NetBackup™ Clustered Primary Server Administrator's Guide

Windows, UNIX, and Linux

Release 11.2.0.1

COHESITY

NetBackup™ Clustered Primary Server Administrator's Guide

Last updated: 2026-09-09

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

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. COHESITY 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.

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 to NetBackup primary server clustering 7

About NetBackup clustering 7
About security certificates in NetBackup 8
NetBackup clustering in virtual environment 8
About NetBackup failover server data protection in a cluster 8
About NetBackup failover server support 9
NetBackup supported cluster solutions 9
About NetBackup limitations with clustering solutions 10

Chapter 2 NetBackup in a Windows Server Failover Clustering 11

About NetBackup on Windows Server Failover Clustering 11
Installation prerequisites for NetBackup on WSFC cluster 12
Installing a NetBackup failover server on WSFC cluster 13
Configuring a NetBackup server on WSFC cluster 14
Upgrading a NetBackup failover server on WSFC cluster 15
Restoring the cluster quorum 17
Restoring the cluster quorum to a node with directory services 18
Preparation for disaster recovery of WSFC 19
Disaster recovery of WSFC 19
Recovering the entire WSFC cluster 20
Recovering all shared disks 20
About recovering NetBackup data on a shared disk 21

Chapter 3 NetBackup in a Veritas Cluster Server on Linux 22

About NetBackup on a Veritas Cluster Server on Linux 22
Installation prerequisites for NetBackup on VCS on Linux 23
About preinstallation checklist for a NetBackup failover server installation on VCS on Linux 24
NetBackup installation information for all VCS configurations 24
NetBackup installation information for specific VCS configurations 25

Installing a failover NetBackup server on VCS on Linux 26
Configuring a failover NetBackup server on VCS on Linux 27
About adding a node to existing cluster 28
Installing or upgrading NetBackup options on VCS on Linux 28
Upgrading a NetBackup failover server on VCS on Linux 29

Chapter 4 NetBackup in a Veritas Cluster Server on Windows 32

About NetBackup in a Veritas Cluster Server on Windows 32
About NetBackup agent for VCS on Windows 33
Installation prerequisites for NetBackup on VCS on Windows 33
Installing a NetBackup failover server on VCS on Windows 35
Configuring a NetBackup server on VCS on Windows 36
Upgrading a NetBackup failover server on VCS on Windows 37
Setting up a detailed monitoring script for the NetBackup server on VCS on Windows 39
Enabling detailed monitoring in VCS Cluster Manager for the NetBackup server 40
Disabling detailed monitoring in VCS Cluster Manager for the NetBackup server 41

Chapter 5 NetBackup on RedHat Pacemaker (PCS) on Linux 42

About NetBackup on a Red Hat Pacemaker (PCS) on Linux 42
Installation prerequisites for NetBackup on PCS Linux 43
Preinstallation checklist for a NetBackup failover server installation on PCS on Linux 43
NetBackup installation on Red Hat Pacemaker Passive Node on Linux 44
Upgrade NetBackup failover server on the PCS Linux 46

Chapter 6 Configuring NetBackup 48

NetBackup configuration overview 49
NetBackup configuration guidelines 50
Device configuration guidelines 51
Configuring devices 52
Configuring NetBackup catalog backups in a cluster 53
About configuring backup policies for a NetBackup clustered server 53
What to back up 54
Guidelines for backing up local disks in a cluster 54

Guidelines for backing up the shared disks 55
Configuring the PBX LocalPortRange setting in a cluster 55
Verifying NetBackup configuration 57
Configuring robotic daemons for monitoring (UNIX/Linux clusters) 58
Configuring additional services (UNIX/Linux clusters) 58
Configuring add-ons for monitoring (UNIX/Linux clusters) 59
Configuring additional services (Windows) 60
Configuring add-ons for monitoring (Windows) 60
About adding license keys 61

Chapter 7 Operational notes 62

General notes on clustered primary server administration 62
About WSFC clusters 63
About NetBackup cluster application management 64
Logging information 64
About the support for multiple IP addresses in NetBackup 65
Log on to server using virtual name 65
Normal error messages when upgrading clustered servers 66

Appendix A NetBackup primary server in a cluster using multiple interfaces 67

About NetBackup primary server in a cluster using multiple interfaces 67
Requirements for use of a NetBackup primary server in a cluster with multiple interfaces 69
Configuring the NetBackup primary server in a cluster using multiple interfaces 69

Chapter 1

Introduction to NetBackup primary server clustering

This chapter includes the following topics:

- About NetBackup clustering
- About NetBackup failover server data protection in a cluster
- About NetBackup failover server support
- NetBackup supported cluster solutions
- About NetBackup limitations with clustering solutions

About NetBackup clustering

Clusters provide high availability of applications and data to users. In a cluster, two or more servers (called nodes) are linked in a network. These servers run the cluster software that allows each node access to the shared disks. If a node becomes unavailable, cluster resources migrate to an available node (this process is called failover). The shared disks and the virtual server are kept available. During failover, users experience only a short interruption in service.

In this documentation, the various cluster solutions are abbreviated as follows:

- Windows Server Failover Clustering as WSFC
- Arctera Volume Manager as Volume Manager
- Veritas Cluster Server as VCS

About security certificates in NetBackup

NetBackup uses security certificates to authenticate NetBackup hosts. The security certificates conform to the X.509 Public Key Infrastructure (PKI) standard. A primary server acts as the Certificate Authority (CA) and issues digital certificates to hosts.

NetBackup provides two types of NetBackup host security certificates: Host ID-based certificates and host name-based certificates.

A security certificate is mandatory when you want to establish a connection with NetBackup hosts.

Note: Generating a security certificate is a one-time activity.

For more information on certificate deployment in a clustered NetBackup setup, see the NetBackup Security and Encryption Guide.

NetBackup clustering in virtual environment

The NetBackup primary servers running on virtual machines can be clustered using supported clustering technologies in similar way as that of physical machines clustering. For the general statement of support for NetBackup in a clustered virtual environment, refer following technote.

https://support.cohesity.com/s/

You can install products like Storage Foundation HA on virtual machines in the same way as you install those on physical machines. However it is different than using VMware HA or vMotion because these two work at the virtual machine container level rather than the application level within the virtual machine.

Note: Using NetBackup within VM high availability, replication or transfer solutions is supported but not qualified by Cohesity (Examples of such solutions are vSphere HA, host-based replication, vMotion, and Storage vMotion (but not limited to VMware)). As a virtualized application, NetBackup is unaware of being deployed within a VM, and support for such operations is provided by the hypervisor vendor.

About NetBackup failover server data protection in a cluster

NetBackup protects the data in a cluster environment in several ways.

When NetBackup is installed as a failover server, a NetBackup server is installed on the cluster as a virtual server application. Then the server can fail over from one

of the nodes to the other. The server is assigned a network name resource (the virtual server name), an IP address resource, and a disk resource. The NetBackup server fails over from one node to another if a failure occurs on the active node. This failover provides high availability of the NetBackup server itself.

For failover primary servers, the virtual server name is used as the name of the primary server. This virtual name is used for all media servers and clients that use this primary server.

When a failover occurs, the backup jobs that were running are rescheduled with the normal NetBackup retry logic for a failed backup. The NetBackup services are started on another node and the backup processing resumes.

The NetBackup failover primary servers operate in an active-passive failover configuration. The active node and the passive (or failover node) must be the same version of the primary server.

The use of stand-alone media servers and NetBackup clients in a cluster is also briefly described later in this document.

About NetBackup failover server support

The following topics include provide instructions for each clustering technology:

- See “Upgrading a NetBackup failover server on WSFC cluster” on page 15.
- See “Upgrading a NetBackup failover server on VCS on Linux” on page 29.
- See “Upgrading a NetBackup failover server on VCS on Windows” on page 37.

NetBackup supported cluster solutions

For information on the supported cluster environments, see the NetBackup software compatibility list.

https://support.cohesity.com/s/article/article-100040093

Refer to Table 1-1 for information on how to install and configure NetBackup in each supported cluster environment.

Table 1-1 Supported cluster solutions

Cluster solution	See
Windows Server Failover Clustering	See “About NetBackup on Windows Server Failover Clustering” on page 11.

Table 1-1 Supported cluster solutions *(continued)*

Cluster solution	See
Veritas Cluster Server Windows	See "About NetBackup in a Veritas Cluster Server on Windows" on page 32.
Veritas Cluster Server on Linux	See "About NetBackup on a Veritas Cluster Server on Linux" on page 22.

About NetBackup limitations with clustering solutions

The following general limitations exist for NetBackup in a cluster:

- NetBackup does not support the conversion of an existing non-failover NetBackup primary server to a failover NetBackup primary server and vice versa. Contact Cohesity Technical Support.
- All NetBackup nodes must be running the same operating system and NetBackup version.
- NetBackup clustering does not support multiple primary servers in a single cluster.
- NetBackup primary server clustering is supported on Windows as well as Linux platforms.
- NetBackup primary server clustering has an active-passive configuration. NetBackup supports only the active-passive high availability (HA) clustering configuration.
- For information on the supported cluster environments, see the NetBackup software compatibility list.
- For limitations specific to NetBackup options, refer to the NetBackup Release Notes.
- For limitations specific to Media Manager, refer to the NetBackup Administrator's Guide, Volume I.

Chapter 2

NetBackup in a Windows Server Failover Clustering

This chapter includes the following topics:

- About NetBackup on Windows Server Failover Clustering
- Installation prerequisites for NetBackup on WSFC cluster
- Installing a NetBackup failover server on WSFC cluster
- Configuring a NetBackup server on WSFC cluster
- Upgrading a NetBackup failover server on WSFC cluster
- Restoring the cluster quorum
- Restoring the cluster quorum to a node with directory services
- Preparation for disaster recovery of WSFC
- Disaster recovery of WSFC
- Recovering the entire WSFC cluster
- Recovering all shared disks
- About recovering NetBackup data on a shared disk

About NetBackup on Windows Server Failover Clustering

Windows Server Failover Clustering (WSFC) is a high-availability solution for cluster configurations. With Windows Server Failover Clustering you can monitor systems

and application services. Refer to the documentation for WSFC to get a detailed understanding of how WSFC works and how it is installed and administered.

For detailed information on how NetBackup is installed and administered, see the NetBackup Installation Guide and NetBackup Administrator's Guide, Volume I.

NetBackup can be configured in a cluster as a non-failover server and as a standalone media server with virtual storage units. For more information, refer to the NetBackup in Highly Available Environments Administrator's Guide.

Installation prerequisites for NetBackup on WSFC cluster

The following requirements must be met before you install and configure a NetBackup failover server in a WSFC environment:

- Verify that WSFC and the current NetBackup version support your hardware. For a list of supported storage devices, visit the following Web site. Also consult the WSFC documentation.
  https://support.cohesity.com/s/article/article-100040093
- Verify that storage devices are properly installed and configured to work in a Windows environment. Refer to the information on configuring storage devices in the NetBackup Installation Guide.
- Verify that Windows Server Failover Clustering is correctly installed and configured. NetBackup can be installed on as many nodes as WSFC supports. WSFC supports up to 4 or 8 nodes in a cluster, depending on the level of Windows that is installed.
- Physically connect the robotic devices and tape devices to each node where you want to install NetBackup). Connect devices by SCSI or Fibre Channel. Use OS commands to verify that all the devices are connected properly.
  See the NetBackup Device Configuration Guide.
- Verify that you have an IP address and host name (virtual name) to be assigned to the NetBackup cluster group. Use these only for the NetBackup cluster group.
  Also, verify that the disk resource is online on the node from which the NetBackup installation is about to be performed for the first time on the cluster.
  With this release IPv6 is supported with NetBackup.
  See “About the support for multiple IP addresses in NetBackup” on page 65.
- Use Cluster Administrator to verify that the Possible Owners list for each disk resource that NetBackup uses includes each node to which NetBackup can failover.

- Verify that you have the current NetBackup Primary Server version or the current NetBackup server version installation program and a valid license.
- The Windows Server Failover Clustering Administrator must be installed on all NetBackup servers that you use to administer the NetBackup failover primary server remotely. Failover Cluster Manager must also be installed on any NetBackup administration clients.
- You must have administrator rights or domain administrator credentials on the server cluster.
- On Windows, the public network names must be the same on both nodes of the cluster for push installs.
- You should install NetBackup on the same path on all the nodes.

Installing a NetBackup failover server on WSFC cluster

Before you begin installation, review the following notes:

- These instructions assume that this installation is a new installation of a NetBackup failover server.
  To upgrade NetBackup rather than complete an initial installation, follow the upgrade procedure.
  See "Upgrading a NetBackup failover server on WSFC cluster" on page 15.
- You must install the same type of NetBackup server on each node to which NetBackup may failover.
- The virtual name cannot be more than 15 characters because of a Microsoft limitation.

Note: After you configure NetBackup as a cluster group in WSFC, do not change the group name.

The installation program does the following:

- Installs NetBackup on the node with shared disk resource online.
- Pushes the install to each inactive node and the license file is obtained from the shared location:
  `/var/global/licenses`
- Brings the NetBackup resources online.

To upgrade NetBackup rather than complete an initial installation, you follow a different procedure.

See "Upgrading a NetBackup failover server on WSFC cluster" on page 15.

To install a NetBackup failover server in an WSFC cluster

1. Install NetBackup on all nodes of the cluster. This installation can be done in the following ways:

   - Install on the cluster node (with shared disk online) and push install to all other nodes in the cluster.
     Or
   - Install on the cluster node (with shared disk online). After the first node installation, manually install on all other nodes in the cluster.
     If a license file is added and it is later made a part of a cluster that already has a license, a pop-up screen with the following information is displayed:
     The added license will not be used. Existing license of that cluster will only be used for installation.

   Follow the instructions for NetBackup in a clustered environment as described in the NetBackup Installation Guide.

2. When you are prompted to provide the list of servers, enter all servers that need to have access to the NetBackup failover server.

3. Post installation, get security certificates on all the nodes within the cluster.

   For more information on getting a certificate in a clustered NetBackup setup, see the NetBackup Security and Encryption Guide.

4. Post installation, if you have added additional license keys then perform a failover and add these keys to each node in the cluster.

   See "About adding license keys" on page 61.

5. Install any options that require separate installations.

   Most Windows options only require a special license key and do not require a separate installation. See the appropriate NetBackup documentation for the specific option for more information.

6. After the installation is complete, continue with the configuration of NetBackup.

   See "Configuring a NetBackup server on WSFC cluster" on page 14.

Configuring a NetBackup server on WSFC cluster

Do the following steps to configure NetBackup server in a cluster.

Table 2-1 Configuring a NetBackup server on WSFC cluster

Step	Action
1	Review the guidelines for how to configure NetBackup. See "NetBackup configuration guidelines" on page 50.
2	Configure the devices in the cluster. See "Device configuration guidelines" on page 51. See "Configuring devices" on page 52. **Note:** Devices must be configured on each node in the cluster.
3	Verify that the entries for the NetBackup Catalog backups are correct. See "Configuring NetBackup catalog backups in a cluster" on page 53. Catalog backup information is stored on the shared disk and does not need to be configured for each node.
4	Configure backup policies. Backup policies are stored on the shared disk and do not need to be configured for each node. See "About configuring backup policies for a NetBackup clustered server" on page 53.
5	By default, NetBackup options (such as NetBackup Vault) do not cause NetBackup to failover if they fail. You can configure NetBackup options to failover NetBackup if a service or the option fails. See "Configuring add-ons for monitoring (Windows)" on page 60.
6	When you have completed the configuration of NetBackup, verify that NetBackup can fail over properly in the cluster. See "Verifying NetBackup configuration" on page 57.

Upgrading a NetBackup failover server on WSFC cluster

Follow these instructions if you want to upgrade NetBackup.

Note: NetBackup does not support conversion of an existing non-failover NetBackup server to a failover NetBackup server. Contact Cohesity Technical Support.

Note: If you have modified NetBackup cluster configuration manually or the configuration has been modified due to external script, make sure that it is reflected correctly in NetBackup cluster registry.

To upgrade a NetBackup failover server on WSFC cluster

1. Ensure that a good backup of your cluster environment exists that includes a catalog backup.

   See "Configuring NetBackup catalog backups in a cluster" on page 53.

2. For each NetBackup server that runs outside of the cluster, ensure that the server list is accurate. This list should contain the name of each node where NetBackup can run and the name of the virtual server.
3. Take all NetBackup resources offline except for the disk resource, virtual IP, and virtual name before you begin the upgrade install.
4. The upgrade process depends on the release from which you want to upgrade.
   - For upgrades from NetBackup 10.1.1 and earlier, continue with step 5.
   - For upgrades from NetBackup 10.2 and later, continue with step 6.
5. (Upgrades from 10.1.1 and earlier) Perform the following steps:
   - Follow the instructions for how to upgrade NetBackup in a clustered environment as described in the following article.
     https://support.cohesity.com/s/article/article-100055395
   - Start the upgrade.
     Make sure all the critical pre-checks are successful including the pre-check `db_ping_check`.
     Follow the instructions for how to upgrade NetBackup in a clustered environment as described in the NetBackup Installation Guide.

     The installation program does the following:
     - Upgrades NetBackup on the active node.
     - Pushes the install to each inactive node.
     - Brings the NetBackup resources online.
6. (Upgrades from 10.2 and later) Follow the instructions for how to upgrade NetBackup in a clustered environment as described in the NetBackup Installation Guide.

   The installation program does the following:
   - Upgrades NetBackup on the active node.

- Pushes the install to each inactive node.
- Brings the NetBackup resources online.

7 Post upgrade installation, verify if the security certificates are deployed on all the nodes within the cluster. If not, generate security certificates on all the nodes within the cluster.

For more information on deploying a certificate in a clustered NetBackup setup, see the NetBackup Security and Encryption Guide.

8 Upgrade and configure any options.

Most options require only a license key and do not need to be upgraded separately. For information on how to install and configure a specific option, see the appropriate NetBackup documentation for that option.

Restoring the cluster quorum

The cluster quorum is backed up as part of System State or Shadow Copy Components for each node. To restore the cluster quorum, other nodes in the cluster must be offline. If you cannot take the other nodes in the cluster offline before you restore the cluster quorum, follow the instructions in the next procedure.

To force the restore of the cluster quorum when other nodes are online

1 Create the following registry entry:

```
HKEY_LOCAL_MACHINE\Software\VERITAS\NetBackup\CurrentVersion\
Config\Cluster_Database_Force_Restore
```

The actual registry entry must be on a single line. If required, create this registry value as data type REG_SZ with a value of YES. When this value is set, the cluster service is stopped for any nodes that are online.

2 If Active Directory is running on the target server or the target server is currently a domain controller, the restore procedure is different.

See “Restoring the cluster quorum to a node with directory services” on page 18.

To restore the cluster quorum

1 If the other nodes in the cluster are online, create the registry entry as described in the previous procedure.

2 In the NetBackup **Backup, Archive, and Restore** interface, open a **Restore** window.

3 Select the backup image (or range of images) that contains the backup of the **System State** or **Shadow Copy Components** for this node of the cluster.

4 In the **All Folders** pane, select **System_State** or **Shadow Copy Components**.

5 If the disk where the cluster quorum previously resided is changed, set the registry entry. This action forces the restore to continue.

See "To force the restore of the cluster quorum when other nodes are online" on page 17.

The disk may have been replaced with a new one. Or the disk configuration may have been changed so that the cluster quorum now resides on a different disk. In the latter case, the drive letter can remain the same for the disk that contained the cluster quorum. The drive letter can remain the same even if the configuration has changed. It can also remain the same if the disk signatures in the restore media do not match the signatures in the cluster quorum.

6 Continue the restore.

7 When the restore operation is complete, restart the cluster node. Or use the Failover Cluster Manager to restart the cluster service on any nodes where it was stopped.

Restoring the cluster quorum to a node with directory services

To restore the quorum to a node that is either running Active Directory or that is currently a domain controller, the node must be in Directory Services Restore Mode. The cluster services cannot run in this mode. So the cluster quorum must be restored separately, after the System State or the Shadow Copy Components are restored and after the node is restarted.

To restore the cluster quorum to a node running Active Directory or that is currently a domain controller

1 In the NetBackup Backup, Archive, and Restore interface, open a **Restore** window.

2 Select the backup image (or range of images) that contains the backup you want to restore.

3 Exclude the cluster quorum from the restore, as follows:

- Expand **System_State** and then deselect **Cluster_Database**.
- Expand **Shadow Copy Components > System State** and then deselect **Cluster_Quorum**.

4 Continue the restore.

5. When the restore operation is complete, restart the cluster node in Safe (repair) mode. Then select Directory Services Restore Mode.
6. Start the NetBackup service(s).
7. Open the NetBackup Backup, Archive, and Restore interface.
8. Select only the cluster quorum, as follows:
   - Expand **System_State** and select only **Cluster_Database**.
   - Expand **Shadow Copy Components > System State** and select only **Cluster_Quorum**.
9. If the disk where the cluster quorum previously resided is changed, you may have to set the registry entry. This action forces the restore to continue.

   See "To force the restore of the cluster quorum when other nodes are online" on page 17.

   The disk may have been replaced with a new one. Or the disk configuration may have been changed so that the cluster quorum now resides on a different disk. In the latter case, the drive letter can remain the same for the disk that contained the cluster quorum. The drive letter can remain the same even if the configuration has changed. It can also remain the same if the disk signatures in the restore media do not match the signatures in the cluster quorum.
10. Continue the restore.
11. When the restore is complete, restart the target node.
12. Use Failover Cluster Manager to restart the cluster service on any nodes where it was stopped.

Preparation for disaster recovery of WSFC

For complete instructions on recovery of WSFC, refer to the Microsoft documentation. Cohesity only provides the instructions for how to restore the objects that you have backed up using NetBackup.

Disaster recovery of WSFC

Various disaster recovery scenarios are discussed in the following topics:

- See "Recovering the entire WSFC cluster" on page 20.
- See "Recovering all shared disks" on page 20.
- See "About recovering NetBackup data on a shared disk" on page 21.

This last topic describes how to recover the shared disk where the NetBackup application resides.

Recovering the entire WSFC cluster

The following procedure describes how to recover the nodes in a cluster to their pre-disaster state.

To recover the entire WSFC cluster

1. On the first node you want to recover, reinstall the Windows operating system, including the last service pack that was applied before the failure.
2. Install any other drivers or applications to make the node operational.
3. After you start the nodes in a cluster, ensure that the drive letters match the original cluster configuration. If the original configuration does not match, you can use the Disk Administrator to control the hard drive numbering scheme of the Windows devices.
4. On all remaining nodes you need to recover, reinstall Windows, including the last service pack that was applied before the failure.
5. Reinstall the cluster services and bring the cluster online.
6. Reinstall the same NetBackup software on the cluster that was installed before the failure.
7. Use the appropriate NetBackup catalog recovery procedure to restore the NetBackup catalog information before continuing.

   See the NetBackup Troubleshooting Guide for more information on recovering the NetBackup catalog database.
8. Restore the data files through the virtual server.
9. If you must restore a database to the shared drives, see the *NetBackup Administrator's Guide* for your NetBackup agent to continue the restore.

   https://support.cohesity.com/s/article/article-100040135

Recovering all shared disks

The following procedure describes how to recover the shared disks in WSFC cluster.

To recover all shared disks

1. Uninstall the cluster software from both nodes.
2. Replace and repartition the shared disks.

3 Reinstall the cluster software.

4 Ensure that all NetBackup shared disks are assigned the same drive letters that were used when NetBackup was originally installed and configured.

5 To reconfigure NetBackup for the cluster, do the following on the active node:

- Run the following command:

```
bpclusterutil -ci
```

- Recreate the database.
- Run the following commands:

```
tpext
bpclusterutil -online
```

6 Use the appropriate NetBackup catalog recovery procedure to restore the NetBackup catalog information on the shared disk before continuing. See the NetBackup Troubleshooting Guide for more information on recovering the NetBackup catalog database.

7 Restore any data on the shared disks.

About recovering NetBackup data on a shared disk

To recover the shared disk that the NetBackup failover server used, follow the appropriate NetBackup catalog recovery procedure to restore the catalog information on the shared disk.

See the NetBackup Troubleshooting Guide for more information on recovering the NetBackup catalog database.

Chapter 3

NetBackup in a Veritas Cluster Server on Linux

This chapter includes the following topics:

- About NetBackup on a Veritas Cluster Server on Linux
- Installation prerequisites for NetBackup on VCS on Linux
- About preinstallation checklist for a NetBackup failover server installation on VCS on Linux
- Installing a failover NetBackup server on VCS on Linux
- Configuring a failover NetBackup server on VCS on Linux
- About adding a node to existing cluster
- Installing or upgrading NetBackup options on VCS on Linux
- Upgrading a NetBackup failover server on VCS on Linux

About NetBackup on a Veritas Cluster Server on Linux

Veritas Cluster Server (VCS) is a high-availability solution for cluster configurations. VCS enables you to monitor systems and application services and to restart services on a different system when hardware or software fails.

NetBackup can be configured in a cluster as a non-failover server and as a standalone media server with virtual storage units. For more information, see the NetBackup in Highly Available Environments Administrator's Guide.

NetBackup supports the use of the Global Cluster Option (GCO) with VCS. For information on how to configure and use GCO with NetBackup, refer to the NetBackup in Highly Available Environments Administrator's Guide.

Installation prerequisites for NetBackup on VCS on Linux

The following requirements must be met before you install and configure a NetBackup failover server:

- Verify that VCS and the current NetBackup Primary Server version support your hardware. For a list of supported storage devices, visit the following Web site: https://support.cohesity.com/s/article/article-100040093
- Verify that the supported version of VCS is correctly installed and configured on Linux. Follow the steps in the *Cluster Server Installation Guide*.
- Verify that no VCS resource group and resource exist with the same name as the one you intend to use for NetBackup.
- Make sure that the shared disk is configured and accessible to all cluster nodes where you want to install NetBackup. Also, verify that you can mount the disk.
- Verify that you have an IP address (virtual IP) and a host name (virtual name) to assign to the NetBackup resource in VCS. Use these only for the NetBackup resource.
  Also, ping the IP address and verify that the IP address is not plumbed.
  For VCS-UNIX, IP address of the Nodes and Virtual Name must be of same type (IPv6 or IPv4).
  With this release IPv6 is supported with NetBackup.
  See "About the support for multiple IP addresses in NetBackup" on page 65.

  Note: Node IP type must be same as virtual IP type.

- Make sure that each node in the cluster, where you want to install NetBackup, is SSH equivalent. As the root user you must be able to perform a remote logon to each node in the cluster without entering a password. This configuration is only necessary for installation, upgrades, and configuration of the NetBackup server and any NetBackup options. After installation and configuration are complete SSH can be disabled.
- For a clustered NetBackup primary server, if the primary server is the robotic control host, physically connect the robotic devices and tape devices to each node where you want to install NetBackup. Connect devices by SCSI or Fibre

Channel. Use OS commands to verify that all the devices are connected properly. Refer to the NetBackup Device Configuration Guide.

- Verify that you have the current version of the NetBackup primary server installation program and a valid license key.

About preinstallation checklist for a NetBackup failover server installation on VCS on Linux

The NetBackup Primary Server requests certain cluster-related information during installation. Fill up the checklist for all configurations and the checklist for your specific configuration before you begin installation.

See "NetBackup installation information for all VCS configurations" on page 24.

See "NetBackup installation information for specific VCS configurations" on page 25.

Note: The configuration utility unless specified otherwise treats all attribute values globally.

NetBackup installation information for all VCS configurations

The following information is required for all VCS cluster configurations:

- Virtual name for NetBackup
- IP address
- Subnet mask or Prefix length
- Node name

  Following information is required for each node:

  - IP address
  - Network device name (NIC)

You also need to configure the service user and database user the same way on each cluster node:

- For the service user, the username, group name, and UID must be the same on all the cluster nodes.
- For the database user, the username, group name, and UID must be the same on all the cluster nodes.

NetBackup installation information for specific VCS configurations

The following information is required if you use VCS. Review the scenario that fits your configuration.

Table 3-1 Scenario 1 - VCS with VxVM

Resource	Example
Disk group Resource	
Disk group	nbudg
Start Volumes	0 or 1
Stop Volumes	0 or 1
Volume Resource (optional)	
Volume	nbuvol
Mount Resource	
Mount Point	/opt/VRTSnbu
Block Device	/dev/vx/dsk/nbudg/nbuvol
FS Type	vxfs
Mount Option	(optional)
Fsck Option	(if you add other options, -y is also required)

Table 3-2 Scenario 2- VCS with no Volume Manager

Resource	Example
Mount Point	/opt/VRTSnbu
Block Device	/dev/dsk/clt1dos3
FS Type	vxfs
Mount Option	(optional)
Fsck Option	(if you add other options, -y is also required)

Installing a failover NetBackup server on VCS on Linux

This topic describes how to install and configure a new NetBackup Primary Server as a failover application on a VCS on UNIX or Linux. To upgrade NetBackup, you must follow a different procedure.

See "Upgrading a NetBackup failover server on VCS on Linux" on page 29.

Note: You must install the NetBackup primary server on each node to which NetBackup may failover. You cannot have a separate failover primary server in your NetBackup configuration.

The following procedure describes how to install and configure a NetBackup failover server in a VCS cluster.

Note: NetBackup automatically detects supported clustering technology and prompts questions based on it. If you are not prompted for these questions on a clustered setup, please exit from the script and verify that cluster is configured correctly.

To install a NetBackup failover server

1. Fill out the checklist for all configurations and the checklist for your specific environment.

   See "NetBackup installation information for all VCS configurations" on page 24.

   See "About preinstallation checklist for a NetBackup failover server installation on VCS on Linux" on page 24.

2. Make sure that the shared disk is not mounted on any node in the cluster.

   If applicable, unmount the NetBackup shared mount point. Stop the volume the mount point is on and deport the disk group for that volume on all nodes of the cluster.

3. Follow the instructions for how to install NetBackup in the NetBackup Installation Guide.

   Be sure that you:

   - Install NetBackup on each node to which it can failover.
   - Use the virtual name for the NetBackup server name.

Caution: When you are prompted, you must provide the same virtual cluster name that you provided during the installation. This name must be in the same format (FQDN/short) on all the nodes.

4. When NetBackup is installed on the clustered setup a confirmation prompt is displayed.
   - When you install NetBackup on the first node, you are prompted to confirm creation of a NetBackup cluster. Type **Yes** to set up NetBackup in HA mode.
   - When you install NetBackup on the subsequent nodes, information about already created NetBackup cluster group is displayed. You are prompted to join the group.
5. When you are prompted for cluster-specific configuration details, refer to the checklist and provide details accordingly.
6. Allow NetBackup to be installed in a cluster. When a NetBackup failover server is installed:
   - On the first node, a single node cluster resource group for NetBackup is created and brought online.
   - On the other nodes, the installed node is added to the cluster resource group.
7. Post installation, get security certificates on all the nodes within the cluster.

   For more information on getting a certificate in a clustered NetBackup setup, see the NetBackup Security and Encryption Guide.
8. Install any NetBackup options.

   See “Installing or upgrading NetBackup options on VCS on Linux ” on page 28.
9. Continue with configuration of NetBackup.

   See “Configuring a failover NetBackup server on VCS on Linux” on page 27.

Configuring a failover NetBackup server on VCS on Linux

To configure NetBackup server in a cluster, do the following:

Table 3-3 Configuring a failover NetBackup server on VCS on UNIX/Linux

Step	Action
1	Review the guidelines for how to configure NetBackup. See "NetBackup configuration guidelines" on page 50.
2	Configure the devices in the cluster. See "Device configuration guidelines" on page 51. See "Configuring devices" on page 52. **Note:** Devices must be configured on each node in the cluster.
3	Verify that the entries for the NetBackup Catalog backups are correct. See "Configuring NetBackup catalog backups in a cluster" on page 53. Catalog backup information is stored on the shared disk and does not need to be configured for each node.
4	Configure backup policies. Backup policies are stored on the shared disk and do not need to be configured for each node. See "About configuring backup policies for a NetBackup clustered server" on page 53.
5	When you have completed configuration of NetBackup, verify that NetBackup can failover properly in the cluster. See "Verifying NetBackup configuration" on page 57.

About adding a node to existing cluster

To add a node to the existing cluster, add the node to the VCS cluster before NetBackup is installed. The installer automatically detects the new node and adds it to the NetBackup cluster configuration.

Installing or upgrading NetBackup options on VCS on Linux

Install or upgrade NetBackup options (for example, Language Packs) on all cluster nodes where the NetBackup server is installed. In addition, freeze the NetBackup group before installing any options.

Note: Before you upgrade any options, ensure that the NetBackup resource is online in the cluster. Also ensure that server processes are running on the active node.

To install or upgrade a NetBackup option on VCS on UNIX/Linux

1. Enable the VCS configuration in read and write mode with `haconf -makerw`
2. Freeze the NetBackup group with `hagrp -freeze` *`nbu_group_name`* `-persistent`.
3. Run the following command on the active node to disable the NetBackup agent monitor:

   ```
   touch /usr/openv/netbackup/bin/cluster/frozen
   ```

4. Install the options on each inactive node in the cluster where NetBackup is installed. See the specific NetBackup documentation for each option for instructions on installation and configuration.
5. On the active node, perform the same installation.
6. Unfreeze the NetBackup group with `hagrp -unfreeze` *`nbu_group _name`* `-persistent`
7. Enable the VCS configuration in read-only mode with `haconf -dump -makero`
8. Run the following command on the active node to enable the NetBackup agent monitor:

   ```
   rm -f /usr/openv/netbackup/bin/cluster/frozen
   ```

Upgrading a NetBackup failover server on VCS on Linux

Note: NetBackup does not support conversion of an existing non-failover NetBackup server to a failover NetBackup server. Contact Cohesity Enterprise technical support.

Note: Cohesity requires that you use the latest VCS agent that is installed with NetBackup 11.2.0.1. Older versions of the agent are not supported.

To upgrade a NetBackup failover server

1. Ensure that a good backup of your cluster environment exists that includes a catalog backup.

   See "Configuring NetBackup catalog backups in a cluster" on page 53.

2. For each NetBackup server that runs outside of the cluster, ensure that the server list is accurate. This list should contain the name of each node where NetBackup can run and the name of the virtual server.

3. Take the VCS NetBackup cluster resource offline before you begin the upgrade.

   Note: Make sure that shared disk and IP resources are online during the upgrade on active node.

4. Enable the VCS configuration in read and write mode with `haconf -makerw`

5. Freeze the NetBackup group using the following command:

   ```
   hagrp -freeze <nbu_group_name> -persistent
   ```

6. Stop the NetBackup cluster agent on all nodes of the NetBackup Group using the following command:

   ```
   haagent -stop NetBackup -force -sys <node>
   ```

7. The upgrade process depends on the release from which you want to upgrade.
   - For upgrades from NetBackup 10.1.1 and earlier, continue with step 8.
   - For upgrades from NetBackup 10.2 and later, continue with step 9.

8. (Upgrades from 10.1.1 and earlier) Perform the following steps:
   - Follow the instructions for how to upgrade NetBackup in a clustered environment as described in the following article.
     https://support.cohesity.com/s/article/article-100055395
   - Make sure all the critical pre-checks are successful including the pre-check `db_ping_check`.
   - On the active node, install the NetBackup server software.
     Follow the instructions for how to upgrade NetBackup as described in the NetBackup Installation Guide.
     If required to specify the server name, provide the virtual name of the server.

9. (Upgrades from 10.2 and later) On the active node, install the NetBackup server software.

Note the following:

- Follow the instructions for how to upgrade NetBackup as described in the *NetBackup Installation Guide*.
  https://support.cohesity.com/s/article/article-100040135
- If required to specify the server name, provide the virtual name of the server.

10 On each inactive node to which NetBackup may fail over, install the NetBackup server software.

Note the following:

- Follow the instructions for how to upgrade NetBackup as described in the NetBackup Installation Guide.
- If required to specify the server name, provide the virtual name of the server.

11 Post upgrade installation, verify if the security certificates are deployed on all the nodes within the cluster. If not, generate security certificates on all the nodes within the cluster.

For more information on deploying a certificate in a clustered NetBackup setup, see the NetBackup Security and Encryption Guide.

12 Start the VCS NetBackup cluster agent on all nodes of the NetBackup Group. Use the following command:

```
haagent -start NetBackup -sys <node>
```

13 Enable the VCS configuration in read and write mode with `haconf -makerw`

14 Unfreeze the NetBackup group using the following command:

```
hagrp -unfreeze <nbu_group_name> -persistent
```

15 Enable the VCS configuration in read-only mode with `haconf -dump -makero`

16 Take the NetBackup group offline and then bring online.

17 On each node where NetBackup server is installed, upgrade NetBackup options.

See “Installing or upgrading NetBackup options on VCS on Linux ” on page 28.

18 Verify that NetBackup can failover properly in the cluster.

See “Verifying NetBackup configuration” on page 57.

Note: During freezing or unfreezing the groups, make sure that the status of configuration is in Read-Write mode.

Chapter 4

NetBackup in a Veritas Cluster Server on Windows

This chapter includes the following topics:

- About NetBackup in a Veritas Cluster Server on Windows
- About NetBackup agent for VCS on Windows
- Installation prerequisites for NetBackup on VCS on Windows
- Installing a NetBackup failover server on VCS on Windows
- Configuring a NetBackup server on VCS on Windows
- Upgrading a NetBackup failover server on VCS on Windows
- Setting up a detailed monitoring script for the NetBackup server on VCS on Windows
- Enabling detailed monitoring in VCS Cluster Manager for the NetBackup server
- Disabling detailed monitoring in VCS Cluster Manager for the NetBackup server

About NetBackup in a Veritas Cluster Server on Windows

Veritas Cluster Server(VCS) is a high-availability solution for cluster configurations. With VCS you can monitor systems and application services, and restart services

on a different system when hardware or software fails. For information about VCS, refer to the *Cluster Server Administrator's Guide*.

NetBackup can be configured in a cluster as a non-failover server and as a standalone media server with virtual storage units. Refer to the NetBackup in Highly Available Environments Administrator's Guidefor more information.

About NetBackup agent for VCS on Windows

The NetBackup agent for VCS monitors specific NetBackup resources, determines the status of these resources, and starts or stops NetBackup according to external events. The agent includes VCS type declarations and agent executables. The NetBackup resource type represents the agent. When the agent detects an application failure, the NetBackup service group is failed over to another system in the cluster. NetBackup is installed and configured on this stem.

The following table describes the specific agent operations.

Online	Brings the NetBackup services online.
Offline	Takes the NetBackup services offline.
Monitor	Verifies the status of NetBackup services. Detailed monitoring is also available. See “Setting up a detailed monitoring script for the NetBackup server on VCS on Windows” on page 39.
Clean	Stops all NetBackup daemons if there is a detection of an unexpected offline operation or an ineffective online operation.

Additional monitoring capabilities are available for add-on products.

See “Configuring add-ons for monitoring (Windows)” on page 60.

NetBackup supports the use of the Global Cluster Option (GCO) with VCS. For information on how to configure and use GCO with NetBackup, refer to the NetBackup in Highly Available Environments Administrator's Guide.

Installation prerequisites for NetBackup on VCS on Windows

The following requirements must be met before you install and configure a NetBackup failover server:

- Verify that VCS and the current NetBackup version support your hardware. For a list of supported storage devices, visit the following Web site:
  https://support.cohesity.com/s/article/article-100040093
- Verify that storage devices have been properly installed and configured to work in a Windows environment. Refer to the section on how to configure storage devices in the NetBackup Installation Guide.
- Verify that you have installed Veritas Storage Foundation HA and correctly configured VCS. NetBackup can be installed on as many nodes as VCS supports. The NetBackup service group is created during the installation.
- For VCS Windows (SFW-HA 4.1 and SFW-HA 4.2) make sure the patch available and is installed before you install or upgrade to the current NetBackup version. The patch is available at the Cohesity Support site:

Note: In few cases, after the NetBackup primary server cluster installation, the resource is not installed into the service group. In case the resource of type "NetBackupVCS" is added manually, the attributes of NetBackupVCS are blank and this resource cannot probe on cluster servers. For work-around, contact Technical Support Team.

- Verify the cluster disk groups and dynamic volumes for NetBackup have been created on the shared storage. Refer to the *Storage Foundation Administrator's Guide* for details on how to create these.
- All disk resources that you want NetBackup to use must be configured in Veritas Enterprise Administrator (VEA) before you install NetBackup.
- Verify that you have an IP address and host name (virtual name) to be assigned to the NetBackup resource in VCS. Only use these for the NetBackup cluster group.The virtual name cannot be more than 15 characters.
  Also, verify that the disk resource is online on the node from which the NetBackup installation is about to be performed for the first time on the cluster.
- For a clustered NetBackup primary server, if the primary server is the robotic control host, physically connect the robotic devices and tape devices to each node where you want to install NetBackup. Connect devices by SCSI or Fibre Channel. Use OS commands to verify that all the devices are connected properly. Refer to the NetBackup Device Configuration Guide.
- Verify that you have the current NetBackup Enterprise Server version or the current NetBackup server version installation program and a valid license key.
- On Windows, the public network names must be same on both nodes of the cluster for push-installs.

- You should install NetBackup on the same path on all nodes.

Installing a NetBackup failover server on VCS on Windows

This section describes how to install and configure a new NetBackup primary server as a failover application in a VCS for Windows cluster. If you want to upgrade NetBackup, rather than complete an initial installation, you must follow a different procedure.

See "Upgrading a NetBackup failover server on VCS on Windows" on page 37.

Review the following notes before you begin installation:

- These instructions assume that this installation is a new installation of a NetBackup failover server.
- You must install the same type of NetBackup server on each node to which NetBackup may failover.
- After you configure NetBackup as a cluster group in VCS, do not change the group name.
- The virtual name cannot be more than 15 characters.

The installation program does the following:

- Installs NetBackup on the active node.
- Pushes the install to each inactive node and the license file is obtained from the shared location: `var/global/licenses`.
- Brings the NetBackup resources online.

The following procedure describes how to install a NetBackup failover server in a VCS cluster.

To install a NetBackup failover server on a VCS cluster

1. Install NetBackup on all nodes of the cluster. This installation can be done in the following ways:
   - Install on the cluster node (with shared disk online) and push install to all other nodes in the cluster.
     Or
   - Install on the cluster node (with shared disk online). After the first node installation, manually install on all other nodes in the cluster.

Follow the instructions for how to install NetBackup in a clustered environment as described in the NetBackup Installation Guide.

2 Post installation, get security certificates on all the nodes within the cluster.

For more information on getting a certificate in a clustered NetBackup setup, see the NetBackup Security and Encryption Guide.

3 When you are prompted to provide the list of servers, enter all servers that must have access to the NetBackup failover server.

4 Licenses are stored at the shared drive in `var/global/licenses` and the inactive node continues from here.

See "About adding license keys" on page 61.

5 Install options that require separate installations.

Most options only require a special license key and do not require a separate installation. See the appropriate NetBackup documentation for the specific option for more information.

6 After the installation is complete, continue with the configuration of NetBackup.

See "Configuring a NetBackup server on VCS on Windows" on page 36.

Configuring a NetBackup server on VCS on Windows

Do the following steps to configure NetBackup server on a VCS cluster on Windows.

Table 4-1 Configuring a NetBackup server on VCS on Windows

Step	Action
1	Review the guidelines for how to configure NetBackup. See "NetBackup configuration guidelines" on page 50.
2	Configure the devices in the cluster. See "Device configuration guidelines" on page 51. See "Configuring devices" on page 52. **Note:** Devices must be configured on each node in the cluster.
3	Verify that the entries for the NetBackup Catalog backups are correct. See "Configuring NetBackup catalog backups in a cluster" on page 53.

Table 4-1 Configuring a NetBackup server on VCS on Windows *(continued)*

Step	Action
4	Catalog backup information is stored on the shared disk and does not need to be configured for each node. Configure backup policies. Backup policies are stored on the shared disk and do not need to be configured for each node. See "About configuring backup policies for a NetBackup clustered server" on page 53.
5	By default, NetBackup options (such as NetBackup Vault) do not cause NetBackup to failover if they fail. You can configure NetBackup options to failover NetBackup if a service or the option fails. See "Configuring add-ons for monitoring (Windows)" on page 60.
6	When you have completed the installation and configuration of NetBackup, verify that NetBackup can fail over properly in the cluster. See "Verifying NetBackup configuration" on page 57.

Upgrading a NetBackup failover server on VCS on Windows

Follow these instructions if you want to upgrade NetBackup.

Note: NetBackup does not support conversion of an existing non-failover NetBackup server to a failover NetBackup server. Contact Cohesity Technical Support.

Note: If you have modified NetBackup cluster configuration manually or the configuration has been modified due to external script, make sure that it is reflected correctly in NetBackup cluster registry.

To upgrade a NetBackup failover server

1. Ensure that a good backup of your cluster environment exists that includes a catalog backup.

   See "Configuring NetBackup catalog backups in a cluster" on page 53.

2. For each NetBackup server that runs outside of the cluster, ensure that the server list is accurate. This list should contain the name of each node where NetBackup can run and the name of the virtual server.

3 Take the VCS NetBackup resource offline before you begin the upgrade.

Note: Make sure that shared disk and IP resources are online during the upgrade on active node.

4 The upgrade process depends on the release from which you want to upgrade.

- For upgrades from NetBackup 10.1.1 and earlier, continue with step 5.
- For upgrades from NetBackup 10.2 and later, continue with step 6.

5 (Upgrades from 10.1.1 and earlier) Perform the following steps:

- Follow the instructions for how to upgrade NetBackup in a clustered environment as described in the following article.
  https://support.cohesity.com/s/article/article-100055395
- Start the upgrade.
  Make sure all the critical pre-checks are successful including the pre-check `db_ping_check`.
  Follow the instructions for how to upgrade NetBackup in a clustered environment as described in the NetBackup Installation Guide.

  The installation program does the following:
  - Upgrades NetBackup on the active node.
  - Pushes the install to each inactive node.
  - Brings the NetBackup resources online.

6 (Upgrades from 10.2 and later) Follow the instructions for how to upgrade NetBackup in a clustered environment as described in the NetBackup Installation Guide.

The installation program does the following:

- Upgrades NetBackup on the active node.
- Pushes the install to each inactive node.
- Brings the NetBackup resources online.

7 Post upgrade installation, verify if the security certificates are deployed on all the nodes within the cluster. If not, generate security certificates on all the nodes within the cluster.

   For more information on deploying a certificate in a clustered NetBackup setup, see the NetBackup Security and Encryption Guide.

8 Upgrade and configure NetBackup options.

   Most options require only a license key and do not need to be upgraded separately. For information on how to install and configure a specific option, see the appropriate NetBackup documentation for that option.

Note: When you upgrade NetBackup on cluster, NetBackup resource goes into faulted state. You must clear the fault after upgrade is complete. For details, contact Cohesity Technical Support.

Setting up a detailed monitoring script for the NetBackup server on VCS on Windows

In the detail monitoring mode, the NetBackup agent runs a script to verify that NetBackup is available. A sample script, `DetailedMonitor.bat`, is provided with the agent for this purpose. You can customize the script to meet your configuration requirements.

Note: Before setting up detailed monitoring, the NetBackup agent must run base level of monitoring.

This topic describes how to set up detailed monitoring for a NetBackup server that is installed in a VCS for Windows environment. The script file must exist on all nodes in the service group's system list.

To set up a detailed monitoring script for the NetBackup server on VCS on Windows

1. Configure and run the NetBackup agent with the basic monitoring.
2. For each node in the NetBackup service group, create a backup policy that performs a user backup of the file
   install_path\bin\cluster\VCS\DetailedMonitor.txt.

   install_path is the home directory of NetBackup.

   For example, `C:\Program Files\VERITAS\NetBackup`

   For example, if your NetBackup service group contains five nodes, you must create five different policies, each referencing a different node.
3. Make a copy of following file and edit it to fit your configuration.

   install_path\bin\cluster\DetailedMonitor.bat

   - Replace VIRTSRVR with the virtual server name for the NetBackup primary or media server.
   - Make any other edits necessary.
4. From the command line, type the following command to verify the script runs without errors:

   ```
   DetailedMonitorProd
   ```

5. Continue with the following topic to enable detailed monitoring:

   See "Enabling detailed monitoring in VCS Cluster Manager for the NetBackup server" on page 40.

Enabling detailed monitoring in VCS Cluster Manager for the NetBackup server

This topic describes how to set the detail monitoring option for the NetBackup server from the VCS Cluster Manager.

To enable detailed monitoring in VCS Cluster Manager for the NetBackup server

1. In Cluster Explorer, right-click the NetBackup service group, choose **Offline**, and select the node where you want to bring the service group offline.
2. Click **Yes**.
3. In the left pane, click the NetBackup resource.

4. On the **Properties** tab, select the `Monscript` attribute from the list, and click **Edit**.
5. Provide the full path to the NetBackup monitor script that you created.
6. Click **OK**.
7. Save your configuration.
8. In the left pane, right-click the NetBackup service group, select **Online**, and select the node where you want to bring the service group online.
9. Click **Yes**.

Disabling detailed monitoring in VCS Cluster Manager for the NetBackup server

This section describes how to disable the detail monitoring option for the NetBackup server from the VCS Cluster Manager.

To disable detailed monitoring in VCS Cluster Manager for the NetBackup server

1. In Cluster Explorer, right-click on the NetBackup service group, choose **Offline**, and select the node where you want to bring the service group offline.
2. Click **Yes**.
3. In the left pane, click the NetBackup resource.
4. On the **Properties** tab, select the **Monscript** attribute from the list, and click **Edit**.
5. Remove the path information.
6. Click **OK**.
7. Save your configuration.
8. In the left pane, right-click the NetBackup service group, select **Online**, and select the node where you want to bring the service group online.
9. Click **Yes**.

Chapter 5

NetBackup on RedHat Pacemaker (PCS) on Linux

This chapter includes the following topics:

- About NetBackup on a Red Hat Pacemaker (PCS) on Linux
- Installation prerequisites for NetBackup on PCS Linux
- Preinstallation checklist for a NetBackup failover server installation on PCS on Linux
- NetBackup installation on Red Hat Pacemaker Passive Node on Linux
- Upgrade NetBackup failover server on the PCS Linux

About NetBackup on a Red Hat Pacemaker (PCS) on Linux

Red Hat Pacemaker is high-availability cluster resource manager which is owned by Red Hat. It ensures that the cluster service remains available whenever it detects resource or node level failure.

PCS enables you to monitor resources/services on an active node. When an active node or resources goes in failure state, then the PCS moves the services to a passive node .

Installation prerequisites for NetBackup on PCS Linux

The following requirements must be met before you install and configure a NetBackup on Pacemaker cluster:

- Verify that Red Hat Pacemaker (PCS) cluster is correctly configured on Linux which is up and running.
- Verify that no PCS resource group and resource exist with the same name as the one you intend to use for NetBackup.
- Make sure STONITH is disabled in Pacemaker Cluster Configuration as it is not supported for fresh install.
- Make sure that the shared disk is configured and accessible to all cluster nodes where you want to install NetBackup. Also, verify that you can mount the disk.
- Verify that you have an IP address (virtual IP) and a host name (virtual name) to assign to the NetBackup resource in PCS. Use these only for the NetBackup resource in PCS. Also, ping the IP address and verify that the IP address is not plumbed.
- Make sure that each node in the cluster, where you want to install NetBackup, is Secure Sell Protocol (SSH) equivalent. As the root user you must be able to perform a remote sign in to each node in the cluster without entering a password. This configuration is only necessary for installation and configuration of the NetBackup server and any NetBackup options.
- Verify that you have the current NetBackup Primary Server version installation program and a valid license key.
- For RHEL 10.x, before starting the NetBackup installation, ensure that the following directory exists on all cluster nodes:

```
mkdir -p /etc/corosync/uidgid.d
chmod 755 /etc/corosync/uidgid.d
```

Preinstallation checklist for a NetBackup failover server installation on PCS on Linux

During installation, NetBackup Primary server requests following cluster-related information:

You also need to configure the service user and database user the same way on each cluster node:

- For the service user, the username, group name, and UID must be the same on all the cluster nodes.
- For the database user, the username, group name, and UID must be the same on all the cluster nodes.

The following information is required for all Red Hat Pacemaker cluster configurations:

- Virtual IP Resource:
  - Virtual IP Resource Name
  - Virtual name for NetBackup
  - Subnet mask or Prefix length
  - Network device name (NIC)
- Mount Resource:
  - Mount Resource name
  - Mount Point
  - Block Device
  - FS Type

NetBackup installation on Red Hat Pacemaker Passive Node on Linux

This topic describes how to install and configure a new NetBackup Primary server as a failover application on a Red Hat Pacemaker on Linux.

Note: You must install the NetBackup primary server on each node to which NetBackup may failover. You cannot have a separate failover primary server in the NetBackup configuration.

The following procedure describes how to install and configure a NetBackup failover server in a PCS cluster.

Note: NetBackup automatically detects supported clustering technology and prompts questions based on it. If there are no prompts for questions on a clustered setup, do exit from the script and verify that the cluster is configured correctly.

To install a NetBackup failover server

1. Follow the instructions from NetBackup Installation Guide, to install NetBackup. Be sure that you: Install NetBackup on each node to which it can fail over. Use the virtual name for the NetBackup server name.

   Warning: When you are prompted, you must provide the same virtual cluster name that you provided during the installation. This name must be in the same format (FQDN/short) on all the nodes.

2. When NetBackup is installed on the clustered setup a confirmation prompt is displayed. When you install NetBackup on the first node, you are prompted to confirm creation of a NetBackup cluster.

   Type Yes to set up NetBackup in HA mode. When you install NetBackup on the subsequent nodes, information about already created NetBackup cluster group is displayed. You are prompted to join the group.

3. When you are prompted for cluster-specific configuration details, refer to the checklist and provide details accordingly.

4. Allow NetBackup to be installed in a cluster. When a NetBackup failover server is installed: On the first node, a single node cluster resource group for NetBackup is created and brought online. On the other nodes, the installed node is added to the cluster resource group.

5. Post installation, get the security certificates on all the nodes within the cluster. For more information, to get a certificate in a clustered NetBackup setup, refer to the *NetBackup Security and Encryption Guide*.

Recommendations when the PCS resource goes in blocked state:

When PCS maker resource enters in blocked state, run the following commands to refresh the pacemaker:

- `pcs resource refresh`
- Once all resources are up and running, run the command `pcs resource cleanup`
- In case of RHEL Pacemaker cluster, the Host mappings do not get automatically discovered. Then, you must provide the details on how to generate the host mappings.
- For example, RHEL Pacemaker cluster is configured with nodes such as Node1, Node2, and virtual name. Follow the steps to add manually the virtual name as a shared mapping between Node1 and Node2:

To add host mappings manually

1. On the left, select **Security > Host mappings**.
2. Select the host and click **Manage mappings**.
3. Click **Add**.
4. Enter the host name or IP address and click **Save**.
5. Click **Close**.

Note: If NetBackup automatically discovers any shared or cluster names associated with the NetBackup hosts in your environment, and which are not auto approved then follow the steps:

To approve the host mappings that NetBackup discovers

1. On the left, select **Security > Host mappings**.
2. Click the **Mappings to approve** tab.
3. Click the name of the host.
4. Review the mappings for the host and click **Approve** if you want to use the discovered mapping.

   Click **Reject** if you do not want to associate the mapping with the host.

   The rejected mappings do not appear in the list until NetBackup discovers them again.
5. Click **Save**.

Upgrade NetBackup failover server on the PCS Linux

Before you upgrade any options, ensure that the NetBackup resource is online in the cluster. Also ensure that server processes are running on the active node.

To upgrade NetBackup failover server on PCS Linux

1. Ensure the NetBackup resource is online in the cluster and that server processes are running on the active node before proceeding with any upgrades.
2. Confirm the existence of a catalog backup for your cluster environment. For more details, refer to the *Configuring NetBackup catalog backups in a cluster*.

3 Prior to the upgrade, take the PCS NetBackup cluster resource offline.

Note: Ensure that shared disk and IP resources remain online on the active node during the upgrade process.

4 Freeze the PCS cluster using the command: `pcs property set maintenance-mode=true`

5 Disable the NetBackup cluster agent resource on all nodes of the NetBackup group: `pcs resource disable <nbu_cluster_agent_resource_name>`

6 The upgrade procedure will vary depending on the current release you are upgrading from.

7 Install the NetBackup server software on the active node:

- Ensure to follow the upgrade instructions provided in the *NetBackup Installation Guide*.
- Specify the virtual server name if required.

8 Install the NetBackup server software on each inactive node that may potentially fail over.

9 After completing the upgrade installation, verify if security certificates are deployed on all cluster nodes. Generate certificates if necessary. For detailed instructions, refer to the *NetBackup Security and Encryption Guide*.

10 Enable the PCS NetBackup cluster agent resource on all nodes:`pcs resource enable <nbu_cluster_agent_resource_name>`

11 Unfreeze the PCS cluster to resume normal operation:`pcs property set maintenance-mode=false`

12 Confirm that all Pacemaker resources are online.

13 Verify the proper failover functionality of NetBackup within the cluster. see, *Verifying NetBackup configuration*.

These steps ensure a systematic and controlled upgrade process for the NetBackup failover server while maintaining cluster integrity and service availability.

Chapter 6

Configuring NetBackup

This chapter includes the following topics:

- NetBackup configuration overview
- NetBackup configuration guidelines
- Device configuration guidelines
- Configuring devices
- Configuring NetBackup catalog backups in a cluster
- About configuring backup policies for a NetBackup clustered server
- What to back up
- Guidelines for backing up local disks in a cluster
- Guidelines for backing up the shared disks
- Configuring the PBX LocalPortRange setting in a cluster
- Verifying NetBackup configuration
- Configuring robotic daemons for monitoring (UNIX/Linux clusters)
- Configuring additional services (UNIX/Linux clusters)
- Configuring add-ons for monitoring (UNIX/Linux clusters)
- Configuring additional services (Windows)
- Configuring add-ons for monitoring (Windows)
- About adding license keys

NetBackup configuration overview

NetBackup configuration includes creating storage devices, volumes, the catalog backup, and backup policies. You can perform these tasks from the NetBackup web UI. For detailed instructions about configuring NetBackup, see the NetBackup Administrator's Guide, Volume I.

Table 6-1 summarizes the information that applies to each cluster environment.

Table 6-1 Configuring NetBackup

Cluster Type	Section	Description
All	See "NetBackup configuration guidelines" on page 50.	General guidelines to follow when you configure the NetBackup server in a cluster.
All	See "Device configuration guidelines" on page 51.	General guidelines to follow when you configure devices for a NetBackup server in a cluster.
All	See "Configuring devices" on page 52.	Device configuration guidelines.
All	See "Configuring NetBackup catalog backups in a cluster" on page 53.	Instructions for verifying NetBackup Catalog Backup entries are correct.
All	See "About configuring backup policies for a NetBackup clustered server" on page 53.	Configuring automatic backup policies.
All	See "Verifying NetBackup configuration" on page 57.	Instructions to verify that NetBackup is configured correctly.
UNIX/Linux	See "Configuring robotic daemons for monitoring (UNIX/Linux clusters)" on page 58.	How to configure robotic daemons to fail over NetBackup
UNIX/Linux	See "Configuring add-ons for monitoring (UNIX/Linux clusters)" on page 59.	How to configure NetBackup add-on products to fail over NetBackup in a UNIX/Linux cluster.
Windows	See "Configuring add-ons for monitoring (Windows)" on page 60.	How to configure NetBackup add-on products to fail over NetBackup in Windows.
All	See "About adding license keys" on page 61.	Additional license keys in a cluster environment.

NetBackup configuration guidelines

Review the following guidelines before you configure NetBackup:

- To ensure that all nodes in the NetBackup failover group are properly registered in the EMM database, you must failover the NetBackup Group to all nodes in the NetBackup cluster group.
- The NetBackup server list must be set up correctly on each node where NetBackup is configured as a failover server. For NetBackup in a clustered environment, the virtual server name must appear first. After that name, include the node names within the NetBackup group.
- For each NetBackup server that runs outside of the cluster, the server list must contain the name of each node where NetBackup can run. The list must also contain the name of the virtual server.
- NetBackup depends on names to route information between participants in the backup and restore process. Therefore, the use of names must be consistent within a NetBackup configuration. Specific node names and virtual names should not be used interchangeably.
- CLIENT_NAME should be set to the name of the node.
- CLUSTER_NAME should be the virtual server name that is dedicated to the NetBackup Application that runs on the cluster.
- When you make changes to the NetBackup configuration on the active node, be sure to apply the same changes to each node in the cluster.
- NetBackup server host properties in a cluster
  - NetBackup obtains node information from the EMM database. Therefore, changes to the host properties only affect the nodes that are already registered in the EMM database. (You change the host properties only when you fail over to the NetBackup Group to each node.)
  - You can update the properties for all hosts that are listed in host properties. The exception is the Authorization host property, which is only updated on the active node.
- Configuration information is stored on the shared disk and cannot be configured separately for each node. (This information includes backup policies, storage units, and the NetBackup catalog backup.) All other configuration changes must be applied by moving the NetBackup server to each node.
- By default, NetBackup tries to complete a backup job two times (within a 12-hour window) before it allows the job to fail. Backup attempts may be exhausted before the failover of the NetBackup media server completes. If this situation

happens, increase the **Scheduled backup attempts** setting to 6. You can also avoid this problem; set the **Job retry delay** setting to a lower value.

- The **Job retry delay** setting should be set lower to increase the likelihood that NetBackup is able to initiate all scheduled backups.
- The server list for each client you want to back up should contain the name of each node where NetBackup can run. This list should also contain the name of the virtual server.
- Configure the PBX `LocalPortRange` setting consistently on all cluster nodes to ensure that PBX allocates ports from the same range regardless of the active node. For more information, See "Configuring the PBX LocalPortRange setting in a cluster" on page 55.

Device configuration guidelines

The following are guidelines for configuring the devices for a clustered NetBackup server:

- Choose the **SCSI Persistent reserve** protection option, if possible. The use of persistent reserve is recommended, but take care to ensure that your hardware supports it correctly. See the NetBackup Administrator's Guide, Volume II for more information.
  With this option, NetBackup can recover and use a reserved drive after a failover (if NetBackup owns the reservation). If you use SPC-2 SCSI reserve, a drive reset usually is required because the reservation owner is inoperative. Consult the NetBackup Administrator's Guide, Volume I for more information on how to reset a drive and on the **Enable SCSI Reserve** setting.
- Devices that are attached to one node but not to the other node are available only when the node where they are attached is online. For a NetBackup failover primary server, attach all of the devices to each node where NetBackup is installed. Use shared SCSI or Fibre Channel connections as necessary to share the devices.
- For a NetBackup media server failover configuration, configure devices from the NetBackup primary server with the active node name as the NetBackup media server name.
- For any tape devices that are in a robotic library, ensure that the robot drive number field is set correctly. Use the drive numbering scheme that the manufacturer of the robotic library has implemented. NetBackup considers the first drive in the robot as robot drive number 1. If the manufacturer's drive numbering scheme starts with a different number such as 0, adjust it accordingly.

- Ensure that the robot numbers the failover server uses are consistent on all servers that use that robot. If the robot number that is defined on one node, does not match the number that is defined on another node, backups may fail.
- When you create the storage units that reside on the cluster, select the virtual name of the failover NetBackup server for the **Media server** setting.
- If you choose **Any server** for the media server when you create a storage unit, NetBackup selects the virtual NetBackup server when it performs any backup and restore operations.

Configuring devices

This section describes how to configure devices in NetBackup.

Note: To accommodate disparate SCSI connections on each node of the cluster, you must configure devices on each node. First, configure the devices on the active node. Move the NetBackup group to another node and configure the devices on that node. Then move NetBackup to another node and configure the devices on that node, etc.

You can configure NetBackup to failover if a robotic device fails.

See "Configuring robotic daemons for monitoring (UNIX/Linux clusters)" on page 58.

To configure devices

1. Review the device configuration guidelines.

   See "Device configuration guidelines" on page 51.

2. On the active node, run the NetBackup Device Configuration to automatically discover and configure the devices and to create storage units for those devices.

   It is recommended that you use the NetBackup Device Configuration to configure devices.

3. Move the NetBackup group to another node.
4. Refresh the view in the Media and Device Management utility.

5 Run the NetBackup Device Configuration.

6 Continue to configure the devices on each node in the cluster. Repeat step 3 through step 5.

If device paths are not displayed after you refresh the Devices node or run `tpconfig`, the active node of the cluster is not configured properly.

To add new devices

Follow the same procedure as when you initially configured devices in the cluster. First, configure the devices on the active node. Move the NetBackup group to another node and configure the devices on that node. Then move NetBackup to another node and configure the devices on that node, and so on.

Configuring NetBackup catalog backups in a cluster

For complete information on how to configure and run online catalog backups, refer to the NetBackup Administrator's Guide. For information on recovery of the NetBackup catalog, see the NetBackup Troubleshooting Guide.

Note: An online catalog backup does not back up information on the inactive nodes. You must create a separate policy as described in the following step.

To configure an online, hot catalog backup in a cluster

1 Follow the instructions for creating online catalog backups as described in the NetBackup Administrator's Guide.

2 Create a policy to back up the following directory on each node in the cluster.

Windows	*install_path*\netbackup\var
UNIX/Linux	/usr/openv/var

About configuring backup policies for a NetBackup clustered server

To back up all data in a cluster, create backup policies that back up the local disks, shared disks, and database files in the cluster.

Review the following topics:

See "What to back up" on page 54.

See "Guidelines for backing up local disks in a cluster" on page 54.

See "Guidelines for backing up the shared disks" on page 55.

What to back up

Back up the following to protect all data in the cluster, including file systems and databases:

- Local disks on each node.
  See "Guidelines for backing up local disks in a cluster" on page 54.
- All disks that attach to the shared SCSI bus.
  See "Guidelines for backing up the shared disks" on page 55.
- Virtual servers, which may contain data or contain database applications. Use NetBackup database agents to back up databases.
- In WSFC and VCS for Windows clusters, also be sure to back up the System State and Shadow Copy Components on each node. For WSFC clusters, you must also back up the cluster quorum. The cluster quorum contains recovery information for the cluster and information about changes to the cluster configuration. The cluster quorum is included in the System State or Shadow Copy Components backup.
  See "Guidelines for backing up local disks in a cluster" on page 54.

Guidelines for backing up local disks in a cluster

To protect the data on the node's local disks, configure a policy that includes the cluster node names in the client list. In addition to this policy, you must also configure a separate policy to back up the shared disks.

See "Guidelines for backing up the shared disks" on page 55.

The following are guidelines for configuring the policy to back up local disks:

- If NetBackup is installed on the cluster as separate NetBackup media servers, configure a policy for each node. Each policy should include the cluster node name as a client. For each policy, select the storage unit that you created for the NetBackup media server that is installed on that cluster node.
- In the **Backup Selections** list, add all the local disks (excluding the shared disks).

- For Windows cluster, always include System_State:\ or Shadow Copy Components:\ in the file list to back up the System State for each cluster node. In a policy for an WSFC cluster, System_State:\ or Shadow Copy Components:\ also backs up the cluster quorum information.

Guidelines for backing up the shared disks

To protect the data on the shared disks, configure a policy that includes the virtual server name in the **Clients** list. This server name must be associated with the shared disk. In addition to this policy, you must also configure a separate policy to back up the local disks.

See "Guidelines for backing up local disks in a cluster" on page 54.

The following are guidelines for configuring the policy to back up the shared disks:

- If NetBackup is installed on the cluster as separate NetBackup media servers, select a storage unit that was created for one of the media servers. Or, select **Any Available**.
- If a storage unit does not have local, direct access to the shared disk drives, the data is backed up across the network. This action occurs even if the storage unit refers to a media server running on a node of the cluster that does not currently have control of the shared disk drives. In the **Backup Selections** list, specify the drive letters or mounted directories of the shared disks.
  Note that a backup fails if two separate cluster nodes control the cluster resource that defines the virtual server name and the resource that defines the shared disks. Ensure that the virtual server name and the shared disks are configured to failover together so that the same node always controls them.
- System State information is included in the backup of the node's local disks. You do not need to include System_State:\ or Shadow Copy Components:\ in the file list for this policy.

Configuring the PBX LocalPortRange setting in a cluster

In a clustered NetBackup environment, configure the PBX LocalPortRange setting identically on all cluster nodes. This ensures that PBX allocates ports from the same range regardless of the active node and helps prevent port-related failures during failover.

Configuration of PBX LocalPortRange setting on UNIX/Linux clusters

Note: Setting this range requires NetBackup and VxPBX to be fully stopped and restarted on the node being configured, causing a brief service outage on that node.

To configure the PBX LocalPortRange setting on UNIX/Linux clusters, perform the following steps:

To configure the PBX LocalPortRange setting on UNIX/Linux clusters

1. Stop NetBackup:

   ```
   /usr/openv/netbackup/bin/bpdown -f -v
   ```

2. Verify that NetBackup processes are stopped:

   ```
   /usr/openv/netbackup/bin/bpps
   ```

   Typically, only bpps appears in the output. If other NetBackup processes remain, stop them by using your standard procedure.

3. Stop VxPBX:

   ```
   /opt/VRTSpbx/bin/vxpbx_exchanged stop
   ```

4. Configure the local port range by using vxpbxcfg:

   ```
   /opt/VRTSpbx/bin/vxpbxcfg -s --localportrange min_port-max_port
   ```

   Replace min_port and max_port with the same port range on every cluster node. For example, 10000-10100. Ensure that the selected port range is allowed by local firewall rules and does not conflict with other applications.

5. Start VxPBX:

   ```
   /opt/VRTSpbx/bin/vxpbx_exchanged start
   ```

6. Start NetBackup:

   ```
   /usr/openv/netbackup/bin/bpup -f -v
   ```

7. Repeat these steps on all cluster nodes to ensure that every node uses the same local port range.

Configuration of PBX LocalPortRange setting on Windows clusters

Note: Setting this range requires NetBackup and VxPBX to be fully stopped and restarted on the node being configured, causing a brief service outage on that node.

To configure the PBX LocalPortRange setting on Windows clusters, perform the following steps:

To configure the PBX LocalPortRange setting on Windows clusters

1. Stop NetBackup. Run the command from an Administrator command prompt. Replace install_path with your NetBackup installation directory.

   ```
   install_path\NetBackup\bin\bpdown /f /v
   ```

2. Verify that NetBackup processes are stopped.

   ```
   install_path\NetBackup\bin\bpps
   ```

3. Stop VxPBX:

   ```
   net stop VRTSpbx
   ```

4. Configure the local port range by using vxpbxcfg.

   ```
   install_path\VxPBX\bin\vxpbxcfg -s --localportrange
   min_port-max_port
   ```

   Replace min_port and max_port with the same port range on all cluster nodes. For example, 10000-10100. Ensure that the selected port range does not conflict with other applications and is allowed by local firewall rules.

5. Start VxPBX:

   ```
   net start VRTSpbx
   ```

6. Start NetBackup:

   ```
   install_path\NetBackup\bin\bpup /f /v
   ```

7. Repeat these steps on all cluster nodes to ensure that every node uses the same local port range.

Verifying NetBackup configuration

After you complete the configuration of storage devices, volumes, the catalog backup, and the backup policies, verify that NetBackup fails over properly in the cluster.

To verify NetBackup configuration

1. Confirm that the NetBackup is online on the primary node, then determine if the following can be completed successfully:

   - Scheduled backups
   - User-directed backups
   - NetBackup catalog backups

- Server-and user-directed restores

2 Switch the NetBackup resource group to another node and perform the same tests in the previous step. Repeat for each node in the cluster where NetBackup is installed.

Configuring robotic daemons for monitoring (UNIX/Linux clusters)

By default, robotic daemons do not cause NetBackup to failover if they fail. You can configure robot daemons to failover NetBackup if a daemon fails.

Note: You must configure robots before you perform the following instructions. Refer to the NetBackup Installation Guide for instructions on how to configure storage devices.

To configure NetBackup to failover if a robotic daemon fails

1 Configure your robots on each node in the cluster.

2 Run the following script:

```
/usr/openv/netbackup/bin/cluster/cluster_config -r
```

3 Choose `a` (Add).

4 Select your robot from the list.

Multiple robots can be selected.

To remove a robotic daemon from monitoring

1 Run the following script:

```
/usr/openv/netbackup/bin/cluster/cluster_config -r
```

2 Choose `d` (Delete).

3 Select the robot type you want to remove.

Configuring additional services (UNIX/Linux clusters)

By default , all the necessary NetBackup services are added to the NetBackup Cluster Group.

To add a service to the NetBackup Cluster Group

- Run the following command:

```
/usr/openv/netbackup/bin/bpclusterutil
-addSvc "ServiceName"
```

This command brings up the service when the group comes online, but the service is not monitored. If the service*ServiceName* fails, it does not cause the group to failover.

To delete a service from the NetBackup Cluster Group

- Run the following command:

```
/usr/openv/netbackup/bin/bpclusterutil
-deleteSvc "ServiceName"
```

  If you delete a critical service, cluster do not failover if that service fails.

Configuring add-ons for monitoring (UNIX/Linux clusters)

By default, add-on products (such as NetBackup Vault) do not cause NetBackup to failover if they fail. These products can be configured to failover NetBackup if an add-on product fails.

To enable monitoring for the optional services

- Run the following command:

```
/usr/openv/netbackup/bin/bpclusterutil
-enableSvc"ServiceName"
```

To disable monitoring for the optional services

- Run the following command:

```
/usr/openv/netbackup/bin/bpclusterutil
-disbleSvc"ServiceName"
```

Monitoring can be turned on or off for only NetBackup Vault Service and NetBackup Key Management Service. The ServiceName parameters for these services are `nbvault`and `nbkms`.

Configuring additional services (Windows)

By default , all the necessary NetBackup services are added to the NetBackup Cluster Group.

To add a service

- Run the following command:

  ```
  <NetBackup_install_path>\NetBackup\bin\bpclusterutil.exe
  -addSvc "ServiceName"
  ```

  This command brings up the service when the group comes online, but the service is not monitored. If the service *ServiceName* fails, it does not cause the group to failover.

To delete a service from a NetBackup Cluster Group

- Run the following command:

  ```
  <NetBackup_install_path>\NetBackup\bin\bpclusterutil.exe
  -deleteSvc "ServiceName"
  ```

Configuring add-ons for monitoring (Windows)

By default, add-on products (such as NetBackup Vault) do not cause NetBackup to failover if they fail. These products can be configured to failover NetBackup if an add-on product fails.

To enable monitoring for the optional services

- Run the following command:

  ```
  <NetBackup_install_path>\NetBackup\bin\bpclusterutil.exe
  -enableSvc "ServiceName"
  ```

To disable monitoring for the optional services

- Run the following command:

  ```
  <NetBackup_install_path>\NetBackup\bin\bpclusterutil.exe
  -disbleSvc "ServiceName"
  ```

Monitoring can be turned on or off only for NetBackup Vault Service and NetBackup Key Management Service. The *ServiceName* parameters for these services are "NetBackup Vault Service", "NetBackup Key Management Service"

About adding license keys

If you add other licenses at the end of a Windows primary server installation or if you add new licenses later, you do not need to failover to add these licenses to each node in the cluster. On Windows, you can also use the `bpminlicense` command. On UNIX/Linux servers, you can use the `get_license` command to add license keys without having to failover to each node. The inactive nodes when becomes active can use those licenses from a shared drive location: `/var/global/licenses`.

Some features and products (such as NetBackup Shared Storage Option) require the keys to also be installed on the media server.

Chapter 7

Operational notes

This chapter includes the following topics:

- General notes on clustered primary server administration
- About WSFC clusters
- About NetBackup cluster application management
- Logging information
- About the support for multiple IP addresses in NetBackup
- Log on to server using virtual name
- Normal error messages when upgrading clustered servers

General notes on clustered primary server administration

Consider the following operational issues to consider when you use NetBackup as a failover server:

- If a NetBackup server fails over and backup jobs are running, one of the following things happen:
  - If checkpoint restart is enabled for backup jobs for the policy, any backups that were running are resumed at the last checkpoint. Note that the schedule window must permit the job to be resumed.
  - If checkpoint restart is not enabled for backup jobs, any backup jobs that were running fail. These jobs show up as failed jobs in the Activity Monitor or NetBackup reports. Scheduled backup jobs are retried according to the normal retry logic. (See the **Job retry delay** and the **Schedule backup attempts** attributes). The schedule window and so on must permit the retry

of the job. After a failover occurs, the user must restart user-directed backups and manual backups.

Refer to the NetBackup Administrator's Guide, Volume I, for more information on checkpoint restart , Job retry delay, and Scheduled backup attempts.

- If a NetBackup primary server fails over, then any restore jobs that were running during that time will fail. These jobs appear as failed jobs in the Activity Monitor and in the NetBackup reports. Even if you try to resume the failed jobs after the server has failed over successfully, the jobs remain in a partial state.

  To resolve this issue, you must trigger such restore jobs again after the primary server has failed over successfully.
- After a failover occurs on a NetBackup failover server, it takes time for the tape devices and media servers to be reset. For example, a tape may have to be rewound before it is made available. Until the device is again ready for use, you may see errors. For example, you may see error 213 (no storage units available for use) or error 219 (the required storage unit is unavailable).
- After a failover, NetBackup may change the status of a drive that is required for a backup or restore to PEND. More information is available about how to use the Device Monitor to resolve a pending request or action.

  See the NetBackup Administrator's Guide, Volume I.
- If a failover occurs while you are using the NetBackup web UI, refresh the browser page. Refreshing the page ensures that the information from the active node is displayed correctly.
- The backup and restore process is the same whether you are in a cluster or a non-cluster environment. See the NetBackup Troubleshooting Guide, for further information on the process for backups and restores.
- True Image Restore (TIR) is not supported for clustered shared drives.

About WSFC clusters

Note the following points before you use NetBackup as a failover server in an WSFC environment:

- If there are no tape devices configured on the controlling node of the NetBackup failover server, the NetBackup Device Manager service resource takes itself offline. If you do not intend to configure tape devices for the NetBackup failover server, you may want to delete the NetBackup Device Manager service resource from the NetBackup group. This way you can avoid seeing the group in a warning state or failed state.
- For WSFC clusters with three or more nodes, the WSFC Move Group command lists all of the nodes in the cluster. You must pick a node that is valid for the

NetBackup failover server to use. (WSFC displays all nodes in the cluster, even those nodes where NetBackup has not been installed.)

- Also refer to the information in the previous sections for further notes that are relevant to all cluster environments.

About NetBackup cluster application management

Only use the cluster application's management tools to start and to stop NetBackup in the cluster. In a UNIX or Linux environment, do not use `bp.start_all` or `bp.kill_all` to start or stop NetBackup.

Logging information

NetBackup records information on the processes. You can use this information to determine why a server has failed over. Logging information is highly useful for troubleshooting.

UNIX and Linux logging

Logging information for UNIX and Linux platforms can be found at the following locations:

- Cluster configuration-related information is recorded in `log.cc.<date>` file, which is located at `/usr/openv/netbackup/logs/cluster`. The configuration scripts creates the log directory, if it is not present.
- Cluster upgrade-related information is recorded in `trace.cluster_upgrade.<process_ID>` file, which is located `at /usr/openv/netbackup/logs/cluster`.
- Agent (Online/Offline/Monitor) related information is recorded in`log.<date>` file, which is located at `/usr/openv/netbackup/logs/cluster`
- Add the following configuration parameter "`DEBUG_LEVEL=1`" to the `/usr/openv/netbackup/bin/cluster/NBU_RSP` file to generated detailed logging.

  Note: This configuration is node-specific and affects the logging level on that enabled node. Enable this option only when required and turn it off when not required for storage considerations.

Windows logging	The cluster configuration status box reports details about cluster configuration. If problems occur, see the status box. Details of the cluster configuration steps that occur during the install are recorded in the install logs. In the logs, you have a record of the parameters used to perform cluster configuration commands and their return statuses. Logging information for Windows platform can be found at the following locations: ■ Cluster configuration and upgrade related information is recorded in `ClusterConfig.<timestamp>.log` file, which is located at `%ALLUSERSPROFILE%\Veritas\NetBackup\InstallLogs`. ■ For Agent (WSFC) use Event Viewer. ■ For Agent (VCS) use NetBackupVCS agent log file, which is located in the log directory of VCS.

About the support for multiple IP addresses in NetBackup

NetBackup supports assigning multiple virtual IP addresses to a clustered primary server. After a clustered primary server installation or upgrade, use the `bpclusterutil -addIP` command to add multiple virtual IP addresses.

If your virtual name resolves into multiple IP addresses, you must add the associated IP addresses using the `bpclusterutil -addIP` command to make NetBackup work seamlessly.

For more details on the command, refer to the NetBackup Commands Reference Guide.

For more information about using IPv6 with NetBackup, refer to the NetBackup Administrator's Guide, Volume I.

For supported versions of cluster technologies, see the NetBackup Software Compatibility List.

Log on to server using virtual name

When connecting to the NetBackup primary server cluster using the NetBackup web UI, always use the virtual name as the server name in the URL.

Normal error messages when upgrading clustered servers

When you upgrade clustered NetBackup servers, you may encounter Windows Event Log messages that indicate that the service **NetBackup Scale-Out Relational Database Manager** failed to start. These messages are generated in a short period of time – normally a window of two to three seconds. These messages coincide with the cluster configuration portion of the upgrade. You should expect these messages and know that they do not reflect a problem with the upgrade.

Appendix A

NetBackup primary server in a cluster using multiple interfaces

This appendix includes the following topics:

- About NetBackup primary server in a cluster using multiple interfaces
- Requirements for use of a NetBackup primary server in a cluster with multiple interfaces
- Configuring the NetBackup primary server in a cluster using multiple interfaces

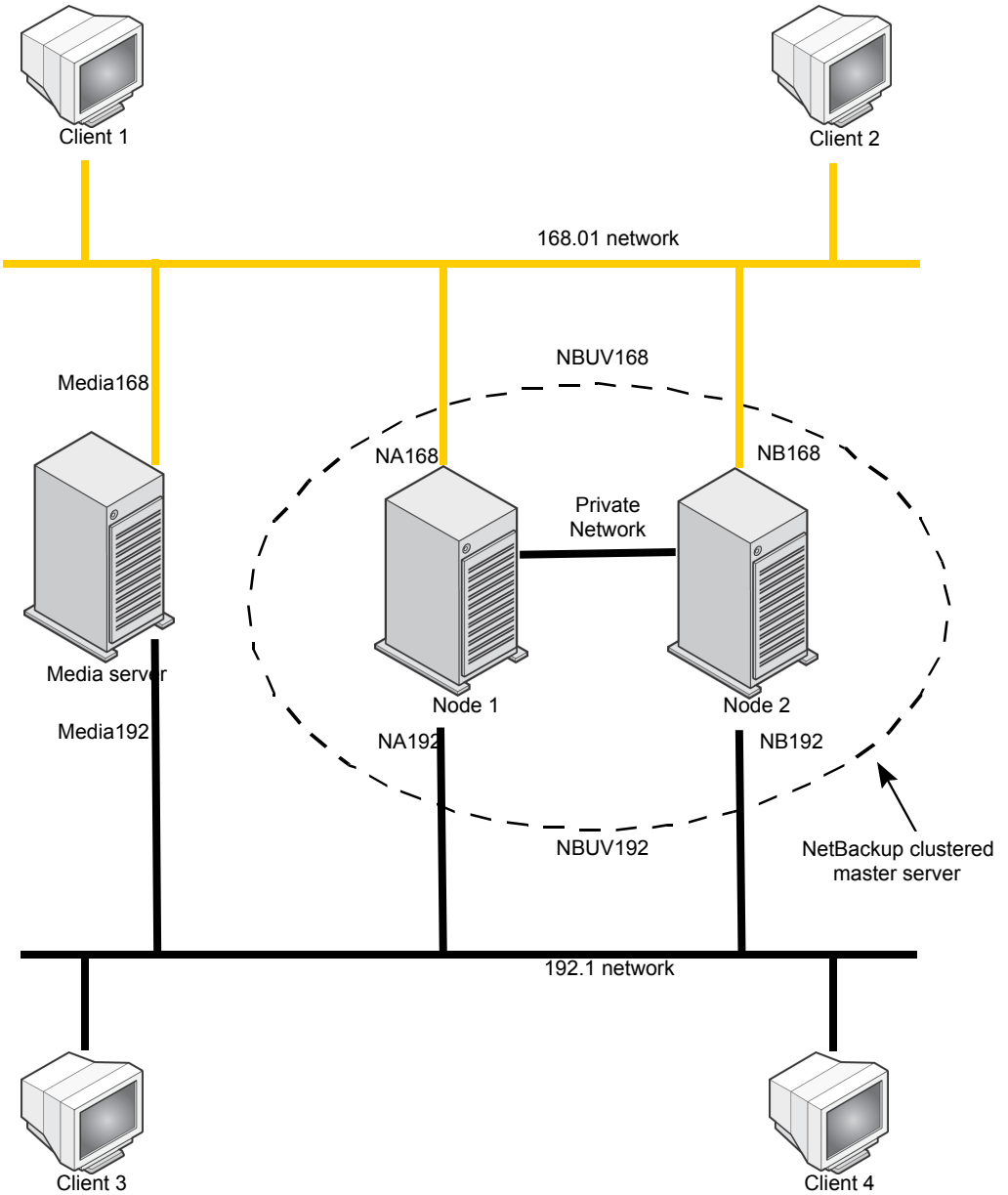
About NetBackup primary server in a cluster using multiple interfaces

In a cluster environment, all NetBackup primary server traffic and communication flow through the network interface that is associated with the virtual name of the primary server. With the ANY_CLUSTER_INTERFACE configuration parameter, you can allow communication through any of the interfaces available to the NetBackup primary server.

The following figure depicts a scenario where a clustered NetBackup primary server has access to two separate networks (168.1 and 192.1). Client computers are attached to both networks and must be backed up. The virtual name for the primary server (for example, NBUV168) can only be associated with one of the networks. So all NetBackup communication only occurs over that specific interface. Clients on other interfaces cannot be contacted.

Figure A-1 shows NetBackup in an environment with multiple network interfaces.

Figure A-1 NetBackup in an environment with multiple network interfaces



Requirements for use of a NetBackup primary server in a cluster with multiple interfaces

The following requirements exist when you use a NetBackup primary server in a cluster with multiple interfaces:

- A cluster environment that is properly installed and configured.
- Verify that you have a clustered NetBackup primary server that is functional.
- A unique virtual name (IP address and host name) associated with each interface.

Configuring the NetBackup primary server in a cluster using multiple interfaces

Perform the following steps to allow communication over an additional network interface.

To configure the NetBackup primary server in a cluster using multiple interfaces

1. For each additional interface, add a virtual name and IP address resource in the NetBackup cluster group.

   This virtual name is the primary server name that the clients reference on their particular network.

2. Configure the ANY_CLUSTER_INTERFACE parameter.
3. On Windows, perform the following steps.
   - In regedit, go to the following.

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion
     \Config
     ```

   - Create a new DWORD value that is called `ANY_CLUSTER_INTERFACE`.
   - Change the **Value Data** to 1.
4. On UNIX/Linux, add the following entry to the `bp.conf`.

   ```
   ANY_CLUSTER_INTERFACE = 1
   ```

5. Add the following to the server list of the primary server.
   - The node names of the primary server, for each network interface.
   - The virtual name of the primary server, for each network interface.

For example, to configure the primary server in an environment with multiple network interfaces, add the following: NBUV168, NBUV192, NA168, NA192, NB168, NB192.

See Figure A-1 on page 68.

6 Add the node name of each media server to the media server list on the primary server.

For example, add Media168 and Media192.

7 Repeat step 2 through step 6 for all nodes where the NetBackup primary server is installed.

8 Update the server list for all NetBackup clients.

The list must include all the possible names for the primary server on their network. For example, for clients on the 168.1 network, include the server names NBUV168, NA_168, and NB_168. For clients on the 192.1 network, include the server names NBUV192, NA_192, and NB_192.