NetBackup™ Web UI Cloud Administrator's Guide

Release 8.1.2

VERITAS™

NetBackup Web UI Cloud Administrator's Guide

Last updated: 2018-09-19

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 cloud assets

This chapter includes the following topics:

About protecting cloud assets

Using NetBackup you can now protect your in-cloud workloads. The cloud data protection framework leverages the CloudPoint (version 2.1.0 and later) 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
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 "Adding configurations for a cloud provider" on page 14.
Asset discovery	NetBackup retrieves the cloud assets pertaining to 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. See "Configuring cloud asset discovery interval " on page 15.
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.
Choose to protect a virtual machine, application, or volume	For each cloud provider, a list of discovered assets is displayed. Subscribe the assets to a protection plan. See the NetBackup Web UI Backup Administrator's Guide.

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

Task	Description
Recover cloud assets	■ You can recovery the assets using the recovery points. See "Recovering a cloud asset to its original location" on page 16. See "Recovering a cloud asset to an alternate location" on page 16. ■ You can also restore the assets using the `nbcloudrestore` CLI utility. **Note:** Do not use the `bprestore` CLI for restores See theNetBackup Commands Reference Guide.
Troubleshooting	See "Troubleshooting cloud workload protection issues" on page 17.

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 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 [-cloud_provider
  cloud_provider_value] [-requiredport IP_port_number]
  ```

  See the NetBackup Commands Reference Guide.

When you configure a CloudPoint server with NetBackup:

- You can associate multiple cloud providers with a CloudPoint server, but you cannot associate multiple CloudPoint servers with a cloud vendor.
- 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.

Adding 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**.

Editing or disabling configurations for a cloud provider

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**.

See “Adding configurations for a cloud provider” on page 14.

Configuring cloud asset discovery interval

By default, asset discovery happens every 4 hours. You can use the `CLOUD_DISCOVERY_INTERVAL`to configure how often NetBackup performs cloud asset discovery. 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/openv/netbackup/bp.conf` file.

2. Restart the nbdisco service.

   Asset discovery is triggered after you restart the service.

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

Note: Cloud assets for Google Cloud Platform cannot be restored to an alternate location.

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.

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 *NetBackup install path*`/volmgr/debug/tpcommand` UNIX `/usr/openv/volmgr/debug/tpcommand`
nbwebservice Plug-ins are configured using NetBackup REST API.	Windows *NetBackup install path*`/webserver/logs` UNIX `/usr/openv/wmc/webserver/logs` `/usr/openv/logs/nbwebservices`
nbemm nbemm stores the CloudPoint server and plug-in information in EMM database	Windows *NetBackup install path*`/bin/vxlogview -o 111` UNIX /usr/openv/netbackup/bin/vxlogview -o 111

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 *NetBackup install path*`/bin/vxlogview -o 400` UNIX `/usr/openv/netbackup/bin/vxlogview -o 400`
Picloud Provides the details of discovery operation.	Windows *NetBackup install path*`/bin/vxlogview -i 497` UNIX `/usr/openv/netbackup/bin/vxlogview -i 497`

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

Process	Logs
nbwebservice To get details about asset DB workflow that are part of the discovery operation. **Note:** Refer to the same log files for details of assets subscribed to protection plan.	Windows *NetBackup install path*/webserver/logs UNIX /usr/openv/wmc/webserver/logs /usr/openv/logs/nbwebservices

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

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

Process	Logs
nbrb 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.	Windows *NetBackup install path*/bin/vxlogview –o 118 UNIX `/usr/openv/netbackup/bin/vxlogview -i 118`

Log files for restore operations

Use the following logs to troubleshoot restore issues.

Table 2-5

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

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 *NetBackup install path*\netbackup\logs UNIX /usr/openv/netbackup/logs/bpdm
ncfnbcs nbcs PID for given job is available in the NetBackup activity monitor.	Windows *NetBackup install path*\bin\vxlogview -i 366 -P *nbcs_process_id* UNIX /usr/openv/netbackup/bin/vxlogview -i 366 -P *nbcs_process_id*