NetBackup™ Flex Scale Best Practices and Troubleshooting Guide

3.5.100

VERITAS
now part of Cohesity

NetBackup Flex Scale Best Practices and Troubleshooting Guide

Last updated: 2026-04-27

Legal Notice

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

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

Support/Service Assistance

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

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

Cohesity Software Running on Partner Hardware

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

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

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

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

Contents

Chapter 1

Introduction

This chapter includes the following topics:

Scope and intended audience

This guide describes the prerequisites and the best practices for configuring a NetBackup Flex Scale cluster. Review the requirements and guidelines carefully before you start the cluster configuration to minimize any issues during the configuration.

This guide is intended for customers and Veritas Support personnel. It is assumed that the reader is familiar with Veritas NetBackup.

About NetBackup Flex Scale

Veritas NetBackup Flex Scale is the next generation, hyper-converged, scale-smart data protection solution that is based on Veritas NetBackup, the industry-leading backup and recovery software. NetBackup Flex Scale provides an automated, containerized, scale-out architecture for a non-disruptive and dynamic node and storage expansion. Infrastructure scales non-disruptively in performance and capacity by simply adding nodes. NetBackup services are installed automatically when you deploy NetBackup Flex Scale. You can manage data protection for your workloads and the complete infrastructure from a single web interface making it easy to manage the growing data protection needs.

About NetBackup Flex Scale nodes

Each NetBackup Flex Scale node is pre-installed with NetBackup Flex Scale software. The nodes are deployed in a cluster that contains a minimum of four nodes and a maximum of 16 nodes. Each NetBackup Flex Scale node is an Intel-based server from a Veritas approved hardware vendor.

The following model from Veritas approved hardware vendor is supported:

Table 1-1

Hardware vendor	Model	Server
Hewlett Packard Enterprise (HPE)	5551	HPE ProLiant DL380 Gen10
HewlettPackardEnterprise(HPE)	5561	HPE ProLiant DL380 Gen11

Download the 5551 model datasheet

Download the 5561 model datasheet

Chapter 2

Configuration requirements

This chapter includes the following topics:

Physical environment

NetBackup Flex Scale nodes must remain unopened and stored in the same location, preferably the datacenter. If cardboard is not allowed in the datacenter, specify where the equipment will be located on the day of installation.

Temperature and cooling requirements

- American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) A3 and A4 Standards.
- Operating temperature: (+10°C to +35°C) (+50°F to +95°F)
- Non-operating temperature: (-30°C to +60°C) (-22°F to +140°F)
- Operating humidity of Appliance: (8% RH to 90% RH)
- Non-operating humidity: (5% RH to 95% RH)

Power requirements and consumption

- Power Cable Specifications: IEC-60320-C14 to IEC-60320-C13, 15A/250V, Black, 4 feet. (For 5551 HPE nodes)
  Power Cable Specifications: IEC 60320 C14 To IEC 60320 C13 - AC 250 V - 10 A - 6.6 Ft - Black (For 5561 HPE nodes)
- AC power requirements:
  - 100 VAC - 127 VAC at 5.7A
  - 200 VAC - 240 VAC at 2.8A
- Typical power consumption: 361 watts
- Maximum power consumption: 500 watts

Rack mounting equipment

NetBackup Flex Scale requires at least four Flex Scale Appliance nodes to form a cluster. Install all the Flex Scale Appliance nodes in an EIA standard rack that is 19 inch (48.26 cm) wide and at least 39.37 inches (100 cm) deep.

Note: 1 inch = 2.54 cm

NetBackup Flex Scale nodes

- Each node is two rack units (2RU) high.
- The compute node rails are extensible to 81.28mm (32in). This distance is the maximum depth that is allowed between rack posts.
- Each 5551 HPE node dimensions are as follows:
  - Height 73.25 cm (28.84 in.)
  - Width 44.8 cm (17.64 in.)
  - Depth 8.75 cm (3.44 in.)
  - Weight 37 kg (81.57 lbs)
- Each 5561 HPE node dimensions are as follows:
  - Height: 73.25 cm (28.84 in.)
  - Width: 44.8 cm (17.64 in.)
  - Depth: 8.75 cm (3.44 in.)
  - Weight: 37 kg (81.57 lbs)

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 MSDP engine 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 either 1 resolvable short host name or Fully Qualified Domain Name (FQDN) for the NetBackup primary server
- 1 public IP address and either 1 resolvable short host name or FQDN for the NetBackup media server per node
- 1 IP address and either1 resolvable short host name or FQDN for the MSDP engine per node

---

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

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

- Resolvable short host name or FQDN of the NetBackup primary server that is external to the cluster
- 1 public IP address and either 1 resolvable short host name or FQDN for the NetBackup media server per node
- 1 IP address and either1 resolvable short host name or FQDN for the MSDP engine 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, short host names, 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 either 1 resolvable short host name or FQDN for the NetBackup Flex Scale management server. The IP address, name, or FQDN assigned to the management server is used to access the NetBackup Flex Scale web UI and the infrastructure management 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 infrastructure management UI.
- IP address details for the dedicated management network and IPMI (optional)
- Private subnet for internal communication between the cluster nodes. Specify the starting private IP address for the subnet.

  If you use IPv4 addresses, the default supported private network subnet mask is 255.255.224.0. You must use a subnet that is equal or larger than 255.255.224.0. If you use IPv6 addresses, specify the IPv6 prefix length. The prefix length must be greater than or equal to 115.

  For example:

```
private_network:
    ipv4:
      ip: 172.16.0.1
      subnet: 255.255.224.0
    ipv6:
      ip: 'fd00::2'
      prefix_length: '115'
```

Note: If you don't plan to configure a DNS server for the cluster, the IP addresses, short host names, 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 2-1

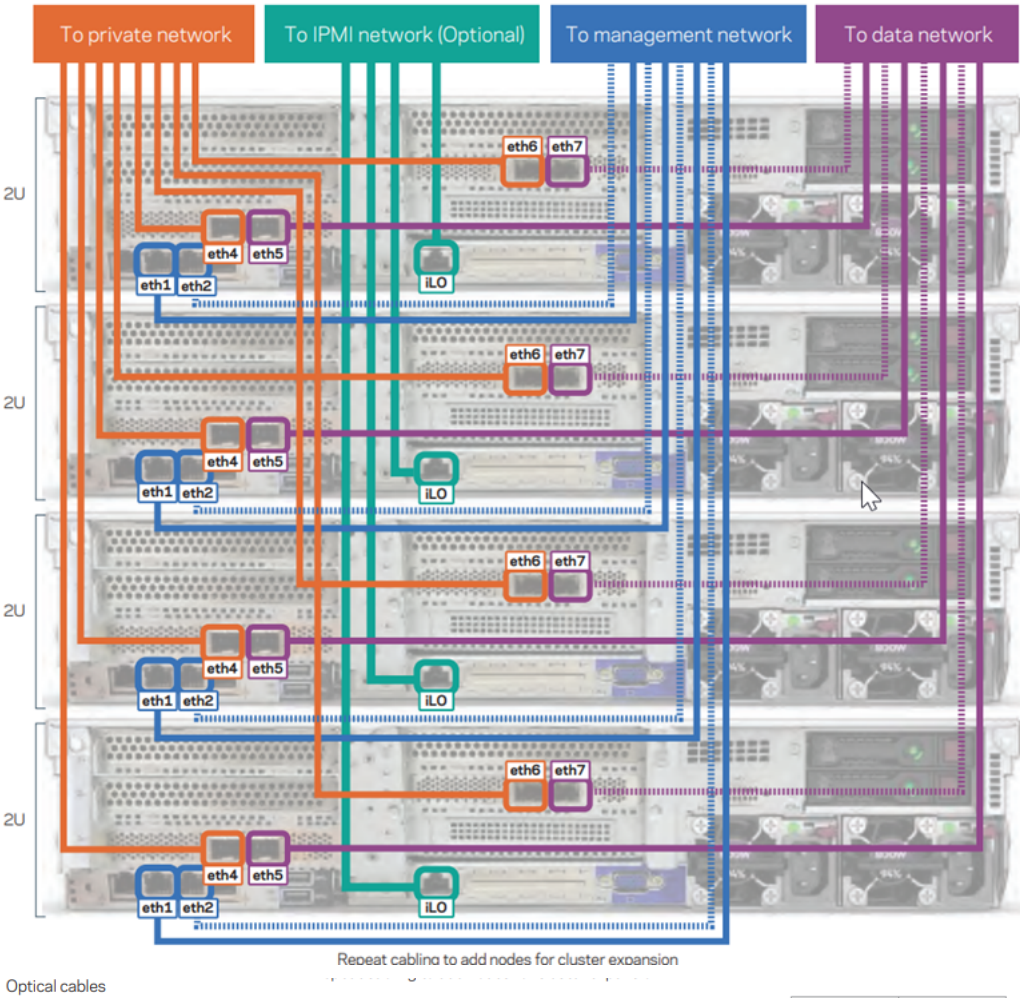
Network	Per node	For cluster	Total
Private	Not required	1 IP address and subnet mask	You can use the default private IP range and subnet mask or specify a custom IP address range and subnet mask. If you use the default private IP address range and subnet mask, you don't need to specify any details.
Management	1 IP address for the management network	1 IP address for the management server 1 IP address for the NetBackup Flex Scale infrastructure management UI	N+2
Data	1 IP address for the media server 1 IP address for the MSDP engine	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.

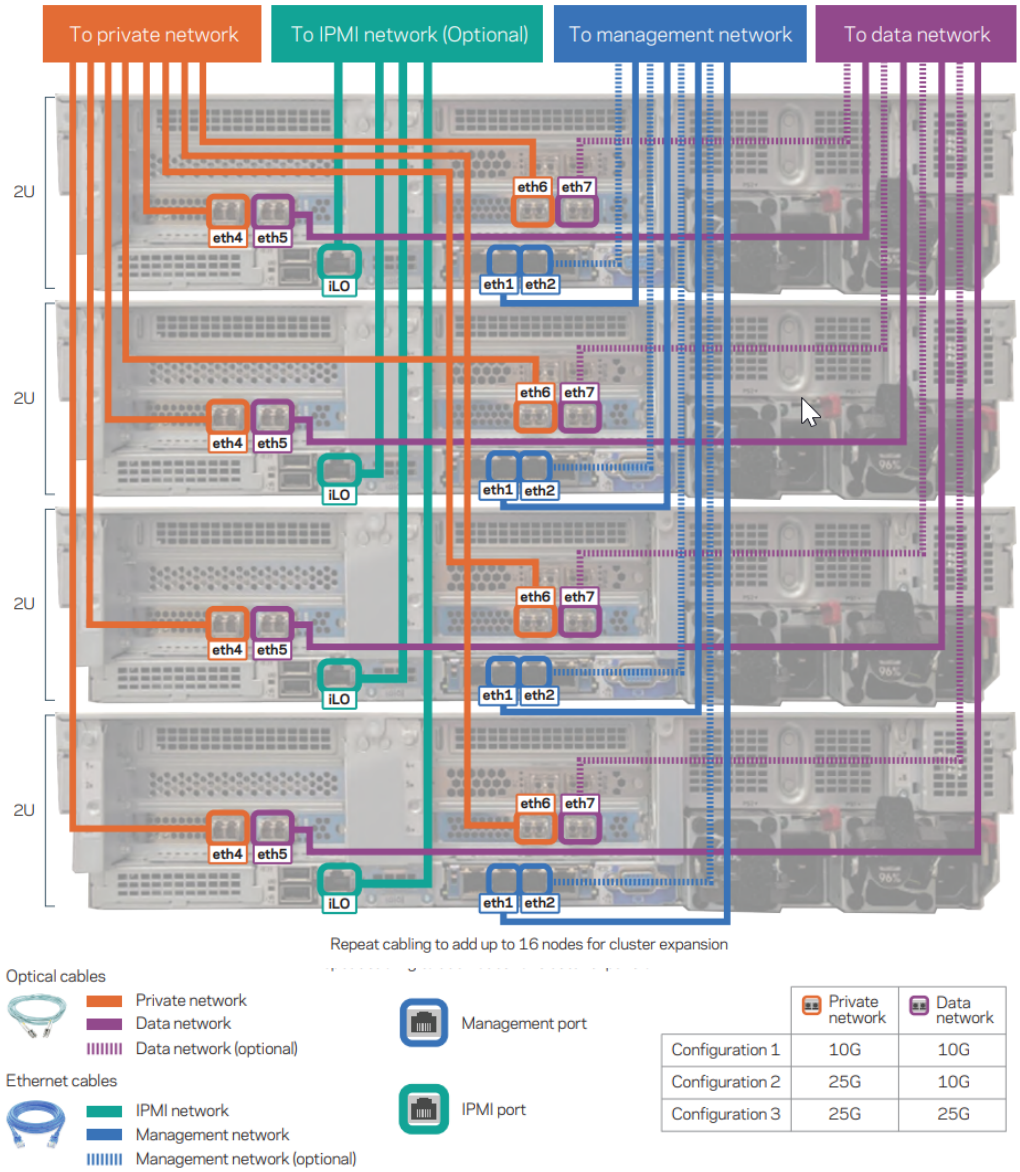
Note: Connection of cables to the nodes is included as part of the installation service, however you are responsible for providing pre-labeled network cabling that has already been connected the network switches.

Figure 2-1 Connecting NetBackup Flex Scale 5551 HPE nodes



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

Figure 2-2 Connecting NetBackup Flex Scale 5561 HPE nodes



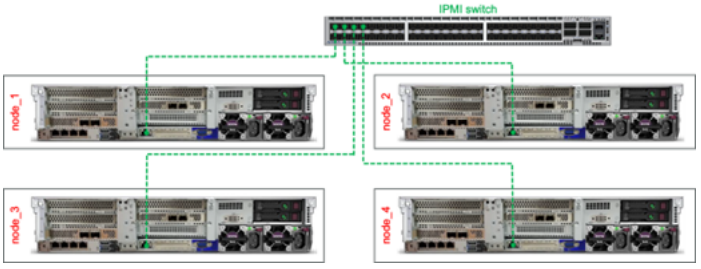
	Private network	Data network
Configuration 1	10G	10G
Configuration 2	25G	10G
Configuration 3	25G	25G

IPMI network

IPMI network is optional and can be used for out-of-band mechanism for hardware management of Flex Scale nodes.

- IPMI network can be on the same subnet as the management or data network.
- When Enterprise or Compliance modes are enabled on Flex Scale, you can enable limitations on IPMI functionality (such as disk configuration). These limitations can optionally be disabled later.
- IPMI addresses can be configured at the time of cluster configuration and each node must have a unique IPMI address.
- DHCP is supported for IPMI addressing.
- The HPE iLO offers a range of security options:
  - Basic Mode: Provides a fundamental level of security for accessing the IPMI interface.
  - High Security Mode: Enhances security with stricter authentication methods.
  - FIPS Mode: Implements the Federal Information Processing Standard (FIPS) for the most robust security level.

The following figure shows the IPMI network connectivity for the 5551 model:



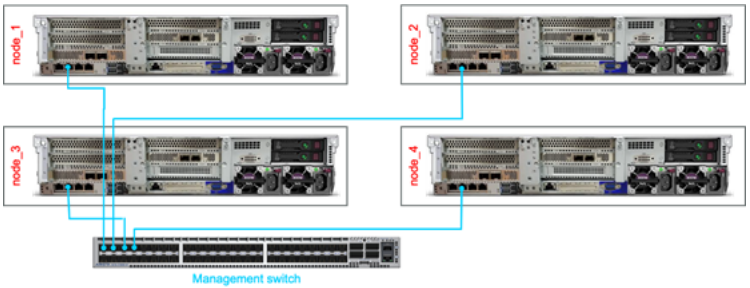
Management network (eth1/bonded eth1 and eth2/VLAN on eth1/VLAN on bonded eth1 and eth2)

The management network is used for administrative access to the node. The management network needs to be manually configured on one of the nodes to start the initial cluster configuration.

- The management network leverages eth1 on each node. You can also enable bonding for eth1 and eth2 interfaces.
  You can configure the management network on an eth1 interface, a bond of eth1 and eth2 interfaces, a VLAN on eth1, or a VLAN on bonded eth1 and eth2 interfaces.
- The management network can reside on its own subnet.
- The management network must be able to access the NTP server.
- The following services and containers use the management network:

- Node management
- Cluster console/API
- Cluster management

The following figure shows the management network connectivity for the 5551 model:



Private network (eth4 and eth6)

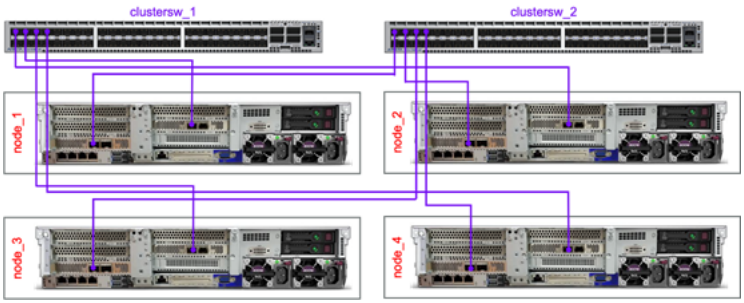
The private network is used only for inter-node communication. This network is very sensitive to network performance and therefore it is highly recommended to use a dedicated private pair of switches. Bonding is not supported for private network interfaces.

- Veritas recommends using two separate Ethernet switches, which are capable of supporting 25 Gb link to isolate the eth4 and eth6 interfaces. If you use a single Ethernet switch, connect the eth4 and eth6 interfaces of each node to switch ports in separate VLANs. The private network needs to be segregated from the other networks (data, management, and ipmi) and also internally, such that eth4 is separated physically or logically using VLANs from eth6.
- Each node will have two connections to the private network on separate NICs. The private network uses eth4 and eth6 on each node. This provides redundancy in the event one NIC fails.
- The private network runs on 25 GBps or 10 GBps Ethernet. If the private network is on 10 GBps, the public network (eth5 and eth7) can be only on 10 GBps. If private network is on 25 GBps, the public network can be either on 10 GBps or 25 GBps. A dedicated line speed per switch port is also required.
- VLAN tagging is not supported for private the network.
- The node discovery process utilizes the AVAHI network and multicast traffic. Ensure that the (broadcast, unknown-unicast, and multicast traffic within the network segments or bridging domains associated with the private networks are

set to flood to ensure node discovery completes without incident. Also, allow the use of AVAHI addresses within the VLAN during the node discovery process.

- The private switch must support jumbo frames and must be a managed switch such that it allows for us to set jumbo frames.. This must be done before cluster configuration.

The following figure shows the private network connectivity for the 5551 model:



Data network (eth5 and eth7)

The data network is used for client to NetBackup backup data movement. Bonding between eth5 and eth7 is optional and can be enabled during cluster configuration or later if required. The following bonding modes are supported: balance-alb, balance-tlb, balance-rr, balance-xor, active-backup, broadcast, 802.3ad. If bonding is configured on the switch side, the same bonding method must to be specified when enabling bonding in the cluster.

For details about bonding, see the *About bonding Ethernet interfaces* section of the *Veritas NetBackup™ Flex Scale Administrator's Guide*.

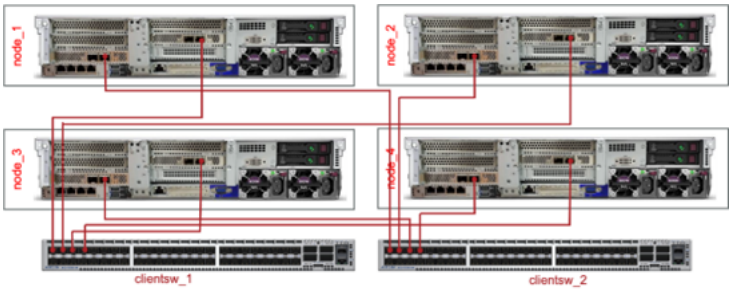
You can keep eth7 network adapter disconnected at the time of initial configuration if you do not want to create a bond on the public data network. You must keep eth7 connected if you want to configure bonding for eth5 and eth7 during the initial configuration. After the initial configuration is complete, if you want to configure a bond on the public data network or want to create secondary data network on eth7, ensure that it is in connected state post initial configuration.

- Each node has two connections to the data network on separate NICs. This provides redundancy in the event one NIC fails.
- The data network runs on 25 GBps or 10 GBps Ethernet. If private network is on 10 GBps, the public network (eth5 and eth7) can be only on 10 GBps. If private network is on 25 GBps, the public network can be either on 10 GBps or 25 GBps.
- Services and containers that utilize the data network:

- Primary container
- Media container (one per node in the cluster)
- MSDP engine container (one per node in the cluster)

- If DNS is utilized, ensure that the data network has connectivity to the DNS server.

The following figure shows the data network connectivity for the 5551 model:



Network requirements

Note the following requirements:

- Private network NICs of all appliance nodes must connect to separate dedicated switches or VLANs 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 172.16.0.0/19 for private network NICs by default. If IP from 172.16.0.0/19 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.
- 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.

- You can choose to have an IPv4 or an IPv6 address for the public network. Mixed mode with an IPv4 and IPv6 is not supported. For example, an IPv6 address for the management network and an IPv4 address for the data network (or vice versa) is not supported.
- The following network configuration is supported:
  - Both the management and the data network in a single subnet, with or without any VLAN.
  - Management and data networks in separate subnet with or without any VLAN, which are reachable from each other.
  - Management and data networks in an isolated subnet with or without any VLAN, which are not reachable from each other.
  - If you add an additional data network, it must be in a separate subnet.

The following details are required for configuring the network settings:

- IP address and subnet mask of the network gateway IP from your existing network
- Gateway details
  Specifying the gateway is optional for the management network if all the components in the management network, such as the API gateway, management console, management DNS, and NTP, AD, and LDAP servers use IP addresses from the same network subnet. As all the components are in the same network subnet, they do not require a gateway IP address to communicate with each other. Similarly, if all the components in the data network, such as the media servers, dedupe engines, primary servers, external primary server, and data DNS use IP addresses from the same network subnet, they do not require the gateway for communication.
  Provide the gateway IP address for the management and the data network only if it is needed for communication with any of the respective network's components. If both the management and the data network are the same and if all components are part of the same subnet, you can skip providing the gateway IP for both management and data 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 short host names or 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 short host names or FQDNs for all the nodes and NetBackup services.

Note: If you configure a DNS, all the IP addresses/FQDNs need not be present in the DNS. The IP addresses and the FQDNs are not required to be resolvable in the DNS. However, if these are present, there should not be a conflict.

If a DNS server is specified and you are using short host names instead of FQDNs, you must also specify the search domain as part of the DNS settings.

The following options are supported for DNS configuration:

- Configure a different DNS server for the management network and the data network. As a 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 short host names or the FQDNs.
- 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 short host names or FQDNs.
- Configure a DNS server only for the management 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 short host names or FQDNs for the data network.
- Configure DNS server only for the data network. Here, you need to specify only the IP addresses for the data network during the cluster configuration, but you must specify both the IP addresses and the corresponding short host names or FQDNs for the management network.
- 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 short host names or FQDNs during the cluster configuration.

  You can either use FQDNs or short host names when you specify the data and management network host names. In the network settings, if a DNS server is specified and short host names are used for configuration, you must also specify the search domain so that the short host names can be resolved.

- 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.

Jumbo frames

Set the maximum transmission unit (MTU) property, which controls the maximum transmission unit size for an Ethernet frame to 9000 bytes. Range is 1500 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 private network (eth4 and eth6 network interfaces) and the public network (eth5 and eth7 network interfaces). To take advantage of jumbo frames, the Ethernet cards, drivers, and switching must all support jumbo frames.

Note: Veritas strongly recommends configuring jumbo frames on private switch interfaces before the cluster configuration and these settings are verified by Veritas manually. For the public network, Veritas cannot verify the settings on the public switch interfaces before the cluster configuration and you must ensure that you verify the settings.

System clock

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

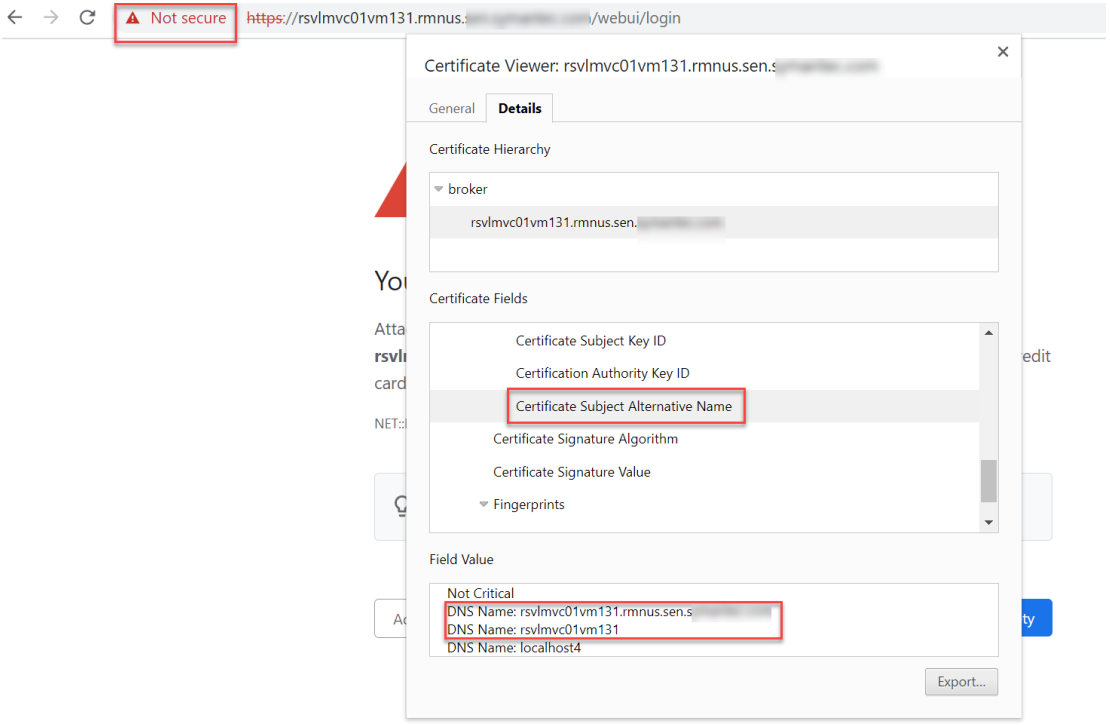
Warning: The cluster configuration may fail if the system clocks are not synchronized across the cluster.

Host names in the NetBackup web service's SSL certificate (for media server-only deployment)

If you plan to deploy a cluster with only media servers, verify the host names in the NetBackup web service's Tomcat SSL certificate. If you attempt to connect to the primary server by using a host name that is not included in the Tomcat web server SSL certificate, the web service connection to the primary server fails.

For version 3.1 and later, ensure that the host name of the primary server is included in the SSL certificate of the NetBackupweb service.

To check the host names in the NetBackup web service's SSL certificate, click the Warning icon in next to the NetBackup web UI URI and click **Show certificate**. Click **Certificate Subject Alternative Name** and note the host names for the DNS entry as shown in the following figure. In the following example, both the host name and FQDN are present in the SSL certificate.



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 port requirements

If a firewall is configured, ensure that the firewall settings allow access to the services and ports used by NetBackup Flex Scale.

Table 2-2 NetBackup Flex Scale ports and services

Port/Type/Direction	Source	Destination	Purpose
22/TCP IN, OUT	SSH client machines	NetBackup Flex Scale management IP	SSH login to host and containers
	NetBackup Flex Scale Management IP	NetBackup Flex Scale Data IP	
53/TCP, UDP IN, OUT	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP	DNS servers	DNS resolution
25/TCP IN, OUT	NetBackup Flex Scale Management IP	SMTP	Sending alerts mail (Email notifications)
389 /TCP, UDP OUT	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP	LDAP	LDAP
636/TCP, UDP OUT			
14161/TCP IN, OUT	NetBackup Flex Scale Management IP of both clusters	Console IP of both clusters Management server FQDN/IP of both clusters	Appliance NetBackup Flex Scale infrastructure management UI
8443/TCP IN, OUT	Jump host/laptop IP to connect web UI	NetBackup Flex Scale Management IP	Cluster configuration web UI (used while configuring the cluster by connecting to a node using its public IP address)
14155/TCP, UDP IN	NetBackup Flex Scale Management IP of both clusters	Heartbeat IP of both clusters	VCS Global Cluster Option (GCO)
4001/TCP, UDP IN	Management Network Client IP Data Network Client IP Jumphost or laptop	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP	mountd NFS mount protocol

Table 2-2 NetBackup Flex Scale ports and services *(continued)*

Port/Type/Direction	Source	Destination	Purpose
755/TCP, UDP IN	Management Network Client IP Data Network Client IP Jump host or laptop	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	NFS statd port
757/TCP, UDP IN	Management Network Client IP Data Network Client IPJumphost or laptop	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	NFS statd port
756 TCP, UDP IN	Management Network Client IP Data Network Client IP Jump host or laptop	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	NFS statd port
4045/TCP, UDP IN	Management Network Client IP Data Network Client IP Jumphost or laptop	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	lockd Processes the lock requests
6667/TCP IN, OUT	Management Network Client IP Data Network Client IP Jump host or laptop	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	VXRSH
11211/TCP IN, OUT	NetBackup Flex Scale Private IP	NetBackup Flex Scale Private IP	Memcached port
7443/TCP IN	NetBackup Flex Scale Private IP	NetBackup Flex Scale Private IP	Hostagent

Table 2-2 NetBackup Flex Scale ports and services *(continued)*

Port/Type/Direction	Source	Destination	Purpose
7080/TCP IN	NetBackup Flex Scale Private IP	NetBackup Flex Scale Private IP	Hostagent
111/TCP, UDP IN	Management Network Client IP Data Network Client IP NetBackup Flex Scale Private IP Jumphost or laptop	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	RPC portmapper services
8080/TCP IN	Management Network Client IP Data Network Client IP NetBackup Flex Scale Private IP	NetBackup Flex Scale Private IP NetBackup Primary server	One GUI NetBackup Flex Scale web UI
67/TCP, UDP IN, OUT	NetBackup Flex Scale Private IP	NetBackup Flex Scale Private IP	DHCP
68/TCP, UPD IN, OUT			
8514/TCP IN	NetBackup Flex Scale Management IP Management Network Client IP	NetBackup Flex Scale Management IP	Log transfer service
2380, 2379/TCP IN	NetBackup Flex Scale Private IP	NetBackup Flex Scale Private IP	ETCD
2049/TCP, UDP IN	NetBackup Flex Scale Data IP Media Server Data Network Client IP	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP Target Storage Server	DataDomain OpenStorage ports nfs++

Table 2-2 NetBackup Flex Scale ports and services *(continued)*

Port/Type/Direction	Source	Destination	Purpose
20048/TCP, UDP IN	NetBackup Flex Scale Management IP Management Network Client IP	NetBackup Flex Scale Management IP	portmapper, NFS, and mountd
445 /TCP IN			CIFS (for the Log/Install shares)
139 /TCP IN			CIFS client to server communication
161/TCP, UDP IN, OUT	Management Network Client IP Jump server or desktop SNMP Server for monitoring	NetBackup Flex Scale Management IP IPMI IP	SNMP
60337/UDP IN	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	
514/UDP IN, OUT	NetBackup Flex Scale Management IP	Syslog Server	rsyslog log forwarding
123 /UDP IN,OUT	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP	NTP servers	NTP synchronization
50000 to 50005/UDP IN, OUT	NetBackup Flex Scale Private IP	NetBackup Flex Scale Private IP	LLT
5353/UDP IN, OUT			

Table 2-2 NetBackup Flex Scale ports and services *(continued)*

Port/Type/Direction	Source	Destination	Purpose
51002/UDP IN, OUT	NetBackup Flex Scale Private IP	NetBackup Flex Scale Private IP	LLT over RDMA
51001/UDP IN, OUT			
162/TCP IN, OUT	Jump server or desktop	NetBackup Flex Scale Management IP IPMI IP	SNMP Monitoring
623/TCP IN	Jump server or desktop	IPMI IP	KVM (optional, used if open)
17990/TCP IN	Jump server or desktop	IPMI IP	iLO
17988/TCP IN			
80/TCP IN	Jump server or desktop	IPMI IP	HTTP
8199/TCP IN, OUT	NetBackup Flex Scale Management IP of both clusters	NetBackup Flex Scale Management IP of both clusters Replication IP of both clusters	Used by Veritas Volume Replicator (VVR) for communication between the vradmind daemons on the Primary and the Secondary.(Required only when catalog replication is configured)
4145/TCP, UDP IN, OUT	NetBackup Flex Scale Management IP of both clusters	NetBackup Flex Scale Management IP of both clusters Replication IP of both clusters	Volume Replicator Connection Server

Table 2-2 NetBackup Flex Scale ports and services *(continued)*

Port/Type/Direction	Source	Destination	Purpose
3269/TCP, UDP IN, OUT	All Clients All Vcenter Servers All ESXi Servers Jjump server or desktop All Primary Servers Ops Center NetBackup IT Analytics	NetBackup Flex Scale Data IP	LDAP GC SSLAD/LDAP SSL/TLS access
8989/TCP IN, OUT	NetBackup Flex Scale Management IP of both clusters	NetBackup Flex Scale Management IP of both clusters Replication IP of both clusters	Volume Replicator Resync Utility

You might need access to additional ports based on the NetBackup features that you plan to use. The following table lists the NetBackup ports and services that you might require for NetBackup Flex Scale. For more details about the ports that are used by NetBackup, see the *Veritas NetBackup™ Network Ports Reference Guide* on SORT.

Table 2-3 NetBackup ports and services

Port/Type/Direction	Source	Destination	Purpose
13724/TCP IN, OUT	NetBackup Flex Scale Data IP NetBackup clients	NetBackup Flex Scale Data IP NetBackup clients	NetBackup vnetd (NetBackup Network service)
443/TCP IN, OUT	Jump host/laptop IP to connect we bUI	NetBackup Primary IP NetBackup Flex Scale Data IP NetBackup Flex Scale Management IP	NetBackup web UI
1556/TCP IN, OUT	NetBackup Primary IP All NetBackup media IP NetBackup clients	NetBackup Primary IP All NetBackup media IP	NetBackup PBX

Table 2-3 NetBackup ports and services *(continued)*

Port/Type/Direction	Source	Destination	Purpose
10101/TCP IN	Management Network Client IP Data Network Client IP NetBackup Flex Scale Private IP NetBackup Clients	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	MSDP Controller and Proxy
10100/TCP IN			
10102/TCP IN, OUT	Management Network Client IP Data Network Client IP NetBackup Flex Scale Private IP NetBackup Clients	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	Deduplication Manager (spad)
10082/TCP IN, OUT			Deduplication Engine (spoold)
10086/TCP IN			NetBackup web service
13786/TCP IN			NetBackup (OpsCenter report generation, primary server)
13783/TC IN			NetBackup (nbatd, primary server, previously vopied)
13782/TCP IN			NetBackup (bpcd, primary and media servers, clients)

Table 2-3 NetBackup ports and services *(continued)*

Port/Type/Direction	Source	Destination	Purpose
13701/TCP IN	Management Network Client IP Data Network Client IP NetBackup Clients	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	NetBackup (vmd, Media servers)
13702/TCP IN			NetBackup (robotic and control daemons, media servers)
13703 to 13719/TCP IN			NetBackup services
13720/TCP IN			NetBackup (bprd, primary server)
13721 TCP IN			NetBackup (bpdbm, primary server)
13722/TCP IN			NetBackup (nbazd, primary server, previously bpjava-msvc)
13723/TCP IN			NetBackup (bpjobd, primary server)
8446/TCP IN	Management Network Client IP Data Network Client IP NetBackup Flex Scale Private IP Copilot Client	NetBackup Flex Scale Management IP NetBackup Flex Scale Data IP NetBackup Flex Scale Private IP	NetBackup (Copilot)

Note the following conventions used in the tables above:

- NetBackup Flex Scale Management IP: IP address assigned to eth1 or bond interface (eth1,eth2)
- NetBackup Flex Scale Data IP: Media, Storage, Primary Server IP address, Secondary Data Network IP address (IP assigned to eth5, eth7 or bond of eth5 and eth7)
- NetBackup Flex Scale Private IP: IP address assigned to eth4, eth6

- Management Network Client IP: Any machine that the customer wants to reach to NetBackup Flex Scale cluster nodes management IP for some business use case (Any Linux, Windows Machine or syslog server or monitoring server, jump host)
- Data Network Client IP: Any NetBackup supported client machine that the customer wants to reach to NetBackup Flex Scale cluster nodes Data IP for some business use case. (Any Linux, Windows Machine, NBU Clients, DB clients, Fibre Channel Clients, VMware Clients, CloudCatalyst, CloudStore, Copilot, OpenStorage, Kubernetes, Microsoft SQL server, MySQL, Nutanix AHV, HBASE, Hadoop, Hyper-V, mongoDB, openStack, Oracle)

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.

Considerations for configuring disaster recovery

If you wish to configure the appliance for disaster recovery (DR), in addition the requirements described in See "NetBackup Flex Scale configuration requirements" on page 10., 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

Chapter 3

Best practices

This chapter includes the following topics:

Management network connectivity

The eth1 port of the node is connected to the management network. Use the `ping` command to verify if the management network is available and the nodes are reachable:

`ping -I` *`eth1-interface-ip destination-ip`*

eth1-interface-ip is the IP address assigned to the eth1 interface.

destination-ip is the destination IP address.

For example:

```
mgmtip22.nbfs.com:~ # ping -I 192.168.70.22 192.168.70.10
PING 192.168.70.10 (192.168.70.10) from 192.168.70.22 : 56(84) bytes
 of data.
64 bytes from 192.168.70.10: icmp_seq=1 ttl=64 time=0.267 ms

--- 192.168.70.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.267/0.267/0.267/0.000 ms
mgmtip22.nbfs.com:~ #
```

If the customer's site does not allow the usage of `ping` command, use the `arping` command instead:

```
arping -I eth1 ipaddress
```

Verify the entries in the routing table for all the nodes:

```
network route show nodename=nodename
```

Private network connectivity

NetBackup Flex Scale uses Avahi to discover the nodes in the private network. When you scan for the nodes that can be added to cluster, Avahi scans the private network and displays all the detected nodes in this network.

NetBackup Flex Scale uses IP address 172.16.0.0/19 for private network NICs by default. If IP from 172.16.0.0/19 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.

To check private network connectivity:

1. Use SSH and log in to the node using the default administrator credentials:

   username: *admin*

   password: *P@ssw0rd*

2. Run the `support elevate` command to elevate to the bash prompt.

   To check if the private network is accessible, run the following command:

   ```
   /opt/IMAppliance/ansible/roles/avahi/bin/mdns-config | jq
   ```

   The following example shows the sample output for four nodes:

```
[
  {
    "domain": "local",
    "hostname": "VTAS9031105",
    "ip": "172.1.2.3",
    "ipv6": "fd00::2"
  },
  {
    "domain": "local",
    "hostname": "VTAS9031104",
    "ip": "172.1.2.4",
    "ipv6": "fd00::3"
  },
  {
    "domain": "local",
    "hostname": "VTAS9031103",
    "ip": "172.1.2.5",
    "ipv6": "fd00::4"
  },
  {
    "domain": "local",
    "hostname": "VTAS9031102",
    "ip": "172.1.2.6",
    "ipv6": "fd00::1"
  }
 ]
```

3 To verify all the nodes in the private network can be discovered, run the following command:

```
avahi-browse -d local _discovery._sub._http._tcp -rt
```

The following example shows the sample output. Ensure all the nodes in the private network are displayed.

```
site1-01:~ # avahi-browse -d local _discovery._sub._http._tcp -rt
+   eth4 IPv6 VTAS9031103                                   Web Site
             local
+   eth4 IPv6 VTAS9031104                                   Web Site
             local
+   eth4 IPv6 VTAS9031102                                   Web Site
             local
+   eth4 IPv6 VTAS9031105                                   Web Site
             local
+   eth4 IPv4 VTAS9031103                                   Web Site
             local
+   eth4 IPv4 VTAS9031104                                   Web Site
             local
+   eth4 IPv4 VTAS9031102                                   Web Site
             local
+   eth4 IPv4 VTAS9031105                                   Web Site
             local
=   eth4 IPv6 VTAS9031102                                   Web Site
             local
   hostname = [VTAS9031102.local]
   address = [fd00::1]
   port = [12345]
   txt = []
=   eth4 IPv4 VTAS9031102                                   Web Site
             local
   hostname = [VTAS9031102.local]
   address = [172.1.2.3]
   port = [12345]
   txt = []
=   eth4 IPv6 VTAS9031104                                   Web Site
             local
   hostname = [VTAS9031104.local]
   address = [fd00::3]
   port = [12345]
   txt = []
=   eth4 IPv4 VTAS9031104                                   Web Site
```

```
            local
   hostname = [VTAS9031104.local]
   address = [172.1.2.4]
   port = [12345]
   txt = []
=   eth4 IPv6 VTAS9031103                                   Web Site
            local
   hostname = [VTAS9031103.local]
   address = [fd00::4]
   port = [12345]
   txt = []
=   eth4 IPv4 VTAS9031103                                   Web Site
            local
   hostname = [VTAS9031103.local]
   address = [172.1.2.5]
   port = [12345]
   txt = []
=   eth4 IPv6 VTAS9031105                                   Web Site
            local
   hostname = [VTAS9031105.local]
   address = [fd00::2]
   port = [12345]
   txt = []
=   eth4 IPv4 VTAS9031105                                   Web Site
            local
   hostname = [VTAS9031105.local]
   address = [172.1.2.6]
   port = [12345]
   txt = []
site1-01:~ #
```

If the 172.16.x.x IP range is restricted in the customer's environment, you must change the IP addresses assigned to the private NICs.

Configuring AutoSupport for the appliance

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

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 lets you manage such issues before they have an adverse effect on your production environment.

You must enable Call Home to allow your appliance to connect with a Veritas AutoSupport server and upload hardware and software information. Call Home alerts you and Veritas in the event of critical conditions that may affect the operational capability of the system, such as hardware component failure. Call Home uploads hardware and software information to a secure Veritas AutoSupport server when an alert is detected. This information may be used by Veritas to proactively open a support case with Technical Support. A Technical Support Engineer contacts you to further diagnose the issue, such as gathering logs and to arrange for replacement field service of the reported component, if needed. The collected hardware information generally includes the information about the appliance hardware and software state, events, configuration, and performance data. The appliance uses the HTTPS protocol and uses port 443 to connect to the Veritas server.

Call Home monitors the following hardware components as they apply to your specific appliance model:

- CPU
  Fan
- Disk
- Power supplies
- DIMM
- Firmware
- Environmental telemetry data
  - System temperature
  - System voltages
  - Fan speeds
  - BBU charge status
  - RAID controllers
  - RAID volume groups
  - System board components by the Integrated Platform Management Interface (IPMI) and the Baseboard Management Controller (BMC) chip
- Storage subsystems (shelves and interconnects)

If Call Home is disabled and an alert condition occurs, the appliance only generates a local email or an SNMP trap to notify you of the alert.

SMTP configuration is required for alerting your internal teams to any hardware or software issues affecting the appliance. You must either configure your mail server to allow the appliance to use it as a mail relay or create an account for the appliance on your mail server and supply login credentials.

Necessary software

Download and install the following software:

- Putty or another SSH client. This is a helpful tool to connect to the appliance node and log on the appliance command-line interface.
- A workstation capable of mounting a CIFS or an NFS share to the appliance or a workstation capable of SCP connections from the appliance. This is needed to transfer files, such as Emergency Engineering Binaries (EEBs), patches, firmware updates, and DataCollect logs.

Chapter 4

NetBackup Flex Scale tuning and sizing

This chapter includes the following topics:

Assigning media servers to a storage server

When you configure a storage policy in NetBackup, you can choose a specific media server. This option restricts the media server you can use at the time the policy is run. However,NetBackup Flex Scale uses its own internal load-balancing mechanism to choose the media server. Ensure that you configure the storage units to use **Any Available media server** option to make the storage unit available to any of the media servers. An alert is generated for NetBackup Flex Scale if a specific media server is specified.

NetBackup Flex Scale tuning

Recommended # of VMs per ESXi for VMware backup

This parameter is set for VMware workloads. When the number of VMs is less than or equal to two per ESXi host, the performance is linear. Set this value to 5 on the ESXi host.

Latency between sites during replication

Network latency between primary and secondary site should be minimal. The recommended value is less than 2 ms. You must have a reliable network with

minimal packet drops and reordering. There should not be a Network Address Translation (NAT) based firewall between the source and the target sites.

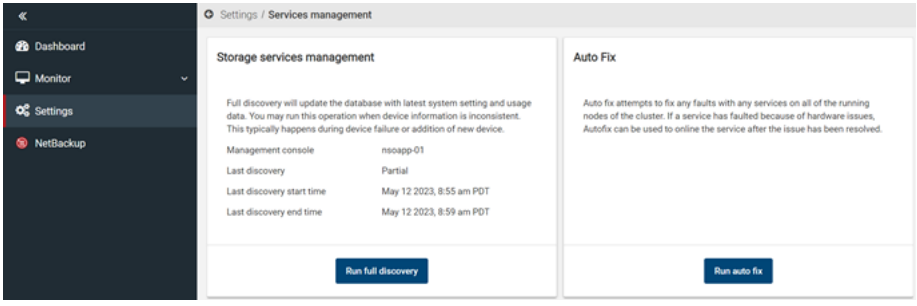
Chapter 5

Troubleshooting NetBackup Flex Scale

This chapter includes the following topics:

Services management

You can use the **Settings > Services management** tab to manage your storage services.



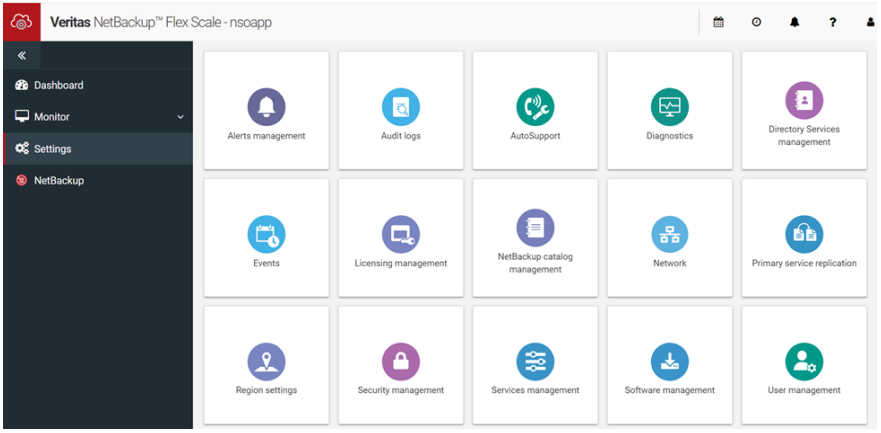
When there is a device failure or a new device is added, the device information may not be consistent. In such a scenario, you can **Run full discovery** to update the database with latest system settings and usage data.

You can fix service-related faults in the nodes of the cluster that are in running state. If a service has faulted because of issues in services such as the volume manager, NLM, deduplication, or the management console, you can **Run auto fix** and bring the service online after the issue has been resolved. No other operation should be initiated when you run AutoFix.

You can also call the `POST/api/appliance/v1.0/management/autofix` RESTful API to run auto fix.

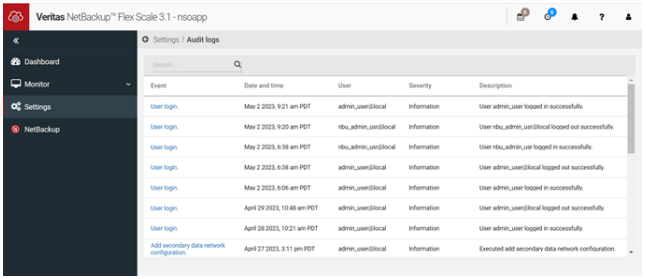
Audit logs

You can use the **Settings > Audit logs** tab to view the list of operations or events that are performed from the GUI or cluster-level CLI. All the operations and events which are triggered are logged on an audit log file as a single entry.



The following information is displayed for each operation or event:

- Event: This specifies the name of the operation or event.
- Date and time: This specifies the date and time when the operation or event was completed.
- User: This specifies the user who initiated the operation or event.
- Severity: This specifies the severity of the logged message for the operation or event.
- Description: This gives information about the operation or event.



You can also search for events by using the search box that is present above the audit log entry table. The search can be done based on event name, username, severity, description or sub-string of description.

The audit logs can be collected as part of **Infrastructure** module from the **Basic** tab of **Generate Log Package**. After you extract the collected log package, the audit logs are present in the `infrastructure/auditlog` directory. The audit logs can also be collected from the **Advanced** tab of **Generate Log Package**. You can collect the audit log file from `/vx/MASTER_LOG_FS/auditlog/auditlog.log` location in the **Advanced** tab.

The audit log captures the operation or event that a user has initiated. If that operation involves execution of some suboperations, then those suboperations also get logged as a new audit log entry.

Collecting logs for cluster nodes

You can collect logs for an individual node in the cluster or for all the cluster nodes for error analysis and troubleshooting. You can choose to collect logs for all the components to get a comprehensive view of the system, or you can collect logs for specific components that have an issue.

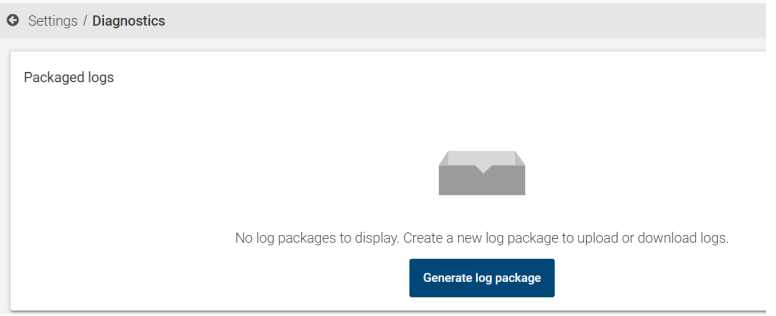
1. Use any one of the following options to log in using the user account that you created:

   - 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, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Cluster Management > Cluster settings > Diagnostics**.

- 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, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Settings > Diagnostics**.

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

2 Click **Generate log package**.



On the Generate log package page, on the Basic tab you can select components or on the Advanced tab you can select individual log files to include in the log package.

3 To select the components for which you want to collect logs:

- On the **Basic** tab under **Log settings**, select the components. To select all the components, click **All**.

Component	Description
Service status	Status of the services running on the cluster nodes
OS	Kernel and user-level debug logs.

Component	Description
Infrastructure	Generic product information, including stack trace for running daemons, policy-based storage provisioning logs, and API gateway logs.
Explorer	Logs and system environment data collected by the `VxExplorer` utility.
Initial deployment	Initial cluster configuration logs. Installation logs are located in the `/opt/VRTS/install/logs/` directory.
NetBackup primary service	Logs for NetBackup server services and components. This component is displayed only if both NetBackup primary and media servers are deployed in the cluster.
Appliance	Hardware-specific logs. Includes HPE Active Health System (AHS) logs. **Note:** If High Security mode is enabled in the HPE iLO Remote Console, AHS logs cannot be downloaded locally and are not included in the log package. To download the AHS logs, log in to the iLO Remote Console. Click **Information > Active Health System Log**. On the Active Health System Log page click **Download**.
NetBackup media service	NetBackup media server logs from nodes.
Upgrade	Upgrade logs.
NetBackup MSDP	Deduplication engine logs for all nodes.
NBSU	Information collected using the NetBackup Support Utility tool.
Performance logs	Logs for collecting performance data.
Common logs	Collect these logs when you are not sure of the exact nature of the problem. These logs can act as a initial pointer to diagnose the actual problem.

- Under **Historical logs**, you can collect archived logs or logs for a specific duration. To include historical logs, click **Archived logs**. To include logs for a specific duration, click **Select date range** and select the duration or select **Custom range** to customize the duration by specifying the start and the end date. Including logs for a specific time period reduces the size of the generated log package and the time required to collect the logs. You

can collect time-based logs for **Infrastructure**, **OS**, **NetBackup primary service**, and **NetBackup media service** components.

- Under **Package options**, specify a name for the log package and optionally the case number if provided by Veritas Support.
- Under **Nodes**, select the nodes for which you want to collect the logs.

Note: If you switch from Basic to Advanced view (or vice versa), all the options that you specified until that point are lost and you will have to specify them again.

---

4 To select individual log files:

- On the **Advanced** tab under **Log settings** expand the nodes and select the log files.
- Under **Package options**, specify a name for the log package and optionally the case number if provided by Veritas Support.

5 Click **Generate**.

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

See "Downloading logs" on page 48.

See "Uploading logs to Veritas Support" on page 47.

Uploading logs to Veritas Support

You can share the logs with the Support personnel to help you diagnose problems.

1 Use any one of the following options to log in using the user account that you created:

- 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, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Cluster Management > Cluster settings > Diagnostics**.

- 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, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Settings > Diagnostics**.

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

2. The existing log packages are displayed under **Packaged logs**.
3. Click the package that you want to upload to and click **Send**.

   On the **Send logs** dialog box, select the following option, specify the details and then click **Send**.

   - **Send using SFTP**: Use the SSH File Transfer Protocol to upload the logs. Specify the following details to use SFTP:

Field	Description
Server address	Remote server name
Port	Port number. By default the SFTP server is configured to listen to port 22.
User name	User name to authenticate with the server
Password	Password to authenticate with the server
Path	Location to upload the logs

Downloading logs

If a node is a part of the cluster, you can download log packages from the node. For information about how to collect logs and create log packages, see Collecting logs for cluster nodes

1. Use any one of the following options to log in using the user account that you created:

   - 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, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Cluster Management > Cluster settings > Diagnostics**.
   - 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, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Settings > Diagnostics**.

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

2. The log packages that are already created are displayed under **Packaged logs**.
3. Click the log package that you want to download and click **Download**.
4. On the **Download logs** dialog box, click **Download**.

Forwarding logs to an external server

You can forward system logs from a NetBackup Flex Scale cluster to an external log management server. System logs (syslog) contain event and notification messages in a specific format. Forwarding the appliance syslogs to an external log management server provides system administrators a centralized location for viewing logs and for further analysis and troubleshooting. The following log servers are supported:

- HP ArcSight

- Splunk

NetBackup Flex Scale appliances use the Rsyslog client to forward logs. In addition to HP ArcSight and Splunk, other log management servers that support the Rsyslog client can also be used to receive syslogs from the appliance.

To secure the log transmission from the appliance to the log management server, you can use the TLS (Transport Layer Security) option. NetBackup Flex Scale currently supports only TLS Anonymous Authentication for log forwarding.

Configuring log forwarding

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

Alerts are generated if the settings on the cluster nodes are inconsistent or if one of the cluster nodes is down and unable to forward the logs to the log server. When you add a node to the cluster, the log forwarding settings are synced to the newly added node.

To configure log forwarding:

1. Use any one of the following options to sign in:
   - 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, the FQDN, or the short host name that you specified for the management server during the cluster configuration, and then in the left pane do one of the following:
     - Click **Cluster Management > Cluster settings > Security management > Log forwarding**
     - Click **Cluster Management > Cluster dashboard > Security Meter > View details > Auditing and alerting > Log forwarding**
   - 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, the FQDN, or the short host name that you specified for the management server and do one of the following:
     - Click **Dashboard > Security Meter > View details > Auditing and alerting > Log forwarding**

- Click **Settings > Security management > Log forwarding**

2 Click **Configure**.

3 Enter the following details:

Field	Description
Server FQDN or IP address	FQDN or the IP address of the external log management server.
Server port	Port number of the external log management server. Default port is 514. You can specify a different port if the cluster nodes are configured to communicate with the log server using that port.
Protocol	Select either UDP or TCP. TCP is the default protocol. With TCP protocol, you can optionally enable TLS log transmission. **Note:** Enabling TLS requires that you upload certificates obtained from CA authority and a private key to the appliance.
Log polling interval	Set the interval in minutes for forwarding the syslogs to the external log server. The options are **15**, **30**, **45**, **60**, **Continuous**. If you select **Continuous**, the appliance continuously forwards logs to the log server.
Device vendor	Unique name for the external log server.
Enable TLS log transmission	If you want to secure the transmission of logs from the appliance to the log server, select **Enable TLS log transmission** and upload the required certificate files. Veritas recommends that you enable TLS for security purposes. This option provides end-to-end security of data sent over the network from the appliance to the log server. You need a CA certificate and the client private key to configure TLS log transmission. This option is available only if you select the TCP protocol. If you enable secure log transmission, upload CA certificate (X.509 certificate for the certificate authority in PEM format), client certificate (X.509 certificate for the appliance to communicate with the log management server, in PEM format), and client certificate key (RSA key of the client certificate) onto your log server and then upload the certificates to the appliance.

Field	Description
Modules	Types of logs that are forwarded to the log server. Only the OS logs are forwarded and the **syslog** option is selected by default.

4 Click **Enable**.

A notification about the task is displayed on the top of the page. To monitor the progress, click **View details**. After the configuration is completed successfully, a notification is displayed on top of the page. The log forwarding status is shown **Enabled** and the start time for forwarding the logs is displayed.

Modifying log forwarding settings using the UI

You can edit only the scheduled interval for forwarding the logs. To edit any other settings, delete the configured log server settings and reconfigure log forwarding.

To edit the settings:

1 Use any one of the following options to sign in:

- 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, the FQDN, or the short host name that you specified for the management server during the cluster configuration, and then in the left pane do one of the following:
  - Click **Cluster Management > Cluster settings > Security management > Log forwarding**
  - Click **Cluster Management > Cluster dashboard > Security Meter > View details > Auditing and alerting > Log forwarding**
- 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, the FQDN, or the short host name that you specified for the management server and do one of the following:
  - Click **Dashboard > Security Meter > View details > Auditing and alerting > Log forwarding**

- Click **Settings > Security management > Log forwarding**

2 Under **Log polling interval**, click **Edit**.

3 Select the time interval and click **Save**.

A notification is displayed on the top of the page. To monitor the progress, click **View details**. After the task is completed successfully a notification is displayed on the top of the page and the changed interval is displayed in the UI.

Removing log forwarding

To stop forwarding logs:

1 Use any one of the following options to sign in:

- 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, the FQDN, or the short host name that you specified for the management server during the cluster configuration, and then in the left pane do one of the following:
  - Click **Cluster Management > Cluster settings > Security management > Log forwarding**
  - Click **Cluster Management > Cluster dashboard > Security Meter > View details > Auditing and alerting > Log forwarding**
- 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, the FQDN, or the short host name that you specified for the management server and do one of the following:
  - Click **Dashboard > Security Meter > View details > Auditing and alerting > Log forwarding**
  - Click **Settings > Security management > Log forwarding**

2 Click **Remove**.

A notification is displayed on the top of the page. To monitor the progress, click **View details**.

Error messages displayed during the pre-upgrade check

The following table lists the error messages that you may come across during the pre-upgrade check, which runs automatically when you start the appliance upgrade:

Table 5-1

Error message	Recommended action
Errors that are displayed during the system self-test.	The appliance runs a self-test to check the current status of the various appliance components. Review the checks for which the status is displayed as FAILED. Try to correct the issue and retry the operation. If the issue persists, use the `support data-collect` command to collect logs and contact Veritas Technical Support.
V-409-776-30019: The password for user *username* will expire in *number_of_days* days.	Change the password before upgrading the appliance.
V-409-776-1111: One or more USB devices are attached to the appliance.	Remove all the attached USB mass storage devices from the appliance, and then try again.
V-409-776-30014: The docker daemon is not configured correctly.	Contact Veritas Technical Support and refer them to article 100051459.
V-409-776-30053: The password for user username is set to the default password.	For increased security, forced password changes are enforced to ensure that known default passwords do not exist on the system. Change the default password before upgrading the appliance.
V-409-776-30054: The password for the IPMI user username is set to the default password.	For increased security, forced password changes are enforced to ensure that known default passwords do not exist on the system. Change the default password for the IPMI user before upgrading the appliance.
V-409-776-30078: GRUB configuration file check failed.	The file /boot/grub2/grub.cfg was modified after system startup. Revert the changes by updating the parameters in the grub.cfg file as per the values that are set in /proc/cmdline.

Table 5-1 *(continued)*

Error message	Recommended action
V-409-776-30117: Failed to get the list of installed EEBs from the cluster nodes.	Contact Veritas Technical Support.
V-409-776-30118: The following EEBs are not installed on node *nodename*: *eeblist*.	Contact Veritas Technical Support and refer them to article 100055285.
V-409-776-1120: The space size is not enough.	Contact Veritas Technical Support to free up space by deleting unwanted files.
V-409-776-1128: Insufficient disk space detected during a pre-upgrade check.	The upgrade process requires a minimum of *size* MB free space under the system disk group.
V-409-776-30033: Unable to resize *directoryname* during an upgrade.	The amount of space used by *directoryname* is greater than the allocated size *size*M. Free up space by deleting unwanted files from *directoryname*.
V-409-776-1105: The current appliance version is same as the software release update version.	View the software version running on the appliance using the `show appliance status` command. Download a newer software release update from the Veritas Download Center.
V-409-776-1106: This appliance has already been running with a version that is greater than the patch version.	View the software version running on the appliance using the `show appliance status` command. Download a newer software release update from the Veritas Download Center.
V-409-776-1112: The appliance isn't *modelnum*.	The appliance model is not a NetBackup Flex Scale appliance. The downloaded software release update is for a NetBackup Flex Scale appliance model.
V-409-776-1121: Version check failed.	Contact Veritas Technical Support.
V-409-776-30050: Upgrading from version *currentversion* to *version* is not supported.	Download a supported upgrade release from the Veritas Download Center.
V-409-776-30030: NetBackup version compatibility check failed. NetBackup media container is not healthy.	Contact Veritas Technical Support to resolve the issue.

Table 5-1 *(continued)*

Error message	Recommended action
V-409-776-30031: NetBackup version compatibility check failed. Failed to get the NetBackup media server version.	Contact Veritas Technical Support to resolve the issue.
V-409-776-30032: NetBackup version compatibility check failed. Failed to get the NetBackup primary server version.	Contact Veritas Technical Support to resolve the issue.
V-409-776-30024: NetBackup version compatibility check failed.	The NetBackup media version is later than the primary server version. Upgrade the NetBackup primary server and make sure that the primary server version is later than or the same as the media server.
V-409-776-30042: Unable to access the target cluster that is set up for replication.	Contact Veritas Technical Support to resolve the issue.
V-409-776-30034: Unable to start the Contact Veritas Technical Support. appliance upgrade because volume recovery tasks are in progress.	Contact Veritas Technical Support.
V-409-776-30044: One or more VxFS file systems are full. Unable to start the appliance upgrade because there is no free space on one or more VxFS file systems.	Contact Veritas Support and ask them to refer to article 100052630.
V-409-776-30076: The NetBackup license has expired or is not valid.	Add a valid NetBackup license or contact Veritas Technical Support.
V-409-776-30077: One or more licenses have expired, or the usable capacity is more than the licensed capacity and you no longer meet compliance standards.	Add a new license to resolve the issue.
V-409-776-30087: Syntax validation failed for the Veritas Cluster Server (VCS) configuration file.	Contact Veritas Technical Support and refer them to article 100054029.
V-409-776-30111: Unable to proceed with the upgrade because the disaster recovery configuration is incorrect.	Contact Veritas Technical Support and ask them to refer to article 100055193.

Table 5-1 *(continued)*

Error message	Recommended action
V-409-776-30116: NetBackup health check failed. The primary server, media server, or the deduplication engine container returned an unhealthy state.	Contact Veritas Support and refer them to article 100055286.
V-409-776-1117: The cluster is not in a valid state for upgrade. A cluster should contain at least four nodes.	Unable to retrieve the node list because of an internal error. Contact Veritas Technical Support.
V-409-776-1113: The cluster is not in a valid state for upgrade. One or more nodes are not in the cluster.	The nodes must be a part of the cluster. Contact Veritas Technical Support.
V-409-776-1114: The cluster is not in a valid state for upgrade. Appliance version is not consistent across the cluster.	The appliance version must be the same for all the nodes in the cluster. Contact Veritas Technical Support.
V-409-776-1125: One or more disks under a volume are not in proper state.	One or more disks reported unhealthy status. Contact Veritas Technical Support.
V-409-776-1110: The service group check failed.	All the service groups are not online. Use the `support services autofix` command from the cluster-level command-line interface to resolve this problem.
V-409-776-1127: Add/Replace node operation is ongoing. Cannot proceed with the upgrade.	Wait for the ongoing operation to complete and then try again.
V-409-776-30163: An OpsCenter server is configured for the NetBackup primary server	To unconfigure the OpsCenter server, log in to the primary server using `ssh` *`NetBackup primary server admin user@NetBackup primary server IP or FQDN`* and delete the OPS_CENTER_SERVER_NAME entry from the `/mnt/nbdata/usr/openv/netbackup/bp.conf` file.

Table 5-1 *(continued)*

Error message	Recommended action

V-409-776-30182: 3005 UID/GID is not free on the cluster	■ Go to the Support Shell environment. Find out the user who has occupied 3005 UID or GID or both.
	■ To check which user has used 3005 UID:
	`getent passwd 3005`
	■ To check which user has used 3005 GID:
	`getent group 3005`
	■ If 3005 UID is occupied by a local user, and this user does not use CIFS, S3 or NFS, delete that user from GUI and add it back again.
	After deleting the local user , if 3005 GID is still not free, contact Veritas Technical Support.
	■ If 3005 UID is occupied by any other user contact Veritas Technical Support.

Troubleshooting NetBackup Flex Scale issues

This section describes common issues that you might encounter when using NetBackup Flex Scale and possible solutions for those issues.

If cluster configuration fails (for example because an IP address that was already in use is specified) and you try to reconfigure the cluster, the UI displays an error but the configuration process continues to run

Cause

If the license key was already registered when the cluster configuration failed and you try to reconfigure the cluster, an error registering the license key is reported in the UI but the configuration process continues to run. The error is displayed in the UI because the configuration process tries to install the same license key which was installed previously during the cluster configuration. However, the configuration process is not terminated and continues to run.

Solution

Before you reconfigure the cluster, delete the license key from all the nodes using the following steps:

1. Log on to each node using the following credentials:

   User: admin

   Password: P@ssw0rd

   The NetBackup Flex Scale Appliance Shell Menu is displayed.
2. To access the root shell type the `support elevate` command.

   To access the root shell when lockdown mode is configured,
3. Run the following command to delete the license key:

   ```
   rm /etc/vx/licenses/lic/Access_Perpetual.slf
   ```

Validation error while adding VMware credentials to NetBackup

For protecting VMware virtual machines, you add the login credentials of the VMware vCenter Server, VMware ESXi server, or VMware vCloud Director server to the NetBackup configuration. While adding the access credentials, you may see the following credential validation error in the NetBackup Java Console UI.

```
VMware credential validation failed. Cannot connect on socket (Status 25)
```

Cause

This issue occurs when the NetBackup Flex Scale appliance cluster is configured using a pure IPv6 address configuration while the VMware system uses IPv4 addresses. NetBackup Flex Scale appliance does not support communication between a pure IPv6 and a pure IPv4 address configuration.

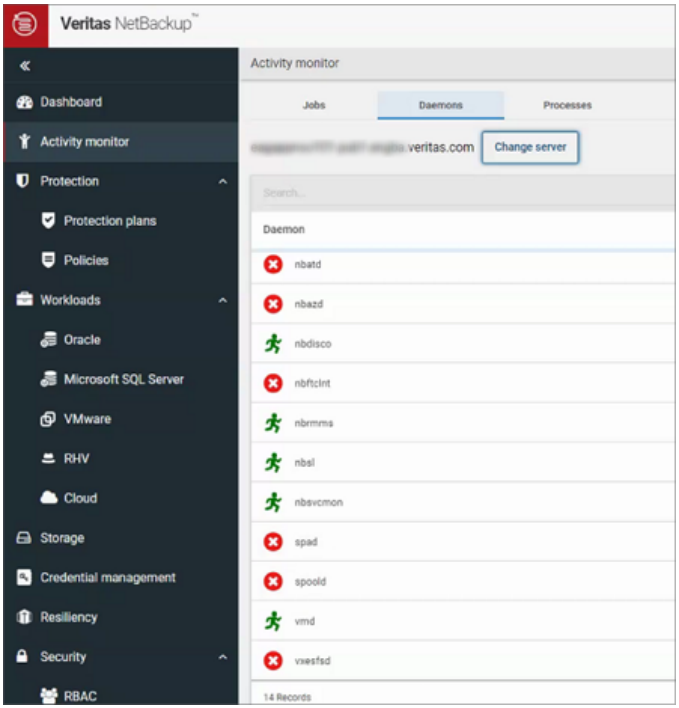
Solution

To resolve this issue, the VMware system must be configured to use either a pure IPv6 address or a mixed mode dual stack IP address configuration.

NetBackup Web UI incorrectly displays some NetBackup Flex Scale processes as failed

The **Activity Monitor > Daemons** tab in the NetBackup Web UI displays the status of the NetBackup processes running in your NetBackup environment. Sometimes, the status of the NetBackup Flex Scale processes such as `spad` and `spoold` may

appear as failed even though the processes themselves are running fine in the cluster.



Solution:

There is no solution at the moment. It is safe to ignore the incorrect status displayed in the NetBackup Web UI.

Unable to create BMR Shared Resource Tree (SRT) on NetBackup Flex Scale Appliance

Cause

This issue occurs because configuration of Bare Metal Restore (BMR) boot server is not supported on the NetBackup Flex Scale Appliance. The following error message is displayed:

```
Failed to setup loop device: No such file or directory.
Cannot mount media, please try again.
```

Solution

You can create a platform specific boot server separately based on the client OS platform which needs to be restored.

NetBackup configuration files are not persistent across operations that require restarting the system

The `VmTools.cfg` and `vixDiskLib.ini` files do not persist after a node is restarted as a part of an operation such as upgrading or replacing a node.

Workaround:

Use the `cp-nbu-config` command to copy the NetBackup configuration files from the user's home space to the specified NetBackup configuration destination directory. A NetBackup administrator can use the `cp-nbu-config` command to create and edit a NetBackup touch configuration file in any of the following directories:

- `/usr/openv/netbackup`
- `/usr/openv/netbackup/bin`
- `/usr/openv/java`
- `/usr/openv/lib/ost-plugins`
- `/usr/openv/netbackup/bin/snapcfg`
- `/usr/openv/netbackup/db/cloudSnap/credential`
- `/usr/openv/netbackup/db/cloudSnap/proxy`
- `/usr/openv/netbackup/db/config`
- `/usr/openv/netbackup/db/event`
- `/usr/openv/netbackup/db/images`
- `/usr/openv/netbackup/db/media`
- `/usr/openv/netbackup/ext/db_ext`
- `/usr/openv/netbackup/ext/db_ext/db2`
- `/usr/openv/var`
- `/usr/openv/volmgr`
- `/usr/openv/volmgr/database`

To create or edit a touch configuration file

1. Log in to the node.
2. Create a new configuration file in the NetBackup administrator home directory, or use the `cp` command to copy an existing configuration file from its original location to the home directory. For example:

   ```
   cp /usr/openv/lib/ost-plugins/pd.conf ~/
   ```

3. Make changes to the file in the home directory.
4. Run the following command to install the file in its original directory or a supported destination directory:

   sudo /opt/veritas/vxapp-manage/cp-nbu-config *configuration-file destination*

   where *configuration-file* is the file that you created or edited, and *destination* is the directory where it needs to be installed.

   ```
   sudo /opt/veritas/vxapp-manage/cp-nbu-config ~/pd.conf
   /usr/openv/lib/ost-plugins
   ```

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 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.

Resource monitoring and remediation

In NetBackup Flex Scale 3.2.100, if memory utilization reaches the threshold of 97%, the NetBackup Flex Scale node is brought down. You can confirm that the node is down in the following ways.

- The ASC `/log/autosupport/collector.log` file has a `INFO` level log entry with a value greater than or equal to 97. Search for the value of the `memory used_percentage` parameter in the `collector.log` file.
- A crash dump file gets created on the system default path.
- The system logs have entry for node reboot.