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

Hypervisor policy

Release 10.0

VERITAS™

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

Last updated: 2022-02-25

Legal Notice

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)

This chapter includes the following topics:

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, Microsoft Hyper-V, and Red Hat Virtualization, lets you back up and restore Nutanix AHV virtual machines.

You can protect the Nutanix AHV virtual machines using the Hypervisor backup policy.

See “About the Hypervisor policy type to protect Nutanix AHV VMs” on page 9.

With NetBackup version 8.3, the Nutanix Acropolis Hypervisor (AHV) plug-in for Hypervisor policy is installed as part of the NetBackup installation.

Starting from version 8.3, NetBackup supports incremental backups for the Nutanix AHV virtual machines.

Changes to the backup policy usage

Starting from NetBackup 8.3, you cannot create new BigData policies to protect your Nutanix AHV VMs.

See "Migrating BigData policy to Hypervisor policy" on page 9.

See "Deprecation of BigData policy to protect Nutanix AHV VMs" on page 10.

High-level steps to protect the Nutanix AHV virtual machines

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

Step	Step overview	Sub-steps and links to the sections
1	Understand NetBackup, Hypervisor policy, and AHV	About the Hypervisor backup policy ■ See "About the Hypervisor policy type to protect Nutanix AHV VMs" on page 9. Migrating an existing BigData policy to Hypervisor policy ■ See "Migrating BigData policy to Hypervisor policy" on page 9. See "NetBackup terminology related to the AHV backup " on page 11. See "NetBackup for AHV environment" on page 11.
2	Read the prerequisites, and things to consider before using the NetBackup for AHV plug-in	■ See "Prerequisites" on page 14. ■ See "Things to consider before using the NetBackup plug-in for Nutanix AHV" on page 15.

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

Step	Step overview	Sub-steps and links to the sections
3	Establish communication between NetBackup and the Nutanix components	Configure secure communication between Nutanix AHV and NetBackup. ■ See "Managing SSL certificates through ECA framework" on page 21. ■ See "Configuring secure communication between the Nutanix Acropolis Hypervisor server and NetBackup host" on page 19. ■ See "Managing SSL certificates on NetBackup Appliance" on page 20. Add the Nutanix Acropolis cluster credentials to the NetBackup primary server. ■ See "Adding the Nutanix Acropolis Hypervisor Cluster credentials for NetBackup" on page 28. Add the name of the backup host to relevant file system allowed lists on the Prism web console and the NetBackup primary server. ■ See "Adding a backup host to the NetBackup primary access list" on page 30. ■ See "Adding a backup host to the Acropolis Cluster access list" on page 31.
4	Create a backup policy	Create a backup policy ■ See "Creating a backup policy using the NetBackup Policies utility" on page 33. ■ See "Creating a backup policy using the NetBackup Command Line Interface" on page 35.
5	Protect the Nutanix AHV virtual machines	Backup the virtual machines. See "Back up the Nutanix AHV virtual machines" on page 41. Recover the virtual machines ■ See "Planning the recovery of a Nutanix AHV VM" on page 45. ■ See "Recovering a Nutanix AHV VM using the Backup, Archive, and Restore console" on page 48. ■ See "Recovering a Nutanix AHV VM using the command line for Hypervisor policy" on page 50.

About the Hypervisor policy type to protect Nutanix AHV VMs

Starting with NetBackup 8.2, you can use the **Hypervisor** policy to protect the Nutanix AHV VMs.

The **Hypervisor** policy type lets you protect hyper converged systems and hypervisors like Nutanix Acropolis Hypervisor (AHV) or Red Hat Virtualization (RHV).

The Hypervisor policy leverages several existing NetBackup features to protect the hypervisor and the virtualization workloads. For example, incremental backups and accelerator for Hypervisor using the hypervisor change block tracking capabilities.

For information about accelerator-enabled backups, refer to the *NetBackup™ Administrator's Guide*.

Starting from NetBackup 8.3, incremental backups for Nutanix AHV are supported with change block tracking capabilities.

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

- 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.

Migrating BigData policy to Hypervisor policy

Use the NetBackup Administration Console to migrate **BigData** backup policy to the **Hypervisor** policy.

Complete the following steps to migrate your existing **BigData** backup policy to the **Hypervisor** policy:

1. Edit the existing **BigData** policy and select the policy type as **Hypervisor**. Ensure that the **Use Accelerator** option is selected if you want to use the Accelerator feature.
2. Verify the changes. During this migration, NetBackup automatically changes the following parameters in the **Backup Selections** tab:

   `Application_Type=Nutanix-AHV` to `Hypervisor_Type=Nutanix-AHV`

Run a backup.

Deprecation of BigData policy to protect Nutanix AHV VMs

Starting from NetBackup 9.0, **BigData** policy cannot be used to protect Nutanix AHV VMs.

If a backup host that is configured in a **BigData** policy has NetBackup version less than 8.3, that policy can protect the Nutanix AHV VMs. Once that backup host is upgraded to NetBackup 8.3 or later, the policy stops protecting the Nutanix AHV VMs.

Migrate the existing **BigData** policy to the **Hypervisor** policy to protect Nutanix AHV on the supported NetBackup versions.

See "Migrating BigData policy to Hypervisor policy" on page 9.

Refer to the following scenarios for more information:

- NetBackup master server and the backup host that is configured in the **BigData** policy are at version earlier than NetBackup 8.3.

  Action:

  - Upgrade NetBackup master server to 9.0 so that your **BigData** policy continues to protect the Nutanix AHV VMs.
  - Once the backup host upgrades to NetBackup 8.3 or a later version, migrate the **BigData** policy to **Hypervisor** policy before the next backup job schedule.

- NetBackup master server has version 8.3 and the backup host that is configured in the **BigData** policy has a version earlier than NetBackup 8.3.

  Action:

  - Upgrade NetBackup master server to 9.0 so that your **BigData** policy continues to protect the Nutanix AHV VMs.
  - Once the backup host upgrades to NetBackup 8.3 or a later version, migrate the **BigData** policy to **Hypervisor** policy before the next backup job schedule.

- Both the NetBackup master server and the backup host that is configured in the **BigData** policy have NetBackup version 8.3.

  Action:

  - Migrate the **BigData** policy to **Hypervisor** policy before you upgrade NetBackup to 9.0.

Note: You can migrate your **BigData** policy to **Hypervisor** policy from NetBackup version 8.2 onwards. In NetBackup 8.2, you need to download and install the Nutanix AHV plug-in on the backup host. From NetBackup 8.3 onwards, the plug-in is part of the NetBackup installation package.

NetBackup terminology related to the AHV backup

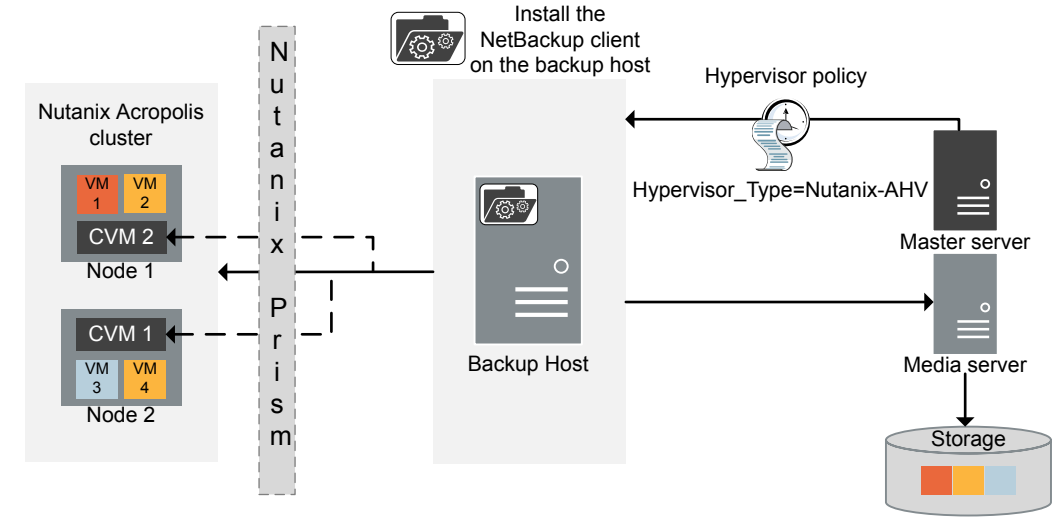
The following table describes the NetBackup terminology that is related to the AHV backup.

Term	Description
Application server	The name of the Acropolis cluster. It is identified using the `Application_Server` parameter during backup selections. You can obtain the Acropolis cluster name from the Prism web console using **Settings > Cluster Details**.
Hypervisor type	The type of hypervisor being backed up. It is identified using the `Hypervisor_Type` parameter during backup selections. For Nutanix AHV, the value for the `Hypervisor_Type` 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 and must have NetBackup client version 8.2 or later with the NetBackup plug-in for Nutanix AHV. It is identified using the `Backup_Host` parameter during backup selections. You can use either of the following configurations as a backup host: ■ NetBackup master server or a 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 primary server" on page 30.

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 of NetBackup for AHV



CVM = Controllor Virtual Machine

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*.

Chapter 2

Prerequisites and things to consider before using Nutanix for AHV

This chapter includes the following topics:

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 information on supported versions and support for Nutanix AHV, see Support for **NetBackup in a Virtual Environment** list from the NetBackup Master Compatibility List page.
- 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.

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 servers.
- 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

For detailed information about licenses and adding licenses, refer to the following:

- How to use NetBackup plug-ins and agents: download, install, and availability information
- "Adding NetBackup licenses" section of the NetBackup Administrator's Guide, Volume I.

Things to consider before using the NetBackup plug-in for Nutanix AHV

- The Hypervisor policy for the NetBackup plug-in for Nutanix AHV requires NetBackup version 8.2 or later on NetBackup master server, media server, and the backup host.
- To use the incremental backup functionality to protect the Nutanix AHV VMs, ensure that NetBackup master server, media server, and the backup host have NetBackup 8.3 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.
  For a list of supported versions, see:
  NetBackup Master Compatibility List
- For accelerator-enabled or incremental backups, if you change the backup host, then the next backup is a full, non-optimized backup.
- The Hypervisor policy does not retain the AHV VM's operating system details. Even if you select the right OS, the OS type is set to default (HP-UX-IA64).
- If a NetBackup client that is shared across several NetBackup master servers is used as a backup host, you must update the NetBackup host properties to

ensure that policy is validated and the backup and restore operations run successfully.

- 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.
- You cannot backup two or more virtual machines with the same display name. Each virtual machine must have a unique display name.
- The restore operation for a partially successful backup is currently not supported.
- NetBackup AHV VMs that are configured with volume groups are not supported.
- Point-in-time (PIT) rollback option is not supported for the restore of the Nutanix AHV VMs.
- Using Policy Configuration Wizard from the NetBackup Administration Console is not supported to create a Hypervisor policy to protect the Nutanix AHV VMs.
- Incremental backups also include the VMs with zeroed or deleted data along with the actual changed data.

See "Creating a backup policy using the NetBackup Policies utility" on page 33.

See "Creating a backup policy using the NetBackup Command Line Interface" on page 35.

NetBackup character restrictions for virtual machine names

When you configure a policy to back up the virtual machines of a Acropolis cluster, add those virtual machines as NetBackup clients. To add a virtual machine to the backup policy, you must provide the display 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 particular VM name contains wrong or invalid characters, then the backup of that particular VM may fail.

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

- Uppercase and lowercase ASCII characters
- Numbers
- Period (.)
  Display name cannot end with a period.
- Hyphen (-)

Display name cannot start with a hyphen.

- Underscore (_)
- Plus sign (+)
- Percent sign (%)
  When you specify display name, replace the % character with %25.
- Left and right parentheses ()
- Spaces

  For **Hypervisor** policy

  - No need to replace space with %20 in the command line, but the Admin Console does not accept space for VM name. Replace space with %20.
  - If the VM name itself contains %20. Replace %20 with %2520.

The following characters are not supported for virtual machine names:

- Chinese characters and other multi-byte characters are not supported in display name.
- Any other characters that are not mentioned in the supported list.

Chapter 3

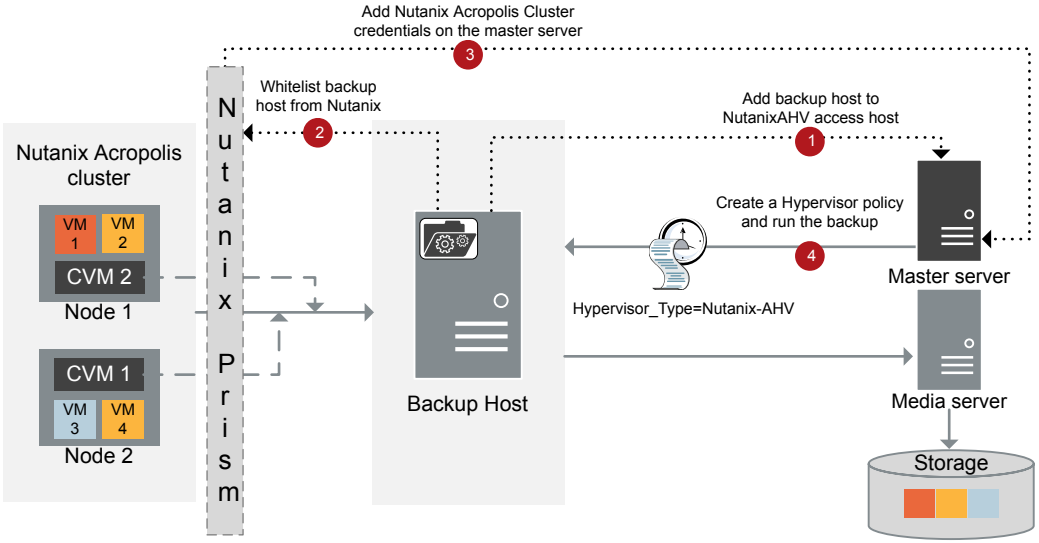
Configuring NetBackup communication with AHV

This chapter includes the following topics:

Establishing communication between NetBackup and Nutanix AHV

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

Figure 3-1 Establishing communication between NetBackup and Nutanix AHV



Configuring secure communication between the Nutanix Acropolis Hypervisor server and NetBackup host

Till NetBackup release 8.2, NetBackup provided configuration settings through a Nutanix specific configuration file `nb_nutanix-ahv.conf` to validate the AHV cluster based on the cluster's public x509 certificate that the AHV server returns during the communication.

NetBackup now supports peer certificate validation for all virtualization servers like VMware, RHV Manager, and Nutanix Acropolis Cluster through a common External Certificate Authority (ECA) framework. This common framework can work with a single set of configuration parameters for all virtualization workloads and provides additional validations like certificate revocation lists.

Note: If you are upgrading from NetBackup 8.2, and you had previously set `enable_ssl_validations` to false in the `nb_nutanix-ahv.conf` file, and want to continue skipping certificate validation, no further action is required.

You can then skip rest of this section, and See "Adding the Nutanix Acropolis Hypervisor Cluster credentials for NetBackup" on page 28.

This framework requires a certificate bundle on each backup host that can contain certificates from one or more Certificate Authorities (CAs). In absence of centralized CAs, even self-signed certificates from different servers can be added to this bundle.

To set the common external CA parameters in NetBackup, See "Managing SSL certificates through ECA framework" on page 21.

Note that when you configure the SSL parameters in NetBackup, you must ensure that the values that you provide for the following options matches with the Acropolis cluster name that is present in the Nutanix SSL certificate:

- **New Virtual Machine Server** name while adding the Acropolis Cluster credentials in NetBackup
  See "Adding the Nutanix Acropolis Hypervisor Cluster credentials for NetBackup" on page 28.
- `Application_Server` parameter while configuring the backup policy
  See "Creating a backup policy using the NetBackup Policies utility" on page 33.

If you use the default certificates from Nutanix that contain the Common Name field as `CN=*.nutanix.local`, NetBackup might fail the SSL validations and not let you backup the AHV VMs. In this scenario, skip the SSL validations. If you want to skip certificate validation, set `enable_ssl_validations` to false in `nb_nutanix-ahv.conf`. You can then skip rest of this section, and See "Adding the Nutanix Acropolis Hypervisor Cluster credentials for NetBackup" on page 28.

Managing SSL certificates on NetBackup Appliance

To manage the SSL certificates on NetBackup Appliance, download the certificate on the appliance on a location that is accessible to the appliance user.

Use the NetBackup `nbcldutil` command to copy the 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:

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

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

Managing SSL certificates through ECA framework

NetBackup can now validate Nutanix Acropolis Hypervisor (AHV) server certificates using their root or intermediate certificate authority (CA) certificates.

For NetBackup 10.0, only `PEM` certificate format is supported for virtualization servers.

For more information, See "VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED for servers and clients" on page 26.

The following procedure is applicable for the NetBackup primary server and all virtualization access hosts.

To configure secure communication between the Nutanix AHV server and virtualization access host

1. Configure a external certificate authority trust store on the virtualization access host.
2. Add CA certificates of the required Nutanix AHV server in the trust store on the access host.

3 Use the `nbsetconfig` command to configure the following NetBackup configuration options on the access host:

For more information on the configuration options, refer to the NetBackup Administrator's Guide.

`ECA_TRUST_STORE_PATH`	Specifies the file path to the certificate bundle file that contains all trusted root CA certificates. This option is specific to file-based certificates. You should not configure this option if Windows certificate store is used. If you have already configured this external CA option, append the Nutanix AHV CA certificates to the existing external certificate trust store. If you have not configured the option, add all the required Nutanix AHV server CA certificates to the trust store and set the option. See "ECA_TRUST_STORE_PATH for NetBackup servers and clients" on page 24.
`ECA_CRL_PATH`	Specifies the path to the directory where the certificate revocation lists (CRL) of the external CA are located. If you have already configured this external CA option, append the Nutanix AHV server CRLs to the CRL cache. If you have not configured the option, add all the required CRLs to the CRL cache and then set the option. See "ECA_CRL_PATH for NetBackup servers and clients" on page 25.
`VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED`	This option affects Nutanix AHV, RHV, and VMware secure communication. Without this option, the secure or insecure communication with workload is decided by each workload and plug-in separately. For Nutanix AHV, secure communication is enabled by default. This option lets you skip the security certificate validation. See "VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED for servers and clients" on page 26.

VIRTUALIZATION_CRL_CHECK	Lets you validate the revocation status of the virtualization server certificate against the CRLs. By default, the option is disabled. See "VIRTUALIZATION_CRL_CHECK for NetBackup servers and clients" on page 27.

For more information on external CA support, refer to the *NetBackup Security and Encryption Guide*.

ECA_TRUST_STORE_PATH for NetBackup servers and clients

The ECA_TRUST_STORE_PATH option specifies the file path to the certificate bundle file that contains all trusted root CA certificates.

This certificate file should have one or more certificates in PEM format.

Do not specify the ECA_TRUST_STORE_PATH option if you use the Windows certificate store.

The trust store supports certificates in the following formats:

- PKCS #7 or P7B file having certificates of the trusted root certificate authorities that are bundled together. This file may either be PEM or DER encoded.
- A file containing the PEM encoded certificates of the trusted root certificate authorities that are concatenated together.

This option is mandatory for file-based certificates.

The root CA certificate in Cloudera distribution can be obtained from the Cloudera administrator. It may have a manual TLS configuration or an Auto-TLS enabled for the Hadoop cluster. For both cases, NetBackup needs a root CA certificate from the administrator.

The root CA certificate from the Hadoop cluster can validate the certificates for all nodes and allow NetBackup to run the backup and restore process in case of the secure (SSL) cluster. This root CA certificate is a bundle of certificates that has been issued to all such nodes.

Certificate from root CA must be configured under ECA_TRUST_STORE_PATH in case of self-signed, third party CA or Local/Intermediate CA environments. For example: In case of AUTO-TLS enabled Cloudera environments, you can typically find the root CA file named with cm-auto-global_cacerts.pem at path /var/lib/cloudera-scm-agent/agent-cert. For more details, refer Cloudera documentation.

Table 3-1 ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, or RHV servers this option must be set on the NetBackup primary server and respective access hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_TRUST_STORE_PATH = Path to the external CA certificate` For example: `c:\rootCA.pem`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_CRL_PATH for NetBackup servers and clients

The `ECA_CRL_PATH` option specifies the path to the directory where the Certificate Revocation Lists (CRL) of the external certificate authority (CA) are located.

These CRLs are copied to NetBackup CRL cache. Revocation status of the external certificate is validated against the CRLs from the CRL cache.

CRLs in the CRL cache are periodically updated with the CRLs in the directory that is specified for `ECA_CRL_PATH` based on the `ECA_CRL_PATH_SYNC_HOURS` option.

If the `ECA_CRL_CHECK` or `HADOOP_CRL_CHECK` option is not set to `DISABLE` (or 0) and the `ECA_CRL_PATH` option is not specified, NetBackup downloads the CRLs from the URLs that are specified in the CRL distribution point (CDP) and uses them to verify revocation status of the peer host's certificate.

Note: For validating the revocation status of a virtualization server certificate, the `VIRTUALIZATION_CRL_CHECK` option is used.

See "VIRTUALIZATION_CRL_CHECK for NetBackup servers and clients" on page 27.

For validating the revocation status of a Hadoop server certificate, the `HADOOP_CRL_CHECK` option is used.

Table 3-2 ECA_CRL_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, RHV servers, or Hadoop, this option must be set on the NetBackup primary server and respective access or backup hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format to specify a path to the CRL directory: `ECA_CRL_PATH = Path to the CRL directory`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED for servers and clients

The `VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED` option enables the validation of virtualization server certificates using its root or intermediate certificate authority (CA) certificates.

Before you enable the option, review the steps from the 'Validating VMware virtualization server certificates in NetBackup ' section in the NetBackup for VMware Administrator's Guide.

By default, the `VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED` option is set to `UNDEFINED`.

The security certificate validation is enabled for RHV and Nutanix AHV servers, but is disabled for VMware servers.

Note: In a scenario where an external CA can be configured for one virtualization server, but not for the other, two separate backup hosts must be used. The VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED option must be set to YES for the backup host where the external CA can be configured. The VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED must be set to YESfor the backup host where the external CA can be configured. The option must be set to NO for the other backup host.

Table 3-3 VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED information

Usage	Description
Where to use	On NetBackup primary server or all access hosts.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format to enable certificate validation for the RHV, VMware, or Nutanix AHV servers: VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED = YES
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

VIRTUALIZATION_CRL_CHECK for NetBackup servers and clients

The VIRTUALIZATION_CRL_CHECK option lets you specify the revocation check level for external certificates of the virtualization server. Based on the check, revocation status of the virtualization server certificate is validated against the certificate revocation list (CRL) during host communication.

By default, the VIRTUALIZATION_CRL_CHECK option is disabled. If you want to validate the revocation status of the virtualization server certificate against certificate revocation list (CRL), set the option to a different value.

You can choose to use the CRLs from the directory that is specified for the ECA_CRL_PATH configuration option or the CRL distribution point (CDP).

See “ECA_CRL_PATH for NetBackup servers and clients” on page 25.

Table 3-4 VIRTUALIZATION_CRL_CHECK information

Usage	Description
Where to use	On NetBackup primary server or all access hosts.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `VIRTUALIZATION_CRL_CHECK = CRL check` You can specify one of the following: ■ DISABLE (or 0) - Revocation check is disabled. Revocation status of the certificate is not validated against the CRL during host communication. This is the default value. ■ LEAF (or 1) - Revocation status of the leaf certificate is validated against the CRL. ■ CHAIN (or 2) - Revocation status of all certificates from the certificate chain are validated against the CRL.
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

Adding the Nutanix Acropolis Hypervisor Cluster credentials for NetBackup

You must add the credentials for accessing the Acropolis cluster to the NetBackup primary 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 primary server to obtain these credentials.

To add credentials for the Acropolis Hypervisor 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.
- 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.

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/openv/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/openv/volmgr/bin/tpconfig -add -virtual_machine cluster1.nutanix.abc.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 primary server” on page 30.

See "Adding a backup host to the Acropolis Cluster access list" on page 31.

Adding a backup host to the NetBackup primary 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 primary and media server and the Acropolis cluster.

To add a backup host, you must start by creating a **Hypervisor** backup 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 **Hypervisor** backup policy from the NetBackup Administration Console using the Policies utility.

   See "Creating a backup policy using the NetBackup Policies utility" on page 33.

2. On the **Backup Selections** tab, click **New** 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 **Hypervisor** backup policy using the NetBackup Command Line Interface.

   See "Creating a backup policy using the NetBackup Command Line Interface" on page 35.

2. Run the following command to add a backup host

   `bpplclients policy_name -add backup_host hardware operating_system`

   Enter the *hardware operating_system* details of the backup host.

See "Adding a backup host to the NetBackup primary access list" on page 30.

See "Adding a backup host to the Acropolis Cluster access list" on page 31.

Adding a backup host to the NetBackup primary access list

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

To add a backup host to NetBackup primary access list using the NetBackup Administration Console

1. In the **NetBackup Administration Console**, in the left pane, click **NetBackup Management > Host Properties**.
2. In the primary server's ***Host*** **Properties** dialog box, click **NutanixAHV Access Hosts**.
3. To add the backup host to NetBackup primary access list, click **Add**.

   In the **New Server** dialog box, enter the name of the backup host. Click **Add**.

To add a backup host to NetBackup primary access list using the command line

1. Use the `bpsetconfig` command to set the value of `NTNXAHV_PROXY_SERVER` as follows:

   ```
   set NTNXAHV_PROXY_SERVER = FQDN.backup.host
   ```

   Repeat the step to add multiple backup hosts.
2. Save the changes and verify the changes that are stored in the `bp.conf` file using the following command:

   ```
   nbgetconfig | grep NTNXAHV_PROXY_SERVER
   ```

For more information about the `bpsetconfig` and `nbgetconfig` commands, refer to the *NetBackup Commands Reference Guide*.

See "Adding a backup host to the NetBackup primary server" on page 30.

See "Adding a backup host to the Acropolis Cluster access list" on page 31.

Configuring a NetBackup Appliance as a backup host

You can configure a NetBackup Appliance as a backup host.

To manage SSL certificates, See "Managing SSL certificates on NetBackup Appliance" on page 20.

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 allowlist the backup host.

To the backup host:

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

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

See "Adding a backup host to the NetBackup primary server" on page 30.

See "Adding the Nutanix Acropolis Hypervisor Cluster credentials for NetBackup" on page 28.

Chapter 4

Configuring NetBackup policies for AHV

This chapter includes the following topics:

Creating a backup policy using the NetBackup Policies utility

This topic provides information about using the policies utility to create a **Hypervisor** policy for the Acropolis Cluster.

For more information, See "About the Hypervisor policy type to protect Nutanix AHV VMs" on page 9.

To create a Hypervisor policy:

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 **Hypervisor** 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.

For the Hypervisor policy, to use Accelerator, select the **Use Accelerator** option.

Note: Use an OST supported storage unit for using the Accelerator functionality. For example: MSDP

---

5 On the **Schedules** tab, click **New** to create a new schedule.

Starting from version 8.3, NetBackup supports full, differential incremental, and cumulative incremental backups for AHV virtual machines.

For information about incremental backups, refer to the *NetBackup Administrator's Guide, Volume I*.

Note: If you want to disable accelerator in a backup policy that has incremental schedule, it is recommended that you run a full back up immediately after making the update. You can run a full backup manually or re-enable accelerator.

Run a full backup immediately after adding incremental backup schedules to an existing backup policy. This step prevents cumulative incremental backups from running as full backups till the next full backup schedule, and differential incremental to run as full backups and subsequent differential backups to run as incremental backups.

Note: If you enable Accelerator, include at least 2 full backup schedules:

- One full schedule with the Accelerator forced rescan option disabled

- Second full schedule with the Accelerator forced rescan enabled

Configure the forced rescan enabled schedule to run less frequently than the first full backup schedule.

For example, if the first full backup schedule runs weekly, run the second schedule (with the Accelerator forced rescan option enabled) every month. However, the best frequency for this schedule depends upon your environment.

---

6 On the **Clients** tab, enter the display name(s) of the virtual machine(s).

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:

- `Hypervisor_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 RHEL or SUSE. 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>`

Note: The parameters - `Hypervisor_Type`, `Application_Server`, and `Backup_Host` are not case sensitive. However, their values are case-sensitive.

Multiple entries for the `Backup_Host` parameter is not supported.

---

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.

Creating a backup policy using the NetBackup Command Line Interface

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

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

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

UNIX or Linux: /usr/openv/netbackup/bin/admincmd

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

1 Create a policy.

`bppolicynew policy_name`

For example: `bppolicynew nutanix`

2 Set the policy attributes.

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

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

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

The *policy_type* value is **`Hypervisor`**.

To add a storage unit, run the following command:

`bpplinfo policy_name -residence label -modify`

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

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`

Note: If you enable Accelerator, include at least 2 full backup schedules:

- One full schedule with the Accelerator forced rescan option disabled

- Second full schedule with the Accelerator forced rescan enabled

Configure the forced rescan enabled schedule to run less frequently than the first full backup schedule.

For example, if the first full backup schedule runs weekly, run the second schedule (with the Accelerator forced rescan option enabled) every month. However, the best frequency for this schedule depends upon your environment.

To enable the Accelerator forced rescan option, set `checksum_change_detection=1`.

Use the following command to add an incremental backup schedule:

`bpplsched nutanix -add ntnx_DINC -st INCR`

Where the values that the `-st` option supports for Nutanix AHV are:

- `FULL` - for a full backup
- `INCR` - for a differential incremental backup
- `CINC` - for a cumulative incremental backup

Note: You must run a full backup before an incremental backup. If no full backup is run, the incremental backup runs as a full backup. Cumulative incremental backups run as full backups till the next full backup schedule, and differential incremental run as full backups and subsequent differential backups run as incremental backups.

---

4 Select the clients or virtual machines to back up.

```
bpplinclude policy_name -add
"Nutanix-AHV://@NUTANIX_CLUSTER?filter=Displayname AnyOf
\"Nutanix_VM_Hostname\""
```

5 Add a backup host using the following command:

```
bpplclients policy_name -add backup_host hardware operating_system
```

Enter the *hardware operating_system* details of the backup host.

For example, `bpplclients policy_name -add backup_host Nutanix Virtual_Machine`

6 To enable the Accelerator feature:

Accelerator

```
bpplinfo policy_name -modify -use_accelerator 1 -residence
NetBackupSTU -use_virtual_machine 6 -alt_client_name backup_host
-snapshot_method "Hypervisor_snap" –snapshot_method_args
"application_consistent=0,Virtual_machine_backup=1,
vm_identifier=DISPLAYNAME,file_system_optimization=0,exclude_swap=0"
 -fi 1 -offhost_backup 1 -ct "Hypervisor" -active
-application_discovery 1 -blkincr 1
```

Here the `-use_accelerator 1` option is used.

Non-Accelerator

```
bpplinfo policy_name -modify -use_accelerator 0 -residence
NetBackupSTU -use_virtual_machine 6 -alt_client_name backup_host
-snapshot_method "Hypervisor_snap" -snapshot_method_args
"application_consistent=0,Virtual_machine_backup=1,
vm_identifier=DISPLAYNAME,file_system_optimization=0,exclude_swap=0"
 -fi 1 -offhost_backup 1 -ct "Hypervisor" -active
-application_discovery 1
```

7 To enable cumulative or differential incremental backups:

```
bpplinfo policy_name -modify -use_accelerator 0 -residence
STU_name -use_virtual_machine 6 -alt_client_name backup_hostname
 -snapshot_method "Hypervisor_snap" -snapshot_method_args
"application_consistent=0, Virtual_machine_backup=1,
vm_identifier=DISPLAYNAME, file_system_optimization=0,
exclude_swap=0" -fi 1 -offhost_backup 1 -ct "Hypervisor" -active
 -application_discovery 1 -blkincr 1
```

Here the `-blkincr 1` option is used.

The possible keyword values for the `snapshot_method_args` option are as follows:

Keyword values for `snapshot_method_args`	**Value - Description**
`application_consistent=`	**0** - Crash consistent
`virtual_machine_backup=`	**1** - Full VM backup
`vm_identifier=`	Display name
`exclude_swap=`	**0** - Disabled
`snapact=`	**0** - Continue backup

Note: NetBackup for Nutanix AHV does not support application consistent backups. Even if you enter `application_consistent=1`, the backups are set as crash consistent.

8 Validate the policy.

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

For example, `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.

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

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

See "NetBackup commands for protecting the AHV" on page 66.

See "Creating a backup policy using the NetBackup Policies utility" on page 33.

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

Chapter 5

Backup and recovery

This chapter includes the following topics:

Back up the Nutanix AHV virtual machines

You can initiate a backup for the AHV virtual machine using the **Hypervisor** 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 **Hypervisor** policy, refer to the following sections:

- See "About the Hypervisor policy type to protect Nutanix AHV VMs" on page 9. See "Migrating BigData policy to Hypervisor policy" on page 9.
- See "Creating a backup policy using the NetBackup Policies utility" on page 33.
- See "Creating a backup policy using the NetBackup Command Line Interface" on page 35.

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 the **Hypervisor** policy	NetBackup validates the **Hypervisor** policy that you have created to backup the AHV virtual machines. This step happens when you create and save the policy.

Phase	Description
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 3: Discovery of clients and commencing to backup the data on the clients	The backup process triggers three jobs - a parent job. a snapshot job, and a child job. The parent job runs the `nbdiscover` process and the `nbcs` process discovers the VMs for the matching criteria and then starts the snapshot jobs for each of the discovered client. Once the snapshot job completes, a backup job initiates that mounts the snapshot at the `/usr/openv/tmp/ntxmnt` location. The backup job then starts the actual read-write operation to backup the data on a disk.

Phase	Description
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. NetBackup Accelerator and Incremental feature uses Nutanix AHV's changed block tracking mechanism to get the metadata about the blocks that have changed between any two snapshots of a file. Nutanix requires two snapshots to provide this changed block information. NetBackup provides previous backup snapshot details and the current backup snapshot details to get the changed region information. Once this data is collected, NetBackup deletes the previous backup snapshot and keeps the current backup snapshot for next job to get the changed region. Based on the schedules in the policy, the following scenarios occur: ■ Full + Differential incremental backup Only the current backup job's VM snapshot is retained and the previous backup job's snapshot is removed. ■ Full + Cumulative incremental backup Only the last full backup job snapshot is retained and the current backup job snapshot is removed. ■ Full + Differential + Cumulative incremental backup Two snapshots are retained (last full and last differential incremental backup job snapshots) and the previously stored snapshots that are no longer needed for getting the changed block are removed. ■ Accelerator option enabled + Incremental Backup: Only the current backup job's VM snapshot is retained and the previous backup job's snapshot is removed.

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.

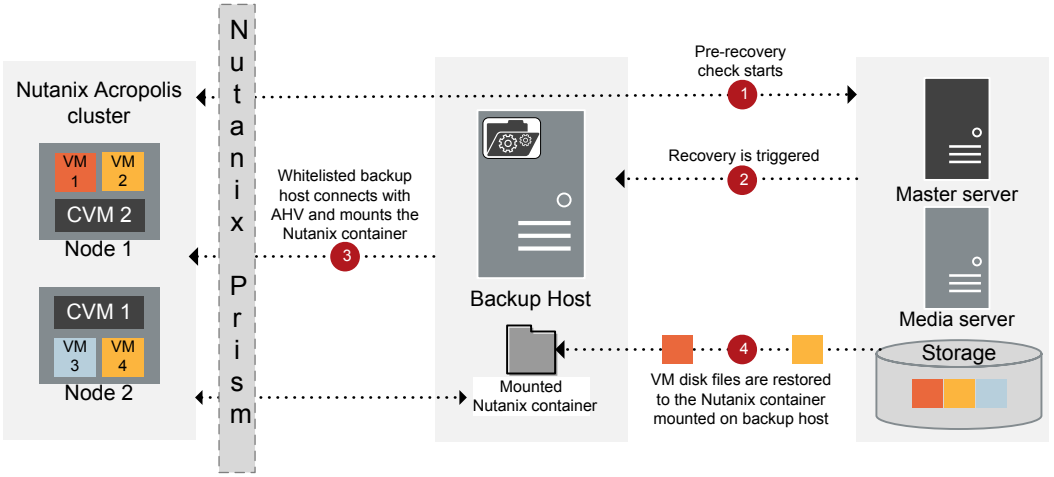
Table 5-1 Restoring Nutanix AHV data

Task	Reference
Understanding and planning the recovery process	■ Overview See "About recovering the Nutanix AHV virtual machines" on page 44. ■ Planning the recovery process See "Planning the recovery of a Nutanix AHV VM" on page 45.
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 48. ■ 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 49.
Recover the Nutanix AHV VM using the command line interface	See "Recovering a Nutanix AHV VM using the command line for Hypervisor policy" on page 50.

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

Table 5-2 Recovery location options

Original location	Alternate location
Recover the virtual machine in the same Nutanix AHV cluster or container that was set during the backup.	Recover the virtual machine to a different AHV cluster or container.

Table 5-2 Recovery location options *(continued)*

Original location	Alternate location
You can modify or set the following configurations before recovering to the original location: ■ Overwrite the existing VM ■ Create new VM ID instead of existing one ■ Remove the network interfaces ■ Retain the MAC address ■ Power on the VM after recovery ■ Overwrite the default job priority	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 ■ Create new VM ID instead of existing one ■ Remove the network interfaces (not valid for alternate restore on a different cluster of the same AHV server) **Note:** To restore to an alternate location, you must select this option. ■ Retain the MAC address (valid only for alternate restore on a different cluster of the same AHV server) ■ 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 as the command line options or in the `rename` file with the command line.

For more information about the `rename` file,

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

Table 5-3 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 Hypervisor policy	Description of recovery options
Overwrite the existing virtual machine	`K`	Overwrite the existing virtual machine in the AHV cluster. Use the `K` command line option to not overwrite the existing virtual machine.

Table 5-3 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 **Hypervisor policy**	Description of recovery options
Create new VM ID instead of existing one	`vmid`	Create a new ID for the VM that is different from the existing value that was set during the backup. Use the `vmid` command line option to retain the VM UUID.
Power on virtual machine after recovery	`vmpoweron`	Turn on the VM after recovery.
Remove network interfaces	`vmsn`	Remove the network interface that was set for the VM during the backup.
Retain the MAC address	`vmmacid`	Retain the MAC address that was set for the VM during the backup.
Change Virtual Machine Name	`vmname` in the rename file: `change vmname to new_name`	Change the virtual machine name to a new name.
Nutanix Acropolis Cluster	`vmserver`	Set the Nutanix AHV cluster where you want to recover the virtual machine.
Override default job priority	NA	Set a custom priority for the recovery job.
Destination Container	`change /<orig_container1> /<disk_uuid1> to /<alt_container1>` Add in the rename file.	Select the Nutanix AHV container where you want to recover the virtual machine. You can select a different destination container for every source container. **Note:** Restore the disks from the same source container to the same destination container.

For more information on using the recovery options using the command line interface, See "Using the command line to recover Nutanix AHV virtual machines for Hypervisor policy" on page 51.

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 45.

Note: For the **BigData** policy, 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 49.

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 **Hypervisor** as the policy type.
     - From the **Workload type for restores** list, select **Nutanix-AHV** as the workload 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 45.
   - See the section called “ About the recovery options” on page 46.

   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

- Use the **BigData** policy to recover images from 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 images that are backed up using the **BigData** policy:
  - 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 backups done using BigData policy.

Recovering a Nutanix AHV VM using the command line for Hypervisor policy

Use the `bprestore` command to recover a Nutanix AHV VM that was backed up using the Hypervisor policy.

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.
2. Use the command line to recover the VM.

   See "Using the command line to recover Nutanix AHV virtual machines for Hypervisor policy" on page 51.

Creating or modifying the rename file

Create or modify the rename file in the `/usr/openv/tmp` directory for the following scenarios:

- Recover the VM to an alternate container
- Recover the VM to the same or an alternate container with a modified VM name

For additional information, See "Planning the recovery of a Nutanix AHV VM" on page 45.

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
Change Virtual Machine Name	`change vmname to newVMname`
Recover the virtual machine to a different AHV container	`change /<original_container1>/<disk_uuid1> to /<alternate_container1>`

Sample rename file

The following `rename.txt` lets you change the VM name.

```
change vmname to newVMname
```

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 for Hypervisor policy" on page 51.

Using the command line to recover Nutanix AHV virtual machines for Hypervisor policy

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

To recover Nutanix AHV VM

1 On the NetBackup master server, 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 47
-L path_progress_log -f filelist -disk_media_server
disk_media_server -vmproxy backup_host -vmhypervisor -vmid
-vmmacid -vmsn -vmpoweron -vmserver NutanixAHV_cluster -K -s date
-e date
```

Where,

`-S`

Specifies the name or FQDN of the NetBackup master server.

`-C`

Specifies the Nutanix AHV VM name that you have backed up.

`-R`

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

`-t 47`

Specifies Hypervisor as the policy type.

`-L progress_log`

Specifies the name of allowlisted 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.

`-vmhypervisor`

Required option for Hypervisors

`-vmproxy`

Specifies the name or the FQDN of the backup host.

`-vmpoweron`

Turn on the VM after recovery.

`-K`

To not overwrite the existing virtual machine in the AHV cluster.

`-s, -e`

Specifies the start and the end date range for the listing the backup images. The `bprestore` command restores only the VMs from the backups that fall within the specified start and end date range. Use the time stamps that are captured during backup.

For more information about the date format, refer to the *NetBackup™ Commands Reference Guide*.

`-vmid`

Retain the VM UUID.

`-vmmacid`

Retain the MAC address of the VM. (This option is valid only for alternate restore on a different cluster of the same AHV server)

`-vmserver`

FQDN or the IP address of the Nutanix AHV cluster where you want to recover the virtual machine. Use the same type that was used to add the Nutanix AHV credentials.

`-vmsn`

Remove the network interface that was set for the VM during the backup.

Example

```
bprestore -S FQDN.master.server.com -C FQDN.client.com -R
<install_directory>\logs\user_ops\rename.txt -t 47 -L
<install_directory>\logs\user_ops\a.log -f filelist -disk_media_server
FQDN.disk.mediaserver.com -vmproxy FQDN.backup.host.com
```

Note: For restoring incremental backup images, if a policy or date range is not specified, then `bprestore` starts with the most recent full backup image. The command then checks all the subsequent incremental and differential backup images. The most recent copy of a file is restored from these images.

Chapter 6

Troubleshooting issues

This chapter includes the following topics:

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, or /usr/openv/logs/

Table 6-1 NetBackup logs related to the AHV

Log folder	Messages related to	Logs reside on
log_filepath\bpbrm	Back up and restore	Media server
log_filepath\bpfis	Snapshot jobs	NetBackup client on the backup host
log_filepath\bpbkar	Backup	NetBackup client on the backup host
log_filepath\bprd	Restore	Master server
log_filepath\bpcd	Back up and restore	NetBackup client on the backup host
/usr/openv/logs/ncfnbcs	Discovery logs (Hypervisor policy)	NetBackup client on the backup host
log_filepath\bpvmutil	Pre-recovery, restore UI, pre-restore, and post-restore (Hypervisor policy)	Master server or NetBackup client on the backup host
/usr/openv/logs/ncfnbrestore	Restore (Hypervisor policy)	Master server or NetBackup client on the backup host
log_filepath\vxms	Back up and Restore (Hypervisor policy)	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

Table 6-2 NetBackup troubleshooting 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: ■ `Hypervisor_Type=Nutanix-AHV` ■ `Application_Server=`*`Fully Qualified Domain Name or the IP address of the Nutanix cluster`* ■ `Backup_Host=`*`Fully Qualified Domain Name or the IP address`*
The backup job fails when the backup selection does not contain the `Backup_Host` parameter.	Add the `Backup_Host` parameter to the backup selections as follows: `Backup_Host=`*`Fully Qualified Domain Name or the IP address`* See "Adding a backup host to the NetBackup primary server" on page 30.
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 16.
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 8.2 and must have the out-of-band plug-in.
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 `Application_Server` parameter.	Verify that you have provided correct credentials. Ensure that the value that you have provided for the `Application_Server` parameters matched the one that you provided while specifying Nutanix Acropolis Cluster credentials. See "Adding the Nutanix Acropolis Hypervisor Cluster credentials for NetBackup" on page 28.

Table 6-2 NetBackup troubleshooting scenarios *(continued)*

Problem	Recommended action
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.
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 allowlist using the Nutanix Prism console.

Unable to unmount a container at the end of a VM restore. The recovery operation is partially successful.
The following error is displayed:
Failed to unmount container %s from mount path %s
OR
Failed to mount restore directory
	1 Delete the container directory from the following path:
	`/usr/openv/tmp/ntxmnt/<JOB_ID>/<container_name>/.restore`
	2 Delete the local directory from:
	`/usr/openv/tmp/ntxmnt/<JOB_ID>`

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.
The policy validation or the backup job fails when you have not provided the certificate trust store path correctly.	Ensure that the Nutanix cluster name used while adding Nutanix server in NetBackup should match with one of the subject name or alternate subject names in the certificate issued to the Nutanix cluster. Ensure that you have downloaded the root certificate of the CA issuing certificate to the Nutanix cluster, or the self-signed certificate of the Nutanix Acropolis server. This certificate must be stored in a PEM file. `ECA_TRUST_STORE_PATH` in `bp.conf` must point to the absolute path of this file.

Table 6-2 NetBackup troubleshooting scenarios *(continued)*

Problem	Recommended action

The Nutanix AHV VM restores successfully but the VM does not boot up.	■ For Nutanix AHV version 5.10 and UEFI boot machines, the following manual step is needed for both BigData policy (with EEB) and Hypervisor policy:
	On the controller VM of Nutanix run:
	`<acli> vm.update <restored_vm_name> uefi_boot=True`
	■ If boot device type that is configured on the backed up VM was NIC then update the boot device setting so that the VM boots up over the network, the following manual step is needed for both BigData policy (with EEB associated with Etrack 3982204) and Hypervisor policy:
	On the controller VM of Nutanix, replace `vm` with the name of the restored VM and `mac_addr` with the MAC address of the virtual interface that the VM must use to boot over the network.
	For example, update the boot device setting of the VM named `nw-boot-vm` so that the restored VM uses the virtual interface with MAC address `00-00-5E-00-53-FF`.
	`<acli> vm.update_boot_device nw-boot-vm mac_addr=00-00-5E-00-53-FF`
	If the VM is with NIC and UEFI, then for UEFI run the following additional steps:
	■ For AHV version 5.11 to set boot configuration as UEFI we also have an option on prism console
	From the Nutanix Prism console, select the VM and click **Update**.
	Select the UEFI firmware under the **Boot Configuration** section.
	Click **Save**. Restart the VM.
	■ If the AHV version is earlier than 5.11 then run the following command from the controller VM:
	`<acli> vm.update <restored_vm_name> uefi_boot=True`
	The following message is listed in the `bpVMutil` logs (`/usr/openv/netbackup/logs/bpVMutil/log_file`):
	Unable to restore the information to boot up the VM. Start the VM manually, if required.
	■ For BigData policy (with EEB associated with Etrack 3982204), run the following step manually for all the UEFI boot machines:
	On the controller VM of Nutanix run:
	`<acli> vm.update <restored_vm_name> uefi_boot=True`

Table 6-2 NetBackup troubleshooting scenarios *(continued)*

Problem	Recommended action
During the Nutanix AHV VM restore using the command line, the following error is displayed: Hypervisor policy restore error (2822)	When you use the command line to restore the Nutanix AHV VMs with a backup host that has NetBackup 8.2 but does not have the Nutanix AHV plug-in, the restore fails. Ensure that the plug-in is installed on the backup host that has NetBackup 8.2.
During the Nutanix AHV VM restore using the command line, the following error is displayed: network read failed (42)	When you use the `bprestore` command with the `-w` option to restore the Nutanix AHV VMs that are backed up using the Hypervisor policy, the restore job fails.
The restore job fails and the following error is displayed in the Activity Monitor: "The combination of the selected recovery options is invalid."	The issue occurs if the recovery option provided is not valid. This error is seen if one of the following scenarios is true: ■ Unsupported recovery options are set in the rename file. The `vmname` value cannot be different that the backup image when the `retainvmuuid` and `overwriteexistingvm` keywords are set to true. ■ If you try to overwrite the existing VM without retaining the VM UUID. Workaround: Ensure that the recovery option are correct before you run the restore operation. For detailed errors, refer to the log `/usr/openv/netbackup/logs/bpVMutil/` on the NetBackup backup host . For more details, refer to the *NetBackup for Nutanix AHV Administrator's Guide*.
The following errors are seen during a backup or restore operation: "Unmount operation failed." "Mount operation failed."	The issue occurs if: ■ The NetBackup backup host is not allowlisted in Nutanix AHV. ■ There is a network error. ■ NFS access or mount issue. Workaround: For backup failures, refer to the `/usr/openv/netbackup/logs/bpbkar/` logs and for restore failures, refer to the `/usr/openv/logs/ncfnbrestore/` logs for the exact reason of failure. You might want to manually unmount the folders of a failed job.

Table 6-2 NetBackup troubleshooting scenarios *(continued)*

Problem	Recommended action
The restore operation is partially successful and the following error is displayed: “Post Restore cleanup is failed”	The issue occurs if: ■ There is an error related to mount or unmount. ■ There is a data deletion issue on the Nutanix AHV cluster. Workaround: Restore is successful just the clean-up has failed. Refer to the `/usr/openv/netbackup/logs/bpVMutil/` log on the NetBackup backup host for the exact reason of failure.
During the policy validation for Incremental policy, if the backup host specified in policy is has NetBackup version 8.2 or earlier, the following error is displayed: "Backup host has an older version of NetBackup. Upgrade to the latest version."	For incremental backups, the NetBackup client on the backup host must be upgraded to version 8.3 or later.

When you restore using NetBackup version 8.2 and the out-of-band plugin the restore process can fail.
The following error is displayed in the activity monitor:
Hypervisor policy restore error. (2822)
In the `/usr/openv/netbackup/logs/bpVMutil` logs, the following errors are logged:
`<16> preRestoreVM: Failed to create: dir /usr/openv/tmp/ntxmnt/*, ret = 6647`
`<2> bpVMutil main: error code: 2879: invalid error number`
`<2> bpVMutil main: EXIT STATUS 2879: invalid error number`
	This issue occurs in the following scenario:
	During the backup, a `ntxmnt` folder is created that is used during the restore process. If the `ntxmnt` folder is not available during restore, then the restore process fails.
	Workaround:
	Manually create the `ntxmnt` in the `/usr/openv/tmp/` directory before you start the restore process.

In the **Hypervisor Policy** > **Backup Selections** tab, if you delete any entry, the **New** button remains disabled and you are unable to re-add the entry that you have deleted.	Workaround: Close the policy without saving the changes and re-open to get the previously saved values. You can then modify the existing entries, if required.

Table 6-2 NetBackup troubleshooting scenarios *(continued)*

Problem	Recommended action
If a policy is created using the command line and an incremental schedule is added but the `-blkincr` option is not set to 1, the following error is displayed: Incorrect configuration for the incremental backup schedule. Set the correct block level incremental value for the backup policy.	Workaround: Modify the policy and set the `-blkincr` option to 1.
When the target server for AIR is a Nutanix AHV server, a failed to get the container list error is seen in the Activity Monitor for a backup operation.	This error can happen when the Nutanix AHV server is not available or accessible when the backups are taken. This can be due to the following reasons: ■ A disaster has occurred at the Nutanix AHV server location. ■ The Nutanix AHV server hardware is replaced. ■ The Nutanix AHV credentials are incorrect or they have expired. ■ The security certificates are incorrect or they have expired. ■ The AIR or DR location where the AHV server is configured is not available or accessible.

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 backup policy, provide the same Fully Qualified Domain Name in the `Application_Server` 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.
When you try to backup the virtual machines that have volume group disks, the backup fails with following message in the `bpbkar` process logs: failed to get `snapshot_file_path` from the JSON file.	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.
When the following status code is displayed: Error code 223: an invalid entry was encountered	Ensure that the credentials to access the Nutanix Acropolis cluster are valid, and Hypervisor server is accessible.

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

Problem	Recommended action
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 Hypervisor Cluster credentials for NetBackup" on page 28. See "Adding a backup host to the NetBackup primary access list" on page 30.
When the following status code is displayed: Error code 4725: An internal error occurred.	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.

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

Problem	Recommended action
When following status code or messages are displayed: (4748) Unable to retrieve the VM. (200) scheduler found no backups due to run	To check for secure communication and any backup policy errors, run the following command. `<NetBackup path>/bin/admincmd/bpclient -M <master server name> -policy <policy name> -validate` Ensure that the Nutanix cluster name used while adding Nutanix server in NetBackup should match with one of the subject name or alternate subject names in the certificate issued to the Nutanix cluster. Ensure that you have downloaded the root certificate of the CA issuing certificate to the Nutanix cluster, or the self-signed certificate of the Nutanix Acropolis server. This certificate must be stored in a PEM file. If the policy validation is working correctly, check that one or more VM names specified in the policy actually exist on the Nutanix AHV server.

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

Appendix A

NetBackup commands to backup and restore Nutanix AHV virtual machines

This appendix includes the following topics:

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 **Hypervisor** backup policy.
`bpplinfo`	Use this command to: ■ Modify the **Hypervisor** policy. ■ Add a storage unit. ■ Limit simultaneous jobs per policy.

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

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