NetBackup™ Web UI VMware Administrator's Guide

Release 8.1.2

VERITAS™

NetBackup Web UI VMware Administrator's Guide

Last updated: 2018-09-17

Document version: NetBackup 8.1.2

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

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 user interface

NetBackup 8.1.2 introduces a new web user interface that 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.
- 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 that are related to security, backup management, or workload protection.
- NetBackup security administrators can manage NetBackup security, certificate management, and RBAC.
- Backup administrators provide protection services to satisfy their service level objectives (SLOs). Protection of assets is achieved through protection plans, job management, and visibility of the protection status of assets.

- Workload administrators can subscribe assets to the protection plans that meet the SLO, monitor protection status, and perform self-service recovery of virtual machines. In NetBackup 8.1.2, workload administrators can manage and configure VMware and cloud workloads.
- Usage reporting tracks the size of backup data on your master servers. You can also easily connect to Veritas Smart Meter to view and manage NetBackup licensing.

Access control in the NetBackup web UI

NetBackup uses role-based access control to grant access to the web UI. This access control includes the tasks a user can perform and the assets the user can view and manage. Access control is accomplished through access rules.

- Access rules associate a user or a user group with a role and an object group. The role defines the permissions a user has. An object group defines the assets and NetBackup objects a user can access. Multiple access rules can be created for a single user or group, allowing for full and flexible customization of user access.
- NetBackup comes with three default roles. Choose the role that best fits a user's needs or create a custom role to meet the requirements for that user.
- Use object groups to define groups of assets or application servers or to indicate the protection plans that users can view or manage. For example, you can grant access for VMware administrators by creating an object group with specific VMware application servers. Also add to the object group the specific protection plans that the VMware administrator can choose to protect VMware assets.
- 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). Users that are configured with EA have full permissions for the web UI and APIs. You cannot use the web UI if you have NetBackup Access Control (NBAC) enabled.

Monitor NetBackup jobs and events

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

- For a NetBackup security administrator, the dashboard lets the administrator see the status of security certificates and of audit events.
- For a backup administrator, the dashboard allows the administrator to see the status of NetBackup jobs. Email notifications can also be configured so they 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.
- You can easily choose either on-premises or snapshot storage.
- When you select from your available storage, you can see any additional features available for that storage. For example, NetBackup Accelerator or Instant Access for backup storage. For long-term storage, the cloud provider, CloudCatalyst, Encryption, or Compression.
- The protection plan wizard helps you select storage for backups, replication, or long-term storage based on the supported storage that is already configured.
- The backup administrator creates and manages protection plans and is therefore responsible for backup schedules and storage.
- The workload administrator primarily selects the protection plans to use to protect assets or asset groups. However, the backup administrator can also subscribe assets to protection plans if needed.

Self-service recovery

The NetBackup web UI makes it easy to recover VMs. You can also use the instant access feature to mount a VM's snapshot for immediate access to its files: you can download the file to your local host or restore the file to its original VM.

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
Access rule	For RBAC, defines a user or a user group, the role or permissions, and the object group that the user or the user group can access. A user or group can have multiple access rules.

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

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*.
Asset	The data to be protected, such as physical clients, virtual machines, and database applications.
Classic policy	In the NetBackup web UI, indicates that a legacy policy protects the asset. Legacy policies are created with the NetBackup Administration Console.
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, these groups appear under the tab **Intelligent VM groups**.
Instant access	An instant access VM created from a NetBackup backup image 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.
Object group	For RBAC, a collection of assets, protection plans, servers, and other resources that the user is granted access to.
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.

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

Term	Definition
RBAC	Role-based access control. Administrators can delegate or limit access to the NetBackup web UI through the access rules that are configured in RBAC. **Note:** The rules that you configure in RBAC do not control access to the NetBackup Administration Console or the CLIs. The web UI is not supported with NetBackup Access Control (NBAC) and cannot be used if NBAC is enabled.
Role	For RBAC, defines the permissions that a user can have. NetBackup has three system-defined roles that allow a user to manage security, protection plans and backups, or to manage workload assets.
Storage	The storage to which the data is backed up, replicated, or duplicated (for long-term retention). Snapshot storage is used for Cloud workloads.
Subscribe, to a protection plan	The action of associating an asset or an asset group with a protection plan. The asset is then protected according to the schedule and the storage settings in the plan. The web UI also refers to *Subscribe* as *Configure protection*. *Unsubscribe* refers to the action of removing an asset from a plan.
Workload	The type of asset. For example, VMware or Cloud.
Workflow	An end-to-end process that can be completed using the NetBackup web UI. For example, you can protect and recover VMware and Cloud assets in NetBackup 8.1.2.

Sign in to a NetBackup master server from the web UI

Users can sign in to a NetBackup master server from a web browser through the NetBackup web UI. For details on supported browsers for the web UI, see the NetBackup Software Compatibility List.

Users must be root or an administrator or have a role that is configured for them in NetBackup RBAC.

To sign in to a NetBackup master server using the NetBackup web UI

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*	**root**
Domain user	*DOMAIN\username*	**WINDOWS\Administrator**

Chapter 2

Managing VMware assets

This chapter includes the following topics:

Add VMware servers

You can add VMware servers and their credentials.

Note: This procedure requires the backup administrator role.

To add VMware servers and their credentials

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

   The tab shows the vCenters and ESXi servers that you can access.

2. Click **+ Add** to add a server, then select the server type and enter its host name and credentials.

   Caution: Make sure to enter the VMware server name and credentials correctly. The NetBackup web UI does not validate the server's host name or credentials. If the server name or credentials are not correct, the web UI cannot perform the operations that require access to the server.

3. Click **Save**.

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

   Important!

   The discovery of VMs and other objects in the vCenter or ESXi server occurs at set intervals according to the `VMWARE_AUTODISCOVERY_INTERVAL` option (the default is 8 hours). Depending on that interval, the server's VMs and other objects may not appear immediately after the server has been added. To discover the VMs and other objects immediately, restart the NetBackup discovery service as explained in the following topic:

   See "Errors encountered when browsing VMware servers" on page 28.

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 **Servers** to begin searching.

   The list includes the vCenters and standalone ESXi servers that you have access to.

   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 **Configure protection** to subscribe the VM to a plan.

Remove VMware servers

VMware servers can be removed by means of the NetBackup Administration Console. Contact the NetBackup administrator.

Create an intelligent VM group

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

Note: This procedure requires the backup administrator role.

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. Click **Add vCenter or standalone ESXi server**.

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

   ---

5 Select the appropriate server and click **Save**.

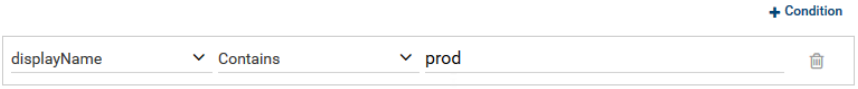
6 Under **Create query for virtual machines**, you can do one of the following:

- Select the default query: **Include all VMs in this server**.
  When the protection plan runs, all VMs that currently reside in the vCenter or ESXi are selected for backup.
- Create your own query: Click **Add condition**.

7 To add a condition, use the drop-downs to select a keyword and operator and then enter a value.

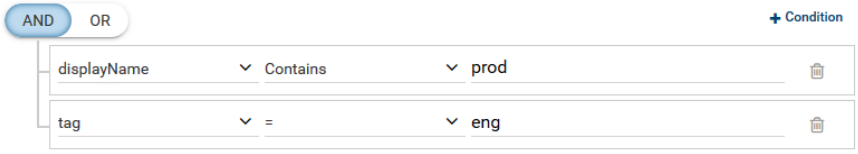
The options are described after this procedure: Query options for creating intelligent VM groups.

The following is an example query:



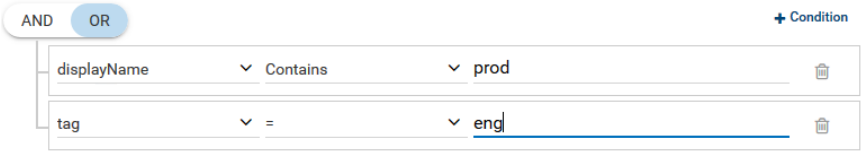
In this example, the query adds to the group any VM that has `prod` in its display name.

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).

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

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

Note: The discovery of VMs in the VMware server occurs at set intervals according to the VMWARE_AUTODISCOVERY_INTERVAL option (the default is 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. To discover the VMs immediately, restart the NetBackup discovery service as explained in the following topic:

See "Errors encountered when browsing VMware servers" on page 28.

---

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

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

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

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

Query options for creating intelligent VM groups

Table 2-1 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.
`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 2-2 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`.

Table 2-2 Query operators *(continued)*

Operator	Description
`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.

Note: This procedure requires the backup administrator role.

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, click its box and click **Delete**.
4. If the group is protected, click on the group, scroll down and click the lock symbol, and click **Unsubscribe**.
5. Click **Remove**.

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 following requirements:

- You must have access to the VMs by means of the appropriate role-based access control (RBAC) that the NetBackup security administrator assigned to you.
- You must have access to the protection plans that the backup administrator has granted you access to (by means of RBAC).
- The appropriate services on the master server must be running and the web UI must be accessible.
  For assistance, contact the backup administrator.

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 VM group and click **Configure protection**.
3. Click on a protection plan and review its details on the right.

   For VMware administrators, RBAC permissions determine which protection plans are listed. For a description of the available protection plan options, see the *NetBackup Web UI Backup Administrator's Guide*, available here:

   http://www.veritas.com/docs/000003214
4. To subscribe the VM or VM group to the selected plan, click **Protect**.

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

Note: To perform an on-demand (manual) backup of a VM, contact the NetBackup administrator. To perform an on-demand backup requires access to the NetBackup Administration Console.

View the protection status of VMs or intelligent VM groups

You can view the current protection plans that VMs or VM groups are subscribed to.

To view the protection status of VMs or VM groups

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

   For a VM, the **Protection** tab shows the details of the plans that the asset is subscribed to.
3. For more details on the protected VM, click **more...**.
4. If the asset is not protected, click its box and click **Configure protection** to subscribe it to a plan.

   See "Protect VMs or intelligent VM groups" on page 17.

Remove protection from VMs or intelligent VM groups

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

To remove protection from a VM or intelligent VM group

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

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

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 instant access feature is supported only for NetBackup appliances. This feature requires that the NetBackup backup image is stored on a Media Server Deduplication Pool (MSDP) storage device. For additional notes and limitations on using instant access VMs:

See "Things to consider before you use the instant access feature" on page 22.

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 you want to recover, 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.

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.

Recover individual files from an instant access VM

You can browse an instant access image of the VM to recover individual files.

Note: For notes and limitations on using instant access VMs:

See "Things to consider before you use the instant access feature" on page 22.

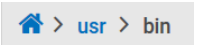
To recover an individual file from an instant access VM

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 you want to recover from, click **Recover > Browse files for single file recovery**.

   NetBackup creates an instant access mount point in the background.
5. Select a single file (not a folder or multiple files).

   Click on a folder to drill into it. Use the home icon to navigate back to higher levels in the hierarchy. For example:

6. Select the recovery method:
   - Click **Download** to download the file to your local host.
     At the prompt, accept the SSL certificate that the NetBackup Appliance web server uses. If your company uses third-party SSL certificates, you can deploy the corresponding root CA SSL certificate to your environment. If you do so, acceptance of the certificate is no longer required.

     Note: The web UI must be able to access the NetBackup media server with the same name or IP address that the NetBackup master server uses to connect to that media server.

     See "Error encountered when downloading files from an instant access VM" on page 29.

- Click **Restore** to restore the file to its original VM.
  Enter the user name and password for the VM and the destination path in the VM (the default is the original file path).

  Note: The web UI does not currently support restoring the file to a different VM or to a different VMware server.

7 Click **Restore**.

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. Classic policies that are created with the NetBackup Administration Console also support instant access when the policy uses the VM instance UUID as the **Primary VM identifier**.
- This feature supports only the **VMware** policy type in NetBackup. For the policy types that the web UI protection plans use, contact the backup administrator.
- This feature is supported only for NetBackup appliances.
- 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/support/en_US/article.000081966

- This feature does not support VMs that have disks that were excluded from the backup. On the NetBackup policy's **Exclude Disks** tab, the **No disks excluded** option must be selected.
- 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 single file restore, LDM volumes and the ReFS file system are not supported, and the Access Control Lists (ACLs) are not preserved.
- 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.
- This feature supports single file restore of file sizes up to 1 GB. For larger files, you can use the **Download** option, or start the VM and copy the required file.
- For single-file 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 encountered when downloading files from an instant access VM" on page 29.
- 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:
  http://www.veritas.com/docs/000003214

Recover a VM to the original location

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

To recover a VM to its original location

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, 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 you want to recover, click **Recover > To original location**.
5. Review or change the following options:

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 recovery	Automatically powers on the VM when the recovery is complete.

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.
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	Enable this option to restore 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**.

6 Click **Start recovery**.

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

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

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

Recover a VM to an alternate location

You can recover a VM to a location other than where it existed when it was backed up.

To recover a VM to an alternate location

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, 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 you want to recover, click **Recover > To alternate location**.

5 Review or change the following options:

Restore to:

- Lists the new VM display name appended with `_copy`.
- Lists the ESXi server or cluster and other destination details. The defaults are from the original VM image. Click **Change** to make different selections.

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 recovery	Automatically powers on the VM when the recovery is complete.

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.
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	Enable this option to restore 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**.

6 Click **Start recovery**.

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

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

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

Errors encountered when browsing VMware servers

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

Table 2-3 Errors browsing VMware servers

Error message or cause	Explanation and recommended action

VM discovery not yet initiated for the VMware server, or the server name is invalid.	■ The vCenter server or ESXi server name or credentials may have been entered incorrectly.
	Recommended action: In the NetBackup Administration Console, click **Media and Device Management > Credentials > Virtual Machine Servers** to verify the server name and credentials and correct them as needed.
	■ If the server was added recently, the VM discovery process for that server may not have occurred yet.
	Recommended action: Stop and restart the discovery service on the NetBackup master server, as follows:
	Note: This procedure requires administrator privilege on the NetBackup master server. For assistance, contact the NetBackup administrator.
	Windows
	Stop the service:
	`install_path\bin\bpdown.exe -e "NetBackup Discovery Framework" -f -v`
	Restart the service:
	`install_path\bin\bpup.exe -e "NetBackup Discovery Framework" -f -v`
	Unix or Linux
	Stop the service:
	`usr/openv/netbackup/bin/nbdisco -terminate`
	Restart the service:
	`usr/openv/netbackup/bin/nbdisco`
	Note: The discovery of VMs in the vCenter or ESXi server occurs at set intervals according to the `VMWARE_AUTODISCOVERY_INTERVAL` option (the default is 8 hours). The following topic explains how to change that interval:
	See "VMWARE_AUTODISCOVERY_INTERVAL option for NetBackup servers" on page 29.

Error encountered 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 2-4 Errors in downloading files

Error message or cause	Explanation and recommended action

`This site can't be reached`
(Chrome)
`Server not found`
(Firefox)
`Hmmm…can't reach this page`
(Edge)
	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.

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.

Table 2-5 VMWARE_AUTODISCOVERY_INTERVAL information

Usage	Description
Where to use	On NetBackup master servers.

Table 2-5 VMWARE_AUTODISCOVERY_INTERVAL information *(continued)*

Usage	Description

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.
	The default is 8 hours. The minimum is 5 minutes, the maximum 1 year.
	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.