NetBackup™ Web UI RHV Administrator's Guide

Release 9.0

VERITAS™

NetBackup Web UI RHV Administrator's Guide

Last updated: 2020-12-14

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

Introducing the NetBackup web user interface

This chapter includes the following topics:

About the NetBackup web UI

The NetBackup web user interface provides the following features:

- Ability to access the master server from a web browser, including Chrome and Firefox. For details on supported browsers for the web UI, see the NetBackup Software Compatibility List.
  Note that the NetBackup web UI may behave differently for different browsers. Some functionality, for example a date picker, may not be available on all browsers. These inconsistencies are due to the capabilities of the browser and not because of a limitation with NetBackup.
- A dashboard that displays a quick overview of the information that is important to you.
- Role-based access control (RBAC) that lets the administrator configure user access to NetBackup and to delegate the tasks such as security, storage management, or workload protection.
- Management of NetBackup security settings, certificates, API keys, and user sessions.

- Protection of assets is achieved through protection plans, job management, and visibility of the protection status of assets. Alternatively, policy management is also available for a limited number of policy types.
- Workload administrators can create protection plans, subscribe assets to the protection plans that meet the SLO, monitor protection status, and perform self-service recovery of virtual machines. The web UI supports the following workloads:
  - Cloud
  - Microsoft SQL Server
  - Oracle
  - Red Hat Virtualization (RHV)
  - VMware
- Usage reporting tracks the size of backup data on your master servers. You can also easily connect to Veritas NetInsights Console to view and manage NetBackup licensing.

Note: The NetBackup web UI is best viewed at a 1280x1024 or higher screen resolution.

Access control in the NetBackup web UI

NetBackup uses role-based access control to grant access to the web UI. Access control is accomplished through roles.

- A role defines the operations that a user can perform and the access that the user has to any workload assets, protection plans, or credentials. A user can have multiple roles, allowing for full and for flexible customization of user access.
- RBAC is only available for the web UI and the APIs.
  Other access control methods for NetBackup are not supported for the web UI and APIs, with the exception of Enhanced Auditing (EA). .

Monitor NetBackup jobs and events

The NetBackup web UI lets administrators more easily monitor NetBackup operations and events and identify any issues that need attention.

- The dashboard displays an overview of NetBackup jobs, certificates, tokens, security events, and usage reporting.
  The dashboard widgets that display depend on a user's RBAC role and permissions.

- Email notifications can be configured so administrators receive notifications when job failures occur. NetBackup supports any ticketing system that can receive inbound email.

Protection plans: One place to configure schedules, storage, and storage options

Protection plans offer the following benefits:

- In addition to schedules for backups, a protection plan can also include a schedule for replication and long-term retention.
- When you select from your available storage, you can see any additional features available for that storage.
- A default workload administrator can create and manage protection plans, including the backup window and retention.
  See *NetBackup Web UI Administrator's Guide* for details on the roles permissions.
- A default workload administrator can select the protection plans to use to protect assets or intelligent groups.

Self-service recovery

The NetBackup web UI makes it easy for a workload administrator to recover VMs or databases. For the workloads that support the instant access feature, users can mount a snapshot for immediate access to a VM's files or to a database.

Terminology

The following table describes the concepts and terms that are introduced with the new web user interface.

Table 1-1 Web user interface terminology and concepts

Term	Definition
Administrator	A user that has complete access and permissions to NetBackup and all of the interfaces, including the NetBackup web UI. The root, administrator, and Enhanced Auditing user all have complete access to NetBackup. In the *NetBackup Web UI* guides, the term *NetBackup administrator* also refers to a user that has full permissions for NetBackup. Usually in reference to a user of the NetBackup Administration Console. Also see *role*.
Asset group	See *intelligent group*.

Table 1-1 Web user interface terminology and concepts *(continued)*

Term	Definition
Asset	The data to be protected, such as physical clients, virtual machines, and database applications.
Backup now	An immediate backup of an asset. NetBackup performs a one-time, full backup of an asset using the selected protection plan. This backup does not affect any scheduled backups.
Classic policy	In the NetBackup web UI, indicates that a legacy policy protects the asset. Legacy policies are created with the NetBackup Administration Console.
External certificate	A security certificate that is issued from any CA other than NetBackup.
Intelligent group	Allows NetBackup to automatically select assets for protection based on the criteria (queries) that you specify. An intelligent group automatically stays up-to-date with changes in the production environment. These groups are also referred to as asset groups. For VMware and RHV, these groups appear under the tab **Intelligent VM groups**.
Instant access	An instant access VM or database that is created from a NetBackup backup image is available almost instantaneously, achieving a near-zero recovery time objective. NetBackup mounts the snapshot directly on the backup storage device and the snapshot is treated as a normal VM or database. Not applicable for RHV in NetBackup version 8.3 or earlier.
NetBackup certificate	A security certificate that is issued from the NetBackup CA.
Protection plan	A protection plan defines when backups are performed, how long the backups are retained, and the type of storage to use. Once a protection plan is set up, assets can be subscribed to the protection plan.
RBAC	Role-based access control. Administrators can delegate or limit access to the NetBackup web UI through the roles that are configured in RBAC. **Note:** The roles that you configure in RBAC do not control access to the NetBackup Administration Console or the CLIs.

Table 1-1 Web user interface terminology and concepts *(continued)*

Term	Definition
Role	For RBAC, defines the operations that a user can perform and the assets or objects that they can access. For example, you can configure a role to mange recovery of specific databases and the credentials that are needed for backups and restores.
Storage	The storage to which the data is backed up, replicated, or duplicated (for long-term retention).
Subscribe, to a protection plan	The action of selecting an asset or an asset group to subscribe to a protection plan. The asset is then protected according to the schedule in the plan. The web UI also refers to *Subscribe* as *Add protection*.
Unsubscribe, from a protection plan	*Unsubscribe* refers to the action of removing protection or removing an asset or asset group from a plan.
Workload	The type of asset. For example, VMware, RHV, or Cloud.

Sign in to the NetBackup web UI

Authorized users can sign in to a NetBackup master server from a web browser, using the NetBackup web UI. The following sign-in options are available:

- Sign in with a username and password
- Sign in with a certificate or smart card
- Sign in with single sign-on (SSO)

Sign in with a username and password

Only authorized users can sign in to NetBackup web UI. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup master server using a username and password

1. Open a web browser and go to the following URL.

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master server that you want to sign in to.

2. Enter your credentials and click **Sign in**.

   For example:

For this type of user	Use this format	Example
Local user	*username*	**jane_doe**
Windows user	*DOMAIN\username*	**WINDOWS\jane_doe**
UNIX user	*username@domain*	**john_doe@unix**

Sign in with a certificate or smart card

You can sign in to NetBackup web UI with a smart card or digital certificate if you are an authorized user. Contact your NetBackup security administrator for more information.

To use a digital certificate that is not on a smart card, you must first upload the certificate to the browser's certificate manager. See the browser documentation for instructions or contact your certificate administrator for more information.

To sign in with a certificate or smart card

1. Open a web browser and go to the following URL.

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master server that you want to sign in to.

2. Click **Sign in with certificate or smart card**.

3. When your browser prompts you, select the certificate.

Sign in with single sign-on (SSO)

You can sign in to NetBackup web UI with the single sign-on (SSO) option if SAML is configured as an identity provider in your NetBackup environment. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup master server using SSO

1. Open a web browser and go to the following URL.

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master server that you want to sign in to.

2. Click **Sign in with single sign-on**.

3. Follow the steps as provided by your administrator.

   On subsequent logons, NetBackup signs you in automatically to the master server.

Sign out of the NetBackup web UI

Note that NetBackup automatically signs you out of the web UI after 24 hours, which is the maximum time that is allowed for a user session. After that time NetBackup requires that you sign in again. You can also sign out if you want to change the sign-in option that you want to use (username and password, smart card, or single sign-on (SSO)).

To sign out of the NetBackup web UI

- On the top right, click the profile icon and click **Sign out**.

Chapter 2

Monitoring and notifications

This chapter includes the following topics:

The NetBackup dashboard

The NetBackup dashboard provides a quick view of the details that are related to your role in your organization.

Table 2-1 The NetBackup dashboard

Dashboard widget	Description
Jobs	Lists job information, including the number of active and queued jobs and the status of attempted and completed jobs.
Certificates	Displays the information about the NetBackup host ID-based security certificates or the external certificates in your environment. For external certificates, the following information is shown for NetBackup 8.2 and later hosts: ■ Total hosts. The total number hosts. The hosts most be online and able to communicate with NetBackup master server. ■ Missing. The number hosts that do not have an external certificate enrolled. ■ Valid. The number of hosts that have an external certificate enrolled. ■ Expired. The number of hosts with expired external certificates.

Table 2-1 The NetBackup dashboard *(continued)*

Dashboard widget	Description
Tokens	Displays the information about the authorization tokens in your environment.
Security events	The **Access history** view includes a record of logon events. The **Audit events** view includes the events that users initiate on the NetBackup master server.
Usage reporting	Lists the size of the backup data for the NetBackup master servers in your organization. This reporting is useful to track capacity licensing. Use the drop-down lists in the top right to select the time period and the view that you want to display. Click on a server name to see specific details for that server.

Monitoring jobs

Use the **Jobs** node to monitor the jobs in your NetBackup environment and view the details for a specific job.

To monitor a job

1. On the left, click **Activity monitor > Jobs**.
2. Click on a job name that you want to view.

   On the **Overview** tab you can view information about a job.

   - The **File List** contains the files that are included in the backup image.
   - The **Status** section shows the status and the status codes that are related to the job. Click the status code number to view information about this status code in the Veritas Knowledge Base.

     See the NetBackup Status Codes Reference Guide.
3. Click the **Details** tab to view the logged details about a job. You can filter the logs by error type using the drop-down menu.

   See “Filter jobs in the job list” on page 14.

Filter jobs in the job list

You can filter the jobs to display the jobs in a specific state. For example, you can display all of the active jobs or all of the suspended jobs.

To filter the job list

1. Click **Jobs**.
2. Above the job list, click the **Filter** option.

3 In the **Filter** window, select a filter option to dynamically change the jobs that are displayed. The filter options are as follows:

- **All**
- **Active**
- **Done**
- **Failed**
- **Incomplete**
- **Partially Successful**
- **Queued**
- **Successful**
- **Suspended**
- **Waiting for Retry**

4 Click **Apply Filters**.

5 To remove the selected filters, click **Clear All**.

Chapter 3

Managing RHV servers

This chapter includes the following topics:

Quick configuration checklist to protect Red Hat Virtualization virtual machines

Use NetBackup Web UI to protect the virtual machines that are created on the Red Hat Virtualization (RHV) platform.

You can also use APIs and command line options to protect and recover the RHV VMs.

See "Using APIs and command line options to manage, protect, or recover RHV virtual machines" on page 50.

The following table describes the high-level steps or a checklist to protect the RHV virtual machines:

Table 3-1 Configure and protect RHV virtual machines using NetBackup

Step overview	Description and reference
Deploy NetBackup to protect RHV VMs	On a very high-level, to protect RHV VMs, you need: ■ NetBackup master server ■ NetBackup media server ■ NetBackup client that can act as a backup host NetBackup master and media servers are supported on any supported server platform of NetBackup, whereas NetBackup client is supported on RHEL, SUSE, or a Windows host. NetBackup appliance including Flex appliance is also supported as a NetBackup master, media server, or as a client that can act as a backup host. NetBackup uses an agentless architecture to protect the RHV VMs. The communication between NetBackup and RHV Manager happens throught APIs.
Configure an RHV access host for backup and recovery	An RHV access host acts as a backup host and a recovery host during backup and recovery respectively. The access host is involved in the data movement during the backup and restore operations. If you plan to use a backup host that is not a NetBackup media server or an appliance, add the backup host to the NetBackup **RHV Access Hosts** list. See "Adding a backup host to the NetBackup master server" on page 27.
Enable secure communication between NetBackup and RHV	The following sections contain more information about setting up a secure communication between NetBackup and RHV: ■ Secure communication See "Configuring secure communication between the Red Hat Virtualization server and NetBackup host" on page 19. ■ Communication ports See "About the ports that NetBackup uses to communicate with RHV" on page 25.
Manage RHV servers and intelligent VM groups	■ Prerequisite: Adding an RHV manager requires the backup administrator role. ■ Managing RHV servers See "Add or browse an RHV manager" on page 26. ■ Managing intelligent VM groups See "Create an intelligent VM group" on page 28. See "Remove an intelligent VM group" on page 33.

Table 3-1 Configure and protect RHV virtual machines using NetBackup *(continued)*

Step overview	Description and reference
Protect the RHV VMs	■ Prerequisite: Adding an RHV manager requires the backup administrator role. ■ Best practices See "Things to know before you protect RHV virtual machines" on page 35. ■ Protecting virtual machines See "Protect RHV VMs or intelligent VM groups" on page 36.
Consider setting global limits on the use of RHV resources	When you protect VMs automatically when they are created, over a period of time the number of VMs protected concurrently can grow large. The large number of concurrent backups can affect the RHV performance as well as backup performance. You can set the global limits to manage the RHV resources efficiently. See "Setting global limits on the use of RHV resources" on page 33.

Additional references

The following table describes the high-level steps or a checklist to recover the RHV virtual machines and additional information:

Table 3-2 RHV VM recovery and additional information

Step overview	Description and reference
Removing protection from VMs	See "Remove protection from VMs or intelligent VM groups" on page 38.
Recover the protected RHV VMs	■ Best practices See "Things to consider before you recover the RHV virtual machines" on page 40. ■ Supported disk format and disk provisioning See "About the supported virtual disk formats and disk provisioning during VM recovery" on page 43. ■ Recover RHV VMs See "Recover an RHV virtual machine" on page 41.
API and command line options to protect RHV VMs	You can use NetBackup APIs or command line options to protect and recover RHV VMs ■ See "Using APIs and command line options to manage, protect, or recover RHV virtual machines" on page 50. ■ See "Additional NetBackup options for RHV configuration" on page 55.

Table 3-2 RHV VM recovery and additional information *(continued)*

Step overview	Description and reference
Troubleshooting information	■ Use the following information to troubleshoot issues regarding RHV protection or recovery See "*Troubleshooting RHV VM protection and recovery*" on page 45.

Configuring secure communication between the Red Hat Virtualization server and NetBackup host

NetBackup can now validate Red Hat Virtualization server certificates using their root or intermediate certificate authority (CA) certificates.

Only `PEM` certificate format is supported for virtualization servers.

For more information, See "VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED for servers and clients" on page 24.

The following procedure is applicable for the NetBackup master server and all RHV access hosts.

To configure secure communication between Red Hat Virtualization server and RHV access host

1. Configure a external certificate authority trust store on the RHV access host.
2. Add CA certificates of the required Red Hat Virtualization server in the trust store on the access host.

   In case of Windows certificate store, add the CA certificate to the Windows Trusted Root Certification Authorities.

   Use the following command:

   ```
   certutil.exe -addstore -f "Root" certificate filename
   ```

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, Volume I.

`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 RHV CA certificates to the existing external certificate trust store. If you have not configured the option, add all the required Red Hat Virtualization server CA certificates to the trust store and set the option. See "ECA_TRUST_STORE_PATH for NetBackup servers and clients" on page 22.
`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 Red Hat Virtualization 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 23.
`VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED`	This option affects Nutanix AHV, RHV, and VMware secure communication. Without this option, the secure or insurce communication with workload is decided by each workload and plug-in separately. For mor information, refer to the respective workload Administrator's Guide. For RHV, 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 24.

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 24.

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.

Table 3-3 ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option. 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 24.

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

Table 3-4 ECA_CRL_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, RHV servers, Nutanix AHV, or Hadoop, this option must be set on the NetBackup master 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. 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.

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 option must be set to NO for the other backup host.

Table 3-5 VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED information

Usage	Description
Where to use	On NetBackup master server or all access hosts.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option. 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 23.

Table 3-6 VIRTUALIZATION_CRL_CHECK information

Usage	Description
Where to use	On NetBackup master server or all access hosts.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option. 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.

About the ports that NetBackup uses to communicate with RHV

The following table describes the ports that NetBackup requires to communicate with RHV:

Table 3-7 Ports required by NetBackup to communicate with RHV

Port	Protocol	Destination	Purpose
80, 443	TCP	RHV Manager	Provides HTTP and HTTPS access to the RHV Manager

Table 3-7 Ports required by NetBackup to communicate with RHV *(continued)*

Port	Protocol	Destination	Purpose
54322	TCP	RHV Hosts (Red Hat Enterprise Linux hosts)	Required for communication with the `ImageIO` daemon (`ovirtimageio-daemon`)
54323	TCP	RHV Manager (`ImageIO` Proxy server)	Required for communication with the `ImageIO` Proxy (`ovirtimageio-proxy`)

Add or browse an RHV manager

You can add and browse RHV managers and their credentials.

To add RHV managers and their credentials

1. On the left, click **RHV** then click the **RHV managers** tab.
2. Click **+ Add** to add an RHV manager and enter the following:
   - RHV manager name
   - Access credentials
   - Select a backup host using the **Backup host for validation**
   - Port number (optional)

   Note: NetBackup recommends that you use the FQDN to add the RHV Manager. Using an IP address or short name to add the RHV Manager can create duplicate entries and cause issues during RBAC enforcement.

   Adding a backup host to the NetBackup master server
3. Click **Save**.
4. To add another RHV Manager credentials, click **Add**.

Inline actions on RHV manager

You can run the following inline actions on an RHV manager:

- **Discover**: Manually discovers the VM assets that belong to the selected RHV manager.
- **Edit**: Modify the RHV manager credentials.

- **Delete**: Removes the RHV manager.

Bulk actions on RHV managers

You can select one or more RHV managers and run the following bulk actions:

- **Validate credentials**: Validates the credentials of the RHV manager.
- **Delete**: Removes the RHV managers.

Browse an RHV manager

You can browse the RHV managers and clusters to locate VMs and view their details such as their protection plans and recovery points.

To browse RHV managers

1. On the left, click **RHV**.
2. Click **RHV managers** to begin searching.

   The list includes the RHV managers and clusters that you have access to.

   The tab shows the RHV managers and clusters that you can access in the following hierarchy:

   ```
   All
   RHV_Managers
    RHV_Manager1
     Cluster1
     Cluster2
    RHV_Manager2
     Cluster3
     Cluster4
   ```

   To locate a server, you can enter a string in the search field.
3. Click on an RHV manager to view details.

   You can navigate back to a higher level by clicking the up-arrow.
4. Click on a VM to view its protection status, recovery points, and restore activity.
5. Click **Add protection** to subscribe the VM to a plan.

Adding a backup host to the NetBackup master server

The backup host or appliance acts as a channel to establish an indirect communication between the NetBackup master server and the RHV manager. The backup host is a NetBackup client that performs backups or restores on behalf of the virtual machines.

A NetBackup master and media server can also be configured as the backup host. However, you do not need to add the master or media server acting as a backup host to the **RHV Access Hosts** list.

The secure communication happens by APIs and uses SSL.

Note: SSL requires that all backup hosts have ECA certificates.

Communication between RHV and backup host requires an open port.

The following operating systems are supported for your backup host:

- Windows
- Red Hat Linux
- SUSE

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

Remove an RHV manager

RHV managers can be removed by means of the bulk or the inline actions from the **RHV manager** tab.

When you remove an RHV manager, you can no longer protect the RHV VMs from the NetBackup.

See "Add or browse an RHV manager" on page 26.

Create an intelligent VM group

You can create an intelligent VM group based on a set of filters called queries. NetBackup automatically selects virtual machines based on the queries and adds them to the group. You can then apply protection to the group. Note that an intelligent group automatically reflects changes in the VM environment and eliminates the need to manually revise the list of VMs in the group.

Note: A background task adds the newly discovered VMS that match the query to the intelligent VM group. This background task runs 5 minutes after the start of the Netbackup Web Management service. After that, the task runs every 30 minutes.

To create an intelligent VM group

1. On the left, click **RHV**.
2. Click the **Intelligent VM groups** tab and then click **+ Add**.
3. Enter a name and description for the group.

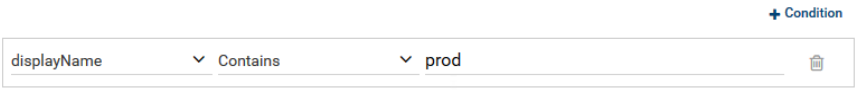
   The intelligent VM group display name length must be between 1 to 256 characters.
4. In the **Select virtual machines** pane, select the appropriate **RHV manager**.

   Note: The web UI lists the servers that you can access based on your role and permissions (RBAC).

   - Select the default query: **Include all VMs**.
     When the protection plan runs, all VMs that are part of the RHV manager are selected for backup.
   - Create your own query: Click **Add condition**.
5. To add a condition, use the drop-downs to select a keyword and operator and then enter a value.

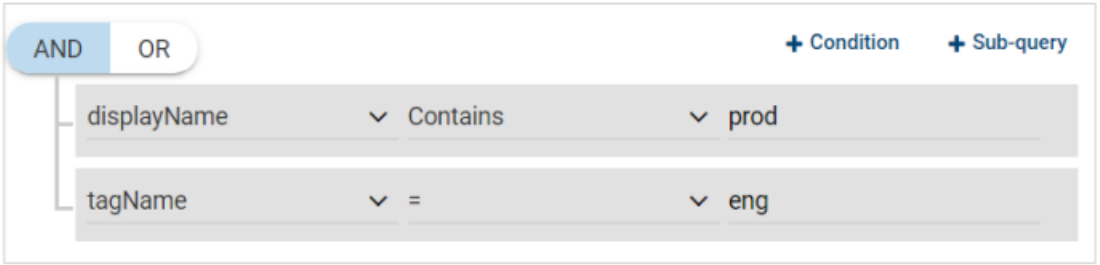
   The options are described after this procedure: Query options for creating intelligent VM groups.

   The following is an example query:



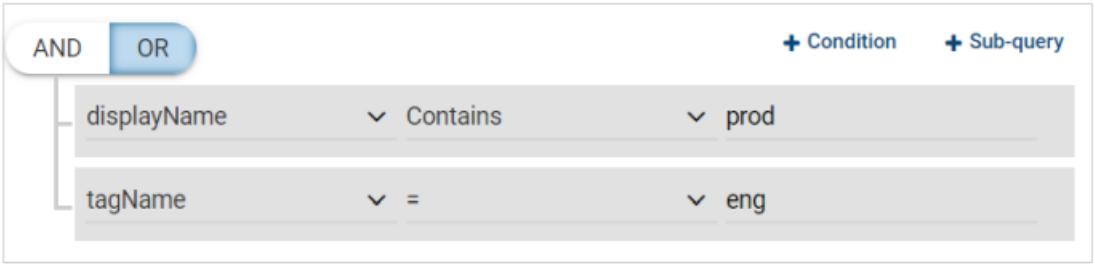
   In this example, the query adds to the group any VM that has `prod` in its display name.

   To change the effect of the query, click **+ Condition** and click **AND** or **OR**, then select the keyword, operator, and value for the condition. For example:



This example uses **AND** to narrow the scope of the query: it selects only the VMs that have `prod` in their display name and that also have a tag named `eng`. If a VM does not have `prod` in its display name as well as a tag named `eng`, that VM is not added to the group.

To broaden the scope of the query, use **OR**:



In this example, **OR** causes the query to add the following to the group:

- The VMs that have `prod` in their display name (regardless of any tags).
- The VMs that have a tag named `eng` (regardless of the display name).

6 To test the query, click **Preview**.

Note: The query-based selection process is dynamic. Changes in the virtual environment can affect which VMs the query selects when the protection plan runs. As a result, the VMs that the query selects later when the protection plan runs may not be identical to those currently listed in the preview.

7 To save the group without adding it to a protection plan, click **Add**. To save and add it to a protection plan, click **Add and protect**, select the plan, and click **Protect**.

Note: When you click **Preview** or save the group, the query options are treated as case-sensitive when the VMs are selected for the group. Under **Virtual machines**, if you click on a VM that was not selected for the group, the **Member of virtual machine groups** field reads `none`.

However, when you add the group to a protection plan, some of the query options are treated as case-insensitive when the protection plan's backup runs. As a result, the same VM may now be included in the group and is backed up.

For the case behavior of each option, see Query options for creating intelligent VM groups.

Note: If you use filters in intelligent group, NetBackup Web UI might not display the accurate list of VMs that match the filter if the VM or the RHV server has non-English characters. However, during the backup, correct VMs are selected even though the VM attributes are non-English. This behavior is only in viewing the VMs in NetBackup Web UI.

Query options for creating intelligent VM groups

Table 3-8 Query keywords

Keyword	Description
`cluster`	The name of the cluster where the VMs reside. Not case-sensitive when the protection plan runs.
`datacenter`	The name of the data center. Not case-sensitive when the protection plan runs.

Table 3-8 Query keywords *(continued)*

Keyword	Description
`displayName`	The VM's display name. Case-sensitive when the protection plan runs.
`tagName`	The name of the VM's tag. Case-sensitive when the protection plan runs.
`vmUuid`	The VM's instance UUID. For example: `501b13c3-52de-9a06-cd9a-ecb23aa975d1` Not case-sensitive when the protection plan runs.
`storageDomainName`	The name of the storage domain. Case-sensitive when the protection plan runs.
`templateName`	The name of the VM template. Case-sensitive when the protection plan runs.

Table 3-9 Query operators

Operator	Description
`Starts with`	Matches the value when it occurs at the start of a string. For example: If the value you enter is `box`, this option matches the string `box_car` but not `flatbox`.
`Ends with`	Matches the value when it occurs at the end of a string. For example: If the value you enter is `dev`, this option matches the string `01dev` but not `01dev99` or `devOP`.
`Contains`	Matches the value you enter wherever that value occurs in the string. For example: If the value you enter is `dev`, this option matches strings such as `01dev`, `01dev99`, `devOP`, and `development_machine`.
=	Matches only the value that you enter. For example: If the value you enter is `VMtest27`, this option matches `VMTest27` (same case), but not `vmtest27`, `vmTEST27`, or `VMtest28`.
!=	Matches any value that is not equal to the value that you enter.

Remove an intelligent VM group

Use the following procedure to remove an intelligent VM group.

To delete an intelligent VM group

1. On the left, click **RHV**.
2. Locate the group under the **Intelligent VM groups** tab.
3. If the group is not protected, click its box and click **Delete**.
4. If the group is protected, click on the group, scroll down and click the lock symbol, and click **Unsubscribe**.
5. Click **Remove**.

Setting global limits on the use of RHV resources

You can use the NetBackup Resource Limit dialog from the NetBackup administration console to control the number of simultaneous backups that can be performed on an RHV resource type. The settings apply to all NetBackup policies for the currently selected master server.

For example, to avoid overloading the overall RHV cluster, you can place a limit on the number of concurrent backup jobs per RHV Cluster. To control input output overhead on the storage domain array, you can limit the number of concurrent backups per storage domain.

Resource limits available for RHV:

- **Backup Jobs per DataCenter**
- **Backup Jobs per Cluster**
- **Backup Jobs per StorageDomain**

To set limits on the use of RHV resources

1. In the NetBackup Administration Console, click **Host Properties > Master Servers** and double-click the NetBackup master server.
2. In the **Properties** screen, scroll down in the left pane and click **Resource Limit**.
3. Under **Application**, click **RHV**.
4. Click in the **Resource Limit** column to set the maximum NetBackup usage for a particular resource type. The settings apply to all policies.

   For each resource type, the default is 0, (No Limit).

Following example illustrates how these limits control simultaneous backups. The settings must be done according to RHV configuration in your environment.

When NetBackup connects to the RHV environment for backup, it makes 1 connection per disk present on the VM. So, if a VM has 2 disks then NetBackup would make 2 connections with the RHV node.

So, consider a case where RHV manager is managing 2 clusters with 2 nodes in each cluster. Let's consider every node is hosting 20 VMs with 2 disks on each VM.

When the job runs, there would be 80 concurrent jobs start if no Resource Limit is set which is default behavior. RHV recommends up to 10 disk connections concurrently per node in the cluster. In the example of each VM with two disks, 5 VMs per node can be ideally backed up concurrently. Hence, in this case of a cluster with two nodes, it is recommended to backup upto 10 VMs concurrently. When the **Backup Jobs per Cluster** is set to 10, this limit is enforced.

Since one data center can manage multiple clusters, **Backup Jobs per DataCenter** resource limit could be higher than **Backup Jobs per Cluster**. You need to determine the values by evaluating the effect of backup on overall environment.

Storage domain in RHV can server multiple clusters in a data center. It serves to protection VM as well as backup. Its performance is dependent on type of storage technology – FC, iSCSI, NFS, gluster etc. Hence limit on storage domain using **Backup Jobs per StorageDomain** can be set based on characteristics of storage domain technology and limit can be higher than **Backup Jobs per Cluster**.

Chapter 4

Protecting RHV virtual machines

This chapter includes the following topics:

Things to know before you protect RHV virtual machines

- You cannot backup the same RHV VM concurrently.
- The VMs without virtual disks cannot be protected.
- Ensure to use the same backup host to backup all template-based VMs (dependent clone).
  For example, VMs `VMRedHat1`, `VMRedHat2` are created from template `RedHat7_Template` as dependent clone and VMs `VMWin1`, `VMWin2` are created from template `Windows2016_Template` as dependent clone.
  While protecting these VMs, use the same backup host for all VMs based on template `RedHat7_Template` or `Windows2016_Template`. Ensure that `VMRedHat1` and `VMRedHat2` share the same backup host. Ensure that `VMWin1` and `VMWin2` share the same backup host.`VMRedHat1`, `VMRedHat2`, `VMWin1` and `VMWin2` can share the same backup host, but it is optional.

- The following QCOW2 image attributes are not supported:
  - Compressed cluster
  - Encrypted disks
  - Virtual disks with internal snapshots
- If the VM virtual disks are locked when the NetBackup services shutdown or crash during a backup, use RHV's `unlock_entity` command to unlock the disks. If the disks are not unlocked, the subsequent backups might fail.
  See "Error run into while backing up RHV virtual machines" on page 47.
- On a file storage (NFS), a QCOW2 disk gets restored as raw disk (thin provision) because of an RHV limitation.
- A thin dependent cloned VM is restored as an independent cloned VM.
- If you want to use a storage that is not available through the NetBackup Web UI like a tape or basic disk based storage unit, you can use APIs or command line options to protect the VMs.

Protect RHV VMs or intelligent VM groups

Use the following procedure to subscribe an asset (RHV VMs or intelligent VM groups) to a protection plan. When you subscribe an asset to a protection plan, you assign predefined backup settings to the asset.

Note: The RBAC role that is assigned to you must give you access to the assets that you want to manage and to the protection plans that you want to use.

To protect RHV VMs or VM groups

1. On the left, click **RHV**.
2. On the **Virtual machines** tab or **Intelligent VM groups** tab, click the box for the VM or the VM group and click **Add protection**.
3. Select a protection plan and click **Next**.
4. If you have the necessary role permissions you can adjust one or more of the following settings:
   - **Schedules and retention**
     Change when backups occur and the backup start window.
   - **Backup options**

Adjust the server or host to use for backups.

5 Click **Protect**.

The results of your choices appear under **Virtual machines** or **Intelligent VM groups**.

Edit protection settings for a RHV asset

If you have the necessary role permissions, you can edit certain settings for a protection plan, including schedules and other options.

- See "Schedules and retention" on page 37.
- See "Backup options" on page 38.

To edit protection settings for a RHV asset

1 On the left, click **Workloads > RHV**.

2 Do one of the following:

Edit the settings for a VM	■ On the **Virtual machines** tab, click on the VM that you want to edit.
Edit the settings for an intelligent group	■ On the **Intelligent VM groups** tab, click on the group that you want to edit.

3 Click **Customize protection > Continue**.

4 If you have the necessary role permissions you can adjust one or more of the following settings:

- **Schedules and retention**
  Change the backup start window.
  See "Schedules and retention" on page 37.
- **Backup options**.
  See "Backup options" on page 38.

5 Click **Protect**.

Schedules and retention

When you have the necessary RBAC permissions, you can adjust the following settings when you subscribe an asset to a protection plan.

Table 4-1

Option	Description
Start window	Set the window during which a backup can start.

Backup options

The user can adjust the following settings when subscribing to a protection plan.

Option	Description
Select server or host to use for backups	The host that performs backups on behalf of the virtual machines. Users can choose **Automatic** to have NetBackup pick the media server, based on the storage unit. Or, the user can select another host from the list. These hosts are other media servers in the environment or hosts that are configured as an access host.

Remove protection from VMs or intelligent VM groups

You can unsubscribe VMs or intelligent VM groups from a protection plan. When the asset is unsubscribed, backups are no longer performed.

To remove protection from a VM or intelligent VM group

1. On the left, click **RHV**.
2. On the **Virtual machines** tab or **Intelligent VM groups** tab, select the VM or the intelligent VM group.
   - For a VM, scroll down and click **Remove protection**.
   - For an intelligent VM group, scroll down and click the lock symbol and then click **Remove protection**.

   Under **Virtual machines** or **Intelligent VM groups**, the asset is listed as **Not protected**.

View the protection status of VMs or intelligent VM groups

To view the protection status of VMs or intelligent VM groups

1. On the left, click **RHV**.
2. On the **Virtual machines** tab or **Intelligent VM groups** tab, click the VM or the intelligent VM group.

   The **Protection** tab shows the details of the plans that the asset is subscribed to.
3. If the asset is not protected, click **Add protection** to select a protection plan.

   See “Protect RHV VMs or intelligent VM groups” on page 36.

Chapter 5

Recovering RHV virtual machines

This chapter includes the following topics:

Things to consider before you recover the RHV virtual machines

- Ensure that the recovery or backup host, that is added to the RHV access hosts, can communicate with the RHV Manager through a port .
- An RHV VM that has chain of disks due to user snapshot or dependency on template, cannot retain the disk chain after a restore.
- Compressed virtual disks are not protected and cannot be recovered.

About the pre-recovery check

The pre-recovery check verifies the following:

- Usage of supported characters and the length in the display name.
- Existence of a VM with the same display name.
- Connectivity with the RHV server and RHV credential validation.

- Availability of the RHV cluster.
- Available space with the storage domain.

Recover an RHV virtual machine

You can recover a VM to the original location where it existed when it was backed up or to a different location.

To recover a VM

1. On the left, click **RHV**.
2. Locate and click on the VM.
3. Click the **Recovery points** tab. In the calendar view on the left, click the date on which the backup occurred.

   The available images are listed in rows with the backup timestamp for each image. The date that is highlighted by green dot has a recovery point for that VM.
4. On the image you want to recover, click **Recover**.
5. To recover to the original location, do not modify the **Recovery targets**.

   To recover to a different location:

   Modify the **Display name**. Select the **RHV manager** and the **RHV cluster** where you want to recover the VM.

   If you are unable to change the **RHV cluster**, See "Error while restoring RHV virtual machines" on page 48.
6. Click **Add** to add a storage domain and select the appropriate storage domain.

   Select different storage domain for the virtual disks or select **Use the same storage domain for all virtual disks** to use the same storage domain for all the virtual disks. Click **Next**.
7. Review or change the following options:

   Recovery options:

Overwrite existing virtual machine	If a VM with the same UUID or same name exists at the destination and if this option is selected then that VM is deleted. If a VM with the same UUID or same name exists at the destination and if this option is not selected then the restore fails and an error is displayed.

Power on after recovery	Automatically turns on the VM when the recovery is complete.
Recovery host	A backup host that you can use during recovery. By default, the recovery host is the backup host that was used during a backup.

Advanced settings:

Retain original network configuration	The restored VM automatically connects to the original network using the retained NICs. Do not enable this option if: ■ The network connections on the destination virtual machine have changed since the backup was made. ■ The original virtual machine still exists and a duplicate VM may cause conflicts.
Create a new VM UUID	Restores the VM with a new UUID instead of the original UUID.
Remove tag associations	Removes the tags which were associated with the VM at the time of backup.

Format of restored virtual disks:

Original provision	Restores the VM's virtual disks with their original provisioning.
Thick provision	Configures the restored virtual disks in the thick format. The virtual disk space is pre-allocated when the disk is created.
Thin provision	Configures the restored virtual disks in the thin format. Restores only the populated blocks and the new blocks are allocated as required.

8 Click **Next** to run the **Pre-recovery check**.

The **Pre-recovery check** validates all the recovery parameters and displays errors, if any. You can fix the errors before starting the recovery.

9 Click **Start recovery**.

If you refresh the display, the **Restore activity** tab shows the job progress.

For information on the recovery status codes, see the NetBackup administrator or the *NetBackup Status Codes Reference Guide*, available here:

http://www.veritas.com/docs/000003214

About the supported virtual disk formats and disk provisioning during VM recovery

RHV supported allocation methods for virtual disks

RHV supports the following allocation methods for virtual disks:

- Pre-allocated (Thick provision)
  Pre-allocated indicates fully-allocated raw disks.
- Thin provision

  Thin provisioned disks are of the following types:

  - Raw sparse (default on file storage such as NFS)
  - QCOW2 (default on block storage such as FC, SAN, iSCSI)

  The thin provisioned virtual disk that is created on block storage is always in QCoW2 format.

Virtual disk provisioning for RHV VM recovery

Based on the disk provisioning option that you select in NetBackup, the virtual disks are created as described in the following table:

Table 5-1 Virtual disk provisioning for RHV VM recovery

The disk provisioning option that is selected during restore	Original disk format during backup		
	RAW sparse	**RAW pre-allocated**	**QCOW2**
Original or default	RAW sparse (QCOW2 on block storage)	RAW pre-allocated	RAW sparse (QCOW2 on block storage)
Thin	RAW sparse (QCOW2 on block storage)	RAW sparse (QCOW2 on block storage)	RAW sparse (QCOW2 on block storage)
Thick	RAW pre-allocated	RAW pre-allocated	RAW pre-allocated

Disk formats for VM templates

- VM templates can have the disks that have RAW or QCOW2 format.
- Storage allocation can be thin (dependent) or clone (independent).
  In Clone (independent) allocation, the contents of template disks are copied to the VM disk.
  In Thin (dependent) allocation, the template disks are referred as base disks for the VM.

- When multiple VMs are deployed from the same template with Thin allocation, then the VMs share the template disks.

Chapter 6

Troubleshooting RHV VM protection and recovery

This chapter includes the following topics:

Troubleshooting tips for NetBackup for RHV

For more information about RHV troubleshooting, check the following details:

- For discovery job failures:
  - Check the **Job details** section for the job in Activity monitor.
  - Check the `ncfnbcs` log.
- For snapshot job failures:
  - Check the **Job details** section for the job in Activity monitor.
  - Check the `bpfis` log.
  - For RHV-related errors, check **Events** section on RHV manager console.
- For backup job failures:
  - Check the **Job details** section for the job in Activity monitor.
  - Check the `bpbkar` and `VxMS` logs.
  - For RHV-related errors, check **Events** section on RHV manager console.

- For restore job failures:
  - Restore job fails with error 2822 (Hypervisor policy restore error)
  - Check the **Job details** section for the job in Activity monitor.
  - Check the `bprd`, `bpVMutil`, `VxMS`, or `ncfnbrestore` logs.
  - For RHV-related errors, check **Events** section on RHV manager console.

Error during the RHV virtual machines discovery phase

The following table describes the problem that might occur when you try to discover RHV virtual machines.

Table 6-1 Error run into during the RHV virtual machines discovery phase

Error message or cause	Explanation and recommended action
The RHV assets are not discovered after the correct RHV manager credentials are added. The VM discovery operation fails.	The maximum allowed length of the RHV manager name is 255 characters, however, if the characters exceed 95, the asset discovery fails. Workaround: ■ Ensure that the RHV manager name has 95 or fewer characters.
The discovery job fails with error 200. (Scheduler found no backups or clients to deploy NetBackup)	Ensure that the query specified in the policy or intelligent VM group is correct. The VMs that need protection are added recently to RHV manager or the VM configuration has changed and the autodiscovery or discover now was not triggered. ■ Run discover now and retry the backup. The maximum allowed length of the RHV manager name is 255 characters, however, if the characters exceed 95, the asset discovery fails. Workaround: Ensure that the RHV manager name has 95 or fewer characters. ■ The asset discovery does not work if the RHV manager credentials are added using `tpconfig`. Workaround: From NetBackup WebUI, run Discover for the specified RHV manager. Ensure that you add the RHV manager credentials using API or NetBackup WebUI.

Table 6-1 Error run into during the RHV virtual machines discovery phase *(continued)*

Error message or cause	Explanation and recommended action
The GET asset API does not work when you use the `tolower` and `toupper` functions.	NetBackup Web UI: For the filter in the intelligent Groups, NetBackup WebUI might not display accurate list of the RHV VMs that match the filter if the VM or the RHV server has non-English characters. However, during the backup, correct VMs are selected even though its attributes are non-English. This behavior is only in viewing the VMs in NetBackup Web UI. GET assets API of asset service: The GET Assets API does not give the desired result if the `tolower` or `toupper` functions are used together for the assets that have non-English characters.
There is a delay in the API response.	For a large number if RHV assets, if you add large and random offsets to an API request, there is an increase in the processing time that leads to a delay in the API response.

Error run into while backing up RHV virtual machines

The following table describes the problem that might occur when you back up RHV virtual machines:

Table 6-2 Error while backing up RHV virtual machines

Error message or cause	Explanation and recommended action
After a NetBackup backup operation, the VM snapshot on the RHV manager is not deleted.	If a disk attached to the VM is in an inactive state, then the RHV manager does not delete the VM snapshot after a backup operation is complete. Workaround: ■ Before the backup operation, verify the state of the disks that are attached to the VM and ensure that they are active. ■ Ensure that the disks are not attached while the VM is running, thus preventing the disk to be in an inactive state.
VM backup fails with the following error: "The virtual machine has no disks or contains only Raw Device Mappings for disks: Status 25"	This temporary error might occur when the VM snapshot is not available for the backup operation. The backup job is successful on the second attempt.

Table 6-2 Error while backing up RHV virtual machines *(continued)*

Error message or cause	Explanation and recommended action
Unable to remove the older snapshots from the RHV manager when the disk is in a locked state. The following error is displayed: A NetBackup snapshot of the virtual machine exist.	Workaround: ■ Refer to the following article for steps to unlock the disk: https://access.redhat.com/solutions/396753 ■ Manually remove the older snapshots from RHV manager.
Accelerator option does not work.	When a backup policy is created using APIs and the use Accelerator option is enabled, the policy gets created but the NetBackup Accelerator feature does not work. NetBackup Accelerator is not supported for RHV.

Error while restoring RHV virtual machines

The following table describes the problem that might occur when you restore an RHV virtual machine.

Table 6-3 Error run into while restoring RHV virtual machines

Error message or cause	Explanation and recommended action
VM recovery to alternate location fails on a Windows master server.	For a Windows NetBackup master server, ensure that the rename file ends with an empty line.
Unable to change the **RHV cluster** while modifying the recovery destination.	If you are unable to see the list of the RHV managers, you might not have access to the RHV manager(s) under the **Application Servers** object group property in RBAC. Contact the NetBackup security administrator to resolve this issue.

Table 6-3 Error run into while restoring RHV virtual machines *(continued)*

Error message or cause	Explanation and recommended action
Pre-recovery check runs successfully when a VM with the same UUID exists in the RHV cluster and the option to overwrite the VM is not enabled, but the VM restore fails. The following error message is seen: Info `bpVMutil` (`pid=1196`) FTL - Virtual machine exists and overwrite option not specified, can not proceed with restore. end Restore; elapsed time Hypervisor policy restore error. (2822)	Pre-recovery check compares the VM display name instead of UUID to find out if VM already exists, hence the check completes successfully. But if the overwrite option is not set, the restore job fails if a VM with the same UUID already exists. Workaround: Restore the VM with a new UUID **1** Start the recovery process. **2** On the **Recovery Options** page, click **Advanced**. **3** Enable **Create a new VM UUID**. **4** Proceed with the recovery process and click **Start recovery** to restore. Overwrite the existing VM that has the same UUID **1** Start the recovery process. **2** On **Recovery Options** page, enable the **Overwrite existing virtual machine** option. **3** Proceed with the recovery process and click **Start recovery** to restore.
When you try to recover an RHV VM image that is imported from a different domain using the Web UI, the pre-recovery check fails and displays that by default the recovery host is the same access host that was used during back up.	During the recovery of imported RHV VM images, for the recovery host, select the access host in the target domain as a recovery host or select the target master server.

Chapter 7

API and command line options for RHV

This chapter includes the following topics:

- Using APIs and command line options to manage, protect, or recover RHV virtual machines
- Additional NetBackup options for RHV configuration

Using APIs and command line options to manage, protect, or recover RHV virtual machines

This topic lists the APIs and command line options to protect or recover the Red Hat Virtualization virtual machines. Only the important variables and options are mentioned in this topic.

Following sections are part of this topic:

- Add the RHV manager credentials
- Validate the RHV manager credentials
- Create an RHV VM backup policy
- Restore the RHV VM at the original location
- Restore the RHV VM to an alternate location

For detailed information on the APIs and command lines, use these references:

- All the NetBackup APIs are listed at the following location:
  Services and Operations Readiness Tools (SORT) > Knowledge Base > Documents

- For more information about the commands, refer to the *NetBackup Commands Reference Guide*.

Add the RHV manager credentials

Table 7-1 Add the RHV manager credentials

API or command line options	Important variables and options
`POST /netbackup/config/servers/vmservers`	■ `serverName` is the name of the RHV manager ■ `vmType` is `RED_HAT_VIRTUALIZATION_MANAGER`
`tpconfig` command	■ `virtual_machine` is the name of the RHV manager. ■ `vm_type` is 10. The number 10 stands for RHV Manager.

Validate the RHV manager credentials

Table 7-2 Validate the RHV manager credentials

API or command line options	Important variables and options
`POST /netbackup/config/servers/vmservers/{serverName}/validate-credential`	■ `{serverName}` is the name of the RHV manager. ■ `validationHost` is a whitelisted Windows or Linux backup host.

Create an RHV VM backup policy

Table 7-3 Create an RHV VM backup policy

API or command line options	Important variables and options
`POST /netbackup/config/policies/`	■ `policyType` is `Hypervisor` ■ `backuphost` is a whitelisted Windows or Linux host. ■ `snapshotMethodArgs` can have the following values to back up a VM using VM UUID: ■ In `backupSelections` > `selections`, use the filter option as "`rhv:/?filter=Displayname Contains <name_filter>`" to filter RHV VMs of a specific name. Apart from `Displayname`, you can use the other filter criteria mentioned for Intelligent VM groups.

Table 7-3 Create an RHV VM backup policy *(continued)*

API or command line options	Important variables and options

`admincmd` command	■ In `bpplclients -add <discoveryhost> Hypervisor Hypervisor`, the hypervisor discovery host is a whitelisted Windows or Linux host.
	■ In `bpplinfo`, the policy type (`-pt`) is `Hypervisor`.
	■ In `bpplinclude`, use the filter option as `"rhv:/?filter=Displayname Contains <name_filter>"` to filter RHV VMs of a specific name.
	■ In `bpplinfo`
	■ Value of `use_virtual_machine` is **5** for RHV VMs.
	■ Value of `snapshot_method` is `Hypervisor_snap`.
	For optimized backup, you can use:
	`file_system_optimization=1`
	`exclude_swap=1`

After you create the policy, other commands like creating the schedule for the policy or triggering the policy backup remain the same. For more information about the commands, refer to the *NetBackup Commands Reference Guide*.

Restore the RHV VM at the original location

Table 7-4 Restore the RHV VM at the original location

API or command line options	Important variables and options

`POST /netbackup/recovery/workloads/rhv/scenarios/full-vm/recover`	■ `client` is the VM identifier of the protected VM. The VM identifier is the VM `UUID`.
	■ `recoveryHost` is a whitelisted Windows or Linux host.
	■ Set the following values:
	`defaultVmDiskProvisioning`
	`powerOnAfterRecovery`
	`overwriteExistingVm`
	`removeNetworkInterfaces`
	`retainVmGuid`
	`removeTagAssociations`

Table 7-4 Restore the RHV VM at the original location *(continued)*

API or command line options	Important variables and options

`bprestore` command	■ `vmproxy` is a whitelisted Windows or Linux backup host.
	■ `vmserver` is the name of the RHV manager.
	■ `vmhypervisor` specifies restore from the **Hypervisor** policy type
	■ Use the following values to modify the VM configuration:
	  ■ `vmst` to remove the VM tags.
	  ■ `vmpoweron` to start the VM after the VM restore.
	  ■ `vmsn` to remove the VMs network interfaces.
	  ■ `vmid` to retain the original VM UUID of the VM. Alternatively, use the `-K` option to retain the existing VM with the same UUID and not overwrite it.
	  ■ `thickdisk` to configure the restored virtual disks in the thick format. The virtual disk space is allocated when the disk is created.
	  ■ `thindisk` to configure the restored virtual disks in the thin format. The populated blocks are restored but the vacant blocks are not initialized or committed.

Restore the RHV VM to an alternate location

Table 7-5 Restore the RHV VM to an alternate location

API or command line options	Important variables and options

`POST /netbackup/recovery/workloads/rhv/scenarios/full-vm/recover`	■ `client` is the VM name of the protected VM. The VM name can either be the display name (`displayName`) or the `UUID`.
	■ `rhvServer` is the name of the alternate RHV manager.
	■ `recoveryHost` is a whitelisted Windows or Linux host.
	■ `vmhypervisor` specifies restore from the **Hypervisor** policy type
	■ Set the following values:
	`defaultVmDiskProvisioning`
	`powerOnAfterRecovery`
	`overwriteExistingVm`
	`removeNetworkInterfaces`
	`retainVmGuid`
	`removeTagAssociations`

Table 7-5 Restore the RHV VM to an alternate location *(continued)*

API or command line options	Important variables and options

`bprestore` command	■ `vmproxy` is a whitelisted Windows or Linux backup host.
	■ `vmserver` is the name of the RHV manager.
	■ Use the following values to modify the VM configuration:
	  ■ `vmst` to remove the VM tags.
	  ■ `vmpoweron` to start the VM after the VM restore.
	  ■ `vmsn` to remove the VMs network interfaces.
	  ■ `vmid` to retain the original VM UUID of the VM. Alternatively, use the `-K` option to retain the existing VM with the same UUID and not overwrite it.
	■ The `-R` option defines the path of the rename file. Use the rename file to recover the VM to an alternate location or change the VM configuration.
	Sample rename file:
	`change vmname to new_vm_name`
	`change /storage_domain_1/disk1_UUID to /storage_domain_2/`
	`change /storage_domain_1/disk2_UUID to /storage_domain_2/`
	`change cluster to new_cluster_name`
	Note: For a Windows NetBackup host, you must add an empty line at the end of the rename file entries.
	See "Additional information about the rename file" on page 54.

Additional information about the rename file

- You can specify destination storage domain for all the disks or for some specific list of disks.
- If you do not specify a destination storage domain for one of the disks, then that disk is restored to the original location.
- If you specify a destination storage domain for a non-existing or invalid disk, the VM restore fails.
- For a Windows NetBackup host, you must add an empty line (carriage return) after all the rename file entries.

Additional NetBackup options for RHV configuration

Use the following NetBackup command options for additional RHV configuration:

- See "OVIRT_IMAGEIO_INACTIVITY_TIMEOUT option for NetBackup servers" on page 55.
- See "RHV_CREATEDISK_TIMEOUT option for NetBackup servers" on page 55.
- See "RHV_AUTODISCOVERY_INTERVAL option for NetBackup servers" on page 56.

OVIRT_IMAGEIO_INACTIVITY_TIMEOUT option for NetBackup servers

This option specifies the timeout period of client inactivity in seconds. When this timeout period is surpassed the oVIRT engine aborts the transfer session. The client inactivity usually occurs when there is a traversal of a disk chain. For example, while backing up a thin-dependent VM or a VM that consists of user snapshots.

Table 7-6 OVIRT_IMAGEIO_INACTIVITY_TIMEOUT information

Usage	Description
Where to use	On NetBackup master servers.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the `OVIRT_IMAGEIO_INACTIVITY_TIMEOUT` option. The default inactive timeout period is 172800 seconds (48 hours).
Example	The following entry tells the NetBackup backup job to set the client inactivity timeout period to 172800 seconds (48 hours). `OVIRT_IMAGEIO_INACTIVITY_TIMEOUT = 172800`
Equivalent Administration Console property	No equivalent exists in the NetBackup Administration Console or web UI.

RHV_CREATEDISK_TIMEOUT option for NetBackup servers

This option specifies the timeout period for creating a virtual disk during the restore of an RHV VM. If the RHV VM with a large pre-allocated disk was backed up and then restored on a file storage such as NFS, then the disk creation function can time out before the restored virtual disk is fully realized.

Table 7-7 RHV_CREATEDISK_TIMEOUT information

Usage	Description
Where to use	On NetBackup master servers.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the `RHV_CREATEDISK_TIMEOUT` option.
Example	The following entry tells the NetBackup backup job to set the create disk timeout period to 172800 seconds (48 hours). `RHV_CREATEDISK_TIMEOUT = 172800` The range for `RHV_CREATEDISK_TIMEOUT` is 0 hours to 48 hours.
Equivalent Administration Console property	No equivalent exists in the NetBackup Administration Console or web UI.

RHV_AUTODISCOVERY_INTERVAL option for NetBackup servers

This option controls how often NetBackup scans the RHV servers to discover virtual machines to display in the NetBackup web UI.

NetBackup attempts autodiscovery first with the same host for which the last discovery attempt was successful. If autodiscovery fails with that host, NetBackup tries again with other hosts in the following order:

- The NetBackup master server
- The access host, client, or proxy server
- The media server

Table 7-8 RHV_AUTODISCOVERY_INTERVAL information

Usage	Description
Where to use	On NetBackup master servers.

Table 7-8 RHV_AUTODISCOVERY_INTERVAL information *(continued)*

Usage	Description

How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	The default is 28,800 seconds (8 hours). The minimum value is 300 seconds (5 minutes) and the maximum is 31,536,000 seconds (1 year).
	Use the following format:
	`RHV_AUTODISCOVERY_INTERVAL = number of seconds`
	For example:
	`RHV_AUTODISCOVERY_INTERVAL = 100000`
	This entry should appear only once in the configuration file.
	Note: After changing this option, stop and restart the NetBackup services. For VM discovery, the `Netbackup Discovery Framework` service must be running.

Equivalent Administration Console property	No equivalent exists in the NetBackup Administration Console or web UI.