

NetBackup™ Web UI Cloud Administrator's Guide

Release 8.2

NetBackup Web UI Cloud Administrator's Guide

Last updated: 2019-06-28

Legal Notice

Copyright © 2019 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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	
		5
	About the NetBackup web user interface	5
	Terminology	7
	Sign in to the NetBackup web UI	9
Chapter 2	Managing cloud assets	11
	About protecting cloud assets	11
	Limitations and considerations	13
	Registering the CloudPoint server with NetBackup	14
	Configurations for a cloud provider	15
	IAM Role for AWS Configuration	16
	Configure snapshot replication	16
	Protecting applications in-cloud with application consistent snapshots	
		18
	Configuring cloud asset discovery interval	20
	Recovering a cloud asset to its original location	21
	Recovering a cloud asset to an alternate location	22
	Perform rollback recovery of cloud assets	22
	Troubleshooting cloud workload protection issues	23

Introducing the NetBackup web user interface

This chapter includes the following topics:

- [About the NetBackup web user interface](#)
- [Terminology](#)
- [Sign in to the NetBackup web UI](#)

About the NetBackup web user interface

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](#).
- 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, certificates, RBAC, API keys, user sessions, and locked NetBackup user accounts.
- 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. The web UI supports the following workloads:
 - Cloud
 - Red Hat Virtualization (RHV)
 - VMware
- 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). 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.
- 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 intelligent 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. For VMware 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 <i>NetBackup Web UI</i> guides, the term <i>NetBackup administrator</i> also refers to a user that has full permissions for NetBackup, usually in reference to a user of the NetBackup Administration Console. Also see <i>Role</i>.
Asset group	See <i>intelligent group</i> .
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.
External certificate	A security certificate 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.
Object group	For RBAC, a collection of assets, protection plans, servers, and other resources that the user is granted access to.
NetBackup certificate	A security certificate 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.

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 selecting a protection plan to protect an asset or an asset group. The asset is then protected according to the schedule and the storage settings in the plan. The web UI also refers to <i>Subscribe</i> as <i>Add protection</i>.
Unsubscribe, from a protection plan	<i>Unsubscribe</i> 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.
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 beginning with NetBackup 8.1.2.

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 user name and password](#)
- [Sign in with a certificate or smart card](#)

Sign in with a user name and password

You can sign in to NetBackup web UI if you are an authorized user. Contact your NetBackup security administrator for more information.

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	<i>username</i>	root
Domain user	<i>DOMAIN\username</i>	WINDOWS\Administrator

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.

Managing cloud assets

This chapter includes the following topics:

- [About protecting cloud assets](#)
- [Limitations and considerations](#)
- [Registering the CloudPoint server with NetBackup](#)
- [Configurations for a cloud provider](#)
- [Configure snapshot replication](#)
- [Protecting applications in-cloud with application consistent snapshots](#)
- [Configuring cloud asset discovery interval](#)
- [Recovering a cloud asset to its original location](#)
- [Recovering a cloud asset to an alternate location](#)
- [Perform rollback recovery of cloud assets](#)
- [Troubleshooting cloud workload protection issues](#)

About protecting cloud assets

Using NetBackup, you can now protect your in-cloud workloads. The cloud data protection framework leverages the CloudPoint infrastructure to drive faster proliferation of cloud providers.

The following table describes the tasks.

Table 2-1 Configuring protection for cloud assets

Task	Description
Before you begin ensure that you have the appropriate permission.	To manage and protect cloud assets in the web UI you must have the workload administrator role or similar permissions. Contact the NetBackup security administrator. See the NetBackup Web UI Security Administrator's Guide Note: For managing hosted applications, you need Manage Assets and Manage Protection Plans permissions.
Deploy CloudPoint	Install CloudPoint in your environment. See the Veritas CloudPoint Administrator's Guide. Review CloudPoint and NetBackup limitations. See "Limitations and considerations" on page 13.
Configure the CloudPoint server using the NetBackup Administration Console	Register the CloudPoint server in NetBackup. See "Registering the CloudPoint server with NetBackup" on page 14.
Add a configuration	All the supported cloud providers are displayed in the web UI. You need to add the cloud account (configure the cloud plug-in) for the cloud provider you need. You can create multiple configurations for each provider. See "Configurations for a cloud provider" on page 15. For Amazon, you can choose to use IAM role. See "IAM Role for AWS Configuration" on page 16.
Asset discovery	NetBackup retrieves the cloud assets pertaining to the cloud accounts that are configured in NetBackup. Assets are populated in NetBackup asset DB. By default, asset discovery happens every 4 hours and is configurable. In case of applications, you can set discovery interval between 15 minutes to 45 minutes. See "Configuring cloud asset discovery interval" on page 20.

Table 2-1 Configuring protection for cloud assets (*continued*)

Task	Description
Create a snapshot only protection plan	Create a snapshot only protection plan. A protection plan is used to schedule backup start windows. See the NetBackup Web UI Backup Administrator's Guide. You can also configure the protection plan for snapshot replication. See "Configure snapshot replication" on page 16.
Choose to protect a virtual machine, application, or volume	For each cloud provider, a list of discovered assets is displayed. Add the assets to a protection plan. See the NetBackup Web UI Backup Administrator's Guide. You can also choose to protect application using application consistent snapshots. See "Protecting applications in-cloud with application consistent snapshots" on page 18.
Recover cloud assets	■ You can recover the assets using the recovery points. See "Recovering a cloud asset to its original location" on page 21. See "Recovering a cloud asset to an alternate location" on page 22. See "Perform rollback recovery of cloud assets " on page 22. ■ You can also restore the assets using the <code>nbccloudrestore</code> CLI utility. Note: Do not use the <code>bprestore</code> CLI for restores See the NetBackup Commands Reference Guide.
Troubleshooting	See "Troubleshooting cloud workload protection issues" on page 23.

Limitations and considerations

Consider the following when protecting cloud workloads

- Deletion of CloudPoint host entry and its associated plug-ins is not supported in NetBackup.
If you delete plug-ins that are configured in NetBackup, you cannot recover any CloudPoint images that are associated with that plug-in.

- Review the *Veritas CloudPoint Administrator's Guide* for information on the capabilities of CloudPoint.
- NetBackup integration is not supported with the CloudPoint freemium version.
- If you have a previous installation of CloudPoint, Veritas recommends that you upgrade the CloudPoint server and not reinstall it.
If you do reinstall the CloudPoint server, you need to reconfigure the CloudPoint server and perform all the protection-related steps.
- When you configure a CloudPoint server using port 0, the default value is used.
- When a snapshot or a restore job fails, you need to clean up data manually on the target destination in the cloud.
- For CloudPoint server, enhanced auditing is not supported. Thus, when you add or update a CloudPoint server, with non-root but NetBackupAdmin rights, during auditing the user is shown as root.

Registering the CloudPoint server with NetBackup

You can register the CloudPoint server using one of the following ways:

- Using the NetBackup Administration Console.
See the [NetBackup Snapshot Client Administrator's Guide](#).
- Using the `-tpconfig` command.

```
tpconfig -add -cloudpoint_server cloudpoint_server_name  
-cloudpoint_server_user_id user_ID [-requiredport IP_port_number]
```


See the [NetBackup Commands Reference Guide](#).

When you configure a CloudPoint server with NetBackup:

- You can associate a specific NetBackup media server with the CloudPoint server.
Media server association is supported only using the `tpconfig` command line.

```
tpconfig -update -cloudpoint_server cloudpoint_server_name  
-add_media_server media_server
```


To associate multiple media servers, you must run the command multiple times. The media server must be on version 8.1.2 or later. If you do not associate a media server, the NetBackup master server is used.
- When you configure a cloud plug-in, ensure that the region is not overlapping with any other plug-in across all the CloudPoint servers that are registered with the master server.

Configurations for a cloud provider

All the cloud providers that are supported by NetBackup are displayed in the NetBackup web UI. You need to add the cloud account (configure the cloud plug-in) for the cloud provider you need. You can create multiple configurations for each provider.

To add a configuration for a Cloud Provider

- 1 On the left, click **Cloud**.
- 2 Click on the **Providers** tab.
The cloud providers that are supported by NetBackup are displayed.
- 3 Click **Add** under the cloud provider for which you want to add a configuration.
- 4 Enter the connection and authentication details in the **Add Configuration** pane.
- 5 Click **Save**.

To edit a configuration for a Cloud Provider

- 1 On the left, click **Cloud**.
- 2 Click on the **Providers** tab.
The cloud providers that are supported by NetBackup are displayed
- 3 Click **configuration** under the cloud provider for which you want to update a configuration.
- 4 From the list, double-click on the configuration you want to update.
- 5 Update the connection and authentication details in the **Add Configuration** pane.
- 6 Click **Save**.

To disable a configuration for Cloud Provider

- 1 On the left, click **Cloud**.
- 2 Click on the **Providers** tab. The supported cloud providers are displayed.
- 3 Click **configuration** under the cloud provider for which you want to disable a configuration.
- 4 From the list, select the configuration you want to delete.
- 5 Click **Disable**.

IAM Role for AWS Configuration

If the snapshot management server (CloudPoint) is deployed in cloud, AWS configuration can be configured to use IAM role for authentication. See [“Configurations for a cloud provider”](#) on page 15.

Before proceeding, ensure the following:

- IAM role is configured within AWS. See the [Veritas CloudPoint documentation](#) for details.
- After you upgrade NetBackup and CloudPoint to the latest version, you need to update the credentials. Run the `tpconfig -update` command.

Note: Post upgrade, credentials are updated to support only IAM role.

The following implementations of IAM role are supported:

- Source account: In this case, the cloud assets that need to be protected are in the same AWS account as CloudPoint. Thus, AWS cloud is aware of the AWS account ID and role name, you need to only select the region.
- Cross account: In this case, the cloud assets that need to be protected are in a different AWS account than CloudPoint. Thus, you need to enter the target account and the target role name details along with the region so that CloudPoint can access those assets. See the [Veritas CloudPoint documentation](#) for details. You need to establish a trust relationship between the source and the target account. For more details, refer to the *Across AWS Accounts Using IAM Roles* related information in the *Amazon Web Services* documentation.

Configure snapshot replication

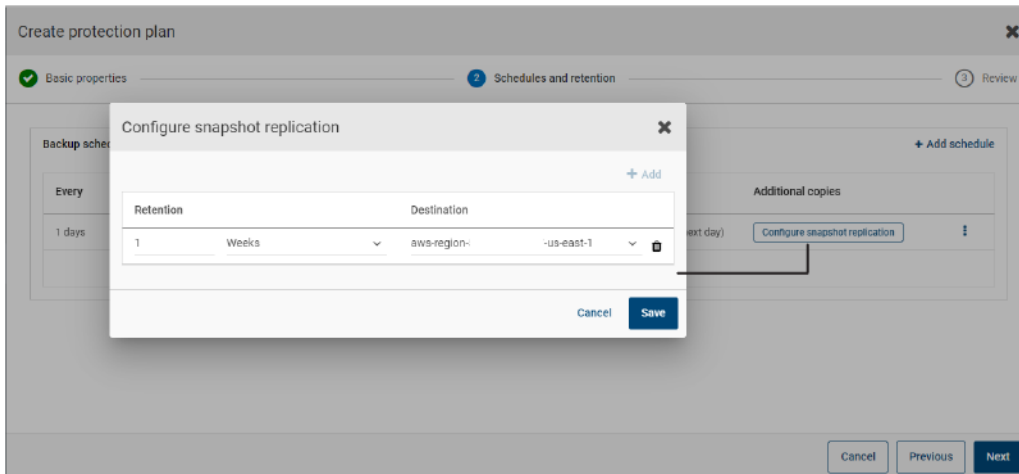
You can choose to replicate snapshots cloud assets from the primary location to a remote or a secondary location. The snapshot management servers (CloudPoint) support cross-region and cross account replication. With snapshot replication you can achieve the following:

- Maintain a copy of cloud assets at a different destination for long-term retention and auditing requirements.
- Recover cloud assets from the replicated copies from another region in case there is a region outage.
- Recover cloud assets from the replicated copies from another account in case the user account is compromised.

Configuration

Review the following information to configure snapshot replication:

- You can configure snapshot replication when you create a protection plan. See the [NetBackup™ Web UI Backup Administrator's Guide](#).



- For cross account replication, you need to establish a trust relationship between the source and the target account. For more details, refer to the *Across AWS Accounts Using IAM Roles* related information in the *Amazon Web Services* documentation.

Considerations

Consider the following when you configure cloud snapshot replication:

- In a single protection plan, replication to only one destination region is supported.
- Even if multiple schedules are configured, the replication destination region that is configured is applied to all the schedules.
- Cloud snapshot replication is supported only for Amazon cloud providers.

Asset protection criteria

Consider the following before adding cloud assets to a protection plan that is configured for cloud snapshot replication:

- Assets must be added to a protection plan that replicates snapshots to a different region.

For example, assets residing in region 'aws_account_1-us-east-1' cannot be subscribed to a protection plan replicating to the same region 'aws_account_1-us-east-1'.

- Assets can be replicated to a different account in the same region.
For example, assets residing in region 'aws_account_1-us-east-1' can be subscribed to a protection plan replicating to the same region but different account 'aws_account_2-us-east-1'.
- Assets that are discovered by a snapshot management server must be replicated to the region that is discovered by the same snapshot management server.
For example, assets that are discovered by snapshot management server 'CP1' cannot be subscribed to a protection plan replicating to a region that is discovered by snapshot management server 'CP2'.
- Only Amazon assets can be subscribed to a protection plan that is configured for cloud snapshot replication.

Managing concurrent snapshots replications

For better performance, you can tune the number of concurrent snapshot replications. Amazon has different limits for each asset type to do concurrent snapshot replications to a single destination region. For example, RDS has a limit for 5, EBS has a limit for 5, and EC2 has a limit for 50. For more details refer to *Copy Snapshot* related information in the *Amazon Web Services* documentation.

In NetBackup this limit is defined using the following parameter in the `bp.conf` file:

```
MAX_CLOUD_SNAPSHOT_REPLICATION_JOBS_PER_DESTINATION
```

The default value is 5.

Protecting applications in-cloud with application consistent snapshots

You can take application consistent (point-in-time) snapshots of the applications that are deployed on virtual machines in cloud. This lets you perform a point-in-time recovery of applications.

You can perform original location and alternate location restores for these workloads.

For alternate location restore, consider the following:

- For MongoDB and MS SQL workloads, the alternate location must be discovered but should not be connected or configured.
- For Oracle workloads, the alternate location must be discovered and configured and not connected.

Before you begin

Ensure that the database is prepared for snapshots. For details review the plug-in configuration notes in the [Veritas CloudPoint documentation](#).

To configure applications for point-in-time recovery

- 1 Connect to the virtual machine that hosts the applications.
 - After the cloud assets are discovered, go the **Virtual Machines** tab.
 - Select the virtual machine where the application is hosted. On the top right, click **Connect VM**
 - Enter the credentials.
 - Click **Connect**.
 - After the virtual machines are connected, the virtual machines state is updated to **Configure**.

Note: For Microsoft SQL, you need perform this process manually. See, the Configuring the Windows-based on-host agent topic in the [Veritas CloudPoint documentation](#). After the next discovery cycle, the status of the virtual machine is updated to **Configure**.

- 2 Select the virtual machine where the application is hosted. On the top right, click **Configure application**.
- 3 After the process is complete, the application status is updated to configured.
- 4 The applications are displayed under the **Applications** tab after the next discovery.
- 5 Apply the protection plan. See the [NetBackup™ Web UI Backup Administrator's Guide](#).

To edit or update virtual machine credentials

- 1 Go to the **Virtual Machines** tab.
- 2 Select the virtual machines for which you want to update credentials. On the top right, click **Edit credentials**.
- 3 Update the credentials and click **Connect**.

To edit or update application configuration

- 1 Go to the **Applications** tab.
- 2 Select the application for which you want to update. On the top right, click **Edit configuration**
- 3 Update the credentials and click **Configure**.

Configuring cloud asset discovery interval

Asset discovery interval is the frequency at which the assets are discovered and populated in NetBackup.

Configure cloud asset discovery interval for VMs

By default, asset discovery of VMs happens every 4 hours. This interval represents hours and can be between 1 to 23. The value must be specified in integers.

To configure the cloud asset discovery interval

- 1 Select appropriate configuration option.
 - Windows
You can configure the discovery interval using the `nbsetconfig` command.
For example

```
nbsetconfig nbsetconfig>  
CLOUD_DISCOVERY_INTERVAL = 2
```


The directory path to this command is `install_path\NetBackup\bin\`
See the [NetBackup Commands Reference Guide](#).
 - UNIX
Set the `CLOUD_DISCOVERY_INTERVAL` parameter in the `/usr/opensv/netbackup/bp.conf` file.
- 2 Restart the `nbdisco` service.

Asset discovery is triggered after you restart the service.

Configure cloud asset discovery interval for hosted applications

By default, asset discovery of hosted applications happens every 15 minutes. This interval represents minutes and can be between 15 to 45. The value must be specified in integers.

To configure the cloud asset discovery interval for hosted applications

- 1 Select appropriate configuration option.

- **Windows**
You can configure the discovery interval using the `nbsetconfig` command.
For example

```
nbsetconfig nbsetconfig>
CLOUD_HOSTED_APP_DISCOVERY_INTERVAL = 15.
```

The directory path to this command is `install_path\NetBackup\bin\`
See the [NetBackup Commands Reference Guide](#).
 - **UNIX**
Set the `CLOUD_HOSTED_APP_DISCOVERY_INTERVAL` parameter in the `/usr/openv/netbackup/bp.conf` file.
- 2 Restart the `nbdisco` service.
Asset discovery is triggered after you restart the service.
The hosted application discovery is triggered after the specified interval.

Recovering a cloud asset to its original location

To recover a cloud asset to its original location

- 1 On the left, click **Cloud**.
- 2 Depending on the cloud asset type, click on the **Virtual Machines**, **Applications**, or **Volumes** tab.
All the discovered cloud assets for the respective category are displayed.
- 3 Double-click on the protected asset that you want recover.
- 4 Click the **Recovery points** tab, then 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, click **Recover > Restore to original location**.
- 6 Click **OK**.
- 7 On the left, click **Jobs** to view the job status.

Recovering a cloud asset to an alternate location

Considerations

- Cloud assets for Google Cloud Platform cannot be restored to an alternate location.
- To restore a replicated copy of EC2 instance to an alternate location, the key-pair names must be same on the source and destination region. If not, create a new key-pair in the destination region that is consistent with the key-pair in the source region.

To recover a cloud asset to an alternate location

- 1 On the left, click **Cloud**.
- 2 Depending on the cloud asset type, click on the **Virtual Machines**, **Applications**, or **Volumes** tab.
All the discovered cloud assets for the respective category are displayed.
- 3 Double-click on the protected asset you want recover.
- 4 Click the **Recovery points** tab, and 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, click **Recover > Restore to alternate location**.
- 6 Enter the location where you want to restore the cloud asset.
- 7 Click **Start Recovery**.
- 8 In the left, click **Jobs** to view the job status.

Perform rollback recovery of cloud assets

The rollback recovery of a cloud asset overwrites the existing data on the original asset. Unlike original or alternate location restore, a new copy is not created of the restored image, but the existing data on the source is replaced.

Note: Snapshot replicas cannot be rolled back.

To perform rollback recovery of the cloud asset

- 1 On the left, click **Cloud**.
- 2 For supported cloud asset type, click on the **Virtual Machines**.
All the discovered cloud assets for the respective category are displayed.
- 3 Double-click on the protected asset you want to recover.
- 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, click **Recover > Rollback**.
- 6 Click **Start recovery**. The existing data is overwritten.
- 7 On the left, click **Jobs** to view the job status.

Troubleshooting cloud workload protection issues

Review the following log files to troubleshoot any issues with protection of cloud assets:

- [Log files for configuration](#)
- [Log files for snapshot creation](#)
- [Log files for restore operations](#)
- [Log files for snapshot deletion](#)

During troubleshooting, ensure that you have also reviewed the limitations. See [“Limitations and considerations”](#) on page 13.

For troubleshooting issues, see the [NetBackup Status Codes Reference Guide](#).

Log files for configuration

Use the following logs to troubleshoot cloud configuration issues.

Table 2-2 Log files for configuration

Process	Logs
tpconfig tpconfig command is one way for registering CloudPoint in NetBackup.	Windows <i>NetBackup install path/volmgr/debug/tpcommand</i> UNIX <i>/usr/opensv/volmgr/debug/tpcommand</i>
nbwebservice Plug-ins are configured using NetBackup REST API.	Windows <i>NetBackup install path/webserver/logs</i> UNIX <i>/usr/opensv/wmc/webserver/logs</i> <i>/usr/opensv/logs/nbwebservices</i>
nbemm nbemm stores the CloudPoint server and plug-in information in EMM database	Windows <i>NetBackup install path/bin/vxlogview -o 111</i> UNIX <i>/usr/opensv/netbackup/bin/vxlogview -o 111</i>

Log files for asset discovery

Use the following logs to troubleshoot asset discovery issues.

Table 2-3 Log files for asset discovery

Process	Logs
nbdisco Verifies if discovery was completed or not.	Windows <i>NetBackup install path/bin/vxlogview -o 400</i> UNIX <i>/usr/opensv/netbackup/bin/vxlogview -o 400</i>
Picloud Provides the details of discovery operation.	Windows <i>NetBackup install path/bin/vxlogview -i 497</i> UNIX <i>/usr/opensv/netbackup/bin/vxlogview -i 497</i>

Table 2-3 Log files for asset discovery (*continued*)

Process	Logs
nbweb service	Windows
To get details about the asset DB workflows that are part of the discovery operation.	<i>NetBackup install path/webserver/logs</i>
Note: Refer to the same log files for details of assets that are added to protection plan.	UNIX
	<i>/usr/opensv/wmc/webserver/logs</i>
	<i>/usr/opensv/logs/nbweb services</i>

Log files for snapshot creation

Use the following logs to troubleshoot snapshot creation issues.

Table 2-4 Log files for snapshot creation

Process	Logs
nbpem	Windows
nbpem PID for given job is available in the NetBackup activity monitor.	<i>NetBackup install path/bin/vxlogview -o 116</i>
	UNIX
	<i>/usr/opensv/netbackup/bin/vxlogview -o 116</i>
nbjm	Windows
nbjm PID for given job is available in the NetBackup activity monitor.	<i>NetBackup install path/bin/vxlogview -o 117</i>
	UNIX
	<i>/usr/opensv/netbackup/bin/vxlogview -o 117</i>
nbcs	Windows
nbcs PID for given job is available in the NetBackup activity monitor.	<i>NetBackup install path/bin/vxlogview -i 366 -P nbcs_process_id</i>
	UNIX
	<i>/usr/opensv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id</i>
	The nbcs logs are available at the following location:
	Windows
	<i>NetBackup install path/logs/ncfnbcs</i>
	UNIX
	<i>/usr/opensv/logs/ncfnbcs</i>

Table 2-4 Log files for snapshot creation (*continued*)

Process	Logs
nbrb	Windows
nbrb is requested to provide a media server for a given job. For Cloud, a particular media server is picked up from the associated list of media servers for a CloudPoint server.	<i>NetBackup install path/bin/vxlogview -o 118</i> UNIX <i>/usr/opensv/netbackup/bin/vxlogview -i 118</i>

Log files for restore operations

Use the following logs to troubleshoot restore issues.

Table 2-5

Process	Logs
nbwebservice	Windows
The snapshot restore operation is triggered by NetBackup REST API.	<i>NetBackup install path/webserver/logs</i> UNIX <i>/usr/opensv/wmc/webserver/logs</i> <i>/usr/opensv/logs/nbwebservices</i>
bprd	Windows
The NetBackup REST API communicates with bprd to initiate restore	<i>NetBackup install path/netbackup/logs</i> UNIX <i>/usr/opensv/netbackup/logs/bprd</i>
ncfnbcs	Windows
nbcs PID for given job is available in the NetBackup activity monitor.	<i>NetBackup install path/bin/vxlogview -i 366 -P nbcs_process_id</i> UNIX <i>/usr/opensv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id</i>

Log files for snapshot deletion

Use the following logs to troubleshoot snapshot deletion issues.

Table 2-6 Log files for snapshot deletion

Process	Logs
bpdm The snapshot delete or clean-up operation is triggered by bpdm.	Windows <i>NetBackup install path/netbackup/logs</i> UNIX <i>/usr/opensv/netbackup/logs/bpdm</i>
ncfnbcs nbcs PID for given job is available in the NetBackup activity monitor.	Windows <i>NetBackup install path/bin/vxlogview -i 366 -P nbcs_process_id</i> UNIX <i>/usr/opensv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id</i>