

Veritas NetBackup™ for Nutanix Acropolis Hypervisor (AHV) Administrator's Guide

Release 8.2



Veritas Acropolis Hypervisor (AHV) Guide

Last updated: 2019-06-28

Legal Notice

Copyright © 2019 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

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

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

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

<https://my.veritas.com>

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

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

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

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

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1	Introduction to NetBackup for Acropolis Hypervisor (AHV)	6
	Protect AHV using NetBackup	6
	NetBackup terminology related to the AHV backup	7
	NetBackup for AHV environment	8
Chapter 2	Prerequisites, notes, and restrictions	11
	Prerequisites	11
	Notes and restrictions	13
	NetBackup character restrictions for virtual machine names	14
Chapter 3	Configuring NetBackup communication with AHV	15
	Establishing communication between components	15
	Adding a backup host to the NetBackup master server	16
	Adding a backup host to the NetBackup master access list	17
	Configuring a NetBackup Appliance as a backup host	18
	Adding a backup host to the Acropolis Cluster access list	18
	Adding the Nutanix Acropolis Cluster credentials for NetBackup	18
	Managing SSL certificates	20
	Managing SSL certificates on NetBackup Appliance	22
	About the nb_nutanix-ahv configuration file	23
Chapter 4	Configuring NetBackup policies for AHV	25
	About the BigData policy type	25
	Creating a BigData policy using the NetBackup Policies utility	26
	Creating a BigData policy using the Backup Policy Configuration Wizard	27
	Creating a BigData policy using the NetBackup Command Line Interface	28

Chapter 5	Backup and recovery	31
	Back up the Nutanix AHV virtual machines	31
	Basic phases in a NetBackup backup of an AHV	31
	Overview of the Nutanix AHV virtual machines recovery process	32
	About recovering the Nutanix AHV virtual machines	33
	Planning the recovery of a Nutanix AHV VM	33
	Recovering a Nutanix AHV VM using the Backup, Archive, and Restore console	36
	Recovering a Nutanix AHV VM using the command line	38
Chapter 6	Troubleshooting issues	43
	Troubleshooting issues related to AHV backup	43
	NetBackup logs	43
	About errors during policy creation, restore, and validation	44
	NetBackup status codes	46
Appendix A	NetBackup commands to backup and restore Nutanix AHV virtual machines	49
	NetBackup commands for protecting the AHV	49
Index		51

Introduction to NetBackup for Acropolis Hypervisor (AHV)

This chapter includes the following topics:

- [Protect AHV using NetBackup](#)
- [NetBackup terminology related to the AHV backup](#)
- [NetBackup for AHV environment](#)

Protect AHV using NetBackup

Virtual infrastructure is one of the key components of today's modern data centers. The ability to back up and restore your virtual machines is essential. It maintains business continuity and deliver superior high availability and disaster recovery (HA-DR) solutions to meet stringent service level agreements.

Veritas NetBackup, in addition to VMware and Microsoft Hyper-V, lets you back up and restore Nutanix AHV virtual machines.

These are the high-level steps to protect the Nutanix AHV virtual machines:

Table 1-1 High-level steps to protect the Nutanix AHV virtual machines

Step	Step overview	Sub-steps and links to the sections
1	Understand NetBackup and AHV	See “NetBackup for AHV environment” on page 8.

Table 1-1 High-level steps to protect the Nutanix AHV virtual machines
(continued)

Step	Step overview	Sub-steps and links to the sections
2	Establish communication between NetBackup and the Nutanix components	Add the name of the backup host to relevant file system whitelists on the Prism web console and the NetBackup master server. ■ See “Adding a backup host to the NetBackup master access list” on page 17. ■ See “Adding a backup host to the Acropolis Cluster access list” on page 18. Add the Nutanix Acropolis cluster credentials to the NetBackup master server. ■ See “Adding the Nutanix Acropolis Cluster credentials for NetBackup” on page 18. Validate SSL certificate from Nutanix. ■ See “Managing SSL certificates ” on page 20.
3	Create a backup policy	Create a BigData policy. ■ See “Creating a BigData policy using the NetBackup Policies utility” on page 26.
4	Read the prerequisites, notes, and restrictions on NetBackup for AHV	■ See “Prerequisites” on page 11. ■ See “Notes and restrictions” on page 13.
5	Protect the Nutanix AHV virtual machines	Backup the virtual machines ■ See “Back up the Nutanix AHV virtual machines” on page 31. Recover the virtual machines ■ See “Planning the recovery of a Nutanix AHV VM” on page 33. ■ See “Recovering a Nutanix AHV VM using the Backup, Archive, and Restore console” on page 36. ■ See “Recovering a Nutanix AHV VM using the command line” on page 38.

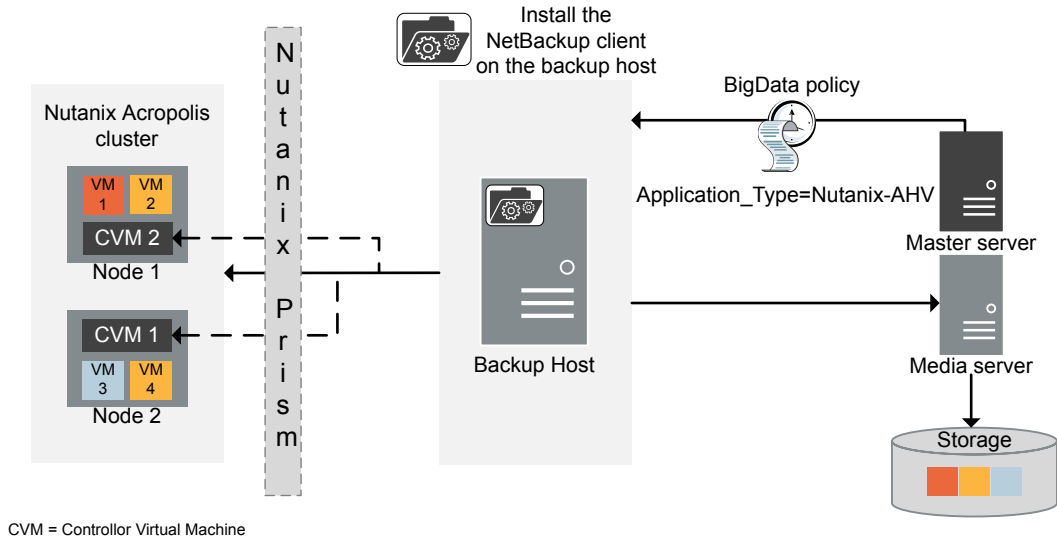
NetBackup terminology related to the AHV backup

The following table describes the NetBackup terminology that is related to the AHV backup.

Term	Description
Application server	The name of the Acropolis cluster. It is identified using the <code>Application_Server</code> parameter during backup selections. You can obtain the Acropolis cluster name from the Prism web console using Settings > Cluster Details.
Application type	The type of application being backed up. It is identified using the <code>Application_Type</code> parameter during backup selections. For Nutanix AHV, the value for the <code>Application_Type</code> parameter is Nutanix-AHV. This value is fixed and cannot be changed.
Backup host	The backup host performs backups on behalf of the virtual machines. The operating system of the backup host must be Linux NetBackup client version 8.1 or later. It is identified using the <code>Backup_Host</code> parameter during backup selections. Veritas recommends the following configuration as a backup host: ■ NetBackup master server on a Linux platform ■ NetBackup media server on a Linux platform ■ NetBackup Appliance and NetBackup virtual appliance ■ NetBackup client on a Linux platform See “Adding a backup host to the NetBackup master server” on page 16.

NetBackup for AHV environment

[Table 1-2](#) describes the components that are required for NetBackup to back up and restore a Nutanix AHV virtual machine.

Figure 1-1 Component overview for NetBackup for AHV**Table 1-2** Components required for NetBackup for AHV

Component	Description and requirements
NetBackup master server	Runs the backup policies and starts backups and restores.
NetBackup media server or a backup host	Reads and writes backup data and manages NetBackup storage media. If your backup host is not a NetBackup master, media, or appliance, install a NetBackup client on the backup host to process backup and restore requests.
Nutanix Acropolis Hypervisor or Acropolis Hypervisor or AHV	Provides a virtualization platform within Nutanix's hyper converged infrastructure.
Nutanix Acropolis cluster	Provides a multi-node cluster configuration that manages storage, computing, and virtualization.

Table 1-2 Components required for NetBackup for AHV (*continued*)

Component	Description and requirements
Nutanix Prism or Prism web console	Prism is an end-to-end management solution for the virtualized data center environments that streamlines and automates common workflows. It eliminates the need for multiple management solutions across data center operations. https://www.nutanix.com/products/prism/

For further details and explanation of the Nutanix terminology, refer to the *Nutanix documentation*.

Prerequisites, notes, and restrictions

This chapter includes the following topics:

- [Prerequisites](#)
- [Notes and restrictions](#)

Prerequisites

The following prerequisites apply to NetBackup for AHV.

- For the required NetBackup licenses, see the following page:
[How to use NetBackup plug-ins and agents: download, install, and availability information](#)
- For a list of supported versions, see:
[NetBackup Master Compatibility List](#)
- Before you initiate a backup of a virtual machine, verify the following:
 - You have appropriate administrative rights and permissions from Nutanix to complete a backup for AHV virtual machines.
For information on getting administrative privileges, refer to the Nutanix documentation.
 - The NetBackup master server can communicate with the backup host.
 - The backup host is able to communicate with the Acropolis cluster.
- Whitelist the backup host on the Acropolis cluster using the file whitelisting option available through the Prism web console or its command line interface.
See [“Adding a backup host to the Acropolis Cluster access list”](#) on page 18.

- If you want to restore a VM to the Nutanix Acropolis cluster or container that you have deleted, you must first recreate the cluster or container. After this recreation is complete, then start the recovery process. Alternatively, you can recover a VM to a different cluster or container.
- If you want to restore a VM to another Nutanix AHV cluster, ensure that the AHV cluster has the same configuration as the original AHV cluster.

Verifying the operating system and platform compatibility

Verify that the NetBackup for AHV is supported on your operating system or platform.

To verify operating system and compatibility

- 1 Go to the following page:
[NetBackup Master Compatibility list](#)
- 2 For information on support for Nutanix AHV, see Support for **NetBackup in a Virtual Environment** list from the [NetBackup Master Compatibility List](#) page.

NetBackup server and client requirements

Verify that the following requirements are met for the NetBackup server:

- The NetBackup server software is installed and operational on the NetBackup server.
- Ensure that you configure any backup media that the storage unit uses.
- The required number of media volumes depend on the following:
 - The devices that are used and storage capacity of the media
 - The sizes of the virtual machines that you want to back up
 - The amount of data that you want to archive
 - The size of your backups
 - The length of retention of the backup images

Verify that the NetBackup client software is installed on the backup host.

License requirements for the Nutanix AHV

NetBackup for AHV requires an Enterprise Client license for each Nutanix Acropolis cluster node.

For detailed information about adding licenses, refer to the "Adding NetBackup licenses" section of the [NetBackup Administrator's Guide, Volume I](#).

Notes and restrictions

The following notes and restrictions apply to NetBackup for AHV.

- Version of the NetBackup master server or media server and the NetBackup client on the backup host require 8.1 or later.
Veritas recommends that you configure a NetBackup media server as a backup host.
- Linux is the required operating system of the backup host.
- NetBackup for Nutanix AHV supports only one backup host for each backup policy.
- To backup other hypervisors that run on a Nutanix Acropolis cluster, use a backup policy specific to that hypervisor. For example, to backup VMware ESX on a Nutanix Acropolis cluster, use a VMware policy. Similarly, to backup Hyper-V on a Nutanix Acropolis cluster, use a Hyper-V policy.
- When you specify the backup selections for a **BigData** policy for the Acropolis cluster, provide the following parameters:
 - `Application_Type=Nutanix-AHV`
The value for this parameter is fixed and cannot be changed.
 - `Application_Server=Fully Qualified Domain Name of the Nutanix Acropolis cluster`
 - `Backup_Host=<Fully Qualified Domain Name>`
- The parameters - `Application_Type`, `Application_Server`, and `Backup_Host` are not case sensitive. However, their values are case-sensitive.
- When you provide multiple entries for the `Application_Type`, or `Application_Server`, only the first valid entry is considered and the rest are ignored. However, providing multiple entries for the `Backup_Host` parameter is not supported.
- Policy validation is not conducted for the policies that are created using the Policy Configuration Wizard.
- You cannot backup two or more virtual machines with the same name. Each virtual machine must have a unique name.
- The restore operation for a partially successful backup is currently not supported.
- NetBackup for AHV cannot backup the virtual machines that have volume groups attached.

See [“Creating a BigData policy using the NetBackup Policies utility”](#) on page 26.

See [“Creating a BigData policy using the NetBackup Command Line Interface”](#) on page 28.

NetBackup character restrictions for virtual machine names

When you configure a **BigData** policy to back up an Acropolis cluster, you are required to add clients or virtual machines. To add a virtual machine to the **BigData** policy, you must provide the name of the virtual machine.

You can obtain the name of the virtual machine from the **VM Name** column on the Prism web console.

The name of the virtual machine is case-sensitive. Certain characters are not allowed in the virtual machine name. If the name contains wrong or invalid characters, the backup may fail.

For NetBackup, the following characters are allowed in the virtual machine names:

- Uppercase and lowercase ASCII characters
- Numbers
- Period (.)
- Hyphen (-)
- Underscore (_)
- Plus sign (+)
- Percent sign (%)
- Left and right parentheses ()
- Spaces
 - If the VM name contains a space, substitute the space with "%20". For example, if the VM name is **Nutanix VM**, you must enter **Nutanix%20VM**.
 - However, if the VM name itself contains "%20", it is interpreted as a space, which makes the virtual machine name invalid or non-existent. This interpretation of "%20" may fail the backup.
For example, the name of your virtual machine is "Nutanix%20VM". The policy interprets "Nutanix%20VM" as "Nutanix VM", which is incorrect and does not exist and thus, failing the policy validation.
 - Further, using a consecutive sequence of "%20" is not allowed.

Configuring NetBackup communication with AHV

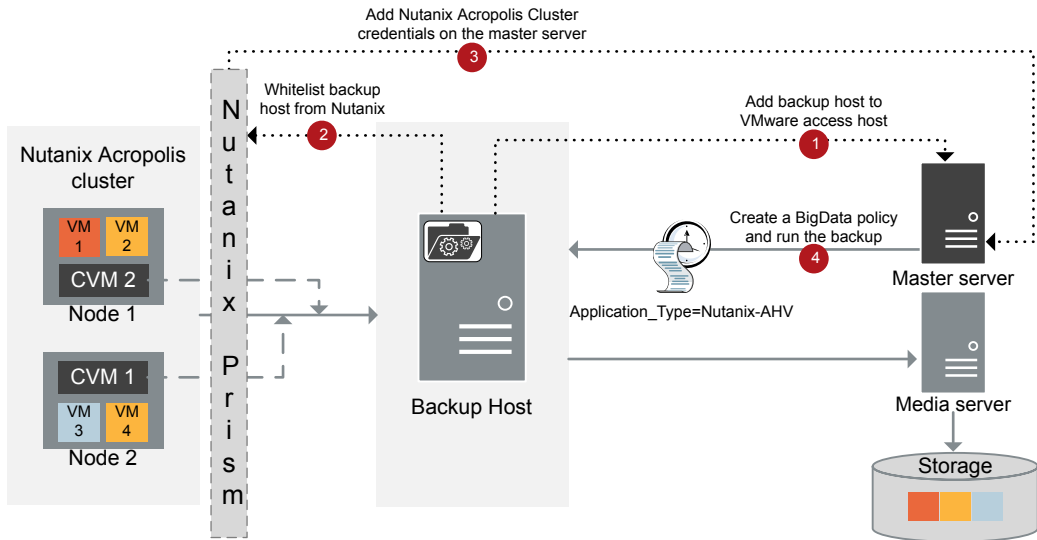
This chapter includes the following topics:

- [Establishing communication between components](#)
- [Adding a backup host to the NetBackup master server](#)
- [Adding a backup host to the Acropolis Cluster access list](#)
- [Adding the Nutanix Acropolis Cluster credentials for NetBackup](#)
- [Managing SSL certificates](#)

Establishing communication between components

The NetBackup master server, media server, the backup host, and the Nutanix Acropolis cluster need to establish communication with each other to complete a backup or restore job. This chapter discusses configuration of these components and establishing communication between them.

Figure 3-1 Communication channels between NetBackup and Nutanix AHV



Adding a backup host to the NetBackup master server

The backup host is a key component in the NetBackup and Nutanix communication environment. The backup host acts as a channel to establish an indirect communication between the NetBackup master server and the Acropolis cluster.

To add a backup host, you must start by creating a **BigData** policy. During policy creation, you are prompted to specify backup selections. In the backup selections, you are required to specify a backup host.

To add a backup host from the NetBackup Administration Console:

- 1 Create a **BigData** policy from the NetBackup Administration Console using the Policies utility.
 See [“Creating a BigData policy using the NetBackup Policies utility”](#) on page 26.
- 2 On the **Backup Selections** tab, click **Add** and enter the following parameter to add a backup host:

`Backup_Host=<Fully Qualified Domain Name>`

To add a backup host from the NetBackup Command Line Interface

- 1 Create a **BigData** policy using the NetBackup Command Line Interface.
 See [“Creating a BigData policy using the NetBackup Command Line Interface”](#) on page 28.
- 2 Run the following command to add a backup host

```
bpplinclude policy_name -add pathname or directive...
```

For example: `bpplinclude nutanix -add Backup_Host=<Fully Qualified Domain Name>`

See [“Adding a backup host to the NetBackup master access list”](#) on page 17.

See [“Adding a backup host to the Acropolis Cluster access list”](#) on page 18.

Adding a backup host to the NetBackup master access list

When the backup host is not a NetBackup media server or an appliance, you need to add the backup host to the NetBackup **VMware Access Hosts** list.

To add a backup host to NetBackup master access list

- 1 In the **NetBackup Administration Console**, in the left pane, click the **Host Properties** node.
- 2 Select an appropriate option from the **Master Servers**, **Media Servers**, and **Clients** options to view the details of your backup host.
 For example, select **Media Servers**, if you have configured a media server as your backup host.
- 3 Select and right-click the backup host to view **Properties**.
- 4 In the **Host Properties** dialog box, click **VMware Access Hosts**.
- 5 To add the backup host to NetBackup master access list, click **Add**.
 In the **New Server** dialog box, enter the name of the backup host. Click **Add**.

Note: Currently, there is no provision to differentiate between a backup host for VMware and Nutanix. Therefore, consider providing an appropriate identifier for the backup host name.

See [“Adding a backup host to the NetBackup master server”](#) on page 16.

See [“Adding a backup host to the Acropolis Cluster access list”](#) on page 18.

Configuring a NetBackup Appliance as a backup host

You can configure a NetBackup Appliance as a backup host.

To manage SSL certificates and to edit the `nb_nutanix-ahv.conf` file, See [“To access and copy the nb_nutanix-ahv.conf file on the appliance”](#) on page 22.

To copy an SSL certificate file, See [“To copy the SSL certificate to an appropriate location on the appliance”](#) on page 23.

Adding a backup host to the Acropolis Cluster access list

The Acropolis cluster must grant access to the backup host.

To grant file system access to the backup host, the Acropolis cluster requires you to whitelist the backup host.

To whitelist the backup host:

- 1 Log on to the Prism web console to access the Acropolis cluster.
- 2 Click **Settings > Filesystem Whitelists**.
- 3 In the **Filesystem Whitelists** dialog box, add the details for the backup host in the **IP ADDRESS/NETMASK** field in the required format.

For accurate steps and menu options, refer to the *Nutanix documentation*.

See [“Adding a backup host to the NetBackup master server”](#) on page 16.

See [“Adding the Nutanix Acropolis Cluster credentials for NetBackup”](#) on page 18.

Adding the Nutanix Acropolis Cluster credentials for NetBackup

You must add the credentials for accessing the Acropolis cluster to the NetBackup master server. There are two options to accomplish this.

The backup host needs to access the Acropolis cluster. To access the Acropolis cluster, the backup host needs to obtain the cluster credentials. Therefore, the backup host communicates with the NetBackup master server to obtain these credentials.

To add credentials for the Acropolis cluster using the NetBackup Administration Console

- 1** In the **NetBackup Administration Console**, in the left pane, click the **Media and Device Management** node.
- 2** Click the **Credentials** node to see the **Virtual Machine Server** option.
- 3** Right-click **Virtual Machine Server** and select **New Virtual Machine Server...**
- 4** In the **New Virtual Machine Server** dialog box, enter a name for the server. Click **OK**.
- 5** In the **Credentials** pane of the **New Virtual Machine Server - <server_name>** dialog box, do the following:

- From the **Virtual Machine Server Type** drop-down list, select **Nutanix Acropolis Cluster**.
- In the **User name** field, enter the user name to access the Nutanix Acropolis Cluster.
- In the **Password** field, enter the password to access the Nutanix Acropolis Cluster.

If you provide an invalid or incorrect credential, you may see the following status code in the Activity Monitor:

Status code: 6629: Unable to complete the operation. Failed to authorize the user or the server.

- The **Validate using backup host** and the **Connect using Port number** options are unavailable for the Nutanix Acropolis Cluster.

Note: The default port number for a Nutanix Acropolis Cluster is 9440. However, the provision to change this port number is available only through the command line interface using the `tpconfig` command.

See [To add credentials for the Acropolis cluster using the NetBackup Command Line Interface](#) for information about using the `tpconfig` for Nutanix Acropolis cluster.

- 6** To save your changes, click **OK**.

You may also add credentials for the Acropolis cluster using the command line interface.

To add credentials for the Acropolis cluster using the NetBackup Command Line Interface

- 1 Go to the following directory:

```
/usr/opensv/volmgr/bin/
```

- 2 From the command line, run:

```
tpconfig -add | -update -virtual_machine virtual_machine_name  
-vm_user_id user_id -vm_type virtual_machine_type -requiredport  
IP_port_number [-password password [-key encryption_key]]
```

For example: `/usr/opensv/volmgr/bin/tpconfig -add -virtual_machine my.virtualmachine.com -vm_user_id admin -vm_type 9 -password abc@123`

For detailed information about the `tpconfig` command, see the *NetBackup Commands Reference Guide*.

See [“Adding a backup host to the NetBackup master server”](#) on page 16.

See [“Adding a backup host to the Acropolis Cluster access list”](#) on page 18.

Managing SSL certificates

This section describes the various ways to manage SSL certificates with NetBackup for AHV.

The Nutanix Acropolis cluster comes with its default certificate. For detailed information about Nutanix certificates, refer to the *Nutanix documentation*.

You may use the default Nutanix certificate or you may choose to install one of the following certificates on the Nutanix Acropolis cluster:

- Self-signed certificates in the Nutanix Cluster.
- Certificates that are signed from a known Certificate Authority (CA)

When the backup host connects to the Nutanix Acropolis cluster, NetBackup validates the SSL certificates that are installed on your system.

As part of SSL validations, NetBackup conducts peer and host validations. NetBackup tries to locate the public certificates that may be placed in the certificate bundle of the operating system. It is likely that the certificate bundle of the operating system is not updated or that the certificates signed from a CA might have expired. To address such issues, you can download the latest certificate bundle for your operating system.

You may also create a certificate bundle for your self-signed certificate.

You may disable the SSL validations depending upon the type of certificate that you have installed. You can disable SSL validations using the `nb_nutanix-ahv.conf` file. This configuration file is bundled with NetBackup and it is located in the `usr/opensv/netbackup` directory on the backup host.

To let NetBackup access the latest SSL certificates, specify the path to the certificate file in the `nb_nutanix-ahv.conf` file using the `cert_authority_file` parameter.

The following topics discuss the implications of using various forms of SSL certificate with NetBackup.

SSL certificate from Nutanix

If you use the default certificates from Nutanix, NetBackup may fail SSL validations and not let you backup AHV virtual machines. To disable SSL validations, edit the `nb_nutanix-ahv.conf` file and set the `enable_ssl_validations` to `false`.

Self-signed certificate

If you use self-signed certificates, ensure that the following are met:

- When you create a **BigData** policy, the value that you provide in the `Application_Server` parameter matches the Acropolis cluster name that is present in the SSL certificate.
- Self-signed public certificates are present in the backup host. Use the `cert_authority_file` parameter in the `nb_nutanix-ahv.conf` to specify the path to the local certificate bundle.

Certificate signed from a known certificate authority

If you use certificates signed from a known certificate authority, ensure that the following is met:

- When you create a **BigData** policy, the value that you provide in the `Application_Server` parameter matches the Acropolis cluster name present in the SSL certificate.
- The SSL root certificates along with intermediate Certificate Authority (if any) are present on the backup host. NetBackup uses these certificates to validate the SSL connection with the Nutanix Acropolis cluster.
- The certificate bundle on your operating system may expire. This can also fail backups. Therefore, update the default certificate paths on your operating system with the latest certificate bundles.

You may have chosen to download and install certificate bundles from different sources. In such case, you can use the `cert_authority_file` parameter in the `nb_nutanix-ahv.conf` to specify the file name (along with the path) to your certificate bundle.

See [“About the nb_nutanix-ahv configuration file”](#) on page 23.

See [“Managing SSL certificates on NetBackup Appliance”](#) on page 22.

Managing SSL certificates on NetBackup Appliance

To manage SSL certificates on appliance, you must have read-write access to the `nb_nutanix-ahv.conf` file. The `nb_nutanix-ahv.conf` file is present in the `usr/openv/netbackup` directory.

To gain read-write access to the `nb_nutanix-ahv.conf`, complete the following:

- Become a NetBackup CLI user to be able to edit the file `nb_nutanix-ahv.conf`. Later, copy the `nb_nutanix-ahv.conf` back to the `/usr/openv/netbackup/` directory on the appliance.
- Copy SSL certificate to an appropriate location on the appliance

To access and copy the `nb_nutanix-ahv.conf` file on the appliance

- 1 Locate the `nb_nutanix-ahv.conf`.
- 2 Log on to the NetBackup Appliance Shell Menu.
- 3 Run the relevant `Manage > NetBackupCLI` commands to become a NetBackup CLI user. Copy the `nb_nutanix-ahv.conf` configuration file to the `/home/nbusers` directory. Ensure that the read-write permissions for the file are at `chmod 644`.
- 4 Edit the `nb_nutanix-ahv.conf` file to make the required changes.

Since the `nb_nutanix-ahv.conf` file is in a JSON file format, ensure that you preserve the JSON integrity.
- 5 To copy the `nb_nutanix-ahv.conf` file from `/home/nbusers` back to `/usr/openv/netbackup/`, run the following command:

```
cp-nbu-config
```

For example: `cp-nbu-config nb_nutanix-ahv.conf /usr/openv/netbackup/`

If the file is present at the destination, it is overwritten without a warning.

- 6 Verify that the file exists in the destination folder.

Use the NetBackup `nbcdutil` command to copy SSL certificate to an appropriate location on the appliance. Ensure that the SSL certificate is valid.

To copy the SSL certificate to an appropriate location on the appliance

- 1 To copy the certificate from a source to a destination, run the following command:

```
nbclutil -copycert -sourcecert  
source_certificate_path_and_name[-destcert  
destination_certificate_path]
```

For example: `nbclutil -copycert -sourcecert /home/maintenance/
nutanixCert.pem -destcert /etc/ssl/certs`

- 2 Update the `cert_authority_file` parameter in the `nb_nutanix-ahv.conf` file with the new path for the SSL certificate on the appliance.

See [“About the nb_nutanix-ahv configuration file”](#) on page 23.

About the nb_nutanix-ahv configuration file

The `nb_nutanix-ahv` configuration file contains the parameters that let you manage your SSL certificate preferences.

The `nb_nutanix-ahv` configuration file is bundled with NetBackup and it is located in the `usr/openv/netbackup` directory on the backup host. The `nb_nutanix-ahv` configuration file uses a `JSON` file format.

The [Table 3-1](#) lists the parameters that the configuration file contains.

Table 3-1 The `nb_nutanix-ahv` configuration file parameters and their description

Parameter	Description
<code>enable_ssl_validations</code>	Specifies whether or not to enable SSL validations for your certificate. The default value for this parameter is <code>true</code>. To disable SSL validations, change the value of this parameter to <code>false</code>.
<code>cert_authority_file</code>	Specifies the file name along with the path to the SSL certificate. By default, the value for this parameter is blank or empty. Here is an example of the parameter with a valid value: <pre>"cert_authority_file": "usr/openv/ca/cert.pem"</pre> Ensure that the certificate bundles are updated on your system.

See [“Managing SSL certificates”](#) on page 20.

Configuring NetBackup policies for AHV

This chapter includes the following topics:

- [About the BigData policy type](#)
- [Creating a BigData policy using the NetBackup Policies utility](#)
- [Creating a BigData policy using the Backup Policy Configuration Wizard](#)
- [Creating a BigData policy using the NetBackup Command Line Interface](#)

About the BigData policy type

Starting with the 8.1 release, NetBackup introduces a new policy type called **BigData**. The **BigData** policy lets you backup and restore big data applications and hyper-converged systems. For example, Hadoop and Nutanix AHV, respectively.

To back up and recover Nutanix AHV virtual machines, you need the Enterprise Client license.

A **BigData** policy differs from other policies in the following respects:

- You must specify **BigData** as the policy type.
- The entries that are provided to add clients and to define backup selections, differ based on the application that you choose to back up.
- During backup selection, you must specify certain parameters and their appropriate values.

Note: To backup other hypervisors that run on a Nutanix Acropolis cluster, configure or use a relevant backup policy for that hypervisor. For example, to backup VMware ESX or a Hyper-V on a Nutanix Acropolis cluster, use or configure a VMware policy or a Hyper-V, respectively.

Creating a BigData policy using the NetBackup Policies utility

This topic provides information about using the policies utility to create a **BigData** policy.

To create a BigData policy for the Acropolis Cluster using the policies utility:

- 1** In the **NetBackup Administration Console**, in the left pane, click **NetBackup Management > Policies**.
- 2** On the **Actions** menu, click **New > Policy**.
- 3** Type a unique name for the new policy in the **Add a New Policy** dialog box. Click **OK**.
- 4** On the **Attributes** tab, select **BigData** as the policy type.

In the **Destination** pane of the **Attributes** tab, select a storage unit type from the **Policy storage** drop-down.

To limit the number of simultaneous jobs per policy, use the **Limit jobs per policy** option.

- 5** On the **Schedules** tab, click **New** to create a new schedule.
Currently, NetBackup supports only full backups for AHV virtual machines.
- 6** On the **Clients** tab, enter the name of the virtual machine. You may add multiple clients.

To obtain the virtual machine name, use the **VM name** column on the Prism web console.

- 7** On the **Backup Selections** tab, click **Add** and enter the following parameters and their values as follows:

- `Application_Type=Nutanix-AHV`
The value for this parameter is fixed and cannot be changed.
- `Backup_Host=<Fully Qualified Domain Name>`
The operating system of the backup host must be a Linux. The backup host can be a NetBackup client or a media server, or a NetBackup Appliance.

- `Application_Server=<Fully Qualified Domain Name of the Nutanix Acropolis cluster>`

8 Click **OK** to save the changes.

Note: The entries that you provide in the **Clients** tab and the **Backup Selections** tab differ based on the application that you choose to back up.

For more information on using NetBackup for big data applications, refer to the [Veritas NetBackup documentation](#) page.

See “[Creating a BigData policy using the Backup Policy Configuration Wizard](#)” on page 27.

See “[Creating a BigData policy using the NetBackup Command Line Interface](#)” on page 28.

Creating a BigData policy using the Backup Policy Configuration Wizard

This topic provides information about using the Backup Policy Configuration Wizard to create a **BigData** policy.

To create a BigData policy for the Acropolis Cluster using the Backup Policy Configuration Wizard:

- 1** In the **NetBackup Administration Console**, in the left pane, click **NetBackup Management**.
 - In the right pane, click **Create a Policy** to open the Backup Policy Configuration Wizard.
 - Alternatively, under the **NetBackup Management** node, click **Policies**.
 - Go to the **Actions** menu, click **New > Policy**
 - Type a unique name for the new policy in the **Add a New Policy** dialog box. Select the **Use Policy Configuration Wizard** check box.
- 2** In the **Backup Policy Configuration Wizard**, under **Create a backup policy for:** select **File systems, databases, applications** option. Click **Next**.
- 3** In the **Policy Name and Type** pane, enter a policy name and select **BigData** as the policy type. Click **Next**.

- 4 In the **Client List** pane, click **Add** to open the **Add Client - Policy** *<policy_name>* dialog box.

In the **Client name** field, enter the Nutanix virtual machine name. Click **Add**.

To obtain the virtual machine name, use the **VM name** column on the Prism web console.

You may add multiple clients. After adding the clients, click **Next**.
- 5 In the **Backup Selections** pane under the **Backup Selection List**, click **Add**.

Enter the following parameters and their values as shown:
 - `Application_Type=Nutanix-AHV`
The value for this parameter is fixed and cannot be changed.
 - `Backup_Host=<Fully Qualified Domain Name>`
The operating system of the backup host must be a Linux. The backup host can be a NetBackup client or a media server, or a NetBackup Appliance.
 - `Application_Server=<Fully Qualified Domain Name of the Nutanix Acropolis cluster>`
- 6 In the **Backup Type** pane, select **Full Backup**. Click **Next**.

Currently, NetBackup supports only full backups for an Acropolis cluster.
- 7 In the **Frequency and Retention** pane, specify the frequency of the backup and retention levels for the backup. Click **Next**.
- 8 To save the changes for the **BigData** policy, click **Finish**.

Click **Help** on any wizard panel for assistance while running the wizard.

See [“Creating a BigData policy using the NetBackup Policies utility”](#) on page 26.

See [“Creating a BigData policy using the NetBackup Command Line Interface”](#) on page 28.

Creating a BigData policy using the NetBackup Command Line Interface

This topic provides information about using the command line interface to create a **BigData** policy.

The NetBackup commands for policy creation are in the following directory:

Windows: `install_path\Veritas\NetBackup\bin\admincmd`

UNIX or Linux: `usr/opensv/netbackup/bin/admincmd`

To define a BigData policy using the command line interface, run these commands on the NetBackup master server.

1 Create a policy.

```
bpolicynew policy_name
```

For example: `bpolicynew nutanix`

2 Set the policy attributes.

```
bpplinfo policy_name -set
```

To modify the policy type attributes, run the following command:

```
bpplinfo policy_name -modify [-v] [-M master_server,...] -pt  
policy_type
```

To add a storage unit, run the following command:

```
bpplinfo policy_name -residence label - modify
```

For example: `bpplinfo nutanix -modify -v -M my.master.server -pt
BigData -residence stu`

To limit the number of simultaneous jobs per policy, run the following command:

```
bpplinfo policy_name [-policyjobs max_jobs]
```

For example: `bpplinfo nutanix -policyjobs 50`

3 Create a policy schedule.

```
bpplsched policy_name [-v] [-M master_server,...] -add sched_label  
[-st sched_type] [-freq frequency]
```

For example: `bpplsched nutanix -add Full -st FULL`

4 Select the clients or virtual machines to back up.

```
bpplclients policy_name [-M master_server,...] [-v] [-generation  
generation] [-reason "string"] -add host_name [-os os]
```

Specify the virtual machine name. You can specify only one virtual machine at a time.

For example: `bpplclients nutanix -add nutanixVM Linux or SUSE or
Windows.`

Note: Currently, we do not validate operating system values.

5 Add backup selections.

To add the parameters that are required for the backup selections, use the `bpplinclude policy_name -add pathname or directive...` command as shown:

- `bpplinclude policy_name -add Application_Type=Nutanix-AHV`
- `bpplinclude policy_name -add Backup_Host=FQDN of the backup host`
- `bpplinclude policy_name -add Application_Server=Fully Qualified Domain Name of the Nutanix Acropolis cluster`

6 Validate the policy.

```
bpclient -policy policy_name -validate
```

```
bpclient -policy nutanix -validate
```

If the policy successfully validates, no output appears. Otherwise, the following error occurs: Error code 48: client hostname could not be found.

7 Use the `bpbackup` command to start the backup.

8 Use the `bprestore` command to start the restore.

See [“NetBackup commands for protecting the AHV”](#) on page 49.

See [“Creating a BigData policy using the Backup Policy Configuration Wizard”](#) on page 27.

See [“Creating a BigData policy using the NetBackup Policies utility”](#) on page 26.

For detailed information about the commands and additional options, refer to the *NetBackup Command Reference Guide*.

Backup and recovery

This chapter includes the following topics:

- [Back up the Nutanix AHV virtual machines](#)
- [Overview of the Nutanix AHV virtual machines recovery process](#)

Back up the Nutanix AHV virtual machines

You can initiate a backup for the AHV virtual machine using the **BigData** policy. You can start the backup manually from a policy, or have it run automatically according to a schedule that is defined in the policy.

To create a **BigData** policy refer to the following sections:

- See [“Creating a BigData policy using the NetBackup Policies utility”](#) on page 26.
- See [“Creating a BigData policy using the NetBackup Command Line Interface”](#) on page 28.

Basic phases in a NetBackup backup of an AHV

The following table provides an overview of the processes that NetBackup undertakes during an AHV backup.

Phase	Description
Phase 1: Validation of a BigData policy	NetBackup validates the BigData policy that you have created to backup the AHV virtual machines.
Phase 2: Initiation of a backup job	A backup job is triggered manually or according to the schedule that you have specified during policy creation.

Phase	Description
Phase 3: Discovery of clients and commencing to backup the data on the clients	The backup process triggers two jobs - a parent job and a child job. - The parent job identifies the added clients or the virtual machines to be backed up and creates a snapshot of the virtual machine. A new process called <code>nbappidiscv</code> is introduced to discover clients and create snapshots. After the snapshot is created, it is mounted on the backup host at the following location: <code>/usr/openv/tmp/ntxmnt</code> - The child job conducts the actual read-write operation to backup the data on a disk.
Phase 4: Completion of the backup job	On successful completion of a backup, the NetBackup client on the backup host unmounts and then deletes the snapshot.

Overview of the Nutanix AHV virtual machines recovery process

Use the **NetBackup, Backup, Archive, and Restore** console, or the command line interface to recover Nutanix AHV virtual machines.

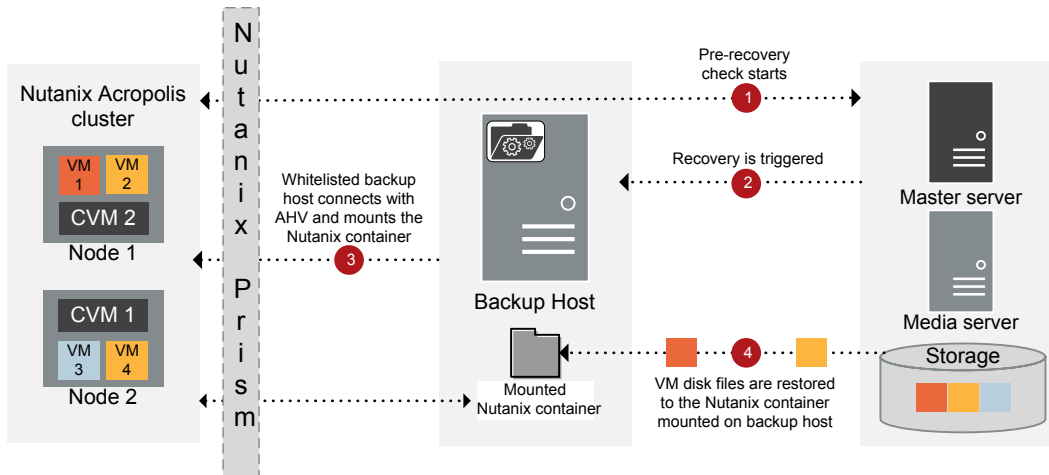
Table 5-1 Restoring Nutanix AHV data

Task	Reference
Understanding and planning the recovery process	- Overview See “About recovering the Nutanix AHV virtual machines” on page 33. - Planning the recovery process See “Planning the recovery of a Nutanix AHV VM” on page 33.
Recover the Nutanix AHV VM using the Backup, Archive, and Restore console	- See “Recovering a Nutanix AHV VM using the Backup, Archive, and Restore console” on page 36. - Recovering images backed up using pre-8.2 NetBackup See “About recovering AHV VMs from the images that are backed up using NetBackup versions 8.1, 8.1.1, or 8.1.2” on page 37.
Recover the Nutanix AHV VM using the command line interface	See “Recovering a Nutanix AHV VM using the command line” on page 38.

About recovering the Nutanix AHV virtual machines

NetBackup can recover your Nutanix AHV virtual machines from **Backup, Archive, and Restore** console and the command line interface.

Figure 5-1 Overview of the Nutanix VM recovery process



Planning the recovery of a Nutanix AHV VM

You can recover your Nutanix AHV VM using NetBackup's **Backup, Archive, and Restore** console or the command line interface. Planning the recovery location and the recovery options is an important pre-requisite before you start the recovery process.

About the recovery location

You have the following recovery location options:

- **Original location**
Recover the virtual machine in the same Nutanix AHV cluster or container that was set during the backup.
You can modify or set the following configurations before recovering to the original location:
 - Overwrite the existing VM
 - Retain the existing VM UUID

- Remove the network interfaces
- Retain the MAC address
- Power on the VM after recovery
- Overwrite the default job priority
- **Alternate location**
Recover the virtual machine to a different AHV cluster or container.
You can modify or set the following configurations before recovering to the original location:
 - Change the AHV cluster
 - Change the storage container
 - Overwrite the existing VM
 - Change the VM name
 - Retain the existing VM UUID
 - Remove the network interfaces

Note: To restore to an alternate location, you must select this option.

- Power on the VM after recovery
- Overwrite the default job priority

About the recovery options

Use the recovery options to modify the virtual machine configuration before you recover the VMs. The recovery options are available in the **Virtual Machine Options** dialog box in the **Backup, Archive, and Restore** console and must be set in the `rename` file for the command line interface option.

For more information about the `rename` file, See [“Creating or modifying the rename file”](#) on page 38.

The following table describes the various recovery options for the **Backup, Archive, and Restore** console and the command line interface:

Table 5-2 Recovery options for the **Backup, Archive, and Restore** console and the command line interface

Recovery option - Backup, Archive, and Restore	Recovery option or keywords - command line	Description of recovery options
Overwrite the existing virtual machine	<code>overwriteexistingvm</code>	Overwrite the existing virtual machine in the AHV cluster.
Create new VM ID instead of existing one	<code>retainvmuuid</code>	Create a new ID for the VM that is different from the existing value that was set during the backup. For command line, to set a different ID, set the value to <code>false</code>. Note: If you select this option or set it to <code>false</code>, the new value is set automatically.
Power on virtual machine after recovery	<code>poweronafterrecovery</code>	Turn on the VM after recovery.
Remove network interfaces	<code>removenetworkinterfaces</code>	Remove the network interface that was set for the VM during the backup. Note: If you use the command line interface to recover the virtual machines to an alternate AHV cluster, set the value in the rename file to <code>true</code>. For command line, to remove the network interface, set the value to <code>true</code>.
Retain the MAC address	<code>retainnicmacaddress</code>	Retain the MAC address that was set for the VM during the backup. Note: If you do not select this option or set it to <code>false</code>, the new value is set automatically.
Change Virtual Machine Name	<code>vmname</code>	Change the virtual machine name to a unique name. Enter the value in the Virtual Machine Name field.
Nutanix Acropolis Cluster	<code>ALT_APPLICATION_SERVER</code>	Select the Nutanix AHV cluster where you want to recover the virtual machine.

Table 5-2 Recovery options for the **Backup, Archive, and Restore** console and the command line interface (*continued*)

Recovery option - Backup, Archive, and Restore	Recovery option or keywords - command line	Description of recovery options
Override default job priority	<code>priority_number</code>	Set a custom priority for the recovery job.
Destination Container	<code>change /<original_container> to /<alternate_container></code>	Select the Nutanix AHV container where you want to recover the virtual machine. You can select a different destination container for every source container.

For more information on using the recovery options using the command line interface, See [“Recovering a Nutanix AHV VM using the command line”](#) on page 38.

Recovering a Nutanix AHV VM using the Backup, Archive, and Restore console

Use these steps in the NetBackup **Backup, Archive, and Restore** console to recover a Nutanix AHV VM.

Before you proceed, See [“Planning the recovery of a Nutanix AHV VM”](#) on page 33.

Note: If the backup host is on NetBackup version earlier than 8.2, then use the following steps to recover the AHV VM:

www.veritas.com/content/support/en_US/doc/127664414-132725336-0/v127698730-132725336

Recovering images backed up using pre-8.2 NetBackup:

See [“About recovering AHV VMs from the images that are backed up using NetBackup versions 8.1, 8.1.1, or 8.1.2”](#) on page 37.

To recover a VM using the NetBackup Admin console's Backup, Archive, and Restore console

- 1 Open the **Backup, Archive, and Restore** interface.
- 2 From the File menu (Windows) or Actions menu (UNIX), open the **Specify NetBackup Machines and Policy Type** wizard and select the following options:
 - From the **Source client for restores** list, select the required VM.
 - Specify the backup host as the destination client.

From the **Destination client for restores** list, select the required backup host.

- From the **Policy type for restores** list, select **BigData** as the policy type. Click **Ok**.

3 From the **Restore Type** drop-down list, select **Virtual Machine Backups**.

4 Select the appropriate date range to restore the complete data set.

Go to the **Backup History** and select the backup images that you want to restore.

In the **Browse Directory** field, enter / (forward slash) to view the backed-up Nutanix VM data that you can recover.

5 In the **Directory Structure** pane, Nutanix AHV VM is displayed. Select the VM to view the containers and the disks that are associated with that VM in the **Contents of Selected Directory** pane.

All the VM disks and associated containers are displayed in the **Contents of Selected Directory** pane.

6 In the **Directory Structure** pane, select the check box for the Nutanix AHV VMs that you want to recover.

7 Click **Restore**.

8 In the **Virtual Machine Recovery** wizard, select the options to recover the VM.

For more information on the recovery location and options:

- See [the section called “About the recovery location”](#) on page 33.
- See [the section called “About the recovery options”](#) on page 34.

Note: VM ID is the VM UUID.

9 After setting the recovery options, start **Run Pre-Recovery Check** to proceed with the VM recovery. If the check fails, then you can fix the issues and rerun the pre-recovery check.

10 Click **Start Recovery**.

11 Verify that the VM gets recovered and instantiated.

About recovering AHV VMs from the images that are backed up using NetBackup versions 8.1, 8.1.1, or 8.1.2

- The pre-recovery validations are supported only from the NetBackup Administration Console.

- The following pre-recovery validations are not supported for older images:
 - Unique or duplicate VM UUID on the AHV cluster
 - Unique or duplicate MAC address
 - Network UUID exists on the cluster
 - Container size validations

However, the validations are done once the `metadata.json` file is restored. The `metadata.json` file is the second entry in the restore files, hence the validations are slightly delayed.
- For the backup images that are taken using NetBackup earlier than 8.2, root disk information was not captured in `metadata.json`. If the boot disk is not the first disk, set the first disk using Nutanix Prism and restart the VM.
- The VM UUID value in the Restore Wizard because it is not captured for older backup images.

Recovering a Nutanix AHV VM using the command line

Use the `bprestore` command to recover a Nutanix AHV VM.

For more information about the `bprestore` command, refer to the *NetBackup Commands Guide*.

Use these steps from the command line interface to recover a Nutanix AHV VM.

1. Create or modify the rename file if you want to recover the VM to an alternate location or modify the VM configuration before recovery.
 See [“Creating or modifying the rename file”](#) on page 38.
2. Use the command line to recover the VM.
 See [“Using the command line to recover Nutanix AHV virtual machines”](#) on page 40.

Creating or modifying the rename file

Create or modify the rename file in the following scenarios:

- Recover the VM to the original location with modified configuration
- Recover the VM to an alternate location
- Recover the VM to an alternate location with modified configuration

For additional information, See [“Planning the recovery of a Nutanix AHV VM”](#) on page 33.

If the rename file is not available, then you must create it and save it as `rename.txt` on the NetBackup master server.

To set the alternate location or modify the configuration, add the following lines in the rename file in the given format:

Scenario	Line to add in the rename file
Overwrite the existing virtual machine	<code>change overwriteexistingvm to true</code>
Create a new UUID instead of the existing one	<code>change retainvmuuid to false</code> Note: If you set the keyword to <code>false</code> , the new value is set automatically.
Power on virtual machine after recovery	<code>change poweronafterrecovery to true</code>
Remove network interfaces	<code>change removenetworkinterfaces to false</code>
Retain the MAC address	<code>change retainnicmacaddress to true</code> Note: If you set the keyword to <code>false</code> , the new value is set automatically.
Change Virtual Machine Name	<code>change vmname to newVMname</code>
Recover the virtual machine to a different AHV cluster	Use the <code>ALT_APPLICATION_SERVER</code> keyword. For example, <code>ALT_APPLICATION_SERVER=FQDN.altapp.server</code>
Recover the virtual machine to a different AHV container	<code>change /<original_container> to /<alternate_container></code>

Sample rename file

The following `rename.txt` lets you change the VM name, VM UUID, and the MAC Address.

```
change vmname to newVMname
change retainvmuuid to false
change retainnicmacaddress to false
```

After making the required changes in the rename file, you can run the `bprestore` command. For more information, See [“Using the command line to recover Nutanix AHV virtual machines”](#) on page 40.

Default values of the keywords in the rename file

If you do not add the keywords in the rename file, the recovery process considers the following default values:

Keyword	Default value
<code>poweronafterrecovery</code>	<code>false</code>
<code>overwriteexistingvm</code>	<code>false</code>
<code>removenetworkinterfaces</code>	<code>false</code>
<code>retainvmuuid</code>	<code>true</code>
<code>retainnicmacaddress</code>	<code>true</code>
<code>vmname</code>	<code>no change</code>
<code>ALT_APPLICATION_SERVER</code>	<code>no change</code>

Using the command line to recover Nutanix AHV virtual machines

You can use the `bprestore` command to recover a backed-up Nutanix AHV VM.

To recover Nutanix AHV VM

- 1 Log on as an Administrator or root user based on windows or UNIX system respectively.
- 2 Run the following command on the NetBackup master server by providing appropriate values:

```
bprestore -S master_server -C client -R path_rename_file -t 44
-L path_progress_log -f filelist -disk_media_server
disk_media_server-D backup_host
```

Where,

-S

Specifies the name or FQDN of the NetBackup master server.

-C

Specifies a Configuration Server as a source to use for finding backups or archives from which to restore files. This name or FQDN must be as it appears in the NetBackup catalog.

-R

Specifies the directory path to a rename file, which is used to recover a virtual machine.

-t 44

Specifies BigData as the policy type.

-L progress_log

Specifies the name of whitelisted file path in which to write progress information.

-f

Specifies a file (*listfile*) that contains a list of files to be restored and can be used instead of the file names option (*filenames*). In *listfile*, list each file path must be on a separate line.

Currently we support a full VM restore. Enter / (forward slash) as the file entry.

-disk_media_server

Name or the FQDN of the disk media server.

-D

Specifies the name or the FQDN of the backup host.

Example

```
bprestore -S FQDN.master.server.com -C FQDN.client.com -R  
<install_directory>\logs\user_ops\rename.txt -t 44 -L  
<install_directory>\logs\user_ops\a.log -f filelist -disk_media_server  
FQDN.disk.mediaserver.com -D FQDN.backup.host.com
```

Troubleshooting issues

This chapter includes the following topics:

- [Troubleshooting issues related to AHV backup](#)
- [NetBackup logs](#)
- [About errors during policy creation, restore, and validation](#)
- [NetBackup status codes](#)

Troubleshooting issues related to AHV backup

This section describes various troubleshooting scenarios and provides information to resolve them.

NetBackup provides specific logs, status codes, and relevant error messages to assist you in troubleshooting any issues that you may encounter.

NetBackup logs

NetBackup maintains process-specific logs for the various processes that are involved in the backup and restore operations. Examining these logs can help you to find the root cause of an issue.

These log folders must already exist in order for logging to occur. If these folders do not exist, you must create them.

The log folders reside on the following directories:

- On Windows: `install_path\NetBackup\logs`
[Table 6-1](#) uses the Windows directory path as an example.
- On UNIX or Linux: `/usr/openv/netbackup/logs`

Table 6-1 NetBackup logs related to the AHV

Log folder	Messages related to	Logs reside on
<code>log_filepath\nbaapidiscv</code>	BigData framework and policy validation	NetBackup client on the backup host
<code>log_filepath\bpbrm</code>	Back up and restore	Media server
<code>log_filepath\bpbkar</code>	Backup	NetBackup client on the backup host
<code>log_filepath\bprd</code>	Restore	Master server
<code>log_filepath\bpcd</code>	Back up and restore	NetBackup client on the backup host
<code>log_filepath\tar</code>	Restore	NetBackup client on the backup host

Note: Certain process logs from the preceding table reside on the NetBackup client on the backup host, which is a Linux computer.

For more details, refer to the [NetBackup Logging Reference Guide](#).

About errors during policy creation, restore, and validation

When you create or save a **BigData** policy, you may encounter certain errors if you do not provide correct and valid inputs.

[Table 6-2](#) discusses these scenarios briefly.

Table 6-2 NetBackup policy creation and validation scenarios

Problem	Recommended action
The policy validation or the backup job fails when you have provided invalid or empty value in the backup selection.	Enter the following parameters in backup selections: - Application_Type=Nutanix-AHV - Application_Server=Fully Qualified Domain Name of the Nutanix cluster - Backup_Host=Fully Qualified Domain Name

Table 6-2 NetBackup policy creation and validation scenarios (*continued*)

Problem	Recommended action
The backup job fails when the backup selection does not contain the <code>Backup_Host</code> parameter.	Add the <code>Backup_Host</code> parameter to the backup selections as follows: <code>Backup_Host=Fully Qualified Domain Name</code> See “Adding a backup host to the NetBackup master server” on page 16.
The backup job fails when you provide an invalid or an empty value when you specify clients or virtual machines to be backed up.	Enter the name of the virtual machines that you want to backup. In addition, verify that the virtual machine name is correct and meets the character restrictions. See “NetBackup character restrictions for virtual machine names” on page 14.
The backup host is not reachable.	Verify the backup host name. The backup host name is the FQDN of the backup host.
Backup fails when the NetBackup client version on the backup host is older than 8.1.	The NetBackup client version on the backup host must be 8.1 or later.
The BigData policy is unable to determine version of backup host.	Verify that the NetBackup client version on the backup host is older than 8.1. The NetBackup client version on the backup host must be 8.1 or later.
The backup job may fail when the operating system of the backup host is not Linux.	The operating system of the backup host must be Linux.
The backup job fails when credentials are invalid or not configured for the <code>Application_Server</code> parameter.	Verify that you have provided correct credentials. Ensure that the value that you have provided for the <code>Application_Server</code> parameters matched the one that you provided while specifying Nutanix Acropolis Cluster credentials. See “Adding the Nutanix Acropolis Cluster credentials for NetBackup” on page 18.
The recovery fails if you select recovery to the original location and the AHV container is unavailable.	Ensure that the AHV container is available, create the container, or use the alternate location option to recover the VM.
The recovery fails and the VM is not created on the alternate cluster because of the unavailability of network connectivity.	Ensure that there is network connectivity between the NetBackup servers and AHV clusters, and retry the recovery process.

Table 6-2 NetBackup policy creation and validation scenarios (*continued*)

Problem	Recommended action
The recovery fails if a different backup or recovery host is used than the one that was used during the backup.	Add the backup or the recovery host that you want to use during the VM recovery to the file system whitelist using the Nutanix Prism console.
Unable to unmount a container at the end of a VM restore. The recovery operation is partially successful. Error 6622 is displayed. Unable to unmount the file system or cleanup the directory from </directory_path_of_mount_point> with error [6622]. You can manually complete these actions.	1 Delete the container directory from the following path: <pre>/usr/openv/tmp/ntxmnt/<JOB_ID>/<container_name>/.restore</pre> 2 Delete the local directory from: <pre>/usr/openv/tmp/ntxmnt/<JOB_ID></pre>
When you select a Windows backup host, VM details are not displayed on the recovery wizard. The No Files Found dialog box is displayed.	Use a Linux backup host.

NetBackup status codes

NetBackup provides status codes to help you understand and troubleshoot issues that can occur.

For information about NetBackup status codes, refer to the *NetBackup Status Codes Reference Guide*.

Table 6-3 Status codes related to NetBackup for AHV

Problem	Recommended action
When a backup fails with the following message: Unknown error <status_code>	To determine the specific issue, search the NetBackup Troubleshooter for the given status code number. The status code provides you with a problem statement and a recommended action to resolve the issue.

Table 6-3 Status codes related to NetBackup for AHV (*continued*)

Problem	Recommended action
When the following status code is displayed: Status 6625: The backup host is either unauthorized to complete operation or it is unable to establish a connection with the application server.	The backup host may be unauthorized to complete an operation due to one of the following reasons: ■ Ensure that you have validated the SSL certificate from the Nutanix Acropolis cluster. ■ Ensure the certificate is generated with the correct host name. The certificate is issued on the Fully Qualified Domain Name of the cluster. Therefore, when you create a BigData policy, provide the same Fully Qualified Domain Name in the <code>Application_Server</code> parameter. The Acropolis cluster name cannot use the short name of the cluster, as it will not match the Fully Qualified Domain Name in the SSL certificate. See “Managing SSL certificates” on page 20.
When the mount operation fails with the following message in the <code>nbaapidiscv</code> process logs: <code>status_code aapi_logmsg: session_id:xxxx_ Nutanix Plugin :Failed to mount /user/.acropolis/snapshot/containerID/vmdisk; Error: Permission denied. You may want to check whether you have added the backup host to the Nutanix Acropolis Cluster using the appropriate whitelist option available through the Prism web console or its command line interface.</code>	The backup host is unable to mount the snapshot. Verify whether you have added the backup host to the Nutanix Acropolis Cluster using the appropriate whitelist option available through the Prism web console or its command line interface. See “Adding a backup host to the Acropolis Cluster access list” on page 18.
When you try to backup the virtual machines that have volume group disks, the backup fails with following message in the <code>nbaapidiscv</code> process logs: <code>status_code aapi_logmsg: session_id: xxxx_ Nutanix Plugin: failed to get snapshot_file_path for the disk. AAPI_Errno = 6647</code>	To determine the specific issue, search the NetBackup Troubleshooter for the given status code number. The status code provides you with a problem statement and a recommended action to resolve the issue. Backup of the virtual machines that have volume groups attached is not supported.

Table 6-3 Status codes related to NetBackup for AHV (*continued*)

Problem	Recommended action
When the following status code is displayed: Error code 223: an invalid entry was encountered	Ensure that you have provided valid credentials to access the Nutanix Acropolis cluster.
When the following status code is displayed: Status code 6654: Unable to retrieve the credentials for the server.	This error can occur if you have not configured the Nutanix Acropolis cluster credentials on the NetBackup master server. This error can also occur if the backup host is unable to access NetBackup and retrieve the cluster credentials. See “Adding the Nutanix Acropolis Cluster credentials for NetBackup” on page 18. See “Adding a backup host to the NetBackup master access list” on page 17.
When the following status code is displayed: Error code 6622: An internal error occurred in the NetBackup process.	This error can occur if you do not have appropriate administrative rights for backing up AHV virtual machines. Ensure that you have appropriate administrative rights and permissions from Nutanix to complete a backup for AHV virtual machines.

For information about NetBackup status codes, refer to the [NetBackup Status Codes Reference Guide](#)

NetBackup commands to backup and restore Nutanix AHV virtual machines

This appendix includes the following topics:

- [NetBackup commands for protecting the AHV](#)

NetBackup commands for protecting the AHV

This section provides information about the NetBackup commands that are used to complete various tasks and operations for protecting the AHV.

Table A-1 NetBackup commands for protecting the AHV

Command	Description
bppolicynew	Use this command to create a new BigData policy.
bpplinfo	Use this command to: ■ Modify the Bigdata policy. ■ Add a storage unit. ■ Limit simultaneous jobs per policy.

Table A-1 NetBackup commands for protecting the AHV *(continued)*

Command	Description
<code>bpplsched</code>	Use this command to: ■ Add schedule. ■ Specify a frequency of the backup.
<code>bpplclients</code>	Use this command to: ■ Add a client. ■ Modify an existing client.
<code>bpplininclude</code>	Use this command to: ■ Add the parameters that are required for configuring a backup host. ■ Modify the parameters.
<code>tpconfig</code>	Use this command to: ■ Add credentials for a Nutanix Acropolis Cluster. ■ Change the default port for a Nutanix Acropolis Cluster.
<code>bpbackup</code>	Use this command to backup a Nutanix AHV virtual machine.
<code>bprestore</code>	Use this command to restore a Nutanix AHV virtual machine.

For detailed information about the commands and the command options, refer to the [NetBackup Commands Reference Guide](#).