NetBackup™ Web UI VMware Administrator's Guide

Release 9.0

VERITAS™

NetBackup Web UI VMware 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.
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 VMware servers

This chapter includes the following topics:

Add VMware servers

Use this procedure to add VMware servers and their credentials.

To add VMware servers and their credentials

1. On the left, click **VMware**, then click the **VMware Servers** tab.

   The tab shows the vCenters and ESXi servers that you can access.
2. Click **+ Add** to add a server.
3. Select the server type and enter its host name, and its credentials.

4 Choose a **Backup host for validation.**.

Note: Adding or updating VMware credentials also automatically starts the discovery of the VMware server. When backup host information is provided in the request, it is used to perform validation of credentials as well as for performing the discovery. For discovery, NetBackup 8.1.2 is the minimum version that is supported for a NetBackup media server or client that serves as a backup host. For older versions, backup host credential validation succeeds, but the discovery of VMware servers fails.

5 Indicate a **Port** number for connection.

If the default port number has not been changed on the VMware server, no port specification is required. If the VMware server has been configured to use a different port, specify that port number.

6 Click **Save**.

Important!

The discovery of VMs and other objects in the vCenter or ESXi server begins when server credentials are added or updated through the web UI or an API. However, the server's VMs and other objects might not appear in the UI immediately. They appear after the discovery process for the VMware server completes. Discovery also occurs at set intervals. (The default interval is every 8 hours.)

To perform autodiscovery of VMware server objects at a different frequency:

See "VMWARE_AUTODISCOVERY_INTERVAL option for NetBackup servers" on page 26.

7 To enter NetBackup credentials for another VMware server, click **+ Add**.

Information is available about troubleshooting problems that may occur:

See "Errors when adding VMware servers" on page 53.

See "Errors when browsing VMware servers" on page 53.

See "Errors for the Status for a newly discovered VM" on page 54.

Validate and update VMware server credentials

To validate VMware credentials

1. On the left, click **VMware**, then click the **VMware Servers** tab.
2. To validate one server's credentials, locate and select the VMware server. To validate the credentials of multiple servers at the same time, locate and select the VMware servers. Then in the row with that server, click **Validate**.

   NetBackup verifies the current credentials for the selected VMware servers.

   If the credentials are not valid, NetBackup indicates **Invalid** under **Credentials**. Use the following steps to update the VMware server credentials.

To update VMware server credentials

1. On the left, click **VMware**, then click the **VMware Servers** tab.
2. Locate and select the VMware server.
3. From the option menu on the right of the row, select **Edit**.
4. Update the credentials as needed.

   Note: Adding or updating VMware credentials also automatically starts the discovery of the VMware server. When backup host information is provided in the request, it is used to perform validation of credentials as well as for performing the discovery. For discovery, NetBackup 8.1.2 is the minimum version that is supported for a NetBackup media server or client that serves as a backup host. For older versions, backup host credential validation succeeds, but the discovery of VMware servers fails.

5. Click **Save**.

   NetBackup verifies the updated credentials for the selected VMware server.

Browse VMware servers

You can browse vCenter servers and standalone ESXi servers to locate VMs and view their details such as their protection plans and recovery points.

To browse VMware servers

1. On the left, click **VMware**.
2. Click **VMware Servers** to begin searching.

   The list includes the names and types of vCenters and standalone ESXi servers that you have access to. You can also review the **Discovery Status** and **Last discovery attempt** to determine whether the server's VMs and other objects have been successfully discovered.

   To locate a server, you can enter a string in the search field.
3. Click on a server to begin drilling into it.

   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.

Remove VMware servers

Use this procedure to delete VMware servers.

To remove a VMware server

1. On the left, click **VMware**, then click the **VMware Servers** tab.

   The tab lists the names and types of vCenters and standalone ESXi servers that you have access to. You can also review the **Discovery Status** and **Last discovery attempt** to determine when the server's VMs and other objects were last discovered.
2. Locate and select the VMware server.
3. From the action menu on the right of the row, select **Delete**.

   Note: If you delete a server, all virtual machines that are associated with the deleted VMware server are no longer protected. You can still recover existing backup images, but backups of VMs on this server will fail.
4. If you are sure that you want to delete the VMware server, click **Delete**.

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

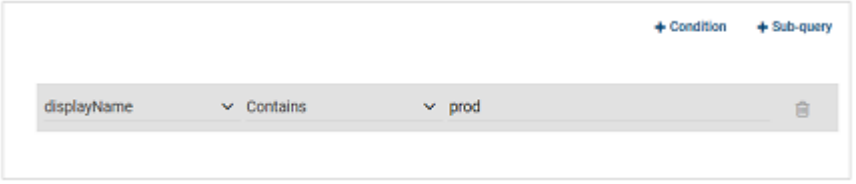
them to the group. You can then apply protection to the group. Note that an intelligent group automatically reflects changes in the VM environment and eliminates the need to manually revise the list of VMs in the group.

To create an intelligent VM group

1. On the left, click **VMware**.
2. Click the **Intelligent VM groups** tab and then click **+ Add**.
3. Enter a name and description for the group.
4. Select the appropriate VMware server.
5. Perform one of the following:
   - Select **Include all VMs**.
     This option uses a default query to select all VMs that currently reside in the vCenter or ESXi for backup when the protection plan runs.
   - To select only the VMs that meet specific conditions, create your own query: Click **Add condition**.
6. 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:

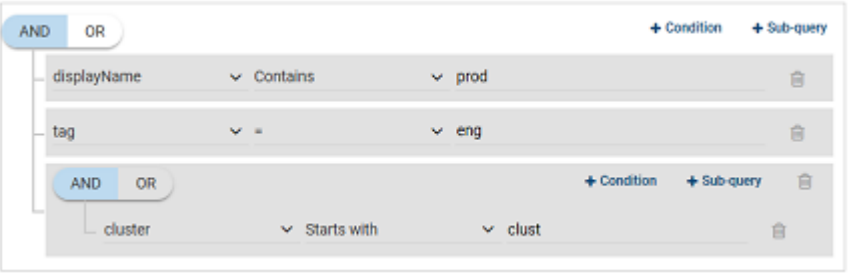
This example uses **AND** to narrow the scope of the query: it selects only the VMs that have `prod` in their display name and that also have a tag named `eng`. If a VM does not have `prod` in its display name as well as a tag named `eng`, that VM is not added to the group.

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).

You can also add sub-queries to a condition, if necessary. Click **+ Sub-query** and click **AND** or **OR**, then select the keyword, operator, and value for the sub-query condition. For example:



In this example, the sub-query causes the query to narrow the scope further. From the VMs that have both `prod` in their display name and a tag named `eng`, only the VMs in clusters that start with `clust` are selected.

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

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.

Note: When using queries in **Intelligent VM groups**, the NetBackup web UI might not display an accurate list of VMs that match the query if the query condition has non-English characters. However, during the backup, the correct VMs are selected even though the VM attributes are non-English.

Using the `not equals` filter condition on any attribute returns assets including those that have no value (null) present for the attribute. For multi-value attributes such as `tag`, the assets that do not match at least one of the values of the attribute are not returned

When the server of an Intelligent VM group is updated, all existing access definitions configured for that Intelligent group are removed because the intelligent group is now registered with the new server namespace. You need to add new access definitions for the updated Intelligent group.

Note: The discovery of VMs in the VMware server occurs at set intervals according to the `VMWARE_AUTODISCOVERY_INTERVAL` option. (The default interval is every 8 hours.) The web UI must discover the VMs on each server before the query can select from them. If a VMware server was recently added in the web UI, its VMs may not have been discovered. More information about this option is available:

See "VMWARE_AUTODISCOVERY_INTERVAL option for NetBackup servers" on page 26.

To discover the VMs immediately:

See "Discover VMware server assets manually" on page 26.

---

8 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 you 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.

Query options for creating intelligent VM groups

Table 3-1 Query keywords

Keyword	Description
`cluster`	The name of the cluster (group of ESXi servers) where the VMs reside. Not case-sensitive when the protection plan runs.
`datacenter`	The name of the datacenter. Not case-sensitive when the protection plan runs.
`datastore`	The name of the datastore. Case-sensitive when the protection plan runs.
`displayName`	The VM's display name. Case-sensitive when the protection plan runs.
`host`	The name of the ESXi server. The ESXi host name must match the name as defined in the vCenter server. Not case-sensitive when the protection plan runs.
`tag`	The name of the VM's tag. Case-sensitive when the protection plan runs.
`dnsName`	The VM's DNS name in vSphere Client. Not case-sensitive when the protection plan runs.

Table 3-1 Query keywords *(continued)*

Keyword	Description
`hostName`	The VM name that is derived from a reverse lookup of its IP address. Not case-sensitive when the protection plan runs.
`instanceUuid`	The VM's instance UUID. For example: `501b13c3-52de-9a06-cd9a-ecb23aa975d1` Not case-sensitive when the protection plan runs.

Table 3-2 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 **VMware**.
2. Locate the group under the **Intelligent VM groups** tab.
3. If the group is not protected, select it and then 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**.

Add a VMware access host

NetBackup uses a special host that is called a VMware access host. It is a &nbuProductName; client that performs backups on behalf of the virtual machines. The access host is the only host on which NetBackup media server or client software is installed. No NetBackup client software is required on the virtual machines. However, the access host must have access to the datastores of the virtual machines. The access host reads the data from the datastore and sends it over the network to the media server.

The VMware access host was formerly called the VMware backup host or the VMware backup proxy server. The access host is referred to as the recovery host when it performs a restore.

Note: Make sure that NetBackup media server software or client software is installed on any access host that you add.

To add a VMware access host

1. On the left, click **VMware**, then click the **Virtual machines** tab.
2. On the right, select **VMware settings > Access hosts**.

   NetBackup lists any access hosts that were previously added.
3. Click **+ Add**.
4. Enter the name of the access host and then click **Add**.

Remove a VMware access host

To remove a VMware access host

1. On the left, click **VMware**, then click the **Virtual machines** tab.
2. On the right, select **VMware settings > Access hosts**.

   NetBackup lists any access hosts that were previously added.
3. Locate the VMware access host and then click the delete icon.
4. To confirm the deletion, click **Delete**.

Discover VMware server assets manually

Use this procedure to manually discover any VMware server so that you can view and protect recently added assets.

Note: Automatic discovery of VMs and other objects in the vCenter or ESXi server begins when server credentials are added or updated through the web UI or an API. However, the server's VMs and other objects might not appear in the UI immediately. They appear after the discovery process for the VMware server completes. Discovery also occurs at set intervals according to the `VMWARE_AUTODISCOVERY_INTERVAL` option. (The default interval is every 8 hours.) More information about this option is available:

See "VMWARE_AUTODISCOVERY_INTERVAL option for NetBackup servers" on page 26.

To manually discover VMware server assets

1. On the left, click **VMware**, then click the **VMware Servers** tab.

   The tab lists the names and types of vCenters and standalone ESXi servers that you have access to. You can also review the **Discovery Status** and **Last discovery attempt** to determine when the server's VMs and other objects were last discovered.

2. Locate and select the VMware server.

3. From the action menu on the right of the row, select **Discover**.

   The discovery operation may fail if the VMware server credentials are invalid. To validate and update the credentials:

   See "Validate and update VMware server credentials" on page 18.

For more information about the protection status of VMs and intelligent VM groups:

See "View the protection status of VMs or intelligent VM groups" on page 33.

See "Errors for the Status for a newly discovered VM" on page 54.

VMWARE_AUTODISCOVERY_INTERVAL option for NetBackup servers

This option controls how often NetBackup scans the vCenter 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 3-3 VMWARE_AUTODISCOVERY_INTERVAL 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 option.
	Note: These commands require administrator privilege on the NetBackup master server. For assistance, contact the NetBackup administrator.
	You can also use the NetBackup configuration APIs to view, add, or change this option. Refer to the NetBackup API documentation on SORT for more information:
	The default is 8 hours. The minimum is 5 minutes, the maximum 1 year. If set to zero, autodiscovery is disabled for all the VMware servers.
	Use the following format:
	`VMWARE_AUTODISCOVERY_INTERVAL = number of seconds`
	For example:
	`VMWARE_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.

Chapter 4

Protecting VMs

This chapter includes the following topics:

Protect VMs or intelligent VM groups

Use the following procedure to subscribe an asset (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 VMs or VM groups

1. On the left, click **VMware**.
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, snapshot options, and exclude options.

- **Advanced options**
  Change or enable any advanced options for the protection plan.

5 Click **Protect**.

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

Edit protection settings for a VMware 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 30.
- See "Backup options and Advanced options" on page 30.

To edit protection settings for a VMware asset

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

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 30.
- **Backup options** and **Advanced** options.
  See "Backup options and Advanced options" on page 30.

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 and Advanced options

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

Backup options

Table 4-2 Backup options for protection plans

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.
If a snapshot exists, perform the following action	Specifies the action that NetBackup takes when a snapshot is discovered before NetBackup creates a new snapshot for the virtual machine backup. For example, users can choose to stop a backup if any snapshots exist. If snapshots are not automatically deleted, the performance of the virtual machine may eventually decline. Undeleted snapshots can cause restore failures due to lack of disk space.
Exclude selected virtual disks from backups	Specifies the virtual disks to exclude from backups. See “Exclude disks from backups” on page 31.

Advanced options

Table 4-3 Advanced options for protection plans

Option	Description
Enable virtual machine quiesce	By default, I/O on the virtual machine is quiesced before NetBackup creates the snapshot. In the majority of cases, you should use this default. Without quiescing file activity, data consistency in the snapshot cannot be guaranteed. If you disable the quiesce, you must analyze the backup data for consistency.
Allow the restore of application data from virtual machine backups	This option allows users to restore application data from full backups of the virtual machine. Note that in NetBackup 8.3 or earlier, application data for Microsoft Exchange Server or Microsoft SharePoint Server must be restored with the NetBackup Backup, Archive, and Restore interface. Data for Microsoft SQL Server must be restored with the NetBackup MS SQL Client. See the documentation for your NetBackup database agent for more details.
Transport mode	Specifies the transport mode to use for backups or how to read the data from the datastore. For more information on transport modes, see the vendor documentation for your virtualization environment.
Snapshot retry options	See “Snapshot retry options” on page 32.

Exclude disks from backups

Excluding virtual disks can reduce the size of the backup, but use these options carefully. They are intended only for the virtual machines that have multiple virtual disks.

Table 4-4 Options for excluding virtual disks

Exclude option	Description
All boot disks	Consider this option if you have another means of recreating the boot disk. The virtual machine’s boot disk is not included in the backup. Any other disks are backed up. **Note:** Data files are available in the restored data disks. However, you cannot start a virtual machine that is restored from this backup.

Table 4-4 Options for excluding virtual disks *(continued)*

Exclude option	Description
All data disks	Consider this option only if you have a separate protection plan that backs up the data disks. The virtual machine's data disks are not included in the backup. Only the boot disk is backed up. **Note:** When the virtual machine is restored from the backup, the virtual machine data for the data disk may be missing or incomplete.
Exclude disks based on a custom attribute	Use this option to allow the VMware administrator to use a custom attribute to control which disks are excluded from backups. The attribute must have comma-separated values of device controllers for the disks to be excluded. For example: `scsi0-0,ide0-0,sata0-0,nvme0-0`. The default value for this attribute is `NB_DISK_EXCLUDE_DISK`. Or, you can choose your own value. If you add disks to the custom attribute value between any differential backups, those disks are excluded from the next backup. The VMware administrator must use a VMware interface to apply the attribute to the disks to exclude. See the NetBackup Plug-in for VMware vSphere Web Client Guide or the NetBackup Plug-in for VMware vSphere Client (HTML5) Guide.
Specific disks to be excluded	Use this option to exclude a specific disk by the disk type, controller, and LUN that represent the virtual device node of the disk. Click **Add** to specify additional disks. If you add controllers between any differential backups, their disks are excluded from the next backup.

Snapshot retry options

For most environments, the default values for the snapshot retry options are appropriate. It may be helpful to adjust these settings based on the size of the virtual machine and the processing load on the VMware server.

Table 4-5 Snapshot retry options

Option	Description
Maximum number of times to retry a snapshot	The number of times the snapshot is retried.
Maximum length of time to complete a snapshot	The time, in minutes, to allow the snapshot operation to complete. If snapshots do not complete, set this option to a specific period to force a time-out. Use the **Maximum length of time to wait before a snapshot is retried** setting to retry the snapshot at a later time.

Table 4-5 Snapshot retry options *(continued)*

Option	Description
Maximum length of time to wait before a snapshot is retried	The time to wait (in seconds) before the snapshot is retried.

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.

Note: When you unsubscribe an asset from a protection plan, there is a possibility that the asset displays **Classic policy** in the web UI. This situation can happen when an asset is subscribed to a protection plan and a backup runs for that asset. Then the asset is unsubscribed from the protection plan while it has a valid backup image. The web UI displays **Classic policy**, but there may or may not be an active policy protecting the asset.

To remove protection from a VM or intelligent VM group

1. On the left, click **VMware**.
2. On the **Virtual machines** tab or **Intelligent VM groups** tab, click the VM or the intelligent VM group.
3. Click **Remove protection > Yes**.

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

View the protection status of VMs or intelligent VM groups

You can view the protections plans that are used to protect VMs or intelligent VM groups.

To view the protection status of VMs or intelligent VM groups

1. On the left, click **VMware**.
2. Select the **Virtual machines** tab or **Intelligent VM groups** tab, as appropriate.

   Note: Sorting on assets across asset types, that is, without the Asset Type filter, returns results grouped by asset types (Virtual Machine and Intelligent VM groups) and sorted within each asset type.

3. Click the VM or the intelligent VM group.

   The **Protection** tab shows the details of the plans that the asset is subscribed to.

   Note: If the asset has been backed up, but Status indicates it has not, see the following information.

   See "Errors for the Status for a newly discovered VM" on page 54.

4. If the asset is not protected, click **Add protection** to select a protection plan.

   See "Protect VMs or intelligent VM groups" on page 28.

Chapter 5

Instant access

This chapter includes the following topics:

Create an instant access VM

You can create an instant access VM from a NetBackup backup image. The VM is available almost instantaneously, achieving a near-zero recovery time objective. NetBackup mounts the VM's snapshot directly on the backup storage device to allow your ESXi host or cluster to treat the snapshot as a normal VM.

The mounted VM snapshot can be used for a variety of purposes. For example:

- Recovering files from the VM, or copying a vmdk file.
- Running tests on the VM, such as testing a patch.
- Troubleshooting or disaster recovery.
- Verifying an application.

Note: This feature is supported for NetBackup Appliance, NetBackup Virtual Appliance, and Build Your Own (BYO) server. This feature requires that the NetBackup backup image is stored on a Media Server Deduplication Pool (MSDP) storage device. More information on using instance access VMs is available:

See "Things to consider before you use the instant access feature" on page 39.

To create an instant access VM

1. On the left, click **VMware**.
2. Locate the VM and click on it.
3. Click the **Recovery points** tab, then click the date on which the backup occurred.

   The available images appear in rows with the backup timestamp for each image.
4. On the image or the copy of the image that has the option to recover using instant access, click **Recover > Create instant access virtual machine**.
5. Review the recovery settings and make changes if needed.

   Note the **Recovery options**:

Allow overwrite of existing virtual machine	If a VM with the same display name exists at the destination, that VM must be deleted before the recovery begins. Otherwise, the recovery fails.
Power on after provisioning	Automatically powers on the VM when the recovery is complete.
Enable vMotion	Starts the migration of the VM after it is created and then displays progress of the VM migration. **Note:** For a NetBackup 8.1.2 storage server, the vMotion option is not used even if it is enabled.

6. Click **Create**.

   NetBackup makes a snapshot of the VM backup image and creates an instant access mount point. The snapshot of the image appears on the **Instant access virtual machines** tab. You can now use the VM like any other VM on the ESXi server.
7. For details on the restored VM, click on the VM under the **Instant access virtual machines** tab and click **View details**.
8. When you are finished with the VM, you can click **Delete** to remove the mounted VM snapshot. The VM is removed from the ESXi server.

Note: If vMotion is enabled and completed successfully, deleting a VM only removes the mounted share. The VM is still available on the ESXi server as this VM is migrated to another datastore.

Restore files and folders from a VM backup image

You can browse an instant access image of the VM to restore files and folders.

Note: More information on using instance access VMs is available:

See "Things to consider before you use the instant access feature" on page 39.

To restore files and folders from a VM backup image

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

   The available images are listed in rows with the backup timestamp for each image.
4. On the image or the copy of the image that has the option to recover using instant access, click **Recover > Restore files and folders**.

   NetBackup creates an instant access mount point in the background.
5. Select the files and click **Add to restore list**.

   Click on a folder to drill into it. Use the folder path to navigate back to higher levels in the hierarchy.

   Enter a file name to search for files.

   The restore list displays the selected files and folders with the location and size of each file.
6. Select the restore options:
   - **Restore everything to the original directory**
     - Enter the name of the target VM (the default is the original VM) and the username and password for the target VM.
   - **Restore everything to a different directory**
     - In **Directory for restore**, enter the destination path for restore.

Note: If the storage server is NetBackup 8.1.2, enter the `Single File Full Path` and not the `Parent Folder Path`.

- Select the **Flatten existing directory structure** check box to restore all files to a single directory.

  Note: If the storage server is NetBackup 8.1.2, this option is automatically used during restore.

- Enter the name of the target VM (the default is the original VM) and the username and password for the target VM.

7 Select the **Overwrite existing files** check box to overwrite all the existing files.

Note: If the storage server is NetBackup 8.1.2, this option is automatically used during restore.

A summary of your selections is displayed.

8 Click **Start recovery** to restore the files.

The **Activity** tab displays the status of the recovery.

Download files and folders from a VM backup image

You can browse an instant access image of the VM to download files and folders.

Note: More information on using instance access VMs is available:

See "Things to consider before you use the instant access feature" on page 39.

To download files and folders from a VM backup image

1 On the left, click **VMware**.

2 Locate and click on the VM.

3 Click the **Recovery points** tab. In the calendar view, click the date on which the backup occurred.

The available images are listed in rows with the backup timestamp for each image.

4 On the image or the copy of the image that has the option to recover using instant access, click **Recover > Download files and folders**.

5 Select the files and click **Add to download list**.

Click on a folder to drill into it. Use the folder path to navigate back to higher levels in the hierarchy.

Enter a file name to search for files.

The download list displays the selected files and folders with the location and size of each file.

6 After the download package is created, click **Download**.

The **Activity** tab displays the status of the recovery.

Things to consider before you use the instant access feature

Note the following about the **Instant access virtual machines** feature:

- This feature is supported with backup copies that are created from protection plans using the web UI or from classic policies that are created with the NetBackup Administration Console.
- This feature is supported for NetBackup Appliance, NetBackup Virtual Appliance, and Build Your Own (BYO) server.
- This feature is limited to 50 concurrent mount points on a Media Server Deduplication Pool (MSDP) media server.
- By default, vSphere allows a maximum of eight NFS mounts per ESXi server. Note that NetBackup requires an NFS mount for each instant access VM you create. To remove the NFS mount, remove the instant access VM when you are done with it.
  If the NFS limit for an ESXi host has been reached and you try to create another instant access VM, the attempt fails. To increase the maximum NFS mounts per ESXi server, see the following VMware article:
  https://kb.vmware.com/s/article/2239
- This feature does not support backups of VMs that have independent disks. VMware does not support snapshots of independent disks in a VM, either persistent disks or non-persistent disks. As a result, independent disks are not backed up.

For more information on independent disks and NetBackup, see the following article:
https://www.veritas.com/docs/000081966

- This feature does not support VMs that have disks that were excluded from the backup. In the 9.0 Administration Console, on the NetBackup policy's **Exclude Disks** tab, select **No disks excluded**. Or, in the NetBackup Web UI, in the protection plan, clear the **Exclude selected virtual disks from backups** check box.
- This feature does not support VMs that have a disk in raw device mapping mode (RDM) or that have a disk in Persistent mode.
- For Windows restore, the ReFS file system is not supported.
- The version of the ESXi server that is used to create a VM using **Instant access virtual machines** must be equal to or newer than the version of the ESXi server that contains the VM backup images.
- For file or folder download with the **Download** option, the NetBackup web UI must be able to access the media server with the same name or IP address that the master server uses to connect to that media server. See “Error when downloading files from an instant access VM” on page 55.
- If the media server appliance uses a third-party certificate, you need to create certain configurations on the NetBackup master server before you use this feature.
  For more information, refer to the "Third-party certificates" and "Implementing third-party SSL certificates" sections in the *NetBackup Appliance Security Guide*, available here:
  https://www.veritas.com/docs/DOC5332
- This feature does not support restore of multiple files or folders, which are located in different volumes, partitions, or disks.
- Use the Windows administrator account credentials when you restore multiple files or folders to a Windows VM. You must be logged on to the target Windows VM with these account credentials.
- Some ACL entries are not in the restored file because ACL entries for these users or groups cannot be restored. For example, TrustedInstallers, All Application Packages.
- The Instant Access feature does not support a Windows 10 compact operating system. To verify if your operating system is compressed, run `compact "/compactos:query"` on the command prompt before backing up your VM.

To disable the compression, run "`compact /compactos:never`" on the command prompt before backing up your VM. You can then use the Instant Access feature for your VM backups.

- To restore files and folders, the target VM must be in a normal state, and not in a sleep or hibernate mode.
- A 5-minutes-alive-session threshold is defined in Appliance and BYO web server NGINX. The files and folders that are selected for download must be compressed and downloaded within this threshold.
- To create an instant access virtual machine, you must have read and write access to the VMware data center where the virtual machine is created.
- To ensure that Instant Access works effectively after the storage server and master server are upgraded from an earlier NetBackup version, restart the NetBackup Web Service on the upgraded master server with the following commands:
  - /usr/openv/netbackup/bin/nbwmc stop
  - /usr/openv/netbackup/bin/nbwmc start

Chapter 6

VM recovery

This chapter includes the following topics:

Recover a VM

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 VM

1. On the left, click **VMware**.
2. Locate and click on the VM.
3. Click 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.
4. On 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. Click **Recover** for the copy that you want to recover.

5 Choose the location to which you want to recover the backup image:

- **Original location**: Recovers the backup image to the original location.
- **Alternate location**: Recovers the backup image to an alternate location.
- **Create instant access virtual machine**: Recovers the backup image to a new instant access virtual machine. This option is available only if the backup image has instant access capability. See "Create an instant access VM" on page 35.
- **Download files and folders**: Downloads the files and folders from a VM backup image. This option is available only if the backup image has instant access capability. See "Download files and folders from a VM backup image" on page 38.
- **Restore files and folders**: Restores the files and folders from a VM backup image. This option is available only if the backup image has instant access capability. See See "Restore files and folders from a VM backup image" on page 37.

6 Review the **Restore to** values.

The default values come from the backup image of the VM. **New display name** is appended with `_copy` if you restore to an alternate location.

- If you recover the backup image to the original location, you cannot change the default values.
- To recover to an alternate location, change the restore values, if necessary. Then click **Next**. More information is available if you cannot change the ESXi server or cluster:
  See "Errors when you change the recovery destination" on page 58.

7 Review or change the **Recover option** values.

For more information about the recovery options, refer to the 90 for VMware Administrator's Guide.

Allow overwrite of existing virtual machine	Deletes any VM with the same display name that exists at the destination. That VM must be deleted before the recovery begins. Otherwise, the recovery fails. **Note:** You must have the **Overwrite Asset** permission to use this option. See your security administrator if you need this permission.
Power on after recovery	Automatically powers on the VM when the recovery is complete.
Recovery host	Indicate the host that you want to use to perform the recovery. By default, the recovery host is the one that performed the backup.

8 Review or change the **Advanced Settings** values.

For more information about the advanced settings, refer to the NetBackup for VMware Administrator's Guide.

Advanced settings:

Create a new BIOS UUID	Restores the VM with a new BIOS UUID instead of the original BIOS UUID.
Create a new instance UUID	Restores the VM with a new instance UUID instead of the original instance UUID.
Remove backing information for devices	For example, this option restores the VM without restoring any ISO file that was mounted when the VM was backed up. If this option is disabled, the recovery might fail if the backing information is not longer available for devices, such as DVD/CD-ROM drives, or serial or parallel ports.
Remove original network configuration	Removes the NIC cards from the VM. Note that for network access, the restored VM requires network configuration. 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.

Retain original hardware version

Restores the VM with its original hardware version (such as 4). It retains the original version even if the target ESXi server by default uses a different hardware version (such as 7 or 8). If the target ESXi server does not support the virtual machine's hardware version, the restore may fail.

If this option is disabled, the restored virtual machine is converted to the default hardware version that the ESXi server uses.

Format of restored virtual disks:

Original provisioning

Restores the VM's virtual disks with their original provisioning.

Thick provisioning lazy zeroed

Configures the restored virtual disks in the thick format. The virtual disk space is allocated when the disk is created. This option restores the populated blocks, but initializes vacant blocks with zeros later, on demand.

Note: If the vmdk is completely written, VMware automatically converts a lazy-zeroed disk to **Thick provisioning eager zeroed**.

Thick provisioning eager zeroed

Configures the restored virtual disks in the thick format. Restores the populated blocks and immediately initializes vacant blocks with zeros (eager zeroed). Creation of the virtual disks may take more time with this option. However, if the restore occurs over a SAN, the eager zeroed feature may speed up the restore by reducing network communication with the vCenter server.

Thin provisioning

Configures the restored virtual disks in the thin format. Restores the populated blocks but does not initialize vacant blocks or commit them. Thin provisioning saves disk space through dynamic growth of the vmdk file. The vmdk files are no larger than the space that the data on the virtual machine requires. The virtual disks automatically increase in size as needed.

Note: If the vmdk is completely written, VMware automatically converts a thin disk to **Thick provisioning eager zeroed**.

Transport mode:

Use transport mode used for backup

Uses the same transport mode that was used when the backup was performed.

Try the selected transport modes in the following order

- **SAN**
  For unencrypted transfer over Fibre Channel (SAN) or iSCSI.
  Note: This mode is not supported for the virtual machines that use VMware Virtual Volumes (VVols).
- **HotADD**
  Lets you run the VMware backup host in a virtual machine. For more information about the HotAdd transport mode, see NetBackup for VMware Administrator's Guide.
  Note: For the virtual machines that use VVols, the virtual machine and the backup host (hotadd) virtual machine must reside on same VVol datastore.
  For instructions on this transport mode and on installing the backup host in a VMware virtual machine, refer to your VMware documentation.
- **LAN**
  Transfer the virtual disk data over the network.
  - **NBD**
    For unencrypted transfer over a local network that uses the Network Block Device (NBD) driver protocol. This mode of transfer is usually slower than Fibre Channel.
  - **NBDSSL**
    For encrypted transfer (SSL) over a local network that uses the Network Block Device (NBD) driver protocol. This mode of transfer is usually slower than Fibre Channel.

9 Click **Pre-recovery check**.

NetBackup verifies the credentials and appropriate paths and connectivity, determines whether the datastore or datastore cluster has available space, and reviews other requirements. For more information about the pre-recovery check, refer to the NetBackup for VMware Administrator's Guide.

10 Resolve any errors.

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

11 Click **Start recovery**.

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

For information on the recovery status codes, see the NetBackup administrator or the 90 Status Codes Reference Guide.

About VMware agentless restore

NetBackup 8.2 and later supports VMware agentless restore. The agentless restore lets you restore individual files and folders to virtual machines where the NetBackup client is not installed. By using VxUpdate, NetBackup can deploy the recovery tool to the virtual machines, restore files and folders, and perform the required cleanup. NetBackup does not require a connection to the target virtual machine to recover the files. All recovery is handled through the ESX server using VMware vSphere Management APIs.

A video is available that describes NetBackup VMware agentless restore:

VMware agentless recovery video

Overview of the agentless restore process

1. The NetBackup master server receives input from either the NetBackup web UI or the Agentless Recovery API. The input is the files and folders for restore along with the VMware authorization credentials for the target virtual machine. These credentials must have administrator or superuser privileges.
2. The master server sends the requested data to the restore host.
3. The restore host confirms that it has the necessary VxUpdate recovery package to perform restore. If it's not available, the restore host downloads the required package from the master server using VxUpdate.
4. The restore host pushes recovery tool to virtual machine using the vSphere management API.
5. The data stream containing the user-selected files and folders is staged in a vmdk that is associated with a temporary virtual machine. Veritas creates the temporary virtual machine for the agentless restore.
6. The vmdk that NetBackup created on the temporary virtual machine is attached to the target virtual machine.
7. The recovery tool is invoked and the files and folders are recovered.
8. NetBackup performs the necessary cleanup. All temporary files and objects that are created as part of the process are deleted or removed. Among the objects that are deleted and removed are the recovery tool, the temporary virtual machine, and the staging vmdk.
9. The job is finished.

Prerequisites and limitations of VMware agentless restores

Prerequisites:

- You must provision VxUpdate packages for all platforms for which you have virtual machines where you want to perform agentless recovery.
- You must have an account with administrator or root permissions on the target virtual machine.
- The target VM is where the files are recovered. It must be powered on and have VMware Tools installed.
- The default staging location on the target VM is `%TEMP%` or `%TMP%` for Windows and the root directory (`/`) for Linux.
- The staging location must exist on the target VM file system.
- You must have the latest version of VMware Tools installed to perform agentless restores.

Limitations:

- VMware agentless restores can only be used for the restore of files and folders.
- In some instances, when you perform an agentless restores, orphaned VMs starting with `NB_` are left behind. Using the ESX server credentials to perform the restore on the target VM even though the vCenter manages the ESX server can cause this condition. This condition is a known limitation of VMware. To resolve the problem, register the vCenter in NetBackup and use vCenter credentials for backups and restores. The orphaned VMs starting with `NB_` can be removed from inventory manually by logging into the vCenter using VMware vSphere Client.
- Restore job fails if NetBackup is unable to use the directory that is specified in the `TMP` or `TEMP` environment variable as the staging directory.
- Restore job fails if NetBackup does not have sufficient privileges to the staging directory or if there is insufficient space in the staging directory.
- If you select **Flatten existing directory structure** and **Overwrite existing files** options, you risk an incorrect restore if it contains multiple files with the same file name. In this case, the last file that is restored is the one that is present when the restore completes.
  If you select **Flatten existing directory structure** and you do not select **Overwrite existing files**, the restore succeeds, and the first file that is restored is present when the restore completes. To prevent this issue, do not select

Flatten existing directory structure when restoring multiple files with the same name.

- The **Flatten existing directory structure** and **Append string to file names** options are only applicable to files. They are not available for directories.
- Multiple restore jobs to the same VM are not supported. The user must start another job as needed for that VM once the first restore job for that VM has completed.
- If a backup and a restore occur simultaneously on the same VM, one or both jobs can have unexpected results. If a backup or a restore exits with a non-zero NetBackup Status Code, one possible cause is simultaneous jobs occurring on the same VM.
- Veritas does not recommend VMware agentless restore if a NetBackup client already exists on the target VM. The NetBackup administrator must use the agent based restore in such cases.
- NetBackup supports the following platforms as the guest operating systems for the target VM:
  - Windows 2012, 2012R2, 2016
  - Red Hat Enterprise Linux (RHEL) 6.8, 7
  - SuSE Linux (SLES) 11, 12

Recover files and folders with VMware agentless restore

To restore VMware files and folders using agentless restore

1. Confirm the target VM is powered on.
2. On the left side of the Web UI, click **VMware**.
3. Locate and click on the VM that contains the files and folders for restore.
4. Click the **Recovery points** tab. In the calendar view, click the date on which the backup occurred.

   The available images are listed in rows with the backup timestamp for each image.
5. On the image you want to recover from, click **Restore files and folders**.
6. Under **Select files**, specify the files and folders you want recovered then click **Next**.

7 Under **Recovery target**, specify the target VM to which you want the files and folders recovered, as well as the administrator credentials for the target VM.

8 On **Recovery options**, specify additional recovery options for the restored files and folders.

9 After you click **Next**, NetBackup performs a pre-recovery check using the options you specified.

10 **Review** displays the status of the pre-recovery check along with the options you selected for the recovery. Once you confirm that they are correct, proceed with the restore.

About restricted restore mode

The restricted restore mode option is a form of VMware agentless restore for restricted environments such as Windows User Account Control (UAC). The user-selected files are first staged to the recovery host and then restored to the virtual machine. The recovery host must have sufficient space for staging.

The default staging location on the recovery host is *install_path*\VERITAS\NetBackup\var\tmp\staging. NetBackup creates this directory with the correct permissions the first time it is accessed. You can change the staging location with the AGENTLESS_RHOST_STAGING_PATH registry setting on the recovery host. This REG_SZ registry key does not exist by default. It must be created in HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Config.

If you change the staging location, Veritas recommends that you let NetBackup create the staging directory. When you let NetBackup create the directory, the permissions are set correctly. For NetBackup to create the new staging directory, the immediate parent directory must exist. If you want the restore to use E:\recovery\staging, then E:\recovery must exist. If the E:\recovery directory does not exist, the restore fails.

If you create the directory yourself, the **SYSTEM**, the domain administrator, and the local administrator accounts must have **Full Control** permissions. Additionally, Access Control Lists inherited from the parent directory are not secure and must be disabled.

Restricted restore mode supports alternate location restores. You can configure the alternate location in the NetBackup web UI.

Limitations of restricted restore mode:

- Restricted restore mode is currently only supported on Windows. The recovery host must also be Windows.

- The file ownership of the restored files is set to the account that was used for the NetBackup backup operation.
- Restore of ACLs is not supported.
- Restricted restore mode does not support renaming of targets for soft links.
- Restricted restore mode creates new files where hard links had previously been used.
- Irregular files such as sparse files, device files, special files, and junction points are not supported.
- A supported version of VMware Tools must be running for the restore to succeed.
- File path length with the directory cannot exceed 260 characters.

Performance considerations

File transport through the required infrastructure for this restore method is significantly slower than VMware agentless restores. As a result of performance concerns, Veritas recommends limiting the restore to fewer than 100 files and less than 1 GB of data.

Chapter 7

Troubleshooting VMware operations

This chapter includes the following topics:

Errors when adding VMware servers

Table 7-1 Errors adding VMware servers

Error message or cause	Explanation and recommended action
Virtualization server credential validation fails.	This error occurs when the NetBackup master server is in a DNAT or a similar setup can access only a few specified NetBackup hosts (`PROXY_SERVERS`). The credentials validation occurs in the following order: ■ The auto-discovered discovery host is used to access the virtualization server. ■ If the autodiscovery does not find any information about the virtualization server on the discovery host, the NetBackup master server is used. Workaround: When you add the virtualization server credentials, select the proxy server that has access to the virtualization server as the backup host for validation. **Note:** Adding or updating VMware credentials also automatically starts the discovery of the VMware server. When backup host information is provided in the request, it is used to perform validation of credentials as well as for performing the discovery. For discovery, NetBackup 8.1.2 is the minimum version that is supported for a NetBackup media server or client that serves as a backup host. For older versions, backup host credential validation succeeds, but the discovery of VMware servers fails.
`Unable to obtain the list of trusted Certificate Authorities.`	This error might occur when VMware server credentials are added, updated, or validated. It occurs if the environment is configured to enabled communication between NetBackup (master server, media server, or client) and vCenter, ESX, or any other VMware entity using authenticated certificates. Workaround: Ensure that certificates are installed and are valid.

Errors when browsing VMware servers

The following table describes the problems that may occur when you click on a server under **VMware servers**.

Table 7-2 Errors browsing VMware servers

Error message or cause	Explanation and recommended action
No VMs or other objects were discovered for the VMware server.	■ If the server was added recently, the VM discovery process for that server may not have completed yet. Recommended action: Wait for the discovery process to finish. **Note:** The discovery of VMs and other objects in the vCenter or ESXi server begins when server credentials are added or updated through the web UI or an API. However, the server's VMs and other objects might not appear in the UI immediately. They appear after the discovery process for the VMware server completes. Discovery also occurs at set intervals according to the `VMWARE_AUTODISCOVERY_INTERVAL` option. (The default interval is every 8 hours.) To perform autodiscovery of VMware server objects at a different frequency: See "VMWARE_AUTODISCOVERY_INTERVAL option for NetBackup servers" on page 26. ■ VMs or other objects of the VMware server may not be accessible for the added VMware server credentials. Recommended action: From the option menu on the right of the row, select **Edit**. Review the VMware server credentials and correct them as needed.

Errors for the Status for a newly discovered VM

The following table describes a problem that may occur when you review the status of a newly discovered VM under **Virtual machines**.

Table 7-3 Errors encountered when you review Status for a newly discovered VM

Error message or cause	Explanation and recommended action
The protection status of a VM indicates that it has not been backed up. However, a backup job that includes the VM has successfully completed.	In the NetBackup web UI, the protection status for a newly discovered VM does not indicate that it is backed up until the next backup of the VM has completed. In some circumstances, a new VM is backed up before the discovery of that VM has happened, as in the following scenario: ■ By default, autodiscovery occurs every 8 hours. ■ A new VM is added to the environment. ■ A backup job completes successfully before discovery completes. For example, a backup job that uses existing policies where the new VM is included as part of the backup selection criteria. ■ Later, discovery completes. However, in the NetBackup web UI, the protection status of the VM indicates that it has not been backed up. If you encounter a similar situation, you can still browse the recovery points and recover them. However, it is only after another backup of the VM successfully completes that the protection status indicates that the VM has been backed up. To review the protection status of a newly discovered VM in the NetBackup web UI, Veritas recommends that you wait until the next successful backup has completed. Then, the protection status of the VM should correctly indicate its protection status.

Error when downloading files from an instant access VM

The following table describes the problems that may occur when you download individual files from an instant access VM.

Table 7-4 Errors in downloading files

Error message or cause	Explanation and recommended action

Chrome: `This site can't be reached`
Firefox: `Server not found`
Edge: `Hmmm…can't reach this page`
	This error can occur for any of the following reasons:
	■ The web UI is unable to access the NetBackup media server with the name or IP address that the NetBackup master server uses to connect to that media server.
	For example: If the master server connects to the media server using `MSserver1.veritas.com`, the web UI must also be able to reach `MSserver1.veritas.com`. If the master server uses a short name for the media server such as `MSserver1`, the web UI must be able to reach `https://MSserver1/...`
	Recommended action: Verify that the master server and the web UI use the same name or IP address to access the media server (check the `hosts` file). For example: If the master server uses the media server's short name, add the media server's short name and IP address to the `hosts` file of the PC or other host where the web UI is running.
	The hosts file location on Windows:
	`C:\Windows\System32\drivers\etc\hosts`
	The hosts file location on UNIX or Linux:
	`/etc/hosts`
	■ The web UI is unable to access the NetBackup media server because that server is behind a firewall.
	Recommended action: Contact the NetBackup security administrator.

Troubleshooting backups and restores of excluded virtual disks

Refer to the following table if you encounter restore issues for a backup that was configured to exclude virtual disks.

Table 7-5 Issues with excluding virtual disks

Issue	Explanation
The boot disk was backed up even though it was excluded from the backup.	The virtual machine only has a boot disk and no other disks.
	The boot disk is part of a managed volume (Windows LDM or Linux LVM). NetBackup can only exclude a boot disk if it is fully contained on a single disk.
	The virtual machine's boot disk is an independent disk and has no other disks.
	NetBackup was not able to identify the boot disk. The boot disk must include the boot partition and the system or the boot directory.
A restored boot disk has no data.	The boot disk is an independent disk. NetBackup cannot back up the data in this type of disk.
A restored virtual machine has a disk that contains missing or incomplete data.	The disk that has missing or incomplete data was excluded from the backup.
A data disk (or disks) was backed up even though it was excluded from the backup.	The virtual machine has only one disk (such as C:). In this case, the single drive is backed up and is not excluded.
A virtual machine is restored to an unexpected state.	You added a disk to the virtual machine and changed the settings that exclude disks. However, you did not create a backup of the entire virtual machine after you made the change.
Not all files can be restored individually.	If you remove disks from the custom attribute value between the differential backups, only those files that changed since the last backup can be restored individually. Alternatively, you can restore the entire virtual disk or the VM. After the next full backup, you can restore any of the files individually.
	If you remove controllers from **Specific disks to be excluded** between the differential backups, only those files that changed since the last backup are available for restore. All files are available for restore after the next full backup.

Restore fails for a virtual machine with multiple datastores

Table 7-6 Issues with restores of a virtual machine with multiple datastores

Issue	Explanation
Restore fails because the datastore did not have enough space for the `.vmdk` files.	This issue can occur when a virtual machine is configured on multiple datastores and a leftover snapshot existed on the virtual machine when it was backed up. NetBackup tries to restore all `.vmdk` files to the snapshot datastore. Alternatively, you can restore the virtual machine to an alternate location.

Errors when you change the recovery destination

Table 7-7 Errors encountered when you change the recovery destination

Issue	Explanation
Cannot see the list of vCenter servers	If you are not able to see the list of the vCenter servers, you might not have access to the vCenter servers under the **Application Servers** object group property in RBAC. Recommended action: Contact the NetBackup security administrator.