

# Veritas NetBackup™ Flex Scale Installation and Configuration Guide

3.0

# Veritas NetBackup Flex Scale Installation and Configuration Guide

Last updated: 2023-07-21

## Legal Notice

Copyright © 2023 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

VERITAS TECHNOLOGIES LLC  
2625 Augustine Drive  
Santa Clara, CA 95054

<http://www.veritas.com>

## Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

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

Japan

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

## Documentation

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

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

## Documentation feedback

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

[NB.docs@veritas.com](mailto:NB.docs@veritas.com)

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

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

## Veritas Services and Operations Readiness Tools (SORT)

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

[https://sort.veritas.com/data/support/SORT\\_Data\\_Sheet.pdf](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# Contents

<b>Chapter 1</b>	<b>Preparing for NetBackup Flex Scale deployment</b>	
	.....	6
	Deployment overview .....	6
	Deployment options .....	7
	NetBackup Flex Scale configuration requirements .....	8
	Firewall and network ports requirements .....	15
	Considerations for using IPv6 addresses .....	17
<b>Chapter 2</b>	<b>Configuring NetBackup Flex Scale</b>	19
	Assigning a public IP address to network adapter eth1 of a node .....	19
	NetBackup Flex Scale configuration methods .....	21
	Configuring NetBackup Flex Scale using the setup wizard .....	21
	Configuring NetBackup Flex Scale using a configuration file .....	49
	YML configuration file for deploying NetBackup primary and media servers .....	55
	YML configuration file for deploying media servers .....	71
	Changing the maintenance user account password .....	90
<b>Chapter 3</b>	<b>Troubleshooting NetBackup Flex Scale deployment</b>	92
	NetBackup Flex Scale logs .....	92
	Connection timeout errors during patch installs, upgrades, and rollback operations .....	94
	Initial configuration wizard displays a driver node not selected error .....	94
	Initial configuration wizard displays a license error after successfully configuring the cluster .....	96
<b>Chapter 4</b>	<b>NetBackup Flex Scale upgrades and patch management</b>	97
	About NetBackup Flex Scale upgrades and EEB .....	97
	About rolling upgrade .....	99
	About the pre-upgrade check .....	100

	Installing EEBs using GUI .....	102
	Installing EEBs using REST APIs .....	103
<b>Chapter 5</b>	<b>Removing NetBackup Flex Scale .....</b>	<b>104</b>
	About disk erasure .....	104
	Configuring data erasure .....	105
	Viewing the data erasure status .....	106
	Aborting data erasure .....	107
	About NetBackup Flex Scale node factory reset .....	107
	Performing a factory reset on a node .....	108
<b>Appendix A</b>	<b>Installing NetBackup Flex Scale .....</b>	<b>110</b>
	About NetBackup Flex Scale software installation .....	110
	Enabling remote IPMI connections .....	111
	Setting up the RAID configuration on the nodes .....	113
	Configuring the BIOS settings on the nodes .....	120
	Downloading the product installer ISO .....	127
	Mounting the ISO file on the nodes .....	128
	Installing NetBackup Flex Scale using the ISO .....	129
	Installing hardware vendor packages .....	131
	Installing Emergency Engineering Binaries (EEBs) .....	132

# Preparing for NetBackup Flex Scale deployment

This chapter includes the following topics:

- [Deployment overview](#)
- [Deployment options](#)
- [NetBackup Flex Scale configuration requirements](#)
- [Firewall and network ports requirements](#)
- [Considerations for using IPv6 addresses](#)

## 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.

Use the [https://www.veritas.com/content/support/en\\_US/article.100053580](https://www.veritas.com/content/support/en_US/article.100053580) 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.

Use the [https://www.veritas.com/content/support/en\\_US/article.100053580](https://www.veritas.com/content/support/en_US/article.100053580) link to refer to the *NetBackup Flex Scale Hardware Cabling* poster.

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.

---

If you plan to leverage your own hardware instead of the out of the box appliance, ensure that you contact Veritas Support to generate and install device certificates on your nodes.

See “[About NetBackup Flex Scale software installation](#)” on page 110.

- **Stage 3 - 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.

See “[Configuring NetBackup Flex Scale using the setup wizard](#)” on page 21.

- **Stage 4 - Sign in and start protecting workloads**

Once the configuration is successful, you simply sign in to the NetBackup UI and create protection plans and start protecting desired workloads.

You can also sign in to the Veritas NetBackup Flex Scale 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. 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.

## NetBackup Flex Scale configuration requirements

A NetBackup Flex Scale appliance configuration consists of a minimum of 4 nodes and a maximum of up to 16 nodes that can host the following components:

- a single instance of a highly-available NetBackup primary server across the cluster
- a single instance of the NetBackup media server per node
- a single instance of the NetBackup storage server per node

For the best possible configuration experience, ensure that you have the following information available with you, depending on the number of nodes in your appliance.

### NetBackup

The following details are required for configuring NetBackup services and components if you deploy a cluster with both NetBackup primary server and media servers:

- 1 public IP address and 1 resolvable host name or Fully Qualified Domain Name (FQDN) for the NetBackup primary server
- 1 public IP address and 1 resolvable host name or FQDN for the NetBackup media server per node
- 1 IP address and 1 resolvable host name or FQDN for the NetBackup storage server per node

---

**Note:** If you don't plan to configure a DNS server for the cluster, the IP addresses and FQDNs are not required to be resolvable.

---

The following details are required if you deploy a cluster with only media servers:

- Resolvable host name or FQDN of the NetBackup primary server that is external to the cluster
- 1 public IP address and 1 resolvable host name or FQDN for the NetBackup media server per node



- 1 IP address and 1 resolvable host name or FQDN for the NetBackup storage server per node
- An API key, which is a pre-authenticated token used to identify a user
- A generic name that the NetBackup primary server uses to identifies all the media servers

---

**Note:** If you don't plan to configure a DNS server for the cluster, the IP addresses and FQDNs are not required to be resolvable.

---

## NetBackup Flex Scale cluster

The following details are required for configuring the NetBackup Flex Scale cluster services and components:

- 1 public IP address or the FQDN for the NetBackup Flex Scale cluster
- If you deploy a cluster with both NetBackup primary server and media servers, 1 public IP address and 1 resolvable host name or FQDN for the NetBackup Flex Scale management and API gateway server. This is also the IP or name that you will use to access the NetBackup Flex Scale UI, which is also called as the infrastructure management console UI.  
If you deploy a cluster with only media servers, the public IP address for the NetBackup Flex Scale cluster is used to access the NetBackup Flex Scale UI.
- IP address details for the dedicated management network and IPMI (optional)
- 1 private IP and a private subnet for the internal communication between the cluster nodes

---

**Note:** If you don't plan to configure a DNS server for the cluster, the IP addresses and FQDNs are not required to be resolvable.

---

The following example shows how to calculate the IP addresses that you need to specify for a cluster with N nodes:

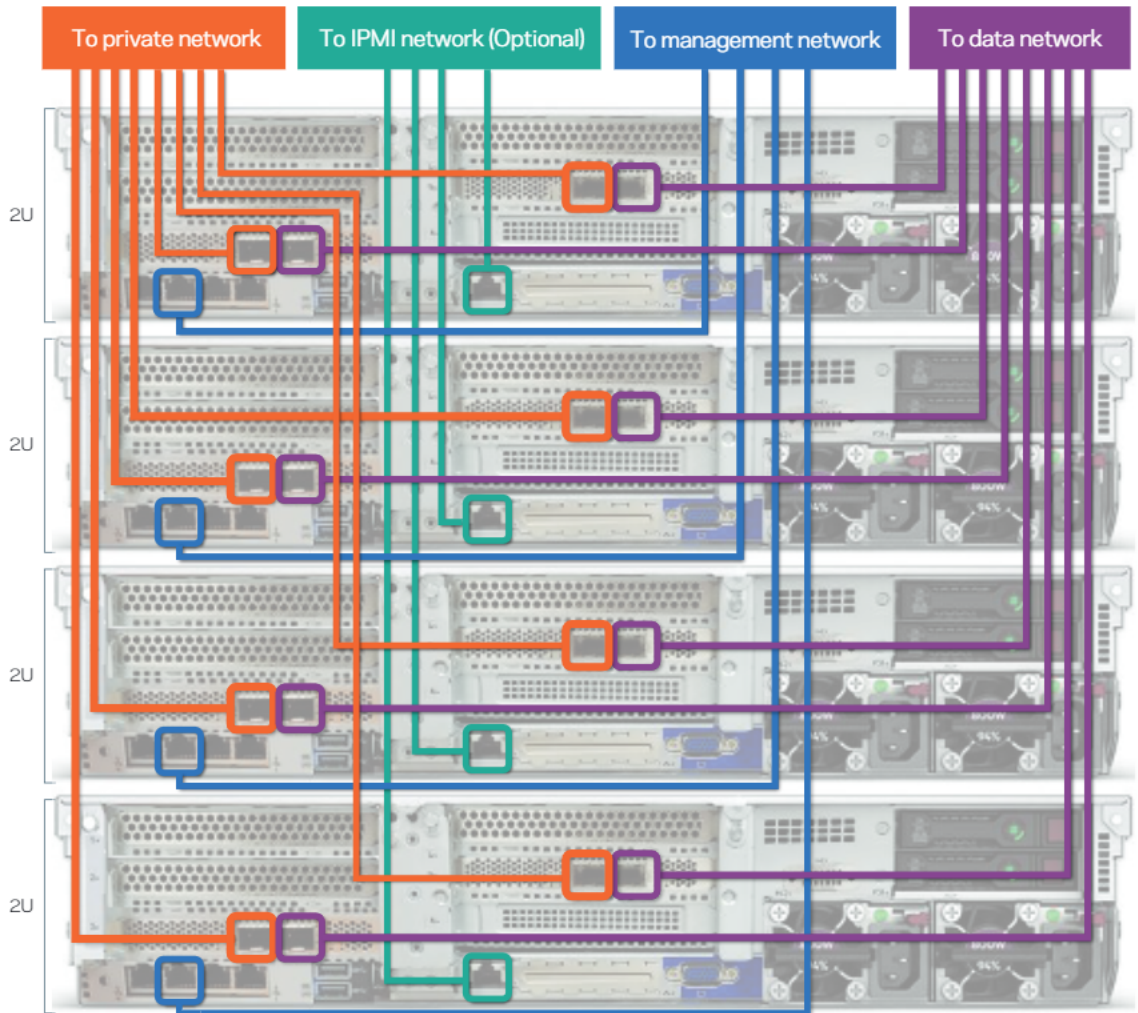
**Table 1-1**

Network	Per node	For cluster	Total
Private	Not required	1 IP address and subnet mask	You can use the default private IP range and subnet mask or specify a custom IP address range and subnet mask. If you use the default private IP address range and subnet mask, you don't need to specify any details.
Management	1 IP address for the management network	1 IP address for the NetBackup Flex Scale management gateway and API server  1 IP address for the NetBackup Flex Scale management console	N+2
Data	1 IP address for the media server  1 IP address for the storage server	1 IP address for the NetBackup primary server	2N+1
IPMI (optional)	1 IP address for the IPMI interface	Not required	N

## Networking

The following cabling diagram shows how to connect four NetBackup Flex Scale nodes. Ensure that you follow the same steps when connecting additional nodes. Make sure that the power cables are long enough to install and service the server nodes.

**Figure 1-1** Connecting NetBackup Flex Scale HPE nodes



Optical cables



Private network  
Data network

Ethernet cables



IPMI network  
Management network



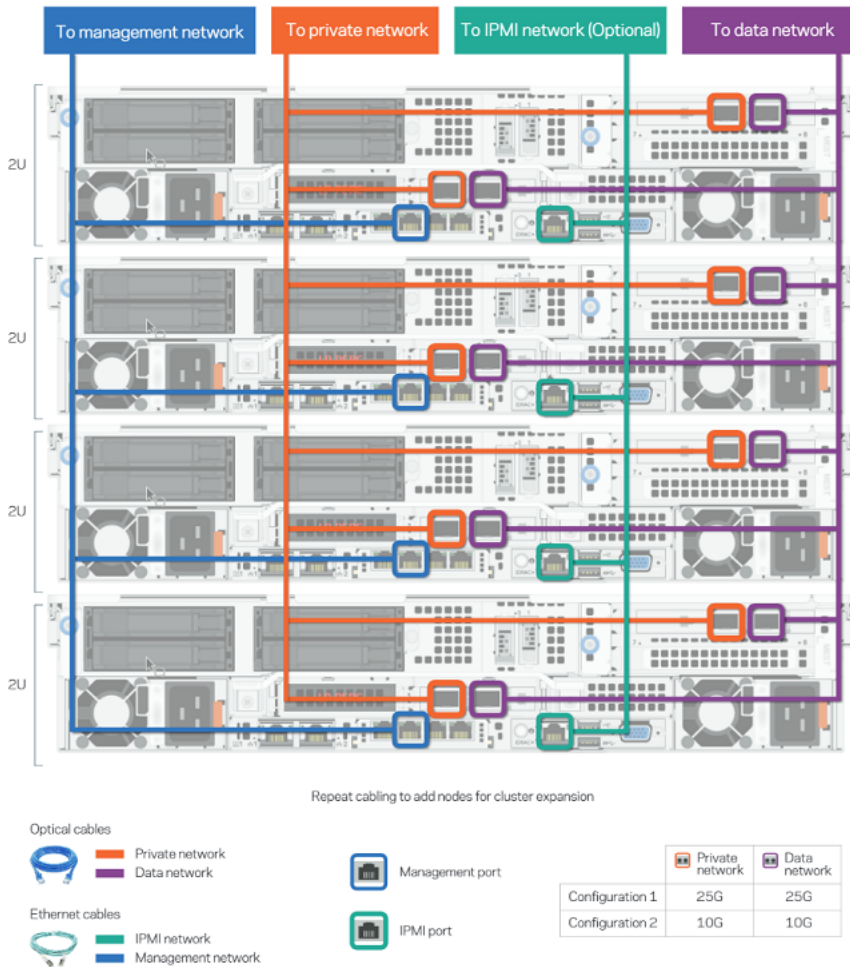
Management port



IPMI port

	Private network	Data network
Configuration 1	25G	25G
Configuration 2	25G	10G
Configuration 3	10G	10G

**Figure 1-2** Connecting NetBackup Flex Scale Dell nodes



Note the following requirements:

- Private network NICs of all appliance nodes must connect to a dedicated switch or VLAN and should be separate from other networks, such as data network and management network.  
 Ensure that the private network is different from the data and the management network and is not reachable from an external network.
- The network switch or switches need to be configured prior to configuring the appliance network interfaces.

- NetBackup Flex Scale uses IP address 172.16.X.X for private network NICs by default. If 172.16.x.x are reserved by the company, change private IP addresses to other local network addresses, such as 192.168.x.x or other subnets such as 172.20.x.x, when you run initial configuration from the GUI.
- It is recommended to use 25 Gb for both data (north-south) network and private (east-west ) network, however 10 Gb may be used with the following caveats:
  - If using 25 Gb network for data ( north-south) network, you must use 25 Gb for the private (east-west) network as well. Using 10Gb for the east-west network is not supported in this case.
  - If using 10 Gb network for data ( north-south) network, you can use 25 Gb or 10 Gb for the private (east-west) network.
- The following network configuration is supported:
  - Both the management and the data network in a single subnet without any VLAN.
  - Management network in a single subnet with or without any VLAN and data network in a separate subnet with a separate VLAN.
  - If you add an additional data network, it must be in a separate subnet with a separate VLAN from any existing network, including the private network.

The following details are required for configuring the network settings:

- IP address and subnet mask of the network gateway server from your existing network
- NTP server details  
 The IP address or the FQDN of the NTP server that you want to use to set and synchronize the system clocks on the cluster nodes.
- DNS details  
 Configuring a DNS server for the cluster is optional. If you configure a DNS server, you need to specify only the IP addresses during the cluster configuration. You do not have to specify the FQDNs during the cluster configuration. If you don't configure a DNS server for the cluster, ensure that you have the IP addresses and the corresponding FQDNs for all the nodes and NetBackup services.

The following options are supported for DNS configuration:

- Configure a DNS server only for the management network. Do not configure a DNS server for the data network. Here, you need to specify only the IP addresses for the management network during the cluster configuration, but you must specify both the IP addresses and the corresponding FQDNs for the data network.

- Configure the same DNS server for the management network and the data network. As DNS server is configured for the cluster, you need to specify only the IP addresses for the cluster configuration; you do not have to specify the FQDNs.
- Do not configure a DNS server for the management network and the data network. As no DNS server is configured for the cluster, the host names and domains are resolved to IP addresses using the `/etc/hosts` file. You need to specify the IP addresses and the corresponding FQDNs during the cluster configuration.
- This is applicable if you are configuring the cluster using a yml file.  
 If you have configured your network to use Virtual LANs then ensure that you provide the VLAN IDs in the yml file. Use the parameter `vlan_id` in the yml configuration template to specify the VLAN ID.  
 For example, if network adapter `eth1` is already tagged with a VLAN ID, you must specify that VLAN ID in the yml file. Here's a snippet from a sample yml configuration file that shows how to specify the VLAN ID:

```
common_network_setting:
management:
  ipv4:
    gateway_ip: 10.xx.xx.10
    subnet_mask: 255.255.248.0
  ipv6:
    prefix_length: ''
    router_ip: ''
  dns:
    dns_server: 172.16.8.12
    search_domain:
      - engba.veritas.com
  vlan_id: '1200'
```

---

**Note:** NetBackup Flex Scale does not block the cluster configuration if you do not specify the VLAN IDs. However, you may not be able to access the cluster nodes from the public network even after the cluster is configured successfully.

---

If you wish to configure the appliance for disaster recovery (DR), the following additional IP addresses are required:

- 1 public IP address for the heartbeat on each site
- 1 public IP address for Veritas Volume Replicator (VVR) replication on each site

---

**Note:** If you plan to configure a DNS server for the cluster, all the IP addresses must have a FQDN that is resolvable from the DNS server. If you don't plan to configure a DNS server for the cluster, the IP addresses and FQDNs are not required to be resolvable.

---

## Jumbo frames

Set the maximum transmission unit (MTU) property, which controls the maximum transmission unit size for an Ethernet frame to 9000 bytes. By default the MTU is set to 1500 bytes. For optimal performance, you must set a larger frame size to enable jumbo frames for the eth4, eth5, eth6, and eth7 network interfaces. To take advantage of jumbo frames, the Ethernet cards, drivers, and switching must all support jumbo frames.

## System clock

Synchronize the system clock on all the nodes before you begin the cluster configuration.

---

**Warning:** The cluster configuration may fail if the system clocks are not synchronized across the cluster.

---

## User accounts

You need at least one user name and password to configure a user account.

If you deploy a cluster with both NetBackup primary server and media servers, use a single user account and assign both Appliance and NetBackup administrator roles to the same account. You can also provide role-based access and create two separate user accounts with an Appliance administrator role and a NetBackup administrator role. You can configure multiple user accounts and assign them the desired roles. But a minimum of one user is required.

For a scale-out media only deployment, you can assign only the Appliance administrator role to the user account.

# Firewall and network ports requirements

If a firewall is configured, then ensure that the firewall settings allow access to the services and ports used by NetBackup Flex Scale. Enable both inbound and outbound communication for these ports and services.

The following table lists the ports and services that must be accessible:

**Table 1-2** NetBackup Flex Scale required ports and services

Port / Protocol / Type	Service	Description
443 / TCP <i>Outbound</i>	HTTPS	<ul style="list-style-type: none"> <li>Used for accessing the NetBackup Web UI.</li> <li>Used for sending Call Home notifications to Veritas support site. If you enable Call Home, you must also enable access to port 25.</li> </ul>
8443 / TCP <i>Inbound and Outbound</i>	HTTPS	Used while configuring the cluster by connecting to a node using its public IP address.
14161 / TCP <i>Inbound and Outbound</i>	HTTPS	
636 / TCP	LDAP and Active Directory	Used for configuring LDAP and AD with secure SSL
389	LDAP and Active directory	Used for configuring LDAP and AD without SSL certificate

The following table lists the optional ports and services for NetBackup Flex Scale:

**Table 1-3** NetBackup Flex Scale optional ports and services

Port / Protocol / Type	Service	Description
22 / TCP <i>Inbound</i>	SFTP	Used for sending product logs to the Veritas support site.
25 / TCP <i>Outbound</i>	SMTP	Used for sending alerts via email.
8199 / TCP <i>Inbound and Outbound</i>	Volume Replicator Administrative service	<p>Used by Veritas Volume Replicator (VVR) for communication between the <code>vradmind</code> daemons on the Primary and the Secondary.</p> <p>(Required only when catalog replication is configured)</p>



**Table 1-3** NetBackup Flex Scale optional ports and services (*continued*)

Port / Protocol / Type	Service	Description
8989 / TCP <i>Inbound and Outbound</i>	Volume Replicator Resync Utility	Used by VVR for communication between the in.vxrsyncd daemons that are used for differences-based synchronization.  (Required only when catalog replication is configured)
4145 / TCP / UDP <i>Inbound and Outbound</i>	Volume Replicator Connection Server	Used by VVR for heartbeat communication between the Primary and Secondary.  (Required only when catalog replication is configured)
14155 / TCP / UDP <i>Inbound and Outbound</i>	VCS Global Cluster Option (GCO)	Heartbeat to monitor remote cluster health.  (Required only when catalog replication is configured)
TCP / UDP Anonymous ports (32768-60999)	Client connections	Ports used for each Primary-Secondary connection for data replication between the Primary and the Secondary. One data port is required on each host.  These are short-lived ports assigned automatically by OS for client side socket connections in client-server communication.
53 / TCP / UDP <i>Inbound and Outbound</i>	DNS	Used for domain name resolution if DNS is not configured for the cluster.

You might need access to additional ports based on the NetBackup features that you plan to use. For more details about the ports that are used by NetBackup, see the *Veritas NetBackup™ Network Ports Reference Guide* on SORT.

## Considerations for using IPv6 addresses

Note the following if you plan to configure a NetBackup Flex Scale cluster using only IPv6 addresses:

NetBackup Flex Scale appliance does not support communication between a pure IPv6 and a pure IPv4 address configuration. A NetBackup Flex Scale cluster with

an all IPv6 address configuration cannot communicate with a system that is assigned an IPv4 address. The system must be configured either using a pure IPv6 address or using a pure IPv4 address network configuration.

A system in this context refers to a host that NetBackup uses to authenticate and then discover the workloads that need to be protected. For example, if you wish to protect VMware virtual machines, then the VMware vCenter Server or the VMware ESXi server that you add to NetBackup must be configured either to use a pure IPv6 address or use a mixed mode dual stack IP address configuration for communicating over an IP network.

# Configuring NetBackup Flex Scale

This chapter includes the following topics:

- [Assigning a public IP address to network adapter eth1 of a node](#)
- [NetBackup Flex Scale configuration methods](#)
- [Configuring NetBackup Flex Scale using the setup wizard](#)
- [Configuring NetBackup Flex Scale using a configuration file](#)
- [Changing the maintenance user account password](#)

## Assigning a public IP address to network adapter 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 you installed NetBackup Flex Scale earlier. 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.

---

**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 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.

See [“Configuring NetBackup Flex Scale using the setup wizard”](#) on page 21.

## NetBackup Flex Scale configuration methods

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

See [“Configuring NetBackup Flex Scale using the setup wizard”](#) on page 21.

See [“Configuring NetBackup Flex Scale using a configuration file”](#) on page 49.

## 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 [“NetBackup Flex Scale configuration requirements”](#) on page 8.
- Verify that you have assigned a public IP to a node. You will use that node to start the configuration process. See [“Assigning a public IP address to network adapter eth1 of a node”](#) on page 19.

## 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 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

---

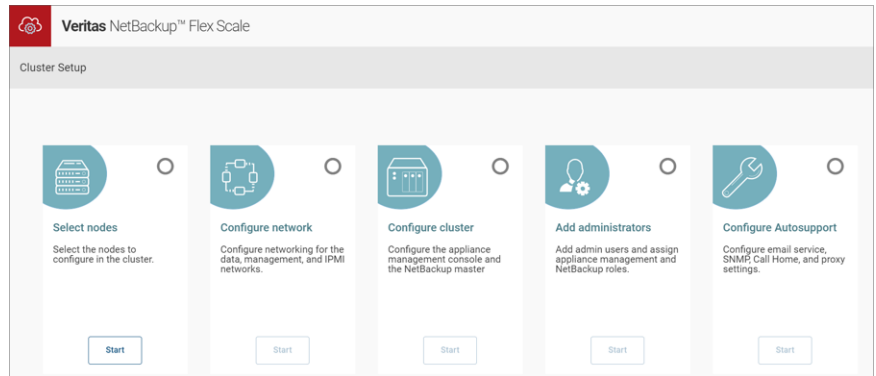
**Note:** The root user account is used only during the cluster configuration. This account is blocked after the cluster is configured successfully.

---

- Click **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**.

- On the Cluster Setup panel, you are presented with a set of configuration options. To configure the cluster, you must click through each of these options and provide the required configuration inputs.

To begin, in the Select nodes box, click **Start**.



- 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: <ul style="list-style-type: none"> <li>The cluster name can contain the following characters: a-z, 0-9, -</li> <li>The cluster name must start with a lowercase letter.</li> <li>The cluster name must not contain uppercase letters.</li> <li>The cluster name must include a minimum of 3 characters and can contain a maximum of 63 characters.</li> </ul>
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 node names are automatically generated based on the cluster and domain name that you specify. The cluster name serves as a prefix for the

node names. You can modify the node names if required. The following conditions are applicable:

- 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. Verify that they do not conflict with the FQDN of any of the management interfaces or any other publicly resolvable FQDNs.
- 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. <b>Note:</b> You cannot add unhealthy nodes to the cluster.
Size	Displays the maximum storage capacity available on the node.
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.



Label	Description
Management(eth1)	Displays the MAC address of network interface eth1 on the node. This interface is used for the cluster management network traffic.

### Import or Export configuration:

- Click **Generate configuration template** if you want to export the current cluster settings as a YML file.  
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.  
The YML file can serve as a reference for future use. Alternatively, you can export a blank configuration file, manually edit that file and 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.
- To import a pre-created configuration, click **Import configuration file** and select the YML file that contains the configuration settings.  
The YML file must contain name-value pairs corresponding to all the parameters that are displayed in the UI.

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

---

**Note:** You cannot select unhealthy nodes to be a part of the cluster. Ensure that you select at least 4 healthy nodes including the node (driver node) from where you launched the cluster configuration workflow. The UI displays an error if the driver node is not selected. Refer to the following for information on how to identify the driver node:

See [“Initial configuration wizard displays a driver node not selected error”](#) on page 94.

---

- 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 server for the cluster, ensure that the IP addresses and the FQDN that you specify are added to the DNS server that you specify here and are resolvable on the network.

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

Parameter	Description
IPv4   IPv6	Click <b>IPv4</b> or <b>IPv6</b> 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.
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 both the management and the data network, select **Enable DNS**. The same DNS server is configured for both the data and the management network. Do not select this option if you want to configure a DNS server only for the management network.

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.

- Media servers
 

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

Parameter	Description
Automatic   Custom	<p>Choose how you wish to assign IP addresses to the media server service on each node.</p> <ul style="list-style-type: none"> <li>Click <b>Automatic</b> 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 <b>Automatic</b> option is selected.</li> <li>Click <b>Custom</b> if you want to specify the IP addresses manually.</li> </ul>
IP address	<p>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.</p> <ul style="list-style-type: none"> <li>You can specify the IP address range separated by a dash. For example, 10.xx.xxx.192-10.xx.xxx.208.</li> <li>You can specify the IP address range in the CIDR format. For example, 10.xx.xxx.192/30.</li> </ul> <p>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</p>
FQDN	If using the Custom option, specify the FQDN for the media server service on each node. The FQDN can contain a maximum of 64 characters.

Parameter	Description
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.

---

- Storage servers  
Specify a public IP address and a FQDN for the storage server service for each node.

Parameter	Description
Automatic   Custom	<p>Choose how you wish to assign IP addresses to the storage server service on each node.</p> <ul style="list-style-type: none"><li>■ Click <b>Automatic</b> 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 <b>Automatic</b> option is selected.</li><li>■ Click <b>Custom</b> if you want to specify the IP addresses manually.</li></ul>
IP address	<p>If using the <b>Automatic</b> 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.</p> <ul style="list-style-type: none"><li>■ You can specify the IP address range separated by a dash. For example, 10. xx. xxx. 192-10. xx. xxx. 208.</li><li>■ You can specify the IP address range in the CIDR format. For example, 10. xx. xxx. 192/30.</li></ul> <p>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</p>
FQDN	If using the <b>Custom</b> option, specify the FQDN for the storage server service on each node. The FQDN can contain a maximum of 64 characters.
IPv4 address	If using the <b>Custom</b> option, specify the IP address for the storage 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.

---

■ Advanced network options

Parameter	Description
Interface Bonding	<p>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.</p> <p>Refer to the <i>NetBackup Flex Scale Administrator's Guide</i> for more details about NIC bonding support.</p>
VLAN ID	<p>If you wish to use a pre-configured virtual LAN, specify the VLAN ID. The ID can be any value between 1 and 4095.</p>

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

■ 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.

**Note:** If you had specified the DNS server settings on the **Data network** tab, the same DNS server settings are displayed for the management network because the same DNS server is configured for both the management and the data network. To edit the DNS settings, you must go back to the **Data network** tab.

- 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.

Parameter	Description
Automatic   Custom	<div>Choose how you wish to assign IP addresses to the management interfaces on each node.</div> <div><div>■ Click <b>Automatic</b> if you want NetBackup Flex Scale to automatically assign IP addresses from the IP range that you specify.</div><div>■ Click <b>Custom</b> if you want to specify the IP addresses manually.</div></div>

Parameter	Description
IP address	<p>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.</p> <ul style="list-style-type: none"> <li>You can specify the IP address range separated by a dash. For example, 10.xx.xxx.192-10.xx.xxx.208.</li> <li>You can specify the IP address range in the CIDR format. For example, 10.xx.xxx.192/30.</li> </ul> <p>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</p>
FQDN	If using the Custom option, specify the FQDN for the management interface on each node.
IPv4 address	If using the Custom option, specify the IP address for the management interface on each node.

- Domain Names System (DNS)

Displays the DNS settings that you specified for the data network earlier. To change these settings, you have to navigate back to the Data network section and edit the DNS details as required.
- Advanced network options

Parameter	Description
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.

- 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	<p>Choose how you wish to assign IP addresses to the IPMI interfaces on each node.</p> <ul style="list-style-type: none"><li>■ Click <b>Automatic</b> if you want NetBackup Flex Scale to automatically assign IP addresses from the IP range that you specify.</li><li>■ Click <b>Custom</b> if you want to specify the IP addresses manually.</li></ul>
IP address	<p>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.</p> <ul style="list-style-type: none"><li>■ You can specify the IP address range separated by a dash. For example, 10.xx.xxx.192-10.xx.xxx.208.</li><li>■ You can specify the IP address range in the CIDR format. For example, 10.xx.xxx.192/30.</li></ul>
IPv4 address   IPv6 address	<p>If using the Custom option, specify the IP address for the IPMI interface on each node.</p>

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

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

- 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.
- 7 Specify the network settings for the NetBackup Flex Scale infrastructure management console UI, the NetBackup primary server, and the cluster management and API gateway 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	<p>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.</p> <p>This is also referred to as the cluster IP address and is the IP that you will use to access the infrastructure management console user interface (UI).</p>

Parameter	Description
Management Server FQDN	<p>If you chose to deploy both the NetBackup primary server and media servers, specify a resolvable 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.</p> <p>The FQDN can contain a maximum of 64 characters.</p> <p><b>Note:</b> This is the internal management server of the NetBackup Flex Scale cluster. Do not specify the name of your public network gateway server here.</p>
Management Server IPv4   Management Server IPv6	<p>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.</p> <p><b>Note:</b> 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.</p> <p>If the cluster is deployed with only media servers, the NetBackup Flex Scale management server is not supported and the console IPv4 or IPv6 address is used to access the UI.</p>

- NetBackup Primary Settings**  
Specify the settings described in the table below if you opted for primary and media server deployment:

Parameter	Description
Host Name	<p>Specify a resolvable 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.</p> <p>The FQDN can contain a maximum of 64 characters.</p> <p>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 storage server services that you specified earlier.</p>
IPv4   IPv6	<p>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.</p>

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

Parameter	Description
Primary server host name	<p>Specify the FQDN 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.</p> <p>The FQDN can contain a maximum of 253 characters.</p> <p>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 storage server services that you specified earlier.</p>

Parameter	Description
API key	<p>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.</p> <p><b>Note:</b> 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.</p> <p>To create an API key:</p> <ol style="list-style-type: none"><li>1 Log in to the NetBackup Web UI using the administrator credentials.</li><li>2 In the left pane, click <b>Security</b>, and then click <b>API keys</b>.</li><li>3 In the upper-right corner, click <b>Add</b>.</li><li>4 Enter a username for which you want to create the API key.</li><li>5 Indicate how long you want the API key to be valid, from today's date. NetBackup calculates the expiration date and displays it.</li><li>6 Click <b>Add</b>.</li></ol> <p>The key is displayed in a popup window.</p> <ol style="list-style-type: none"><li>7 To copy the API key, click <b>Copy and close</b>.</li></ol> <p>Store this key in a safe place. After you click <b>Copy and close</b>, the key cannot be retrieved again.</p>
Media server gateway name	<p>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.</p>

■ Private IP Settings

Parameter	Description
Private IPv4	<p>If using IPv4 addresses, specify a private subnet IP to be used for internal communication between the cluster nodes.</p> <p>For example, you can specify the IP as 172.16.0.1.</p>
Subnet Mask	<p>Specify the subnet mask for the IP address that you specified earlier. You must use a subnet that is equal or larger than 255.252.0.0.</p> <p>For example, 252.252.0.0 or 255.248.0.0. is a valid subnet mask, whereas 255.255.0.0 or 255.255.248.0 are invalid values.</p>
Private IPv6	<p>If using IPv6 addresses, specify a private subnet IP to be used for internal communication between the cluster nodes.</p>
Prefix Length	<p>If using IPv6 addresses, specify the IPv6 prefix length. The prefix length must be greater than or equal to 112.</p>

---

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

---

- Click **Next**.

### Cluster setting

- **Storage server account**

Specify a user account that can be used to access the storage server 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 storage server 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.

**Note:** Refer to the following for the character usage and restrictions applicable to the user name and password for this account:

[https://www.veritas.com/content/support/en\\_US/article.100048511](https://www.veritas.com/content/support/en_US/article.100048511)

■ **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	<p>Specify an NTP server that you want to use to set and synchronize the system clocks on the cluster nodes.</p> <p>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.</p> <p>For example, <code>time.google.com</code>.</p>

■ **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.

---

- **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 be modified or deleted. The maximum retention time is 60 years.

- Click **Next**.

## **Licenses**

Add the desired storage and NetBackup licenses to the cluster.

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, you must add a valid license using the infrastructure management UI later.

Parameter	Description
Storage licenses	<p>Click <b>Add license</b> to add one or more storage licenses to the cluster configuration.</p> <p>A valid storage license is required to maintain a working cluster.</p>
NetBackup licenses	<p>Click <b>Add a license</b> to add a NetBackup license to the cluster configuration. A valid license is necessary to maintain a working cluster.</p> <p><b>Note:</b> You can use the NetBackup Java Console UI to manage the NetBackup licenses that are added to the cluster.</p>

### Summary

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

## 8 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.
Appliance Administrator	<p>Select this option to assign the NetBackup Flex Scale cluster administrator role to this user account.</p> <p>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.</p>
NetBackup Administrator	<p>Select this option to assign the NetBackup administrator role to this user account.</p> <p>This role has the permissions to manage the NetBackup services and operations in the cluster.</p> <p><b>Note:</b> This role is applicable only if the cluster is deployed with both NetBackup primary and media servers.</p>

- 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**.
- Click **Next**.

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.

9 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.
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:

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.

■ **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.

---

**Note:** Call Home configuration is not supported in an IPv6 cluster network configuration.

---

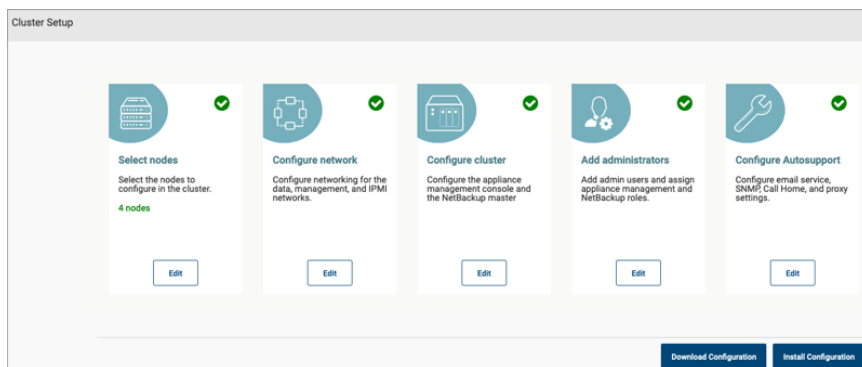
- Click **Enable proxy server** to enable proxy server communication option and then specify the following parameters:

Parameter	Description
Proxy server	Enter the IP address of the proxy server in your network.
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.
- 10** After specifying all the cluster configuration options, you are taken back to the Cluster Setup panel. A green tick mark in the configuration options box indicates that all the required parameters have been specified.

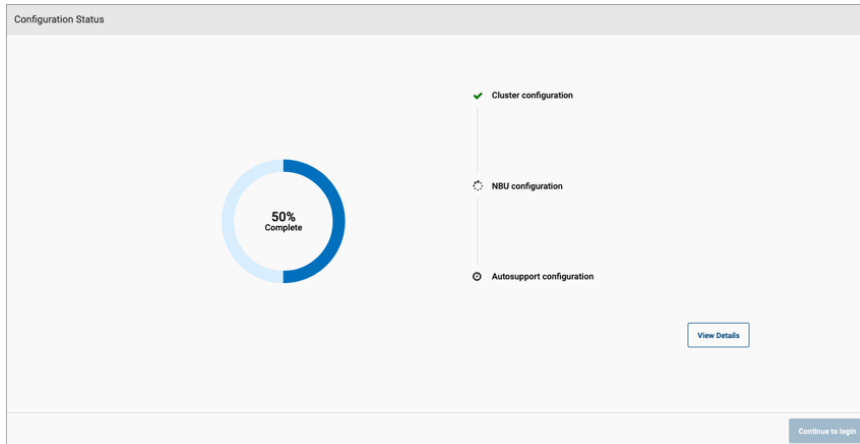


To proceed, do the following:

- 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 **Install Configuration** to start the NetBackup Flex Scale cluster configuration process.

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 storage server services if both the NetBackup primary and media servers are deployed.  
 Configures all the components and services including the media server and storage server services if only media servers are deployed.
- 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.

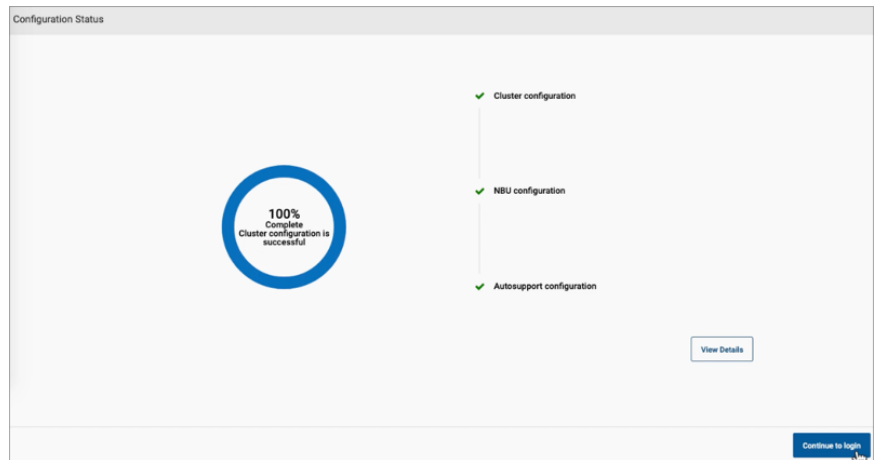
---

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

---

- 11 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:



- 12** 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 8 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 gateway and API server that you specified during the cluster configuration (refer to step 7 earlier).

`https://ManagementServerIPorFQDN/webui`

To view the cluster infrastructure, click **Cluster Monitor > Infrastructure**. Click **Cluster dashboard** in the upper-right corner of the UI to view the NetBackup Flex Scale infrastructure management console in a new browser tab.

**Veritas NetBackup™ Flex Scale**

Cluster dashboard

nbu-hc		600.00 GB	Nodes				Disks			
Console IP	10.221.34.245	Total Storage	4	4	0	4	60	60	0	60
Console node	nbu-hc-01		Total	Healthy	Unhealthy	Online	Total	Healthy	Unhealthy	Online
Cluster ID	VCIDRAVMware-421c1e727439f9...									

Status	Name	Node serial number	Health	Product version	Management IP (et	CPU utilization	Memory utilization
Online	nbu-hc-04	VMware-421c54147215...	Healthy	3.0	10.221.34.185	25.88%	14.9%
Online	nbu-hc-02	VMware-421c1e727439f...	Healthy	3.0	10.221.34.182	15.4%	27.68%
Online	nbu-hc-03	VMware-421ce2d78508...	Healthy	3.0	10.221.34.183	39.35%	15%
Online	nbu-hc-01	VMware-421c7e1375f5f...	Healthy	3.0	10.221.34.184	57.83%	18.02%

Items per page: 5

Discovered nodes

No new nodes.  
No new nodes have been discovered.

Scan for nodes

At this stage, you can also sign in to the NetBackup Flex Scale infrastructure management console 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:

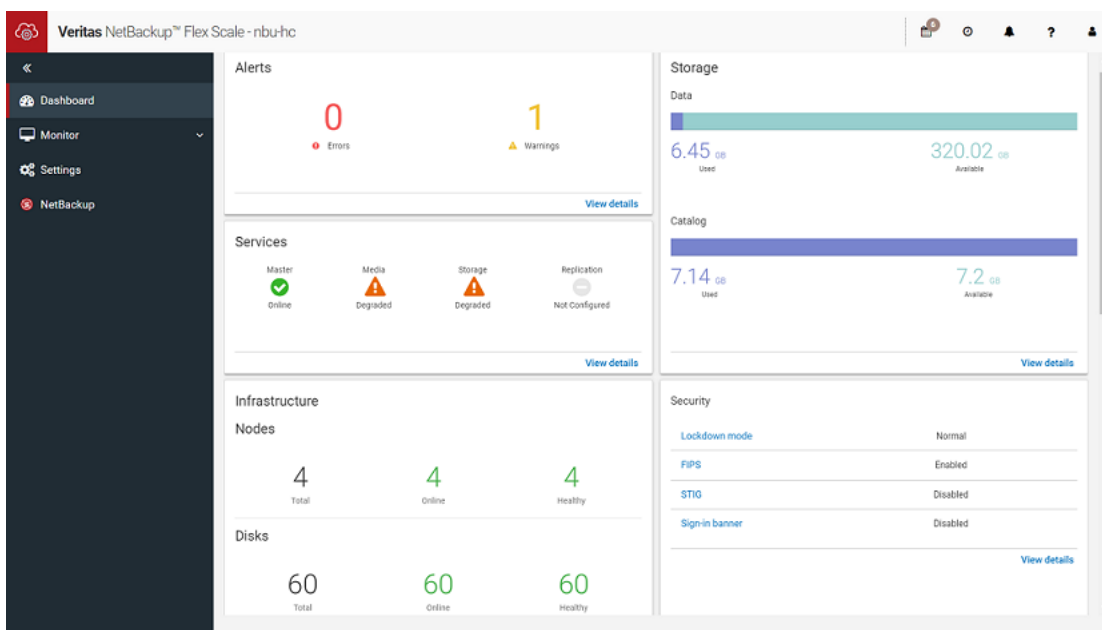
`https://ManagementServerIPorFQDN:14161`

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**.

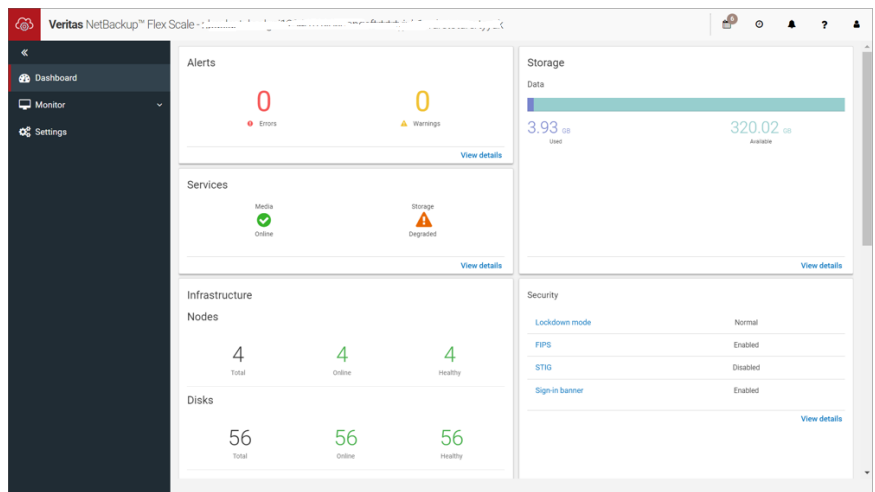




For more information on the NetBackup Flex Scale UI and how to use it to manage your NetBackup Flex Scale cluster, refer to the *Veritas NetBackup Flex Scale Administrator's Guide*.

- 13 If only media servers are configured in the cluster, you can sign in to the NetBackup Flex Scale infrastructure management console 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 console using `https://consoleIP:14161` where *consoleIP* is the public IP address that you specified for the cluster management console 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 8 earlier) and then click **Sign in**.



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

## Configuring NetBackup Flex Scale using a configuration file

You can use a YML-based configuration file to configure the NetBackup Flex Scale cluster. The YML file contains the configuration settings in form of name-value pairs. The name-value pairs correspond to all the parameters that are displayed in the setup wizard.

For details about the YML configuration file:

See [“YML configuration file for deploying NetBackup primary and media servers”](#) on page 55.

See [“YML configuration file for deploying media servers”](#) on page 71.

Before you proceed, ensure that you do the following:

- Verify that you have all the prerequisites necessary for the cluster configuration. See [“NetBackup Flex Scale configuration requirements”](#) on page 8.
- Verify that you have assigned a public IP to a node. You will use that node to start the configuration process. See [“Assigning a public IP address to network adapter eth1 of a node”](#) on page 19.

**To configure the NetBackup Flex Scale cluster using the YML configuration file:**

- 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 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.

---

- Click **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**.  
 On the **Cluster Setup** panel, you are presented with a set of configuration options.
  - 4 In the **Select nodes** area, click **Start**.  
 On the **Select Nodes** panel, the available nodes are discovered automatically. To rediscover the nodes click **Rescan**.
  - 5 On the **Select Nodes** panel, click **Generate configuration template** to download the `config.yml` file, which provides a template for specifying the configuration information.
  - 6 Open the `config.yml` file in a text editor of your choice, update the configuration information, and then click **Import YML**.  
 The YML configuration file is validated for syntax and incorrect attribute values. For example, errors are displayed for a duplicate IP address or if a cluster name includes illegal characters. At this point, no validations are made to check the network connectivity. For example, no validations are performed to check if the specified IP addresses are reachable or are free. Click **Save**.  
 The Cluster Setup panel is displayed and a green check mark is displayed in the **Select nodes** area. The green check mark indicates that all the required parameters are specified for the **Select nodes** configuration option.  
 The configuration settings that you specified in the configuration file as name-value pairs are displayed in the corresponding parameters in the setup wizard.
  - 7 Click **Start** for each of the configuration options displayed on the **Cluster Setup** panel. The configuration settings that you specified in the configuration file as name-value pairs are displayed in the corresponding parameters in the setup wizard. Review the displayed details, and then click **Save**. To change any of the displayed details, click **Edit**, update the settings, and then click **Save**.
  - 8 If you edited any of the configuration settings in the UI, click **Download Configuration** to download the configuration file. The downloaded configuration file contains the updated settings. This file serves as a reference and can be used to import the settings if you want to reconfigure the cluster.

- 9 Click **Install Configuration** to start the NetBackup Flex Scale cluster configuration process. The **Configuration Status** page displays the progress of the cluster configuration.

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 storage server services if both the NetBackup primary and media servers are deployed.  
Configures all the components and services including the media server and storage server services if only media servers are deployed.
- 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.

- 10 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.

- 11** 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 8 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 gateway and API server that you specified during the cluster configuration (refer to step 7 earlier).

`https://ManagementServerIPorFQDN/webui`

To view the cluster infrastructure, click **Cluster Monitor > Infrastructure**. Click **Cluster dashboard** in the upper-right corner of the UI to view the NetBackup Flex Scale infrastructure management console in a new browser tab.

**Veritas NetBackup™ Flex Scale**

Cluster dashboard

nbu-hc		600.00 GB	Nodes				Disks			
Console IP	10.221.34.245	Total Storage	4	4	0	4	60	60	0	60
Console node	nbu-hc-01		Total	Healthy	Unhealthy	Online	Total	Healthy	Unhealthy	Online
Cluster ID	VCIDRAVMware-421c1e727439f9...									

Nodes								
Status	Name	Node serial number	Health	Product version	Management IP (et	CPU utilization	Memory utilization	
Online	nbu-hc-04	VMware-421c54147215...	Healthy	3.0	10.221.34.185	25.88%	14.9%	
Online	nbu-hc-02	VMware-421c1e727439f...	Healthy	3.0	10.221.34.182	15.4%	27.68%	
Online	nbu-hc-03	VMware-421ce2d78508...	Healthy	3.0	10.221.34.183	39.35%	15%	
Online	nbu-hc-01	VMware-421c7e1375f5f...	Healthy	3.0	10.221.34.184	57.83%	18.02%	

Items per page: 5

Discovered nodes

No new nodes.  
No new nodes have been discovered.

Scan for nodes

At this stage, you can also sign in to the NetBackup Flex Scale infrastructure management console 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:

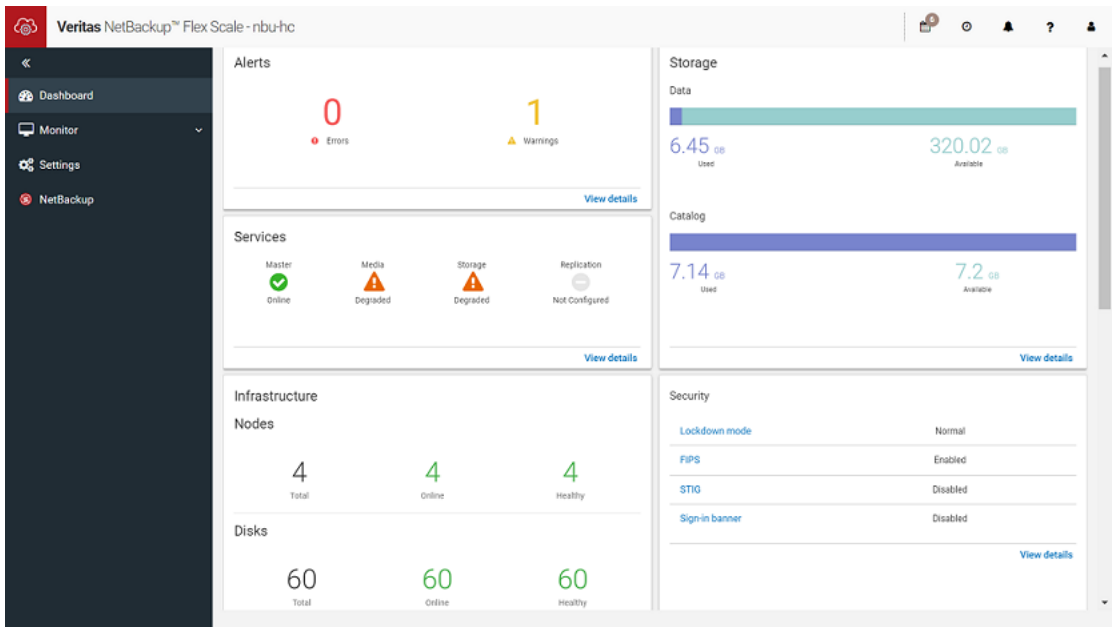
`https://ManagementServerIPorFQDN:14161`

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.

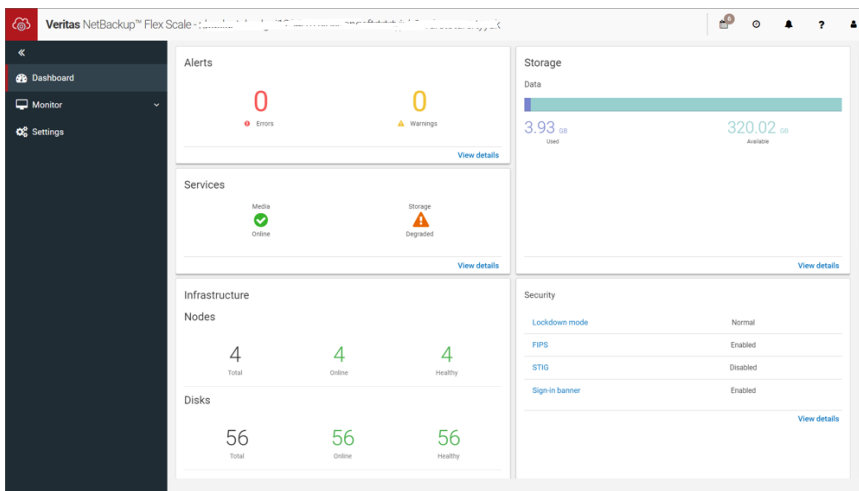
On the sign in page, specify the NetBackup Flex Scale administrator user account with the Appliance administrator role that you created during the cluster configuration, enter the password for the user account, and then click **Sign in**.



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

- 12 If only media servers are configured in the cluster, you can sign in to the NetBackup Flex Scale infrastructure management console 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 console, using `https://consoleIP:14161` where *consoleIP* is the public IP address that you specified for the cluster management console during the cluster configuration.

On the sign in page, specify the NetBackup Flex Scale administrator user account with the Appliance administrator role and password that you created during the cluster configuration (refer to step 7 earlier) and then click **Sign in**.



For more information on the NetBackup Flex Scale 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 for deploying NetBackup primary and media servers

The YML-based configuration file contains the NetBackup Flex Scale cluster configuration settings as name-value pairs. Use the YML configuration file to import a pre-created configuration. 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.

The configuration file contains the following sections:

- **cluster\_setting**
- **common\_network\_setting**
- **nodes\_setting**

The following table describes the parameters in the YAML 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 <code>/etc/hosts</code> 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
<b>call_home</b>	
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 <b>true</b> to enable Call Home. Set to <b>false</b> to disable Call home.
enable_proxy_server	Specify if the appliance connects to the AutoSupport server through a proxy server.  Set to <b>true</b> to enable proxy server. Set to <b>false</b> if a proxy server is not used.



**Table 2-2** (continued)

Parameter	Description
enable_proxy_tunnel	Specify if the proxy server supports SSL tunneling.  Set to <b>true</b> to enable secure communication. Set to <b>false</b> 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.
<b>smtp</b>	
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.
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.

**Table 2-2** (continued)

Parameter	Description
software	Email address of the admin users who will be the recipients of software-related email alerts.
<b>snmp</b>	
server	FQDN or the IP address (IPv4orIPv6) 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 <b>true</b> to enable the SNMP service. Set to <b>false</b> if you do not want to configure the SNMP service.

**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.
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.

**Table 2-3** (continued)

Parameter	Description
license_key	NetBackup license.  You can specify only a single license key during the initial configuration.
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. <ul style="list-style-type: none"> <li>■ The cluster name can contain a-z, 0-9, - characters.</li> <li>■ The cluster name must start with a lowercase letter.</li> <li>■ The cluster name must not contain uppercase letters.</li> <li>■ The cluster name must include a minimum of 3 characters and can contain a maximum of 63 characters.</li> </ul>

Under the **netbackup\_master** section, specify the following details:

**Table 2-4**

Parameter	Description
ipv4_address	Public IPv4 address for the NetBackup primary server service.  <b>Note:</b> You can specify either an IPv4 or an IPv6 address based on the data network settings.

**Table 2-4** (continued)

Parameter	Description
ipv6_address	Public IPv6 address for the NetBackup primary server service.  <b>Note:</b> 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	<p>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.</p> <p>NetBackup Flex Scale supports the following lockdown modes:</p> <ul style="list-style-type: none"> <li>■ Normal: Default mode that does not support WORM storage and data retention.</li> <li>■ 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.</li> <li>■ 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.</li> </ul>
<b>retention</b>	
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 60 years.

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
<b>ipv4</b>	
ip	Specify a private subnet IP to be used for internal communication between the cluster nodes.
subnet	Subnet mask for the specified IP address.
<b>ipv6</b>	
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 112.

Under **user\_management**, specify the following details:

**Table 2-8**

Parameter	Description
<b>storage_server</b>	
password	Password for the user account that can access the storage server containers.
user_name	Name for the user account that can be used to access the storage server containers. This account has the permissions to manage all the storage on the NetBackup Flex Scale cluster nodes.
<b>users</b>	
password	Password for the administrator account.

Table 2-8 (continued)

Parameter	Description
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.

common\_network\_settings

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

dns

Table 2-9

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

data

Table 2-10

Parameter	Description
bond	
enable	Specify if you want to use NIC bonding for eth5 and eth7 for high availability of the network interfaces.

**Table 2-10** (continued)

Parameter	Description
mode	Specify the bonding mode: <ul style="list-style-type: none"> <li>■ <b>balance-rr</b></li> <li>■ <b>active-backup</b></li> <li>■ <b>balance-xor</b></li> <li>■ <b>broadcast</b></li> <li>■ <b>802.3ad</b></li> <li>■ <b>balance-tlb</b></li> <li>■ <b>balance-alb</b></li> </ul>
option	Sub-type <b>layer2</b> , <b>layer(3+4)</b> , and <b>default</b> for bonding mode <b>802.3ad</b> and <b>balance-xorbond</b> types.
<b>ipv4</b>	
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.
<b>ipv6</b>	
prefix_length	If using IPv6 public addresses, specify the IPv6 prefix length.
router_ip	If using IPv6 public addresses, specify the router address.

**Table 2-11**

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

## dns

Configuring a DNS server for the cluster is optional. If you set up a cluster without configuring a DNS server, you must provide both the IP addresses and FQDNs for all the cluster nodes and NetBackup services. If you configure a DNS server for the cluster, you need to specify only the IP addresses during the configuration.

You can configure a DNS server for the following networks:



- Only for the management network.
- Both the management and the data network.  
 Ensure that the same DNS server details are provided if you want to configure a DNS server for the data and management network. Configuring a separate DNS server for the management and data network is not supported.

**Table 2-12**

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.
search_domain	Search domains for resolving host names and IP addresses.

## ipmi

**Table 2-13**

Parameter	Description
<b>ipv4</b>	
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.
<b>ipv6</b>	
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 2-14**

Parameter	Description
<b>ipv4</b>	

**Table 2-14** (continued)

Parameter	Description
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 management network.
<b>ipv6</b>	
prefix_length	If using IPv6 public addresses, specify the IPv6 prefix length.
router_ip	If using IPv6 public addresses, specify the router address.

## dns

Configuring a DNS server for the cluster is optional. If you set up a cluster without configuring a DNS server, you must provide both the IP addresses and FQDNs for all the cluster nodes and NetBackup services. If you configure a DNS server for the cluster, you need to specify only the IP addresses during the configuration.

You can configure a DNS server for the following networks:

- Only for the management network.
- Both the management and the data network.  
 Ensure that the same DNS server details are provided if you want to configure a DNS server for the data and management network. Configuring a separate DNS server for the management and data network is not supported.

**Table 2-15**

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.
search_domain	Search domains for resolving host names and IP addresses.

## nodes\_setting

Node name and details of media server, storage server, and management server for each node

**Table 2-16**

Parameter	Description
hostnames	Name of the nodes, can contain a maximum of 63 characters.
media_server_ip	<p>Public IP address range for the media server service on each node.</p> <ul style="list-style-type: none"> <li>■ You can specify the IP address range separated by a hyphen. For example, 10.xx.xxx.192-10.xx.xxx.208</li> <li>■ You can specify the IP address range in the CIDR format. For example, 10.xx.xxx.192/30</li> <li>■ 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</li> </ul> <p>The FQDN is automatically resolved with DNS lookup.</p>
storage_server_ip	<p>Public IP address range for the storage server service on each node.</p> <ul style="list-style-type: none"> <li>■ You can specify the IP address range separated by a hyphen. For example, 10.xx.xxx.192-10.xx.xxx.208</li> <li>■ You can specify the IP address range in the CIDR format. For example, 10.xx.xxx.192/30</li> </ul> <p>The FQDN is automatically resolved with DNS lookup.</p>
management_interface_ip	<p>Public IP address to be assigned to the designated management network interface (eth1) on each node.</p> <p>You can specify:</p> <ul style="list-style-type: none"> <li>■ A single IP range</li> <li>■ Multiple IP ranges separated by a comma</li> <li>■ Comma-separated individual IP addresses</li> <li>■ A combination of individual IP addresses and IP ranges separated by a comma</li> <li>■ IP addresses in CIDR format</li> </ul>

**Table 2-16** (continued)

Parameter	Description
ipmi_interface	<p>Public IP address to be assigned to the designated IPMI interface on each node.</p> <ul style="list-style-type: none"> <li>■ You can specify the IP address range separated by a dash. For example, 10.xx.xxx.192-10.xx.xxx.208</li> <li>■ You can specify the IP address range in the CIDR format. For example, 10.xx.xxx.192/30</li> </ul> <p>The FQDN is automatically resolved with DNS lookup.</p>

The following example shows a sample YML configuration file where DNS is configured for the management and data network and IP ranges are specified for the node details. The IP addresses are resolved to FQDNs during the initial configuration.

```
# deployment_yaml_version: V3.0

cluster_setting:
  additional_fqdn_entries:
    - ip_address: '10.80.40.1'
      name: ["test.com"]
  autosupport_setting:
    call_home:
      enable_call_home: false
      enable_proxy_server: false
    proxy:
      enable_proxy_tunel: false
      password: ''
      port: ''
      server: ''
      username: ''
  smtp:
    account: sendersort_eagappnso41@mtv.nbuappsmtmp.example.com
    emailServer: nbpipeline-comn.engba.veritas.com
    encryption_enabled: true
    hardware: hadmin_eagappnso41@mtv.nbuappsmtmp.example.com
    notificationInterval: '15'
    password: UEBzc3cwcmQ=
```

```

    senderEmail: sendersort_eagappnso41@mtv.nbuappsmtp.example.com
    serverPort: '25'
    software: hadmin_eagappnso41@mtv.nbuappsmtp.example.com
snmp:
    community: ''
    enable_snmp: false
    port: ''
    server: ''
console_ip_ipv4: 10.85.44.145
console_ip_ipv6:
dr_passphrase: P@ssw0rd
license_key: KLNLP-UA6L-I4VR-OSS4-C6CP-CIR4-KSOS-KY7F-FYU6-PPNC
storage_licenses: []
management_server_fqdn: eagappnso85-pub2.example.com
management_server_ip_ipv4: 10.85.44.146
management_server_ip_ipv6:
name: betatan
netbackup_master:
    ipv4_address: 10.85.44.139
    ipv6_address:
    name: eagappnso66-vip.example.com
ntp_setting:
    server: [10.0.0.12]
    timezone: Pacific
private_network:
    ipv4:
        ip: 172.16.0.1
        subnet: 255.252.0.0
    ipv6:
        ip: 'fd00::2'
        prefix_length: '112'
user_management:
    storage_server:
        - password: P@ssw0rd
          user_name: msdp-usr
    users:
        - password: We!!c0me
          roles:
            - appliance_admin
            - backup_admin
          user_name: admin_user
        - password: P@ssw0rd
          roles:

```

```

- appliance_admin
  user_name: app_admin_user
- password: 123@Admin
  roles:
- backup_admin
  user_name: nbu_admin_usr
common_network_setting:
  dns:
    dns_domain: example.com
  data:
    bond:
      enable: true
      mode: balance-alb
      option: ''
    ipv4:
      gateway_ip: 10.85.40.1
      subnet_mask: 255.255.248.0
    ipv6:
      prefix_length: ''
      router_ip: ''
    vlan_id: ''
  dns:
    dns_server: 10.0.0.12
    search_domain:
      - example.com
  ipmi:
    ipv4:
      gateway_ip: ''
      subnet_mask: ''
    ipv6:
      prefix_length: ''
      router_ip: ''
  management:
    ipv4:
      gateway_ip: 10.10.10.10
      subnet_mask: 255.255.248.0
    ipv6:
      prefix_length: ''
      router_ip: ''
    dns:
      dns_server: 10.0.0.12
      search_domain:
        - example.com

```

```

    vlan_id: ''
nodes_setting:
  hostnames: ["node01", "node02", "node03", "node04"]
  media_server_ip: [10.209.106.0/30]
  storage_server_ip: [10.109.106.0/30]
  management_interface_ip: [10.209.106.9,10.209.106.10,10.209.106.11,
                             10.209.106.12]
  ipmi_interface: [10.209.106.13,10.209.106.14/31,10.209.106.16]

```

## YML configuration file for deploying media servers

The YML-based configuration file contains the NetBackup Flex Scale cluster configuration settings as name-value pairs. Use the YML configuration file to import a pre-created configuration. 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.

The configuration file contains the following sections:

- **cluster\_setting**
- **common\_network\_setting**
- **nodes\_setting**
- **external\_primary\_server\_setting**

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 2-17**

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

Under the **autosupport\_setting** section specify the following details:

**Table 2-18**

Parameter	Description
<b>call_home</b>	
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 <b>true</b> to enable Call Home. Set to <b>false</b> to disable Call home.
enable_proxy_server	Specify if the appliance connects to the AutoSupport server through a proxy server.  Set to <b>true</b> to enable proxy server. Set to <b>false</b> if a proxy server is not used.
enable_proxy_tunnel	Specify if the proxy server supports SSL tunneling.  Set to <b>true</b> to enable secure communication. Set to <b>false</b> 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.
<b>smtp</b>	
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.



**Table 2-18** (continued)

Parameter	Description
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.
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.
<b>snmp</b>	
server	FQDN or the IP address (IPv4orIPv6) 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 <b>true</b> to enable the SNMP service. Set to <b>false</b> if you do not want to configure the SNMP service.

**Table 2-19**

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.

**Table 2-19**      *(continued)*

Parameter	Description
console_ip_ipv6	Public IPv6 address for the NetBackup Flex Scale infrastructure management U. The type of IP address, whether IPv4 or IPv6 depends on the IP addressing you specified for the management network's routing settings.
license_key	NetBackup license.  You can specify only a single license key during the initial configuration.
storage_licenses	Storage license.  You can specify multiple storage licenses during the initial configuration.
name	Cluster name.  <ul style="list-style-type: none"> <li>■ The cluster name can contain a-z, 0-9, - characters.</li> <li>■ The cluster name must start with a lowercase letter.</li> <li>■ The cluster name must not contain uppercase letters.</li> <li>■ The cluster name must include a minimum of 3 characters and can contain a maximum of 63 characters.</li> </ul>

Under the **ntp\_setting** section, specify the following details:

Table 2-20

Parameter	Description
server	<p>NTP server that you want to use to set and synchronize the system clocks on the cluster nodes.</p> <p>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.</p>
timezone	Time zone of the nodes.

Under the **lockdown\_mode** section, specify the following details:

Table 2-21

Parameter	Description
mode	<p>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.</p> <p>NetBackup Flex Scale supports the following lockdown modes:</p> <ul style="list-style-type: none"><li>■ Normal: Default mode that does not support WORM storage and data retention.</li><li>■ 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.</li><li>■ 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.</li></ul>
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 60 years.

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

**Table 2-22**

Parameter	Description
<b>ipv4</b>	
ip	Specify a private subnet IP to be used for internal communication between the cluster nodes.
subnet	Subnet mask for the specified IP address.
<b>ipv6</b>	
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 112.

Under **user\_management**, specify the following details:

**Table 2-23**

Parameter	Description
<b>storage_server</b>	
password	Password for the user account that can access the storage server containers.
user_name	Name for the user account that can be used to access the storage server containers. This account has the permissions to manage all the storage on the NetBackup Flex Scale cluster nodes.
<b>users</b>	
password	Password for the administrator account.

**Table 2-23** (continued)

Parameter	Description
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.
user_name	Name for the administrator account.

## common\_network\_settings

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

### dns

**Table 2-24**

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

### data

**Table 2-25**

Parameter	Description
<b>bond</b>	
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: <ul style="list-style-type: none"> <li>■ <b>balance-rr</b></li> <li>■ <b>active-backup</b></li> <li>■ <b>balance-xor</b></li> <li>■ <b>broadcast</b></li> <li>■ <b>802.3ad</b></li> <li>■ <b>balance-tlb</b></li> <li>■ <b>balance-alb</b></li> </ul>

**Table 2-25** (continued)

Parameter	Description
option	Sub-type <b>layer2</b> , <b>layer(3+4)</b> , and <b>default</b> for bonding mode <b>802.3ad</b> and <b>balance-xorbond</b> types.
<b>ipv4</b>	
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.
<b>ipv6</b>	
prefix_length	If using IPv6 public addresses, specify the IPv6 prefix length.
router_ip	If using IPv6 public addresses, specify the router address.

**Table 2-26**

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

## dns

Configuring a DNS server for the cluster is optional. If you set up a cluster without configuring a DNS server, you must provide both the IP addresses and FQDNs for all the cluster nodes and NetBackup services. If you configure a DNS server for the cluster, you need to specify only the IP addresses during the configuration.

You can configure a DNS server for the following networks:

- Only for the management network.
- Both the management and the data network.  
Ensure that the same DNS server details are provided if you want to configure a DNS server for the data and management network. Configuring a separate DNS server for the management and data network is not supported.

**Table 2-27**

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.
search_domain	Search domains for resolving host names and IP addresses.

## ipmi

**Table 2-28**

Parameter	Description
<b>ipv4</b>	
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.
<b>ipv6</b>	
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 2-29**

Parameter	Description
<b>ipv4</b>	
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 management network.
<b>ipv6</b>	



**Table 2-29** (continued)

Parameter	Description
prefix_length	If using IPv6 public addresses, specify the IPv6 prefix length.
router_ip	If using IPv6 public addresses, specify the router address.

## dns

Configuring a DNS server for the cluster is optional. If you set up a cluster without configuring a DNS server, you must provide both the IP addresses and FQDNs for all the cluster nodes and NetBackup services. If you configure a DNS server for the cluster, you need to specify only the IP addresses during the configuration.

You can configure a DNS server for the following networks:

- Only for the management network.
- Both the management and the data network.  
 Ensure that the same DNS server details are provided if you want to configure a DNS server for the data and management network. Configuring a separate DNS server for the management and data network is not supported.

**Table 2-30**

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.
search_domain	Search domains for resolving host names and IP addresses.

## nodes\_setting

Node name and details of media server, storage server, and management server for each node

**Table 2-31**

Parameter	Description
hostnames	Name of the nodes, can contain a maximum of 63 characters.

**Table 2-31** (continued)

Parameter	Description
media_server_ip	<p>Public IP address range for the media server service on each node.</p> <ul style="list-style-type: none"> <li>You can specify the IP address range separated by a dash. For example, 10.xx.xxx.192-10.xx.xxx.208</li> <li>You can specify the IP address range in the CIDR format. For example, 10.xx.xxx.192/30</li> </ul> <p>The FQDN is automatically resolved with DNS lookup.</p>
storage_server_ip	<p>Public IP address range for the storage server service on each node.</p> <ul style="list-style-type: none"> <li>You can specify the IP address range separated by a dash. For example, 10.xx.xxx.192-10.xx.xxx.208</li> <li>You can specify the IP address range in the CIDR format. For example, 10.xx.xxx.192/30</li> </ul> <p>The FQDN is automatically resolved with DNS lookup.</p>
management_interface_ip	<p>Public IP address to be assigned to the designated management network interface (eth1) on each node.</p> <p>You can specify:</p> <ul style="list-style-type: none"> <li>A single IP range</li> <li>Multiple IP ranges separated by a comma</li> <li>Comma-separated individual IP addresses</li> <li>A combination of individual IP addresses and IP ranges separated by a comma</li> <li>IP addresses in CIDR format</li> </ul>

**Table 2-31** (continued)

Parameter	Description
ipmi_interface	<p>Public IP address to be assigned to the designated IPMI interface on each node.</p> <ul style="list-style-type: none"> <li>You can specify the IP address range separated by a dash. For example, 10.xx.xxx.192-10.xx.xxx.208</li> <li>You can specify the IP address range in the CIDR format. For example, 10.xx.xxx.192/30</li> </ul> <p>The FQDN is automatically resolved with DNS lookup.</p>

## external\_primary\_server\_setting

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

**Table 2-32**

Parameter	Description
name	<p>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.</p> <p>The FQDN can contain a maximum of 253 characters.</p>
ipv4_address	<p>IPv4 address of the external primary server. The type of IP address, whether IPv4 or IPv6 depends on your network settings.</p>
ipv6_address	<p>IPv6 address of the external primary server. The type of IP address, whether IPv4 or IPv6 depends on your network settings.</p>

Table 2-32 (continued)

Parameter	Description
api_key	<p>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.</p> <p>To create an API key:</p> <ol style="list-style-type: none"><li>1 Log in to the NetBackup Web UI using the administrator credentials.</li><li>2 In the left pane, click <b>Security</b>, and then click <b>API keys</b>.</li><li>3 In the upper-right corner, click <b>Add</b>.</li><li>4 Enter a username for which you want to create the API key.</li><li>5 Indicate how long you want the API key to be valid, from today's date. NetBackup calculates the expiration date and displays it.</li><li>6 Click <b>Add</b>.  The key is displayed in a popup window.</li><li>7 To copy the API key, click <b>Copy and close</b>.  Store this key in a safe place. After you click <b>Copy and close</b>, the key cannot be retrieved again.</li></ol>

Table 2-32 (continued)

Parameter	Description
media_server_gateway	<p>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.</p> <p>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 <b>SERVER</b> entry that corresponds to the name specified by the media_server_gateway parameter.</p> <p>For example, for the following settings:</p> <pre>external_primary_server_setting:   name:     "sclhypscontainer3vm06p3.xxx.yyy.com"   ipv4_address: '192.168.2.241'   ipv6_address: ''   api_key: "A0sBjVxO5S8hwfa5cp_QvSqs0Am1Fsy6qzGLK8z2S5ayBfPrCKV6jXOI-cLtXrd"    media_server_gateway:     "nbfsclus001"</pre> <p>Add the <b>SERVER</b> entry as follows in the bp.conf file:</p> <pre>SERVER=nbfsclus001</pre>

The following example shows a sample YAML configuration file where IP ranges are specified for the node details. The IP addresses are resolved to FQDNs during the initial configuration.

```
#
#
# deployment_yaml_version: V3.0
#

common_network_setting:
```

```

dns:
  dns_domain: 'example.com'

data:
  bond:
    enable: false
    mode: ''
    option: ''
  vlan_id: ''
  ipv4:
    gateway_ip: '192.168.1.1'
    subnet_mask: '255.255.248.0'
  ipv6:
    prefix_length: ''
    router_ip: ''
  dns:
    dns_server: '10.0.0.12'
    search_domain: ['example.com']
management:
  vlan_id: ''
  ipv4:
    gateway_ip: '192.168.1.1'
    subnet_mask: '255.255.248.0'
  ipv6:
    prefix_length: ''
    router_ip: ''
  dns:
    dns_server: '10.0.0.12'
    search_domain: ['example.com']
ipmi:
  ipv4:
    gateway_ip: ''
    subnet_mask: ''
  ipv6:
    prefix_length: ''
    router_ip: ''
cluster_setting:
  name: pbclust
  console_ip_ipv4: '192.168.2.205'
  console_ip_ipv6: ''
  lockdown_mode:
    mode : 'Normal'
  retention:

```

```

        min: null
        max: null
        unit : null
private_network:
  ipv4:
    ip: 172.16.0.1
    subnet: 255.252.0.0
  ipv6:
    ip: 'fd00::2'
    prefix_length: '112'
ntp_setting:
  timezone: 'Pacific'
  server: ['10.0.0.34']
autosupport_setting:
  smtp:
    notificationInterval: ''
    hardware: ''
    software: ''
    senderEmail: ''
    emailServer: ''
    account: ''
    password: ''
    serverPort: ''
    encryption_enabled: false
  snmp:
    enable_snmp: false
    server: ''
    port: ''
    community: ''
call_home:
  enable_call_home: false
  enable_proxy_server: false
  proxy:
    enable_proxy_tunnel: false
    server: ''
    port: ''
    username: ''
    password: ''
user_management:
  users:
    - user_name: 'admin_user'
      password: 'We!!c0me'
      roles: ['appliance_admin']

```

```

storage_server:
  - user_name: 'root'
    password: 'We!!c0me'
license_key: ''
storage_licenses: []
additional_fqdn_entries:
  - ip_address: ''
    name: []

nodes_setting:
- host_name: host1.example.com
  media_server:
    name: 'sclacslnxd17pbvm27.example.com'
    ipv4_address: '192.168.2.197'
    ipv6_address: ''
  management_interface:
    name: 'sclacslnxd17pbvm23.example.com'
    ipv4_address: 192.168.2.193
    ipv6_address: ''
  ipmi_interface:
    ipv4_address: ''
    ipv6_address: ''
  storage_server:
    name: 'sclacslnxd17pbvm28.example.com'
    ipv4_address: '192.168.2.198'
    ipv6_address: ''
- host_name: host2.example.com
  media_server:
    name: 'sclacslnxd17pbvm19.example.com'
    ipv4_address: '192.168.2.189'
    ipv6_address: ''
  management_interface:
    name: 'sclacslnxd17pbvm24.example.com'
    ipv4_address: 192.168.2.194
    ipv6_address: ''
  ipmi_interface:
    ipv4_address: ''
    ipv6_address: ''
  storage_server:
    name: 'sclacslnxd17pbvm29.example.com'
    ipv4_address: '192.168.2.199'
    ipv6_address: ''
- host_name: host3.example.com

```



```

media_server:
  name: 'sclacslnxd17pbvm18.example.com'
  ipv4_address: '192.168.2.188'
  ipv6_address: ''
management_interface:
  name: 'sclacslnxd17pbvm25.example.com'
  ipv4_address: 192.168.2.195
  ipv6_address: ''
ipmi_interface:
  ipv4_address: ''
  ipv6_address: ''
storage_server:
  name: 'sclacslnxd17pbvm30.example.com'
  ipv4_address: '192.168.2.200'
  ipv6_address: ''
- host_name: host4.example.com
  media_server:
    name: 'sclacslnxd17pbvm31.example.com'
    ipv4_address: '192.168.2.201'
    ipv6_address: ''
  management_interface:
    name: 'sclacslnxd17pbvm26.example.com'
    ipv4_address: 192.168.2.196
    ipv6_address: ''
  ipmi_interface:
    ipv4_address: ''
    ipv6_address: ''
  storage_server:
    name: 'sclacslnxd17pbvm32.example.com'
    ipv4_address: '192.168.2.202'
    ipv6_address: ''
external_primary_server_setting:
  name: "sclhypscontainer3vm06p3.example.com"
  ipv4_address: '192.168.2.241'
  ipv6_address: ''
  api_key: "A0sBjVxO5S8hwfa5cp_QvSqs0AmYlFsy6qzGLK8z2S5ayBfPnOKV6jXOI-cLtXrd"
  media_server_gateway: "nbfsclus001"

```

# Changing the maintenance user account password

After setting up the cluster, one of the steps you must do is change the default password of the "maintenance" user account. This is an in-built user account that has administrative access to the operating system root and the appliance command-line interface commands and can be used to perform maintenance activity on the cluster nodes.

## To change the maintenance user account password

- ◆ Sign in to the NetBackup Flex Scale infrastructure management console.

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

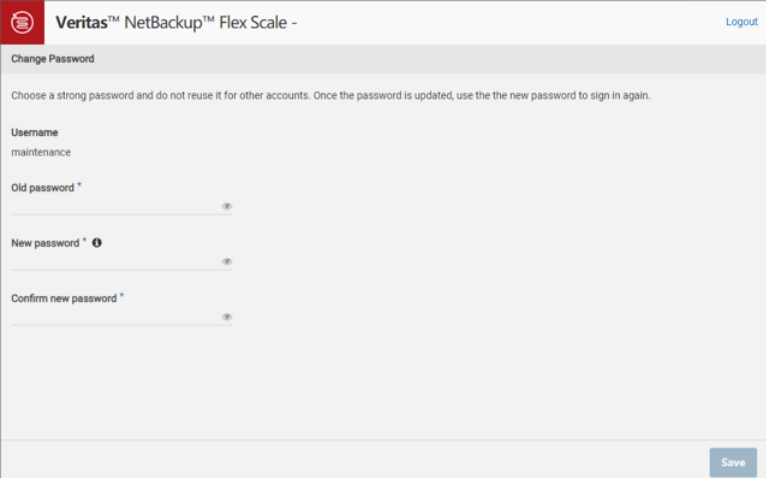
`https://consoleIP:14161`

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

As you are signing in for the first time, you are automatically required to change the default account password.



The screenshot shows the 'Veritas™ NetBackup™ Flex Scale -' web interface. The page title is 'Change Password'. Below the title, there is a instruction: 'Choose a strong password and do not reuse it for other accounts. Once the password is updated, use the new password to sign in again.' The form contains the following fields: 'Username' with the value 'maintenance', 'Old password \*' with a password icon, 'New password \*' with a password icon and an information icon, and 'Confirm new password \*' with a password icon. A 'Save' button is located at the bottom right of the form.

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.

# Troubleshooting NetBackup Flex Scale deployment

This chapter includes the following topics:

- [NetBackup Flex Scale logs](#)
- [Connection timeout errors during patch installs, upgrades, and rollback operations](#)
- [Initial configuration wizard displays a driver node not selected error](#)
- [Initial configuration wizard displays a license error after successfully configuring the cluster](#)

## NetBackup Flex Scale logs

You can refer to the following log files for troubleshooting NetBackup Flex Scale deployment and configuration issues:

**Table 3-1** NetBackup Flex Scale log files

Log file	Description
/log/cpi	Temporary location for storing the installation and cluster configuration logs.

**Table 3-1** NetBackup Flex Scale log files (*continued*)

Log file	Description
/log/VRTSnas/log/appliance_nodes.log	Contains the cluster configuration logs generated by the initial configuration wizard.  These logs appear only on the node (the driver node) from where you configure the cluster.
/log/cpi	Contains NetBackup Flex Scale cluster configuration logs.  These logs appear only on the node (the driver node) from where you launch the quick setup wizard to configure the cluster.
/log/VRTSnas/log/backup_server_config.log	Contains the NetBackup and the MSDP-X configuration logs.  These logs appear on the node on which the management console service is running.
/log/VRTSnas/log/storage_pool_create.log /log/VRTSnas/log/storage_fs_create.log	Contains the storage configuration logs.  These logs appear on the node on which the management console service is running. These logs are found on the driver node, which is the node from where you launched the cluster configuration workflow.
/opt/VRTSnas/log/msdpx_integration.log	Contains the MSDP configuration logs.
/var/log/sds/sds.log	Contains the SDS logs for MSDP-X configuration.  These logs appear on the node on which the management console service is running.
/opt/VxUL/bin/vxlogview /log/app_vxul/409-889-*.log /log/app_vxul/409-14-*.log	Contains logs related to the node factory reset operation.

**Table 3-1** NetBackup Flex Scale log files (*continued*)

Log file	Description
/log/upgrade/upgrade_3.0.log	Contains upgrade logs.
vxlogview -o 776	Use the vxlogview command to view the logs for the pre-upgrade checks.

## Connection timeout errors during patch installs, upgrades, and rollback operations

While performing maintenance activities such as EEB patch installation, software upgrade, or rollback on your NetBackup Flex Scale cluster, the operations may fail with a connection timeout error.

The following message may appear in the product logs:

```
ERROR Unable to connect to <cluster node #>: [Errno 110] Connection
timed out
```

### Cause

This error typically occurs if the network interface eth4 is down on any of the cluster nodes. NetBackup Flex Scale uses eth4 for communication between the cluster nodes. Whenever eth4 is down, it breaks that communication path and all ssh commands fail to execute with a timeout error.

### Solution

Ensure that the network interface eth4 is up on each of the cluster nodes and then perform the maintenance tasks in the cluster.

## Initial configuration wizard displays a driver node not selected error

You select the cluster nodes on the Select Nodes panel of the cluster configuration wizard. While choosing the nodes if the driver node is not part of the selected nodes, the wizard does not allow you to proceed.

You may see the following error:

```
Driver node must be selected for configuring the cluster.
```

---

**Note:** For version 3.0, the driver node is selected by default and you can't clear this selection.

---

## Cause

The node from where you launch the NetBackup Flex Scale cluster configuration wizard workflow is referred to as the driver node. During cluster configuration, the driver node must be included in the list of the nodes that are selected to be a part of the NetBackup Flex Scale cluster. This node is critical because the cluster configuration processes are triggered from the node.

## Solution

Ensure that the driver node is included in the selected nodes. In case the number of cluster nodes is higher, for example, 8 nodes or more, you can perform the following steps to easily identify the driver node:

1. On the Select Nodes panel, click **Export inventory CSV** to download the nodes inventory file.
2. Open the .csv file in a text editor and observe the contents.

The csv file contains a comma separated list of all the available nodes along with other parameters such as the node name, the management IP addresses assigned, the data and management network adapter MAC addresses and so on.

You may see the following types of entries in the file:

```
Model,Product version,Management IP,eth1 mac address,Host name,Serial number,eth5 mac address
5551,1.3,10.xx.xxx.15,00:50:56:b5:c0:8f,lam-01.mydomain.com,virtual-42357921c,00:50:56:b5:96:3a
5551,1.3,,00:50:56:b5:db:81,lam-02.mydomain.com,virtual-423555166e0a8f2e-b217,00:50:56:b5:cf:87
```

3. Identify the node that has the management IP assigned. This is the driver node from where you launched the cluster configuration wizard. Make a note of the node name or the MAC address of the data network adapter or the management network adapter.

---

**Note:** The management IP is the IP address that you used to connect to the node and launch the cluster configuration wizard.

---

4. Go back to the cluster configuration wizard and from the nodes list displayed in the Select Nodes panel find the node that matches the details you noted earlier and then select that node.

5. Click **Save** to update the inventory and continue with the cluster configuration process.

## Initial configuration wizard displays a license error after successfully configuring the cluster

You can add a NetBackup Flex Scale storage license or a NetBackup license while configuring the cluster. The initial configuration wizard displays a license page where you can specify the license details. However, entering the licenses during the cluster configuration itself is not mandatory. In case you skip the licensing page, the cluster is automatically configured with an in-built trial license. After the cluster configuration is successful, the wizard displays the following message:

No valid storage license is provided. A valid license is required to maintain a working cluster. Please add storage licenses after cluster configuration from appliance web GUI.

### Cause

While this error message is harmless and does not affect the cluster, it is displayed as a reminder that you must add a valid license in order to maintain a working cluster configuration.

### Solution

You can use the NetBackup Flex Scale infrastructure management UI to add a license. Veritas recommends that you add proper licenses before you start protecting production workloads with your appliance.



# NetBackup Flex Scale upgrades and patch management

This chapter includes the following topics:

- [About NetBackup Flex Scale upgrades and EEB](#)
- [About rolling upgrade](#)
- [About the pre-upgrade check](#)
- [Installing EEBs using GUI](#)
- [Installing EEBs using REST APIs](#)

## About NetBackup Flex Scale upgrades and EEB

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 console:

```
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.

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 upgrade process attempts to download the latest plug-ins from SORT, which are used to determine if the appliance nodes are healthy and ready for upgrade. If the plug-ins are downloaded successfully, these are used to perform the pre-upgrade tests. If the download fails, the upgrade process checks if the latest plug-ins are already downloaded to the appliance node. If the plug-ins are already downloaded, these are used for the pre-upgrade tests; else the plug-ins that are included in the upgrade package are used to perform the pre-upgrade tests.

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.
- The GUI displays the download package progress.
- You can upload major upgrades, patches, and EEBs from your local systems.
- The GUI displays the details of downloaded and installed major upgrades, patches, and EEBs.
- 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.
- You can install major upgrades, patches, and EEBs only when all nodes are healthy.
- You can rollback EEBs from the system only when all the nodes are healthy.
- Depending on the EEB, you might need to ensure that there are no jobs running before you install or roll back the EEB.
- 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 installation or rollback operations are in progress.
- The GUI displays the progress for operations like installation of major upgrades, patches, EEBs, and rollback of EEBs.

---

**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.

## About rolling upgrade

Starting with version 2.1, NetBackup Flex Scale supports rolling upgrade of the cluster. 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.

An upgrade pre-check runs automatically at the beginning of an upgrade to determine if the system is ready for an upgrade. If the pre-upgrade check fails, you cannot proceed with the upgrade. For details about the tests performed during the pre-upgrade check, See ["About the pre-upgrade check"](#) on page 100.

The following upgrade paths are supported for a rolling upgrade:

- From version 1.3.1 to 2.1
- From version 2.1 to 3.0

If the upgrade fails on a node, all the nodes are automatically rolled back to the previous version. The detailed logs for rolling upgrade are located in the `/log/upgrade/upgrade_3.0.log` directory.

The rolling upgrade is a two-phase process. In phase A, the infrastructure packages are upgraded. The infrastructure packages are upgraded on mirror partitions on all the cluster nodes in parallel. As the upgrade happens on a copy of the original partition, the original partition is not affected and NetBackup backup and restore jobs continue running on all the nodes in the cluster. After the packages are upgraded, each node is restarted successively and the node joins the cluster with the new upgraded packages from the mirrored partition.

In phase B, the NetBackup services and containers are stopped and NetBackup and MSDP packages are upgraded on all the nodes. This phase results in downtime,

which causes the ongoing backup and restore jobs to fail. After the packages are upgraded the services are restarted. You must restart the jobs once the upgrade is complete. Jobs that are configured to create checkpoints during a backup, such as file system jobs, can be suspended before an upgrade. The jobs resume after the upgrade is complete.

For details about how to perform a rolling upgrade,

For details about upgrade logs See [“NetBackup Flex Scale logs”](#) on page 92.

## About the pre-upgrade check

The pre-upgrade check determines if the system is ready for an upgrade. The pre-upgrade check runs automatically when you start the upgrade. The pre-upgrade check runs at the beginning of an upgrade and checks for any potential problems that might result in an upgrade failure. If the pre-upgrade check fails, the upgrade cannot proceed. You must resolve the issues before you upgrade the cluster.

The following tests are performed during the pre-upgrade check:

- System self test to verify the health of system and software services, such as network, MSDP, and NetBackup.
- Version check to ensure that the upgrade path is supported and the current system can be upgraded to the target version.
- The Docker daemon is configured correctly.
- Hardware vendor package that is compliant with the appliance is present on the cluster.

---

**Note:** Vendor package is also required for VMware-based deployments. Note that VMware-based deployments are not supported in production environment and can only be used for proof of concept or in demo environment.

---

- Sufficient free space is available for the upgrade.
- No other bootable devices are present that may interfere when restarting the nodes during the upgrade.
- For scale-out media server deployments, the NetBackup primary server version is compatible with the media server version.
- The administrator password does not expire within seven days.
- All the cluster nodes are up and healthy with the same software version installed on all the nodes.

- No add node, replace node, or restore jobs are running on the cluster nodes.

## Running a pre-upgrade check for an upgrade package

Starting with version 3.0, you can run a pre-upgrade check independently after you download an upgrade package from the Veritas website or when you upload an upgrade package from a local system.

### To run a pre-upgrade check independently on an upgrade package:

- 1 Use any one of the following options to log in using the user account that you created when you configured the cluster:
  - Use a user account with both Appliance Administrator and NetBackup Administrator role, or a user account with only an Appliance administrator role to log in to the NetBackup Flex Scale web interface  
`https://ManagementServerIPorFQDN/webui` where *ManagementServerIPorFQDN* is the public IP address or the FQDN that you specified for the NetBackup Flex Scale management server during the cluster configuration. In the left pane click **Cluster Monitor > Infrastructure**, and then click **Cluster Dashboard**.
  - Use a user account with an Appliance Administrator role to log in to the NetBackup Flex Scale infrastructure management console  
`https://ManagementServerIPorFQDN:14161` where *ManagementServerIPorFQDN* is the public IP address or the FQDN that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration.
- 2 In the left navigation click **Settings**, and then **Software management**.
- 3 If not already done so, download the upgrade package from the Veritas website, or upload the upgrade package from a local system:

To download the upgrade package:

- On the software management page click **Software updates**.
- To check if any upgrade packages are available on the Veritas website, click **Check online for upgrade**. If any upgrade packages are available on the website, the list of available upgrade packages is displayed under **Available upgrades**.
- Download the upgrade package. Under **Available upgrades**, next to the upgrade package that you want to download from the Actions menu (vertical ellipsis) click **Download package**. After the download is complete, the package is displayed under **Downloaded package files** and the status is displayed as **Available**.

To upload an upgrade package:

- Click **Upload file**.
  - Select the file and then click **Upload**. After uploading the package, it is displayed under **Downloaded package files**.
- 4 To start the pre-upgrade check, under **Downloaded package files** for the upgrade package, 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**.

## Installing EEBs using GUI

You can perform an upgrade by installing EEBs using the GUI.

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

See [“About NetBackup Flex Scale upgrades and EEB”](#) on page 97.

### To install an EEB using the GUI

- 1 Download the EEB on the local system.
- 2 Go to **Settings > Software management > Add-ons**.
- 3 To upload EEBs:
  - If you already have EEBs in your system, all the EEBs (available and installed) are displayed. Select the EEB and click **Install**.
  - If the EEB that you want to add is not in the list, click the **Add** icon. In the **Upload EEBs** screen, click **Choose add-ons** to choose add-ons. Click **Add** to upload the EEB to the system.  
In the **Add-ons** pane, select the EEB that you want to install and click **Install**.
  - If you have no EEBs in your system, click **Choose add-ons** to choose add-ons. Click **Add** to upload the EEB to the system. In the **Add-ons** pane, select the EEB that you want to install and click **Install**.
- 4 Upgrade package progress information is displayed on top of the page. Expand the task to see sub tasks.
- 5 After the upload is complete, you can choose to install or remove the EEBs. After installing an EEB, you can choose to roll back the EEB.

If the EEB fails to install or roll back on any one of the cluster nodes, you can view the details about the failure by clicking **View details**.

# 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}
```

# Removing NetBackup Flex Scale

This chapter includes the following topics:

- [About disk erasure](#)
- [About NetBackup Flex Scale node factory reset](#)
- [Performing a factory reset on a node](#)

## 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 108.

---

**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] (yes)
```

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] (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] (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.

---

**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.

---

# Installing NetBackup Flex Scale

This appendix includes the following topics:

- [About NetBackup Flex Scale software installation](#)
- [Enabling remote IPMI connections](#)
- [Setting up the RAID configuration on the nodes](#)
- [Configuring the BIOS settings on the nodes](#)
- [Downloading the product installer ISO](#)
- [Mounting the ISO file on the nodes](#)
- [Installing NetBackup Flex Scale using the ISO](#)
- [Installing hardware vendor packages](#)
- [Installing Emergency Engineering Binaries \(EEBs\)](#)

## 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.

See [“Configuring NetBackup Flex Scale using the setup wizard”](#) on page 21.

The installation instructions provided here are intended to serve only as a reference. They are useful in case you decide to wipe the appliance clean and start a fresh deployment.

If you plan to leverage your own hardware instead of the out of the box appliance, ensure that you contact Veritas Support to generate and install device certificates on your nodes.

Refer to the following:

See [“Enabling remote IPMI connections”](#) on page 111.

See [“Setting up the RAID configuration on the nodes”](#) on page 113.

See [“Configuring the BIOS settings on the nodes”](#) on page 120.

See [“Downloading the product installer ISO”](#) on page 127.

See [“Mounting the ISO file on the nodes”](#) on page 128.

See [“Installing NetBackup Flex Scale using the ISO”](#) on page 129.

See [“Installing hardware vendor packages”](#) on page 131.

See [“Installing Emergency Engineering Binaries \(EEBs\)”](#) on page 132.

## 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.

iLO Federation
Remote Console & Media
Power & Thermal
Performance
iLO Dedicated Network Port
iLO Shared Network Port
Remote Support
Administration
Security
Management
Intelligent Provisioning

Server

Server Name

[Not set]

Server FQDN / IP Address

[Not set]

Account Service

Authentication Failures Before Delay

1 failure causes no delay

Authentication Failure Delay Time

10 seconds

Authentication Failure Logging

Enabled - Every 3rd Failure

Minimum Password Length

8

Password Complexity

Disabled

Network

Anonymous Data

Enabled

IPMI/DCMI over LAN

Disabled

IPMI/DCMI over LAN Port

623

Remote Console

Enabled

Remote Console Port

17990

Secure Shell (SSH)

Enabled

Secure Shell (SSH) Port

22

SNMP

Enabled

SNMP Port

161

SNMP Trap Port

162

Virtual Media

Enabled

Virtual Media Port

17988

Virtual Serial Port Log

Disabled

Web Server

Enabled

Web Server Non-SSL Port

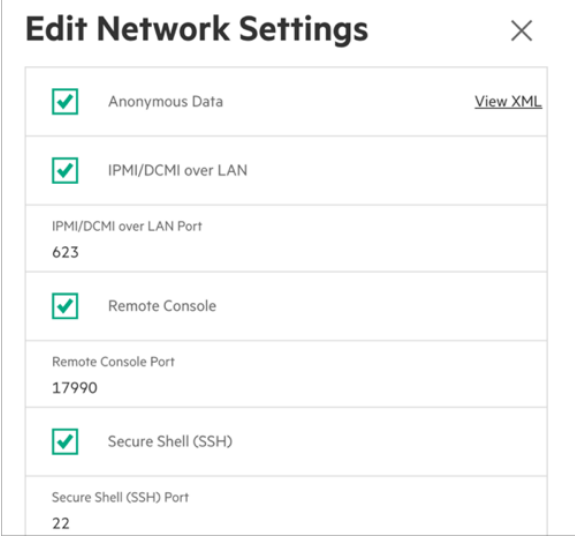
80

Web Server SSL Port

443



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



Edit Network Settings	
<input checked="" type="checkbox"/>	Anonymous Data <a href="#">View XML</a>
<input checked="" type="checkbox"/>	IPMI/DCMI over LAN
	IPMI/DCMI over LAN Port 623
<input checked="" type="checkbox"/>	Remote Console
	Remote Console Port 17990
<input checked="" type="checkbox"/>	Secure Shell (SSH)
	Secure Shell (SSH) Port 22

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

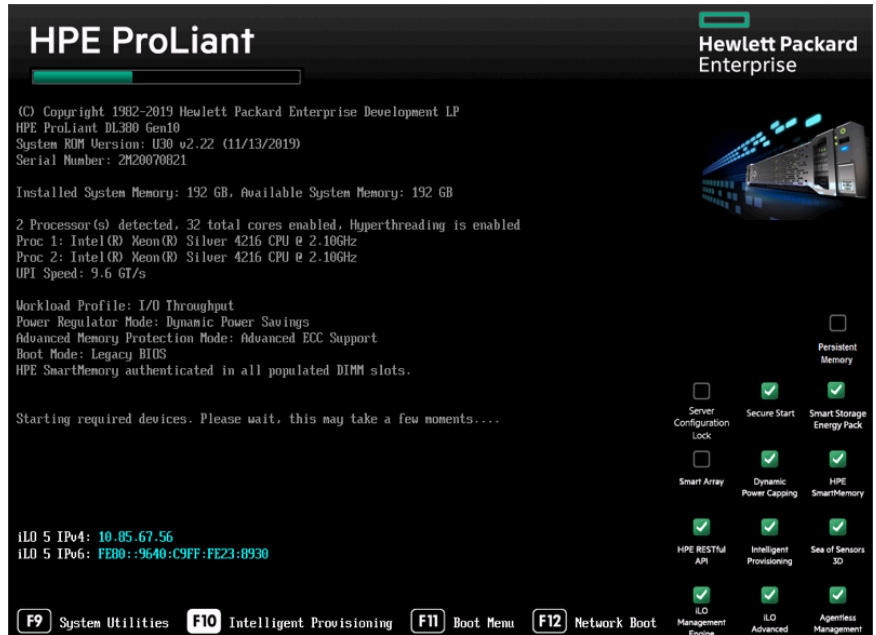
## Setting up the RAID configuration on the nodes

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.

## To initialize RAID on the node

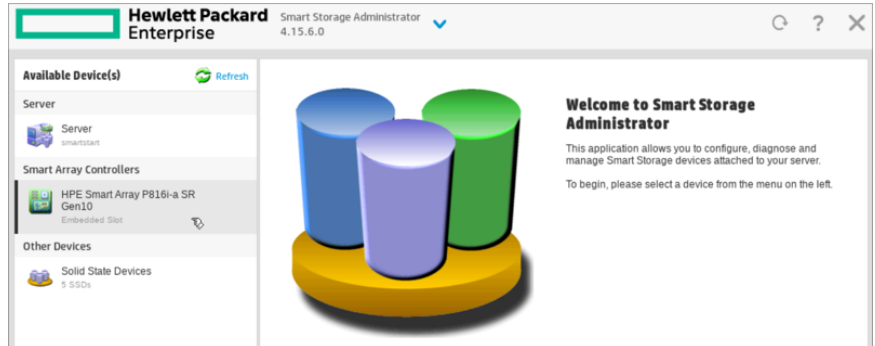
- 1 Power ON the node and press the **F10** key on the boot screen to launch the Intelligent Provisioning module.



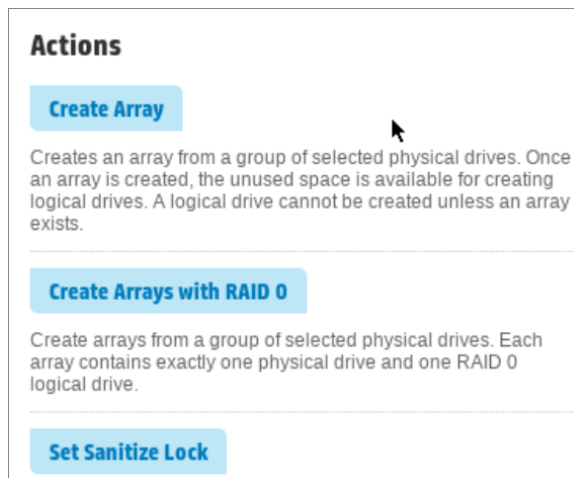
- 2 Click **Smart Storage Administrator** to begin the RAID configuration.



- 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.

**HPE Smart Array P816i-a SR Gen10** Embedded Slot > **Create Array**

■ In a dual domain configuration, mixing single and dual ported SAS drives can lead to a loss of redundancy.  
 ■ To avoid wasting drive capacity, select physical drives that are the same size for the new array. [Hide](#)

**Select Physical Drives for the New Array** [\(What's this...?\)](#)

Drive Type: **SATA SSD** Group By: **Enclosure**

**Internal Drive Cage at Port 31 : Box 6**

☒ Select All (2)


**1.9 TB** SATA SSD Bay 1 **1.9 TB** SATA SSD Bay 2

Selected: 2  
 Size: 3.49 TiB (3.84 TB)

**Create Array** **Cancel**

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.


**HPE Smart Array P816i-a SR Gen10**  
 Embedded Slot

Create Logical Drive

■ The logical drive must be smaller than 2 TiB if it is used as a boot volume, the OS does not support hybrid MBR boot code, and the system has legacy BIOS firmware.  
 ▲ One or more selected drives are connected to mixed mode ports and directly exposed to the OS. These drives will become unavailable to the OS after this operation.

**RAID Level** (What's this...?)
 

☐ RAID 0  
☒ RAID 1

**Strip Size / Full Stripe Size** (What's this...?)
 

☐ 16 KiB / 16 KiB  
☐ 32 KiB / 32 KiB  
☒ 64 KiB / 64 KiB  
☐ 128 KiB / 128 KiB  
☐ 256 KiB / 256 KiB  
☐ 512 KiB / 512 KiB  
☐ 1024 KiB / 1024 KiB

**Sectors/Track** (What's this...?)
 

☐ 63  
☒ 32

**Size** (What's this...?)
 

☒ Maximum Size: 1831388 MiB (1.7 TiB)  
☐ Custom Size

**SSD Over Provisioning Optimization** (What's this...?)
 

☐ Perform SSD Over Provisioning Optimization on the Array  
☒ Do not perform SSD Over Provisioning Optimization on the Array


Create Logical Drive

Cancel

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**.

 **HPE Smart Array P816i-a SR Gen10** Embedded Slot > Create Logical Drive

■ Logical Drive was successfully created. Please choose one of the actions below.

**Array Details**

Status	OK
Used Space	3.4 TiB (100.00%)
Total Usable Space	3.4 TiB
Acceleration Mode	HPE SSD Smart Path is enabled for all logical drives in the array

**Logical Drives**

Logical Drive 1	1.75 TiB (1.92 TB)
-----------------	--------------------

**Physical Drives**

1.9 TB SATA 512e SSD at Port 3I : Box 6 : Bay 1
1.9 TB SATA 512e SSD at Port 3I : Box 6 : Bay 2


**Device Path**

HPE Smart Array P816i-a SR Gen10 in Embedded Slot

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**.


**HPE Smart Array P816i-a SR Gen10**  
 Embedded Slot

(activate on failure only) to predictive spare activation and back.

---

**Clear Configuration**

Resets the controller's configuration to its default state. Any existing arrays or logical drives will be deleted, and any data on the logical drives will be lost. Please confirm this is the desired action before proceeding.

---

**Manage Power Settings**

Modifies the controller's power mode and enables or disables survival mode for supported controllers. A reboot or cold boot may be required after changing power modes to optimize power savings and performance.

---

**Manage Drive Write Cache Policy**

Manage the physical drive's write cache policy.

---

**Set Bootable Logical Drive/Volume**

Sets the primary and secondary boot logical drives/volumes. Local logical drives as well as remote logical drives/volumes are listed for selection as primary and/or secondary boot logical drives/volumes for the controller.

---

**Check Online Firmware Activation Readiness**

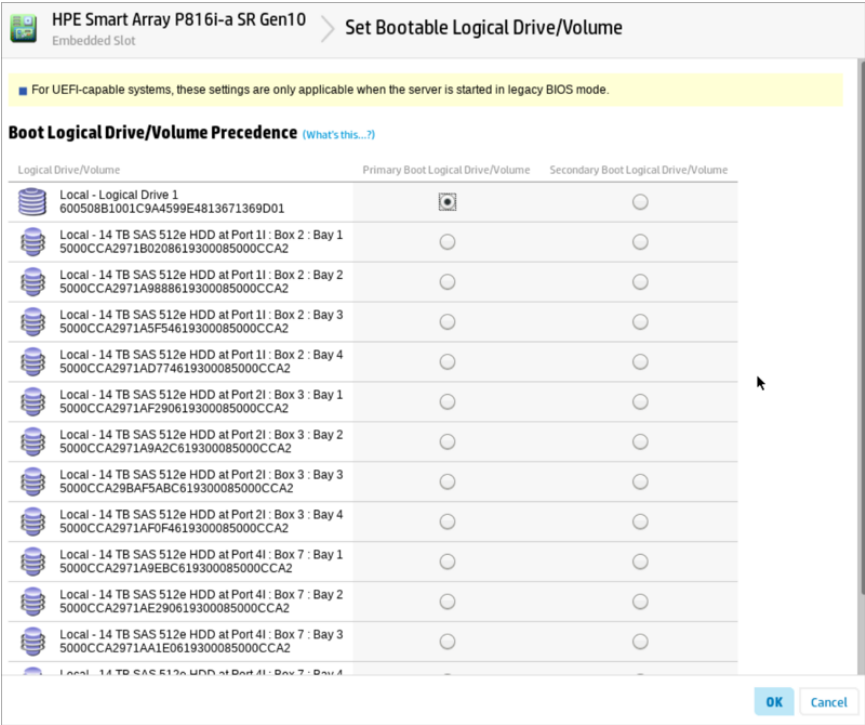
Check the current configuration to determine if an Online Firmware Activation is allowed.

---

**Manage Device Identification LEDs**

Turn the physical drive identification LED(s) On or Off

- 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.

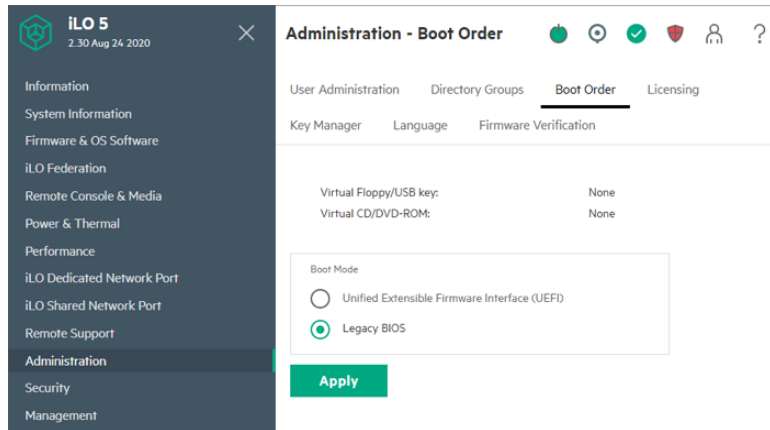
# Configuring the BIOS settings on the nodes

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**.

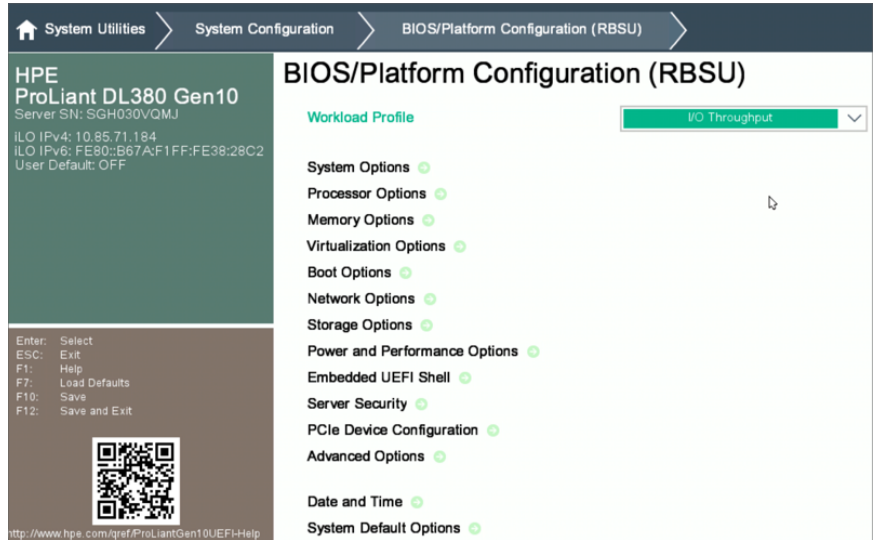


- 3 Reboot the node for the changes to take effect.

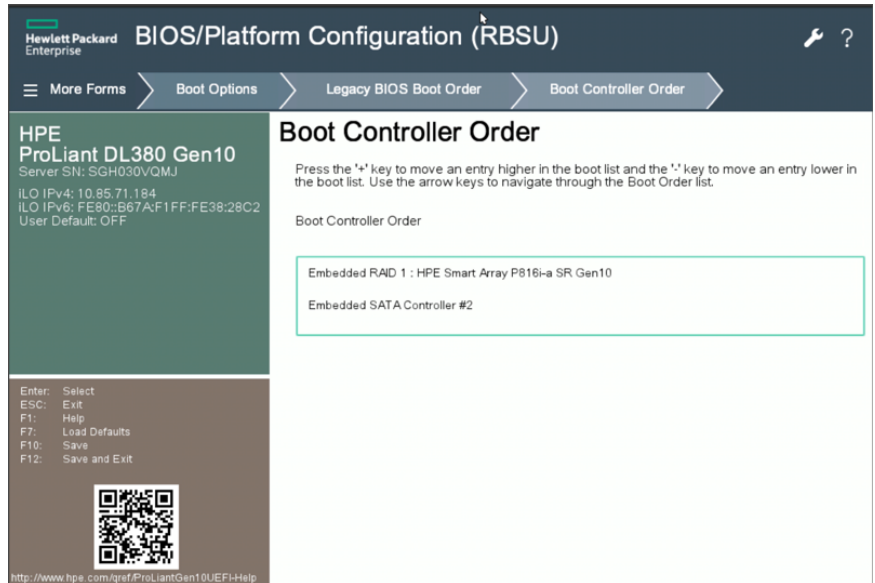
- 4 After the node restarts successfully, reboot it again and press the **F9** key on the boot screen to open the System Utilities.



- 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.

**More Forms** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options**

**HPE ProLiant DL380 Gen10**  
Server SN: SGH030VQM.J  
ILO IPv4: 10.85.71.184  
ILO IPv6: FE80::B67A:F1FF:FE38:28C2  
User Default: OFF

Enter: Select  
ESC: Exit  
F1: Help  
F7: Load Defaults  
F10: Save  
F12: Save and Exit

<http://www.hpe.com/gen10UEFI-Help>

### Network Boot Options

**Pre-Boot Network Environment**

**IPv6 DHCP Unique Identifier**

**Network Boot Retry Support**

**Network Boot Retry Count**

**HTTP Support**

**ISCSI Policy**

**Embedded FlexibleLOM 1 Port 1 : HPE Ethernet 1Gb 4-port 366FLR Adapter - NIC**

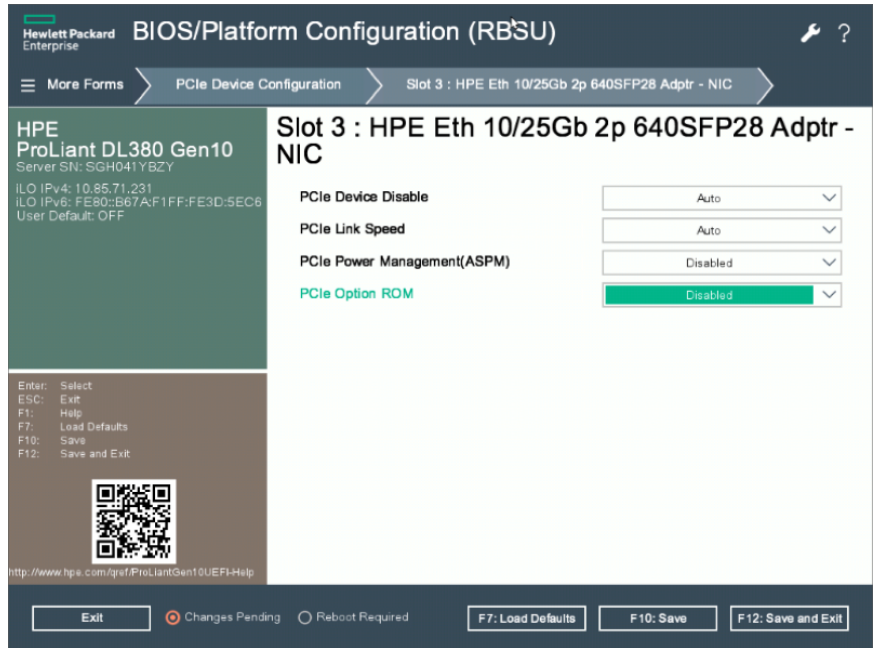
**Embedded FlexibleLOM 1 Port 2 : HPE Ethernet 1Gb 4-port 366FLR Adapter - NIC**

**Embedded FlexibleLOM 1 Port 3 : HPE Ethernet 1Gb 4-port 366FLR Adapter - NIC**

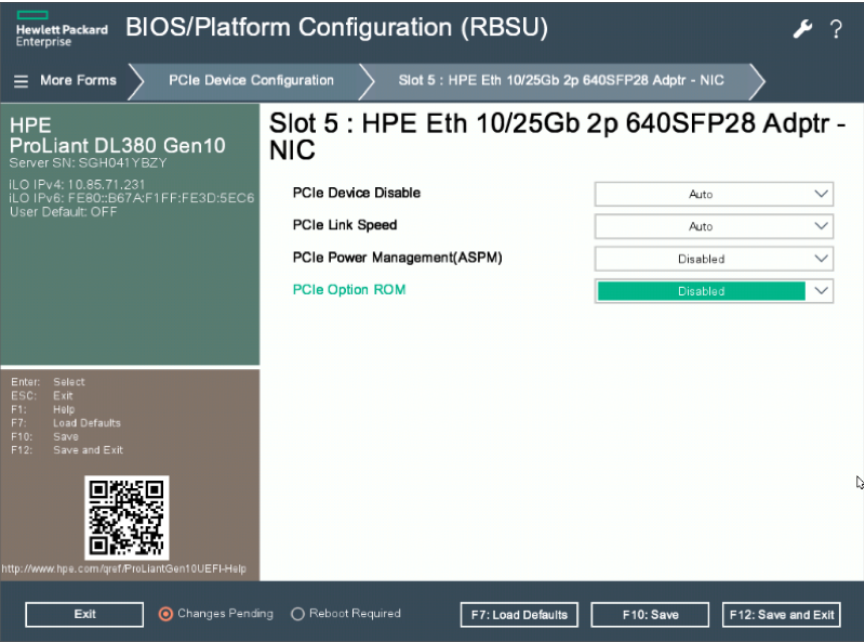
**Embedded FlexibleLOM 1 Port 4 : HPE Ethernet 1Gb 4-port 366FLR Adapter - NIC**

PCIe Slot Network Boot

- 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
nbfs-3.0-20220301145658.iso	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 128.

## 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.



## 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.

## Connecting the ISO to a Dell server node

For Dell PowerEdge R750 servers, use the Integrated Dell Remote Access Controller (iDRAC) and ensure that you use the virtual CDROM drive from the boot menu options to mount the ISO. Do not use a USB storage drive to mount the ISO.

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.

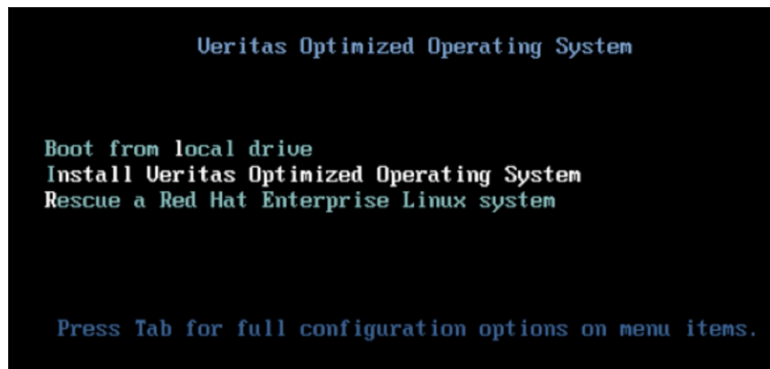
---

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 127.  
See [“Mounting the ISO file on the nodes”](#) on page 128.
- 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.

See [“Configuring NetBackup Flex Scale using the setup wizard”](#) on page 21.

## Installing hardware vendor packages

If you don't use the out of the box appliance that is pre-installed with an operating system and the NetBackup Flex Scale software and instead install the ISO image manually, ensure that you install the hardware vendor package that is compatible with your hardware vendor platform. You can download the vendor package from the Veritas Support website.

### To install the hardware vendor package:

- 1 Open an SSH session and log on to the appliance node as an admin user.
- 2 To verify that the hardware vendor package is not already installed on the appliance, on the Appliance shell menu run the following command:

```
system self-test software
```

If the vendor package is not installed, the vendor utilities test fails.

```
Checking whether required vendor utilities are installed... [FAIL]
```

- 3 Use the following command to open an NFS share:

```
system software share open
```

- 4 To download the vendor package, on a local system, complete the following steps:

- 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.

- Download the hardware vendor package from the Veritas support website. Choose the vendor package that is compatible with your appliance hardware platform:
    - VRTSnbfs\_DELL\_Utilityies\_5562\_v1.0.tar 3.58MB
    - VRTSnbfs\_HPE\_Utilityies\_5551\_v1.0.tar 32.01MB
  - Copy the package from your local system to the mapped directory.
  - Unmount the share.
- 5 On the appliance node, in the Appliance shell menu, run the following command to close the NFS share:

```
system software share close
```

- 6 To install the vendor package, enter the following command:

```
system install hw-vendor-packages
```

The following message is displayed after the package is installed successfully:

```
[Info] V-409-775-30005: Installed the hardware vendor package on  
the system  
successfully.
```

Optionally, you can run the self test again to ensure that the vendor utilities test completes successfully:

```
system self-test software
```

```
Checking whether required vendor utilities are installed... [PASS]
```

## Installing Emergency Engineering Binaries (EEBs)

Emergency Engineering Binaries (EEBs) provide critical fixes that are not included as part of the ISO image. If you factory reset a node or install the NetBackup Flex Scale ISO image on the node to start a fresh deployment, you do not have access to product REST APIs or the UI. In such cases if you are required to install EEBs, you must install these manually using the following procedure.

---

**Note:** Use a computer that is connected to the appliance and the Internet to complete the following steps:

---

- 1 Open an SSH session and log on to the appliance node as the admin user.
- 2 In the NetBackup Flex Scale Appliance shell menu, use the following command to open NFS shares:

```
system software share open
```

- 3 On the local computer, complete the following steps:
  - 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.
  - Download the EEB from the Veritas Support website site ([https://www.veritas.com/support/en\\_US](https://www.veritas.com/support/en_US)). On the Veritas Support website click Downloads, which redirects you to the Download Center. You must sign in with your Veritas account credentials to download the EEB.
  - Copy the EEB from your local computer to the mapped directory.
  - Unmount or unmap the share.
- 4 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
```

- 5 To display the list of downloaded updates, enter the following command. Make a note of the EEB that you want to install.

```
system software downloaded
```

- 6 To install the EEB, enter the following command:

```
system software install-update update-name=eeb_name
```

where *eeb\_name* is the name of the EEB that you want to install. Ensure that the name you enter matches the name of the EEB that was downloaded to the appliance.

The following message is displayed after the EEB is installed successfully:

- [Info] V-409-777-7003: Installed EEB *eeb\_name* successfully.

- 7 To verify that the EEB you installed is displayed in the list of installed EEBs, run the following command:

```
system software installed-eebs
```