISO image file. To be able to install NetBackup Flex Scale in your environment, you must first download the ISO image from the Veritas product website.

Table A-1 NetBackup Flex Scale installer ISO

ISO file name	Size
	9 GB (approximately)

Note: The actual ISO file name may vary depending on the product release version.

After downloading the ISO file locally, Veritas recommends that you use md5sum to verify that the MD5 hash value of the file matches with the one provided on the website. This validates the data integrity of the downloaded file.

To verify the MD5 hash of the installer file

1. Run the following command from the location where you have downloaded the installer file:

   `md5sum filename`

   Here, substitute `filename` with the actual ISO image file name.

   The output of the command displays a unique alphanumeric code and that is the MD5 hash value of the file.

   For example, your command output might resemble the following:

   `>> md5sum nbfs-1.3-20201104200100.iso`

   `>> c6779ec2960296ed9a04f08d67f64422 nbfs-1.3-20201104200100.iso`

   Here, the value "`c6779ec2960296ed9a04f08d67f64422`" represents the hash value.

2. Make a note of the hash value and match it with the value published on the website from where you downloaded the file.

   If the hash values match, it indicates that the file and its contents are authentic and have not been tampered with.

Once you have verified the data integrity of the file, you can use the ISO to install the software on the server nodes.

See “Mounting the ISO file on the nodes” on page 150.

Mounting the ISO file on the nodes

To install NetBackup Flex Scale, you are required to mount the product installer ISO image file on the node and then boot the server from that ISO image.

How you connect the ISO to the node depends on how you manage the server hardware. The most common method is to use hardware vendor’s remote management console and mount an ISO using a virtual CDROM device or a USB storage drive. You can copy the ISO on a laptop and then connect the laptop directly to the server node using the dedicated service port. You then launch the remote management console interface from a web browser and then mount the ISO to the node.

A separate mount point for the ISO is required for each node. For example, for a four-node cluster, create four different mount points and attach the ISO separately for each node.

Note: The process of attaching the ISO to the cluster nodes is impacted if there is poor network connectivity between the download ISO location and the cluster nodes.

Connecting the ISO to an HPE server node

For HPE ProLiant DL380 Gen10 servers, you can use the HPE iLO Remote Console administration interface and use the boot menu options to connect the ISO to the node.

Refer to your server hardware vendor's documentation for instructions on how to boot a server node from an ISO image file.

Installing NetBackup Flex Scale using the ISO

The following procedure describes how to install Veritas NetBackup Flex Scale on a single node.

To install Veritas NetBackup Flex Scale, you must first mount the product installation ISO image on the server node, boot the server from the ISO, choose the Veritas NetBackup Flex Scale install option, and then complete the installation. The overall installation process takes approximately 40 minutes for each node.

Note: After installing the NetBackup Flex Scale ISO, the GRUB menu is protected using the maintenance account password. To access the GRUB menu at system boot time, you must enter this password.

Before you proceed with the installation, ensure that:

- All the hardware is assembled and the server nodes are mounted on a designated rack
- All the power and networking connections are made as per the instructions
- The hardware vendor's default RAID management software on all the server nodes is disabled
- All the servers are enabled to boot from a configured device and you are able to modify the server boot options

To install Veritas NetBackup Flex Scale using the installer ISO

1. Connect the NetBackup Flex Scale installer ISO file to one of the server nodes.

   See "Downloading the product installer ISO" on page 149.

   See "Mounting the ISO file on the nodes" on page 150.

2. Power ON the server node and when you see the boot screen, press the **F11** key to load the boot menu.

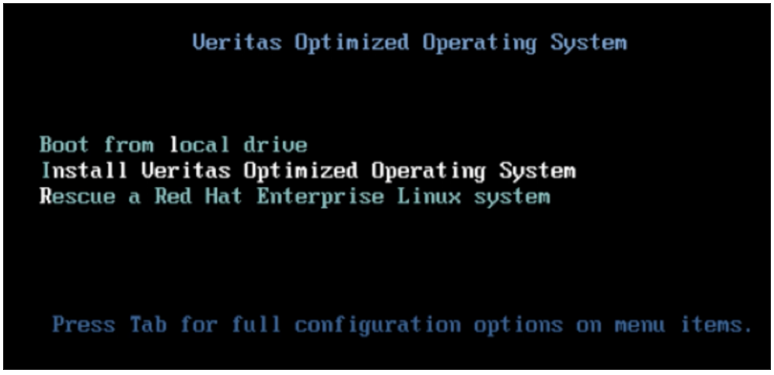
   The actual function key can vary depending on your server hardware vendor. For example, the boot menu function key could be F9 or F11 or even the ESC key.

3. From the boot menu, use the arrow buttons to select the device that contains the NetBackup Flex Scale installer ISO.

   For example, you can select a virtual CD ROM or a USB storage drive as the option.

4. Press the **Enter** key. The node restarts and automatically boots using the ISO file.

5. On the install options screen, use the arrow keys on your keyboard to select the **Install Veritas Optimized Operating System** option.



6. Press the **Enter** key to begin the software installation.

   The installer loads the installer image and begins to install all the required packages. You will see several messages on the screen as the installer runs through the installation process.

   The installer performs the following tasks as part of the installation:

   - runs the pre-install scripts and checks the system and storage
   - installs the customized operating system

- creates partitions and configures the file systems
- installs the software packages and creates default users
- runs the post-install scripts and starts all the services

The installer then displays a welcome message on the screen that confirms that the installation has completed successfully

7 This completes the installation on one node. Now, repeat these steps and install NetBackup Flex Scale on all the remaining nodes.

8 After installing NetBackup Flex Scale on all the server nodes, proceed to the cluster configuration workflow.

Appendix B

Upgrading a NetBackup Flex Scale node

This appendix includes the following topics:

Upgrading a node that is not in a cluster

You can directly upgrade a NetBackup Flex Scale node from a lower version to a higher version. Use the following procedure to upgrade an out of the box appliance node that is on a lower version and is not yet a part of the cluster to a higher version.

To upgrade a node

1. Download the upgrade RPM file to a Windows system that can access the Download Center and the NetBackup Flex Scale node.
   - Go to the Veritas Support website (https://www.veritas.com/support/en_US) and click Downloads, which redirects you to the Download Center.
   - In the Veritas Download Center, in the **Products** list, select **Appliances**, in the **Sub product** list select **NetBackup Flex Scale**. Select the required version and click **Explore**.
   - Expand **Updates**.
     Select the required file from this section and click **Download**. You must sign in with your Veritas account credentials to download the upgrade file.
2. Open an SSH session and log on to the appliance node as the admin user.
3. In the NetBackup Flex Scale Appliance shell menu, use the following command to open NFS shares:

   ```
   system software share open
   ```

4. On the local system where you downloaded the upgrade file, complete the following steps to copy the upgrade file to the `/system/inst/patch/incoming` folder of the appliance node:
   - Mount the NFS share:
     `Node_management_IP``:/system/inst/patch/incoming`
     where *Node_management_IP* is the IP address that is assigned to the eth1 network interface of the node.
   - Copy the upgrade file from your local system to the mapped directory.
   - Unmount or unmap the share.
5. On the appliance node, in the NetBackup Flex Scale Appliance shell menu, enter the following command to close the NFS shares:
   `system software share close`
6. To install the upgrade file, run the following command:
   `system software install-update update-name=`*`update-name`* where *update-name* is the name of the upgrade file that you want to install.
7. To check the upgrade status, run the following command:
   `system software upgrade-status`