NetBackup™ for KVM Administrator's Guide

Release 11.1

VERITAS
now part of Cohesity

Last updated: 2025-11-24

Legal Notice

Cohesity, Inc.
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 Cohesity 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 Cohesity website.

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity 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

This chapter includes the following topics:

About NetBackup for KVM

NetBackup for KVM provides backup and restore of the KVM virtual machines that run on KVM hosts. This workload provides the following capabilities:

- Automatically creates consistent (quiesced) backups.
- Performs full backups of guest virtual machines on KVM hosts.
- Backs up the virtual machines that are either powered on or powered off.
- Can recover backups to the original KVM host or a different KVM host.
- Can restore virtual machines from the backup.
- Performs backups directly from the KVM hosts. No additional management application layer (for example, oVirt) is required.
- Supports the disk formats QCOW2.

In this guide, a KVM "domain" is referred to as virtual machine or VM.

Chapter 2

Installation and configuration overview

This chapter includes the following topics:

Planning the installation for NetBackup for KVM

Table 2-1 Installation steps for NetBackup for KVM

Step	Action	Description
Step 1	Verify the operating system and platform compatibility.	See "Verifying the operating system and platform compatibility " on page 7.
Step 2	Verify that a supported version of libvirt is installed on each KVM host.	See "Verifying the operating system and platform compatibility " on page 7.
Step 3	Install the NetBackup client software on the KVM hosts that have the virtual machines that you want to back up.	See "NetBackup server and client requirements" on page 8.

Verifying the operating system and platform compatibility

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

To verify operating system and compatibility

1. Go to the NetBackup compatibility list site.

   https://www.veritas.com/support/en_US/article.100040093

2. For information on the supported KVM versions and support versions of libvirt, select the link for following document:

   NetBackup Software Compatibility List

NetBackup server and client requirements

Before you install NetBackup, review the requirements for the NetBackup server and the NetBackup clients.

NetBackup server requirements

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

- The NetBackup server software is installed and operational on the NetBackup server.
  See the NetBackup Installation Guide.
- Make sure that you configure any backup media that the storage unit uses. The number of media volumes that are required depends on several things:
  - The devices that are used and the storage capacity of the media.
  - The sizes of the databases that you want to back up.
  - The amount of data that you want to archive.
  - The size of your backups.
  - The frequency of backups or archives.
  - The length of retention of the backup images.

  See the NetBackup Web UI Administrator's Guide.

NetBackup client requirements

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

- The client software is installed on each KVM host. Also verify that a supported version of libvrt is installed on each KVM host.
- To use the new features that are included in NetBackup for KVM in NetBackup 11.1, you must upgrade your NetBackup for KVM clients to NetBackup 11.1. The NetBackup media server must use the same version as the NetBackup for KVM client or a higher version than the client.

NetBackup configuration overview

After the installation of NetBackup, continue with the following configuration tasks.

Table 2-2 NetBackup configuration tasks

Sequence	Tasks
Phase 1	Add the KVM hosts. You must complete the discovery of KVM assets before you configure any RBAC roles for this workload. See “Add KVM hosts” on page 10.
Phase 2	Configure the NetBackup RBAC roles for KVM administrators. Contact your NetBackup administrator for assistance. See “RBAC roles for the KVM administrator” on page 16.
Phase 3	Create a NetBackup policy for KVM. See “Add a policy for KVM” on page 20.
Phase 4	Perform a backup. See “Perform a manual backup” on page 35.

Chapter 3

Managing KVM hosts

This chapter includes the following topics:

Add KVM hosts

To discover virtual machines in the KVM environment you must first add the KVM hosts to NetBackup.

To add a KVM host

1. On the left, select **Workloads > KVM**, then select the **Hosts** tab.
2. In the right pane, select **Add**.

   NetBackup displays the Linux hosts where the NetBackup client is installed.
3. In the **Machine** field, select the host from the list.
4. Select **Save**.

   NetBackup validates the KVM host and starts autodiscovery. When discovery completes, the list of virtual machines displays.

About KVM discovery

NetBackup automatically starts the discovery of the KVM virtual machines when you add a KVM host to NetBackup. Autodiscovery also occurs at set intervals. (The default interval is every 8 hours.)

You can change the autodiscovery frequency.

See "Change the autodiscovery frequency of KVM assets" on page 11.

To discover the VMs immediately, see the following topic:

See "Discover KVM host assets manually" on page 11.

Change the autodiscovery frequency of KVM assets

Automatic discovery of KVM virtual machines occurs at regular intervals. The default frequency is every 8 hours. Use this procedure to change the autodiscovery frequency.

To change the frequency of autodiscovery of KVM assets

1. On the left, select **Workloads > KVM**.
2. At the top right, select **KVM settings > Autodiscovery**.
3. Locate the **Frequency** setting and select **Edit**.
4. Type the value or use the up and down arrows to choose the frequency value.

   The range from which you can choose is 1 hour to 24 hours. To set the autodiscovery frequency in minutes or seconds or to disable autodiscovery, you must use the KVM autodiscovery API.
5. Select **Save**.

Discover KVM host assets manually

You can manually start the NetBackup discovery process if you want to immediately discover new KVM virtual machines in your environment.

To discover new KVM virtual machines

1. On the left, select **Workloads > KVM**.
2. Select the **Hosts** tab.
3. Select the checkbox for each host that contains the virtual machines that you want to discover.
4. Select **Discover**.

Browse KVM assets

You can browse KVM virtual machines to view their details such as how they are protected and recovery points that are available. You can browse KVM hosts to see discovery information for those hosts.

Browse KVM virtual machines

On the **Virtual machines** tab you can view and manage virtual machines, including how they are protected.

To browse KVM virtual machines

1. On the left, select **Workloads > KVM**.
2. Select the **Virtual machines** tab.
3. To view the available actions for a virtual machine, select the check box for the virtual machine.
4. To view the details for a virtual machine, select the link for the virtual machine. You can perform the following tasks.
   - To see the available recovery points for the virtual machine, select **Recovery points**.
   - To view the restore jobs for the virtual machine, select **Restore activity**.
   - To view the roles that have access to the virtual machine, select the **Permissions** tab.

Browse KVM hosts

On the **Hosts** tab you can view and manage KVM hosts.

To browse KVM hosts

1. On the left, select **Workloads > KVM**.
2. Select the **Hosts** tab.

   You can view their discovery status, the last discovery attempt, the validation status of each host, and when each host was last validated.
3. To view the available actions for hosts, select the check box for each host.

Validate a KVM host

You can validate a KVM host to confirm that NetBackup can connect to the KVM host and that a compatible libvrt version is installed. You may also need to validate a host in the following situations:

- The KVM host was disconnected (for example, for maintenance).
- The NetBackup server or client software was upgraded on the KVM host.
- A new libvirt version was installed on the KVM host.

To validate a KVM host

1. On the left, select **Workloads > KVM**, then select the **Hosts** tab.
2. In the right pane, locate the KVM host.
3. Select **Actions > Validate**.

Remove a KVM host

If you no longer need to protect a KVM host, you can remove it from the list of registered KVM hosts.

Note the following:

- VMs continue to display in NetBackup until all the existing images have expired and 30 days have passed since the last discovery.
- The KVM host still exists as a client in NetBackup until you uninstall the NetBackup server or client software from the KVM host.

To remove a KVM host

1. On the left, select **Workloads > KVM**, then select the **Hosts** tab.
2. In the right pane, locate the KVM host.
3. Select **Actions > Remove**.
4. Remove the KVM host from any NetBackup policies.

Change resource limits for KVM resource types

KVM resource limits control the number of backups that can be performed simultaneously on a KVM host. The settings apply to all NetBackup policies for the primary server that you selected.

For example, to avoid overloading the KVM host, you can place a limit on the number of concurrent backup jobs per KVM host with the setting **Backup Jobs per KVM Host**.

To change the resource limits for KVM resource types

1. Review the limitations for resource limits.

   See the section called “Limitations on global limits for KVM resources” on page 15.

2. On the left, select **Workloads > KVM**.
3. On the top right, select **KVM settings > Resource limits**.

   For each resource, the default value is **0** (No limit).

   Limits indicates the number of simultaneous backups that can be performed for the KVM hosts or host. This value is the global limit. The **Override** value indicates how many KVM hosts have any limits that are different from the global limit.
4. To change the limit for the resource **Backup Jobs per KVM Host**, select **Edit**.
5. Choose from the following options.

Set a global limit for all KVM hosts.	Locate the **Global** setting and select the **Limits** value that you want to apply. This value limits the number of simultaneous backups for all KVM hosts.
Set a limit for a specific KVM host.	Select **Add**. From the list, enter the name of the KVM host. Select the **Limits** value that you want to apply. This value limits the number of simultaneous backups that are performed for the KVM host.

6. Select **Save**.

   At any point you can select **Reset default values** to remove all the overrides and set all global KVM resource limits to their default values.

Example

The following example illustrates how these limits control simultaneous backups. The settings must be done according to KVM configuration in your environment. Consider a case where a KVM host hosts 20 VMs. When the job runs there are 20 concurrent jobs that start if no resource limit is set, which is default behavior. When the **Backup Jobs per KVM Host** is set to 10, this limit is enforced and 10 backup jobs run concurrently.

Limitations on global limits for KVM resources

The following limitations apply to setting global limits on the use of KVM resources:

- New and changed resource limits may not take effect immediately. It can take a couple of jobs before the resource limit updates are in effect.
- To limit the number of simultaneous jobs per policy, use the **Limit jobs per policy** setting on the policy **Attributes** tab.

Chapter 4

Configuring RBAC roles for KVM administrators

This chapter includes the following topics:

RBAC roles for the KVM administrator

NetBackup enables control over which users can access which KVM resources using Role Based Access Control (RBAC). You can grant RBAC access globally (to all KVM assets) or for specific KVM hosts or individual virtual machines.

The Default KVM Administrator role has access to all KVM assets (global).

Note the following:

- If you choose to create a custom role for KVM assets, permissions can be configured only at the KVM host level or at the KVM virtual machine level.
- To create an RBAC role, you must have the RBAC Administrator role or the permissions to create roles.
- Contact your NetBackup administrator for assistance with creating roles.

Assigning permissions at specific KVM object levels

The RBAC administrator create RBAC roles for KVM that assign permissions to specific KVM objects.

To manage permissions for a KVM host

1. On the left, go to **Workloads > KVM**. Then select the **Hosts** tab.
2. In the right pane, locate and select the KVM host. Then select **Manage permissions**.
3. Select **Add**.
4. Select the role name and the permissions that you want to assign.
5. Select **Save**.

To manage permissions for a KVM virtual machine

1. On the left, go to **Workloads > KVM**. Then select the **Virtual machines** tab.
2. Locate and select the virtual machine. Then select **Manage permissions**.
3. Select **Add**.
4. Select the role name and the permissions that you want to assign.
5. Select **Save**.

Chapter 5

Protecting KVM virtual machines

This chapter includes the following topics:

About configuring a backup policy for KVM

A backup policy defines the backup criteria for a group of KVM virtual machines.

These criteria include the following:

- Storage unit and media to use
- Policy attributes
- Backup schedules

- The KVM hosts where the virtual machines reside
- A query that defines which virtual machines to back up

See “Add a policy for KVM” on page 20.

Limitations for KVM backups

The following limitations exist for backups of KVM hosts.

- You cannot backup the same KVM virtual machine concurrently.
- The VMs without virtual disks cannot be protected.
- The following QCOW2 image attributes are not supported:
  - Compressed cluster
  - Encrypted disks

About automatic virtual machine selection

You can configure NetBackup to automatically select virtual machines based on a range of criteria. You specify the criteria (rules) in the **Query builder** on the NetBackup policy **Backup selections** tab. NetBackup creates a list of the virtual machines that currently meet the rules and adds those virtual machines to the backup.

Automatic selection of virtual machines has the following advantages:

- Simplifies the policy configuration for sites with large virtual environments. You do not need to manually select virtual machines from a long list of hosts: NetBackup selects all the virtual machines that meet the selection rules in the policy's Query builder.
- It allows the backup list to stay up to date with changes in the virtual environment. Eliminates the need to revise the backup list whenever a virtual machine is added or removed.
- Virtual machine selection takes place dynamically at the time of the backup.

Examples of automatic virtual machine selection are the following:

Table 5-1 Examples for automatic virtual machine selection

Example	Description
Limit the backup list to the virtual machines that are currently turned on	If some of your virtual machines are occasionally turned off, NetBackup can be configured to automatically exclude those from the backup list. Among the virtual machines it discovers, NetBackup backs up only the virtual machines that are turned on.
Back up virtual machines based on KVM host	For example, a query rule can select all the virtual machines that reside on a particular KVM host.

Add a policy for KVM

This topic describes how to create a NetBackup policy to back up the KVM virtual machines on one or more KVM hosts.

To add a policy for KVM

1. Open the NetBackup web UI.
2. On the left, select **Protection > Policies**. Then select **Add**.
3. Type a unique name for the new policy.
4. From the **Policy type** list, select **KVM**.
5. Complete the entries on the **Attributes** tab.

   See "About policy attributes" on page 21.
6. Add other policy information as follows:
   - Add schedules.
   - Add the KVM hosts.
     See "Add KVM hosts to a policy" on page 22.
   - Create a query that dynamically selects the virtual machines.
     See "Configure a query to select KVM virtual machines for backup" on page 23.
   - Select the **KVM attributes** tab to set KVM-related options.
     See "Backup options on the KVM attributes tab" on page 30.
7. When you have completed the policy configuration, select **Create**.

About policy attributes

With a few exceptions, policy attributes for a KVM policy are managed in the same way as for most other policy types. Certain policy attributes vary according to your specific backup strategy and system configuration.

For more information on policy attributes, see the NetBackup Administrator's Guide, Volume I.

Table 5-2 Policy attributes for NetBackup for KVM policies

Attribute	Description
Policy type	Determines the types of clients that can be backed up with the policy. For KVM virtual machines, select the policy type **KVM**
Keyword phrase	A textual description of a backup. Useful for browsing backups and restores.

Schedule properties

Table 5-3 Description of schedule properties

Property	Description
Type of backup	Specifies the type of backup that this schedule can control. The selection list shows only the backup types that apply to the policy you want to configure.
Schedule type	You can schedule an automatic backup in one of the following ways: ■ **Calendar** The **Calendar** option lets you schedule the backup operations that are based on specific dates, recurring week days, or recurring days of the month. ■ **Frequency** The **Frequency** specifies the period of time that can elapse until the next backup operation begins on this schedule. For example, assume that the frequency is 7 days and a successful backup occurs on Wednesday. The next full backup does not occur until the following Wednesday.

Table 5-3 Description of schedule properties *(continued)*

Property	Description
Retention	Specifies a retention period to keep backup copies of files before they are deleted. The retention level also denotes a schedule priority within the policy. A higher level has a higher priority. Set the time period to retain at least two full backups of your database. In this way, if one full backup is lost, you have another full backup to restore. For example, if your database is backed up once every Sunday morning, you should select a retention period of at least 2 weeks. The retention period for an application backup schedule refers to the length of time that NetBackup keeps backup images. The retention period for an automatic schedule controls how long NetBackup keeps records of when scheduled backups occurred. For example, if your database is backed up once every Sunday morning, you should select a retention period of at least 2 weeks.
Effect of type of schedule on retention period	The type of schedule you select affects the retention period as follows: ■ Frequency-based scheduling Set a retention period that is longer than the frequency setting for the schedule. For example, if the frequency setting is set to one week, set the retention period to be more than one week. The NetBackup scheduler compares the latest record of the automatic backup schedule to the frequency of that automatic backup schedule. This comparison is done to determine whether a backup is due. So if you set the retention period to expire the record too early, the scheduled backup frequency is unpredictable. However, if you set the retention period to be longer than necessary, the NetBackup catalog accumulates unnecessary records. ■ Calendar-based scheduling The retention period setting is not significant for calendar-based scheduling.

Add KVM hosts to a policy

The KVM hosts list contains the list of the KVM hosts on which the virtual machines reside that you want to back up. A policy must have a least one KVM host.

For installation requirements, see the following topic.

See “NetBackup server and client requirements” on page 8.

To add KVM hosts to a policy

1. Open the policy and select the **KVM hosts** tab.
2. Select **Add**.
3. Select the name of the host.
4. Select **Select**.

Configure a query to select KVM virtual machines for backup

NetBackup automatically selects KVM virtual machines for backup based on the query criteria that you enter. You specify the criteria (rules) in the Query builder in the policy **Backup selections** tab. You can set up rules to include certain virtual machines for backup, or to exclude virtual machines.

Note: In the NetBackup web UI, you must use OData keywords and OData operators in query rules:

See "Query builder reference for KVM virtual machines" on page 24.

When the backup job runs, NetBackup creates a list of the virtual machines that currently meet the query rules and backs them up.

To configure the VMs in the backup selections list

1. In the policy, select the **Backup selections** tab.
2. To create a rule, make selections from the menus.

   For the first rule, you can start with the **Field** list, depending on the type of rule. (For the first rule, the only selections available for the field **Join** are blank (none), or NOT.)

   Then make a selection for **Operator**.

   For the **Value** field: Select the folder icon to browse for values, enter the value manually, or in some cases select a value from the list. The characters you enter manually in the **Value** field must be enclosed in single quotes. Note that browsing for values may take some time in large virtual environments.

   See "Query builder reference for KVM virtual machines" on page 24.
3. Select **Add** to add the rule to the **Query** pane.
4. Create more rules as needed.

   See "Example queries to select VMs for backup" on page 28.
5. To see which virtual machines NetBackup currently selects based on your query, select **Test query**.

   The Virtual machines in your current environment that match the rules for selection in the policy are labeled **Included**. Note however that the Test query option does not create the backup list for the policy.

   See "Test a VM query" on page 28.

6 To perform an immediate discovery to update the asset information, scroll to the bottom of the **Test query** modal and select **Discover now**.

Note: NetBackup does not run discovery when the KVM policy runs. To reflect any new VMs in the policy, you must manually run discovery to discover those VMs.

7 When you are finished reviewing the query results, select **Close**.

8 You can specify how long NetBackup uses the latest query results as the backup list for future executions of the policy. Set the time period in **Reuse VM selection query results for**.

See "About the Reuse VM selection query results option" on page 29.

9 To create queries manually instead of using the menus, click **Advanced mode**.

See "Use Advanced mode to create a query for virtual machine selection" on page 27.

Query builder reference for KVM virtual machines

You can use the Query builder to enter rules for the automatic selection of KVM virtual machines for backup.

Note: The advanced mode of the Query builder uses OData keywords and operators.

Table 5-4 describes the fields and options for creating credential rules with the Query builder.

Table 5-4 Query builder options for KVM virtual machines

Query Builder fields	Description
and **or**	When you add two or more conditions, you can select a connector to join the rules.
Field	Select a parameter on which to build the rule. See Table 5-5 on page 25.
Operator	Select an operator. The available operators depend on the parameter that is selected for the **Field**. See Table 5-6 on page 26.

Table 5-4 Query builder options for KVM virtual machines *(continued)*

Query Builder fields	Description
Value	Specifies a **Value** for the **Field** parameter. The **Value** field can be a list of possible values or a manual entry, depending on the selections that are made in the other fields. See the section called "Value" on page 27.

Field (keywords)

Table 5-5 describes the keywords that are available in the **Field** dropdown. The values for each keyword (in the **Value** field) are case-sensitive.

Note: Use OData **Field** keywords are indicated for when you build queries for credential rules with the NetBackup APIs.

Table 5-5 Keywords in the **Field** list

Field keyword	OData field keyword	Description
description	`description`	The description of the virtual machine.
displayName	`displayName`	The virtual machine's display name.
kvmHostName	`kvmHostName`	The name of the KVM host.
powerState	`powerState`	The power state of the virtual machine.
title	`title`	The title from the metadata for the virtual machine.
uuid	`uuid`	The UUID of the virtual machine.

Operators

Table 5-6 describes the operators available in the **Operator** list. The table also indicates whether the values for each keyword (in the **Value** field) are case-sensitive.

Table 5-6 Operators in the **Operator** list

Operator	OData operator	Description
Contains	`contains`	Matches the value in the **Value** field wherever that value occurs in the string. Values are case-sensitive. For example: If the **Value** entry is 'dev', **Contains** matches strings such as '01dev', '01dev99', and 'devOP'. The name 'Development_machine' is not matched.
EndsWith	`endswith`	Matches the value in the **Value** field when it occurs at the end of a string. For example: If the Value entry is 'dev', **Ends with** matches the string '01dev' but not '01dev99', 'devOP', or 'development_machine'.
Equal	equal	Matches only the value that is specified in the **Value** field. Values are case-sensitive. For example: If the display name to search for is 'VMtest27', **Equal** matches the virtual machine name VMtest27. The names VMTest27 or vmtest27 or vmTEST27 are not matched.
Greater	greater	Matches any value that is greater than the specified **Value**, according to the UTF-8 collating sequence.
GreaterEqual	greaterEqual	Matches any value that is greater than or equal to the value in the **Value** field, according to the UTF-8 collating sequence.
In	in	Matches any of the specified values in the **Value** field. For example: If the hosts in the **Value** field are 'kvm01','kvm02,'kvm03', **In** matches any KVM host that has one of those names. If the names of your KVM hosts are not identical to any of the specified values, no match occurs. A host named KVM01A is not a match.
Less	less	Matches any value that is less than the specified **Value**, according to the UTF-8 collating sequence.
LessEqual	lessEqual	Matches any value that is less than or equal to the specified **Value**, according to the UTF-8 collating sequence.
NotEqual	`ne`	Matches any value that is not equal to the value in the **Value** field.
StartsWith	`startswith`	Matches the value in the **Value** field when it occurs at the start of a string. For example: If the **Value** entry is 'box', **Starts with** matches the string 'box_car' but not 'flatbox'.

Value

Table 5-7 describes the characters that can be entered in the **Value** field. The **Field** keyword determines case sensitivity.

Note: The character string you enter in the **Value** field must be enclosed in single quotes.

Table 5-7 Characters you can enter for Value

Character types	String characters allowed
Alphanumerics	A to Z, a to z, 0 to 9, - (minus sign), and special characters. **Note:** Decimal numbers only.
Wildcards	* (asterisk) matches everything. For example: **'*prod*'** matches the string **'prod'** preceded or followed by any characters. **?** (question mark) matches any single character. For example: **'prod??'** matches the string **'prod'** followed by any two characters.
Escape character.	\ (backslash) escapes the wildcard or meta-character that follows it. For example: To search for a string that contains an asterisk (such as test*), enter 'test*'
Quotation marks	Note: The characters you enter in **Value** must be enclosed in single quotes. To search for a string that contains quotation marks, escape each quote (\'). For example: To search for a string that includes single quotes (such as **'name'**), enter **'\'name\''**

Use Advanced mode to create a query for virtual machine selection

The Query builder's Advanced mode provides more flexibility in crafting rules for virtual machine selection, including the use of parentheses for grouping.

Note: In the NetBackup web UI, you must use OData keywords and OData operators in query rules:

See "Query builder reference for KVM virtual machines" on page 24.

To use Advanced mode to create a query for virtual machine selection

1. Create a KVM policy.
2. Select the **Backup selections** tab.

3. Locate **Query builder** and select **Advanced mode**.
4. You can use the Query builder menus to add query rules. You can also type in rules manually.

   Here are some example queries:

   `startswith(displayName, 'vm3')` and `powerState eq 'Shut Off'`

   `contains(kvmHostName, 'hostab')`
5. To insert a rule between existing rules, place the cursor where you want the new rule to start and type it in.

   When you create a rule with the drown-down menus, it appears at the end of the query. You can cut and paste it into the proper location.
6. To establish the proper order of evaluation in compound queries, use parentheses to group rules as needed. Compound queries contain two or more rules, joined by: and, and not, or, or not.

Example queries to select VMs for backup

This topic provides examples of the kinds of queries that you can create to automatically select KVM virtual machines for backup.

In the following example, the query selects KVM virtual machines with a host name that ends with the string `domain.com`. The query string with OData keywords and operators is: `endswith(kvmHostName), 'domain.com')`

Field	Operator	Value
kvmHostName	Ends with	domain.com

In the following example, the query selects a KVM virtual machine with the UUID `100faa79-1119-4c49-8f32-b4a165ee51d`. The query string with OData keywords and operators is: `uuid eq '100faa79-1119-4c49-8f32-b4a165ee51d6'`

Field	Operator	Value
uuid	Equal	100faa79-1119-4c49-8f32-b4a165ee51d6

Test a VM query

You can test a query that you create to preview the VMs for KVM that NetBackup discovers in the current NetBackup environment.

To test a VM query

1. Open the KVM policy.
2. Select the **Backup selections** tab.
3. Locate and select **Test query**.

   The following information is displayed:

Query	The query criteria.
All	Displays the number of VMs in the NetBackup environment.
Included	Displays the number of VMs that match the query criteria.
Excluded	Displays the number of VMs that do not match the query criteria.
Failed	The virtual machine cannot be selected for backup because of a host name problem or other error. Also, the query cannot exclude the virtual machine. An explanation is included with the VM.
List of VMs	The names of the VMs in the NetBackup environment, based on the tab that you selected.

4. To perform an immediate discovery to update the asset information, scroll to the bottom of the **Test query** modal and select **Discover now**.

   Note: NetBackup does not run discovery when the KVM policy runs. To reflect any new VMs in the policy, you must manually run discovery to discover those VMs.
5. Select **Close** when you are finished.

About the Reuse VM selection query results option

The Test query screen lists the virtual machines that NetBackup discovered in your KVM environment. Because the automatic selection feature is dynamic, later changes in the environment may affect which virtual machines match the query rules. For example: if virtual machines are added later, the current test results may not be identical to the virtual machines that are selected when the backup runs.

During the period you specify on **Reuse VM selection query results for**, NetBackup reuses the current list of virtual machines as the backup list. It does not consult the Query builder or rediscover virtual machines.

Note the following about the **Reuse VM selection query results** option:

- It determines how long the query results are reused.
- It has no effect on when the NetBackup policy schedule runs.
- The option is invalidated if the query rules are changed or if the policy attributes that affect discovery are changed. In that case, NetBackup rediscovers virtual machines the next time the policy runs.

For example: assume that the **Reuse VM selection query results for** option is set to 8 hours and your query selects turned-on virtual machines. If additional virtual machines are turned on during the 8-hour period, they are not added to the policy's backup list. The policy backs up the virtual machines that were last added to the list (such as when the policy was created). After 8 hours, when the policy runs next, the recently turned-on virtual machines are discovered and added to the backup list.

Assume that the next backup occurs before the **Reuse** period expires and a virtual machine was renamed during the Reuse period. Then NetBackup backs up the renamed virtual machine under its original name. Because the reuse period has not expired, NetBackup does not rediscover virtual machines and therefore cannot identify the virtual machine by its new name. (NetBackup identifies the virtual machine by its instance UUID.) To have backed up the virtual machine with its new name, the **Reuse** period should have been set to a shorter interval and the discovery process should have been initiated.

Note: The virtual machines that are selected for backup are not displayed on the policy **Backup selections** tab. To see which virtual machines NetBackup has selected and backed up, refer to the following topic.

See “Test a VM query” on page 28.

Backup options on the KVM attributes tab

The **KVM** tab displays when you select KVM as the policy type.

The following topics describe the KVM backup options.

See “Optimizations options (KVM)” on page 31.

See “Primary VM identifier options (KVM)” on page 31.

See “Existing snapshot handling options (KVM)” on page 34.

See “KVM - Advanced attributes” on page 34.

Optimizations options (KVM)

The following options set the type and scope of the KVM virtual machine backup.

Table 5-8 Optimizations

Option	Description
Enable file recovery from VM backup	This option allows restore of individual files from the backup. With or without this option, you can restore the entire virtual machine. To perform a KVM backup to a deduplication storage unit, select this option. This option provides the best deduplication rates. To back up a virtual machine that contains Arctera InfoScale volumes, disable this option. Also make sure that the **Exclude deleted blocks** option is disabled. **Note:** For a Linux virtual machine, the name of an LVM volume can include any of the following special characters: . (period), _ (underscore), - (hyphen). No other special characters are supported. If other special characters are in the volume name, the **Enable file recovery from VM backup** option does not work. As a result, you cannot restore individual files from that volume.
Exclude deleted blocks	Reduces the size of the backup image by excluding any unused or deleted blocks within the file system on the virtual machine. This option supports the following file systems: Windows NTFS, and Linux ext2, ext3, ext4, and XFS. This option uses proprietary mapping technology to identify vacant sectors (allocated but empty) within the file system. To back up a virtual machine that contains Arctera InfoScale volumes, disable this option. Also make sure that the **Enable file recovery from VM backup** option is disabled.
Exclude swap and paging files	Reduces the size of the backup image by excluding the data in the guest OS system paging file (Windows) or the swap file (Linux). **Note:** This option does not exclude the swapping and paging files from the backup: it only excludes the data in those files. If the files are restored, they are restored as empty files. **Note:** For a Linux virtual machine, this option disables the swap file when you restore the virtual machine. You must reconfigure the swap file after the virtual machine is restored. To allow the virtual machine to be restored with its swap file enabled, do not select **Exclude swap and paging files**.

Primary VM identifier options (KVM)

This setting specifies the type of name by which NetBackup recognizes virtual machines when it selects them for backup.

The name you use for the **Primary VM identifier** may have restrictions.

See "NetBackup character restrictions for the Primary VM identifier" on page 32.

Table 5-9 Primary VM identifier

Option	Description
VM display name	The name of a virtual machine in a KVM environment. When the virtual machines are included in a NetBackup policy, restrictions apply to the characters that are allowed in the virtual machine display name. See "NetBackup character restrictions for the Primary VM identifier" on page 32.
VM UUID	The globally unique ID that is assigned to the virtual machine when the virtual machine is created. This ID uniquely identifies the virtual machine on a KVM host.

NetBackup character restrictions for the Primary VM identifier

For virtual machines in a NetBackup policy, certain characters are not allowed in their names. The backup policy **Primary VM identifier** field identifies the name type that NetBackup uses to select VMs.

See "Primary VM identifier options (KVM)" on page 31.

If the name contains disallowed characters, backups or restores may fail.

The following table describes the characters and strings that NetBackup does not allow for backup or restore in the **Primary VM identifier**, except where noted.

Table 5-10 Disallowed characters and strings in the Primary VM identifier

Character/string	Description	Notes
"	Quotation mark, Unicode x22.	
$	Dollar sign, Unicode x24.	
'	Apostrophe, Unicode x27.	
*	Asterisk, Unicode x2A.	
,	Comma, Unicode x2C.	
:	Colon, Unicode x3A.	
;	Semi-colon, Unicode x3B.	
?	Question mark, Unicode x3F.	
@	At sign, Unicode x40.	
|	Vertical line, Unicode x7C.	

Table 5-10 Disallowed characters and strings in the Primary VM identifier *(continued)*

Character/string	Description	Notes
`	Grave accent, Unicode x60.	
´	Acute accent, Unicode xB4.	
%	Percent sign, Unicode x25.	In an intelligent policy query and VM search results, NetBackup converts % in the display name of **Included** VMs to the literal string **%25**. When you specify a display name in a query, replace the % character with **%25**.
&	Ampersand sign, Unicode x26.	
<	Less than sign, Unicode x3C.	
>	Greater than sign, Unicode x3E.	
-	Hyphen-minus, Unicode x2D.	Disallowed in the first position only.
/	Solidus, Unicode x2F.	Disallowed in the VM display name; allowed in other objects.
\	Reverse solidus, Unicode x5C.	Disallowed in the VM display name; allowed in other objects.
.	Full stop (period), Unicode x2E.	Disallowed in the VM display name when in the last position; allowed in other objects.
□	Space, Unicode x20.	In an intelligent policy query and VM search results, NetBackup converts a space character in the display name of **Included** VMs to the literal string **%20**. When you specify a display name in a query, replace the space character with **%20**.
Unicode characters greater than x7F (non-ASCII)		Disallowed when the backup policy specifies the VM display name as the primary VM identifier.
%2f	Literal string, not a Unicode character definition.	Disallowed in the VM display name; allowed in other objects.

Table 5-10 Disallowed characters and strings in the Primary VM identifier *(continued)*

Character/string	Description	Notes
%5c	Literal string, not a Unicode character definition.	Disallowed in the VM display name; allowed in other objects.

Additional character restrictions for VM names can be found in the *NetBackup Cloud Administrator's Guide*, available from this location:

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

Existing snapshot handling options (KVM)

Undeleted snapshots can contribute to disk space and performance issues. NetBackup offers the following options to clean up snapshots as part of the backup process.

Table 5-11 Existing snapshot handling: Options

Option	Description
Remove NetBackup snapshots and continue the backup	If a virtual machine snapshot exists that a NetBackup backup previously created: NetBackup removes the old snapshot, creates an updated snapshot, and proceeds with the virtual machine backup.
Continue the backup	NetBackup ignores any existing virtual machine snapshots (including snapshots previously created by NetBackup) and proceeds with snapshot creation and the backup.
Stop the backup if any snapshots exist	If any snapshot exists on the virtual machine, NetBackup stops the job for that virtual machine only.
Stop the backup if NetBackup snapshots exist	If a virtual machine snapshot exists that a NetBackup backup previously created, NetBackup stops the job for that virtual machine only.

KVM - Advanced attributes

The following additional parameters are available for KVM backups. In most situations, the best settings are the defaults.

Table 5-12 KVM advanced attributes

Configuration parameter	Description
Virtual machine quiesce	This option is enabled by default. In the great majority of cases, you should accept the default. I/O on the virtual machine is quiesced before NetBackup creates the snapshot. Without quiescing file activity, data consistency in the snapshot cannot be guaranteed. If not consistent, the backed-up data may be of little or no value. If this option is disabled, the snapshot is created without quiescing I/O on the virtual machine. In this case, you must perform your own analysis for data consistency in the backup data. Caution: Cohesity does not recommend that you disable quiesce. In most cases, this option should be enabled. **Note:** If the QEMU guest agent is not installed, the backup fails. **Perform snapshot without quiescing if quiesced snapshots fail** Select this option to automatically perform the snapshot with quiescing if any backups of quiesced snapshots fail.

View the protection status of KVM virtual machines

You can view the protection status for the policies that are used to protect VMs on KVM hosts.

To view the protection status KVM virtual machines

1. On the left, select **Workloads > KVM**.
2. Select the **Virtual machines** tab.

   The **Last successful backup** column indicates the date and time of the last successful backup. The **Protected by policy** column indicates the name of the policy that protects the virtual machine.

Perform a manual backup

After you configure the servers and assets in your environment, you can test the configuration settings with a manual backup. Perform a manual backup (or backups) from a policy with the automatic backup schedules that you created.

To perform a manual backup from a policy

1. On the left, select **Protection > Policies**.
2. Select the policy you want to test.
3. Select **Manual backup**.
4. Select the schedule that you want to use for the manual backup.
5. Select the clients that you want to include for the manual backup.

Chapter 6

Recovering KVM virtual machines

This chapter includes the following topics:

Considerations and limitations for KVM recovery

Before you perform KVM recovery, review the following considerations and limitations:

- You can only recover to a storage pool that NetBackup has discovered. If no storage pools have been discovered, you must first create a storage pool and then run discovery to discover that storage pool.
- Recovery is supported only from full backups.
- If a VM disk did not reside in a storage pool at time of backup, the recovery option **Restore to the original location** is not available.

About the pre-recovery check

The pre-recovery check verifies the following:

- Use of supported characters and the character length of the display name.
- Existence of a VM with the same display name or UUID.
- Connectivity with the KVM host.

- Available space on the destination volume.

Recover a KVM virtual machine

You can recover a VM to its original location where it existed when it was backed up or to different location. You can choose to recover from the default copy of the backup image or from an alternate copy, if one exists. The default copy is also known as the primary copy.

To recover a KVM virtual machine

1. On the left, select **Workloads > KVM**.
2. Select the **Virtual machines** tab.
3. Locate and select the VM. Then select **Recover**.
4. Select the **Recovery points** tab. In the calendar view on the left, select the date on which the backup occurred.

   The available images are listed in rows with the backup timestamp for each image.
5. For the image that you want to recover, select one of the following image recovery options:
   - **Recover**
     Recover from the default copy of the backup image. This option is displayed if only one copy exists.
   - **Recover from default copy**
     Recover from the default copy of the backup image. This option is displayed if more than one copy exists.
   - ***nn* copies**
     Recover from the default copy or a different copy of the backup image. NetBackup allows up to ten copies of the same backup image. All available copies are displayed when you select this option. For each copy, the **Storage** name, **Storage server**, and the **Storage server type** are displayed.
6. Select **Restore virtual machine** for the copy that you want to recover.
7. In the **Recovery target** step, do the following:
   - Review the **Restore to** values.
     The default values are populated from the backup image of the VM.
   - If you want to apply a different display name, enter that name.
   - To recover to a different KVM host, search for that host name.

- To recover to alternate storage, select **Restore to alternate storage**. For each disk, select the **Destination storage pool** and enter the **Destination volume** to which you want to recover.

8 Select **Next**.

9 Review the restore options.

Allow overwrite of existing virtual machine	NetBackup deletes any VM with the same display name or UUID that exists at the destination, before the recovery starts. Note that, NetBackup deletes any VM with the same display name or UUID, it may not be the same VM, but another VM having the same display name or UUID.
Power on after recovery	Automatically turns on the VM when the recovery is complete.
Create a new VM UUID	Restores the VM with a new VM UUID instead of the original VM UUID.

10 Select **Next**.

11 NetBackup performs the pre-recovery checks.

12 Resolve any errors.

You can choose to ignore the errors. However, the recovery may fail.

13 Select **Start recovery**.

Select the **Restore activity** tab to monitor a job's progress. Select a specific job to view its details.

Chapter 7

Troubleshooting KVM backups and recovery

This chapter includes the following topics:

NetBackup logging for KVM

For log messages about KVM backups or KVM restores, see the following NetBackup log directories.

Table 7-1

Log directory	Contains the messages on	Resides on
install_path\NetBackup\logs\bpbrm	Backup and restore	Primary or media server
install_path\NetBackup\logs\bptm	Backup and restore	Media server
install_path\NetBackup\logs\bpfis	Snapshot creation and backup	KVM host
install_path\NetBackup\logs\bpcd	Snapshot creation and backup	KVM host
install_path\NetBackup\logs\bpbkar	Backup	KVM host
install_path\NetBackup\logs\bprd	Restore	Primary server
install_path\NetBackup\logs\bpVMutil	KVM host configuration, discovery, and restores	KVM host
install_path\NetBackup\logs\nbproxy	Policy configuration	KVM host

Table 7-1 *(continued)*

Log directory	Contains the messages on	Resides on
install_path\NetBackup\logs\ncfnbcs (originator ID 366) ncfnbcs uses unified logging. See the NetBackup Logging Reference Guide for information on how to use unified logs.	Automatic virtual machine selection and KVM host configuration and discovery	Primary server, KVM host
install_path\NetBackup\logs\ncfnbrestore (originator ID 357) ncfnbrestore uses unified logging. See the *NetBackup Logging Reference Guide* for information on how to use unified logs.	Restore	KVM host
Windows: *install_path*\NetBackup\logs\vxms Linux: /usr/openv/netbackup/logs/vxms	File mapping during backup	KVM host See "Configuring VxMS logging " on page 41. Note: The use of VxMS logging can reduce the performance of the backup host.
install_path\NetBackup\logs\nbwebservice	KVM host configuration and discovery	Primary server

Note: Except for unified logging directories, these log directories must already exist in order for logging to occur. If these directories do not exist, create them.

To create most of these log directories, run the following command on the NetBackup servers and KVM hosts:

Windows:`install_path\NetBackup\logs\mklogdir.bat`

UNIX (on primary or media servers):`/opt/openv/netbackup/logs/mklogdir`

See "Configuring VxMS logging " on page 41..

More detail is available on snapshot logs and logging levels. See the NetBackup NAS Administrator's Guide. A broader discussion of logging is available. See the NetBackup Logging Reference Guide.

Configuring VxMS logging

The following procedures describe how to configure VxMS logging for NetBackup.

VxMS logging on a Linux backup host

To configure VxMS logging on a Linux backup host

1. Create the VxMS log directory:

   `/usr/openv/netbackup/logs/vxms`

   Note: For logging to occur, the VxMS directory must exist.

   Note: If you have run the NetBackup `mklogdir` command, the VxMS log directory already exists.

2. Add the following to the `/usr/openv/netbackup/bp.conf` file:

   `VXMS_VERBOSE=<numeric value of 0 or greater>`

   See Table 7-2 for the available logging levels.

3. To change the log location, enter the following in the `bp.conf` file:

   `vxmslogdir=path to new log location`

   Note: If the VxMS log location is changed, the Logging Assistant does not collect the logs.

VxMS logging on a Windows backup host

To configure VxMS logging on a Windows backup host

1. Create the VxMS log directory:

   install_path`\NetBackup\logs\vxms`

   Note: For logging to occur, the VxMS folder must exist.

   Note: If you have run the NetBackup `mklogdir.bat` command, the VxMS log directory already exists.

2. In the Windows registry, create the DWORD registry entry `VXMS_VERBOSE` in the following location:

   HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > NetBackup > CurrentVersion > Config

3. To configure the logging level, set the numeric value of `VXMS_VERBOSE` to 0 or greater. Larger numbers result in more verbose logs.

   See Table 7-2 for the available logging levels.

4. To change the log location:

   - Open regedit and go to the following location:
     HKEY_LOCAL_MACHINE > SOFTWARE > Veritas > NetBackup > CurrentVersion

- Create the registry entry `vxmslogdir` with a string value `(REG_SZ)`. For the string value, specify the full path to an existing folder.

Note: You can use NTFS compression on VxMS log folders to compress the log size. The new logs are written in compressed form only.

Note: If the VxMS log location is changed, the Logging Assistant does not collect the logs.

VxMS logging levels

Table 7-2 lists the VxMS logging levels.

Note: Logging levels higher than 5 cannot be set in the Logging Assistant.

Note: Logging levels higher than 5 should be used in very unusual cases only. At that level, the log files and metadata dumps may place significant demands on disk space and host performance.

Table 7-2 VxMS logging levels

Level	Description
0	No logging.
1	Error logging.
2	Level 1 + warning messages.
3	Level 2 + informative messages.
4	Same as level 3.
5	Highly verbose (includes level 1) + auxiliary evidence files (`.mmf, .dump, VDDK logs, .xml, .rvpmem`). You can set the logging level for the VDDK messages.
6	VIX (VMware virtual machine metadata) dumps only.
7	VHD (Hyper-V virtual machine metadata) dumps only.
> 7	Full verbose + level 5 + level 6 + level 7.

Troubleshooting a KVM discovery or a validate operation

Discovery or Validate operation fails for the KVM host

Recommended action: Ensure sure that the KVM host is reachable and that NetBackup services are up.

A backup of a virtual machine without a storage pool cannot be restored to the original location

If the virtual machine disk files did not reside on the storage pool during the backup, the pre-recovery check fails if the user attempts to restore to the original location. In this case, restore to an alternate location. By default for this kind of restore, the **Destination storage pool** and the **Destination volume** values are empty for the virtual machine. Select the wanted values before you continue with the restore.

A backup job fails with error 4726 - Failed to create snapshot of the specified VM.

The `bpbrm` logs on the media server contain the following message:

```
12:41:49.943 [3275984.3275984] <2> get_bpfis_msg: bpfis buff: FTL - Unable to
quiesce VM filesystem.
Verify the QEMU guest agent is installed and running.
12:41:49.943 [3275984.3275984] <32> get_bpfis_msg: from client alpine2: FTL - Unable
to quiesce VM filesystem.
Verify the QEMU guest agent is installed and running.
12:41:49.944 [3275984.3275984] <2> set_job_details: Tfile (12): LOG 1752774109 32
bpbrm 3275984 from client
alpine2: FTL - Unable to quiesce VM filesystem. Verify the QEMU guest agent is
installed and running.
12:41:49.944 [3275984.3275984] <2> send_job_file: job ID 12, ftype = 3 msg len = 146,
msg = LOG 1752774109 32
bpbrm 3275984 from client alpine2: FTL - Unable to quiesce VM filesystem. Verify the
QEMU guest agent is installed and running.
```

This error can occur if the **Virtual machine quiesce** option is selected without the option **Perform snapshot without quiescing if quiesced snapshots fail** for the backup policy.

A snapshot may fail if the virtual machine can't be quiesced. This error usually means that the QEMU agent isn't installed or isn't running on the guest system. To fix this issue, you can either resolve the QEMU agent issue on the guest VM to

allow for a successful quiesce operation. Or, select the option **Perform snapshot without quiescing if quiesced snapshots fail** option.

A backup of a virtual machine fails if the QEMU guest agent is not installed

The KVM advanced attribute **Virtual machine quiesce** is enabled by default and requires that the QEMU guest agent is installed. If not, the backup fails.