NetBackup™ Web UI Backup Administrator's Guide

Release 8.1.2

VERITAS™

NetBackup Web UI Backup 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**

The NetBackup dashboard

The NetBackup dashboard provides a quick view of the details that are related to your role in your organization.

Table 1-2 The NetBackup dashboard for the backup administrator

Dashboard widget	Description
Jobs	Lists job information, including the number of active and queued jobs and the status of attempted and completed jobs.
Usage reporting	Lists the size of the backup data for the NetBackup master servers in your organization. This reporting is useful for tracking capacity licensing. Use the drop-down lists in the top right to select the time period and the view that you want to display. Click on a server name to see specific details for that server. Additional details are available for how to configure NetBackup to display master server information in this widget. See "Track backup data size on your master servers" on page 26.

Chapter 2

Managing protection plans

This chapter includes the following topics:

Create a protection plan

A protection plan defines when backups are performed, how long the backups are retained, and the type of storage to use. Once you have set up a protection plan, you can subscribe assets to that protection plan.

Before you create a protection plan, you must configure all storage options. You must configure those storage options in the NetBackup Administration Console. Refer to the following procedure (step 8) for the types of storage options that can be configured.

To create a protection plan

1. On the left, click **Protection plans** and then click **Create**.
2. Enter a **Name** and **Description** for the plan and click **Next**.
3. In **Schedule backups**, select how often you want this schedule to run and how long to keep the backup.

   Click **Save** to finish this schedule. If you want to add another backup schedule, click **Save and add another**.

4 (Optional) To replicate the backup, turn on **Replicate**.

To use the **Replicate** option, the backup storage must be a source in a targeted A.I.R. environment. The **Replication target** is configured in step 8.

For more information about replication, review *About NetBackup Auto Image Replication* in the NetBackup Administrator's Guide, Volume I.

5 You can adjust the **Backup start window** to define when the backups can start.

Backups can start at any time during the day but the schedule shows the default windows at setup. The system defaults windows are: 8:00 A.M. to 8:00 P.M. Monday thru Friday and open for Saturday and Sunday. You can leave the defaults in place or change the backup window for any day of the week. Also, backup windows are applied to all schedules.

6 (Optional) To keep a copy in long-term storage, turn on **Keep a copy for long-term retention**.

NetBackup immediately duplicates a copy to long-term storage after the backup completes.

Only one schedule can have the **Keep a copy for long-term retention** option selected.

7 Click **Next**.

8 Configure the storage options for this protection plan.

When creating a protection plan, select only the storage that a NetBackup 8.1.2 or newer media server can access.

Storage option	Requirements	Description
Snapshot storage only	CloudPoint is required for this option.	Configure CloudPoint in the NetBackup Administration Console using the Snapshot Management Server feature. If you use the Snapshot only storage option, no other storage option can be selected. Go to step 9.
Backup storage	OpenStorage is required for this option. Tape, storage unit groups, and Replication Director not supported.	Click **Change** to select the storage target. Click **Use selected storage** after selecting the storage target. The NetBackup **Accelerator** feature allows protection plans to execute faster than traditional backups, by creating a compact data stream that uses less network bandwidth. If the storage server on the NetBackup master server supports NetBackup Accelerator, this feature is included in the protection plan. For more details on NetBackup Accelerator, contact the NetBackup administrator or see the NetBackup Administrator's Guide, Volume I or the NetBackup for VMware Administrator's Guide. The **Instant access** feature allows the plan's VM recovery points to support the creation of instant access VMs.
Replication target	The backup storage must be a source in a targeted A.I.R. environment.	Click **Change** to select the replication target master server. Select a master server and then select a storage lifecycle policy. Click **Use selected replication target** to return to the storage options screen.
Long-term retention storage	OpenStorage is required for this option. Tape, storage unit groups, and Replication Director not supported.	Click **Change** to select the cloud storage provider. Click **Use selected storage** after selecting the cloud provider target.

9 Click **Next**.

10 Review the plan details and click **Save**.

Edit or delete a protection plan

Edit a protection plan

You can make changes to various elements of a protection plan. The **Name**, **Description**, and **Storage options** are available to edit.

To edit a protection plan

1. On the left, click **Protection plans**.
2. Click on the protection plan that you want to edit.
3. Click **Edit** on the top right of the screen.
4. (Optional) Edit the **Name** or the **Description** of the protection plan.
5. (Optional) Click **Change** to edit the **Backup storage**, **Replication target**, or the **Long-term storage**.

See "Create a protection plan" on page 11.

Delete a protection plan

Before you delete a protection plan, you need to add the assets to another protection plan. Moving the assets to another protection plan ensures that the data is protected on those assets that this plan protects. You cannot delete a protection plan unless all assets have been removed from the protection plan.

To delete a protection plan

1. Make note of the protection plan you want to add the assets to (new or existing).

   See "Create a protection plan" on page 11.
2. Locate the assets that currently protected by the plan you want to delete.
3. Subscribe the assets to the new or an existing protection plan.

   See "Subscribe an asset or an asset group to a protection plan" on page 15.
4. Unsubscribe the assets from the protection plan you want to delete.
5. On the left, click **Protection plans**.
6. Select the protection plan you want to delete.
7. Click **Delete** on the top right of the screen.

Subscribe an asset or an asset group to a protection plan

You can subscribe a single asset or a group of assets to a protection plan. An asset or a group of assets can be subscribed to multiple protection plans. Before you can subscribe assets to a protection plan, you must create a protection plan.

Note: To subscribe an asset group to a protection plan, an RBAC role must have the **Role permissions** of **Manage Appservers and Asset Groups** selected.

For more information on RBAC roles, review the NetBackup Web UI Security Administrator's Guide.

To subscribe an asset or an asset group to a protection plan

1. On the left, click the workload type (for example: **VMware**).
2. Select an asset type (for example: **Virtual machines**, **Intelligent VM groups**).
3. Select the box next to the specific asset name.
4. On the top right, click **Configure protection**.
5. Select a protection plan from the list.
6. Review the details for the protection plan.
7. Click **Protect**.

See "Create a protection plan" on page 11.

Unsubscribe an asset from a protection plan

You can unsubscribe individual assets or groups of assets from a protection plan.

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

To unsubscribe a single asset from a protection plan

1. On the left, click the workload type (for example: **VMware**).
2. Select a single asset type (for example: **Virtual machines**).

3 Click on the specific asset name.

If you select the box, you need to click the name of the asset or click **View details** in the toolbar.

4 On the protection plan you want to unsubscribe from, click **Unsubscribe from protection plan**.

To unsubscribe a group of assets from the protection plan

1 On the left, click the workload type (for example: **VMware**).

2 Select a group asset type (for example: **Intelligent VM groups**).

3 Click on the specific group asset name.

4 Click the padlock at the bottom.

5 Click **Unsubsribe** in the **Protected by** field.

6 Click **Yes** to confirm removal.

See "Create a protection plan" on page 11.

See "Edit or delete a protection plan" on page 14.

About a NetBackup classic policy

You can protect an asset using a NetBackup classic policy, a protection plan, or both at the same time. This topic answers some common questions about NetBackup classic policies in the NetBackup web UI.

Table 2-1 Classic policy FAQ

Question	Answer
In the web UI's **Protected by** column, what does **Classic policy only** mean?	The asset is not currently subscribed to a protection plan. However, it was subscribed to a protection plan or covered by a classic policy at one time and it has a **Last backup** status. There may or may not be an active classic policy protecting the asset (contact the NetBackup administrator to find out).
Where can I find the details of a classic policy?	The details of a classic policy are not visible in the web UI. To manage a classic policy, a NetBackup administrator can use the NetBackup Administration Console or the NetBackup CLIs. Also, the NetBackup administrator or the backup admin can manage and create policies using the NetBackup APIs.

Table 2-1 Classic policy FAQ *(continued)*

Question	Answer
When should I subscribe an asset to a protection plan versus protecting the asset with a classic policy?	Only a NetBackup administrator can create a classic policy. If you do not have the required permissions to subscribe assets to protection plans, ask the backup administrator to configure the protection plan. The backup administrator may choose to protect the asset through a protection plan (web UI) or through a classic policy (Administration Console).
Can I use both a protection plan and a classic policy to protect an asset?	Yes. The web UI shows the details of the protection plan but not the details of the classic policy. You can contact the NetBackup administrator for the classic policy details.
What action should I take when an asset is unsubscribed from a protection plan and the web UI shows **Classic policy only** for that asset?	You can ask the NetBackup administrator if a classic policy protects the asset.

Backup administrator tasks for VMware protection plans

The following VMware tasks require backup administrator permissions:

- *Add VMware servers and their credentials*
- *Create an intelligent VM group*
- *Delete an intelligent VM group*

Please see the NetBackup Web UI VMware Administrator's Guide for instructions on these tasks.

Chapter 3

Managing jobs

This chapter includes the following topics:

Monitoring jobs

Use the **Jobs** node to monitor the jobs in your NetBackup environment and view the details for a specific job.

To monitor a job

1. Click **Jobs** and select the job name or check the box of the job that you want to view. You can select the checkbox for a job to perform a particular action on that job, such as restarting the job. Under **Status**, click the status code to view the status code message.
   - Select the **Overview** tab to view information about a job.
   - The **Details** tab displays the **File List** and **Status**. The **File List** contains the files that are included in the backup image. Select the **Details** tab to view the logged details about a job. You can filter the logs by error type. Under **Status**, click the status code number to view information about this status code in the Veritas Knowledge Base.
     See the NetBackup Status Codes Reference Guide.
2. From here, you can perform additional tasks.

   See "Jobs: canceling, suspending, restarting, resuming, deleting" on page 19.

Jobs: canceling, suspending, restarting, resuming, deleting

To manage jobs

1. Click **Jobs**.
2. Select one or more jobs.
3. The top menu shows the actions that you are able to perform for the selected jobs.

Cancel	You can cancel the jobs that have not yet completed. They can be in one of the following states: queued, re-queued, active, incomplete, or suspended. When a parent job is canceled, any child jobs are also canceled.
Suspend	You can suspend backup and restore jobs that contain checkpoints.
Restart	You can restart the jobs that have completed, failed, or that have been canceled or suspended. A new job ID is created for the new job.
Resume	You can resume the jobs that have been suspended or are in an incomplete state.
Delete	You can delete the jobs that have completed. When a parent job is deleted, any child jobs are also deleted.

Filter jobs in the job list

You can filter the jobs to display the jobs in a specific state. For example, you can display all of the active jobs or all of the suspended jobs.

To filter the job list

1. Click **Jobs**.
2. Above the job list, click the **Filter** option.
3. In the **Filter** window, select a filter option to dynamically change the jobs that are displayed. The filter options are as follows:
   - **All**
   - **Active**
   - **Done**

- **Failed**
- **Incomplete**
- **Partially Successful**
- **Queued**
- **Successful**
- **Suspended**
- **Waiting for Retry**

4 Click **Apply Filters**.

5 To remove the selected filters, click **Clear All**.

Chapter 4

Configuring email notifications for alerting

This chapter includes the following topics:

About NetBackup alerts

The backup administrator can configure NetBackup to send email notifications when job failures occur. These notifications can also be directed to a supported ticketing system.

This feature saves NetBackup administrators from spending time monitoring NetBackup for job failures and manually creating tickets to track issues. NetBackup supports the ticketing systems that use inbound email service for ticket creation. For example, ServiceNow, Remedy, or HP Service Manager (HPSM).

NetBackup generates alerts based on certain status codes.

See “About the status codes supported for alerts” on page 23.

Alerts that are similar or have a similar reason for failure are marked as duplicates. Email notifications for duplicate alerts are not sent for the next 24 hours. If an email notification cannot be sent, NetBackup tries the notification every 2 hours, up to three retry attempts.

NetBackup audits an event if changes are made to the alert settings or when it cannot generate an alert or send an email notification.

For more information, refer to the NetBackup Security and Encryption Guide.

How to configure email notifications for alerting

Based on certain job failure conditions or NetBackup status codes, alerts are generated and sent to your ticketing system through email notifications.

See "About NetBackup alerts" on page 21.

See "About the status codes supported for alerts" on page 23.

The following table lists the procedures that you need to do to generate alerts and tickets.

Table 4-1 NetBackup alerts and ticket generation

Step	Action	Reference topic
1	Review the prerequisites.	See "Prerequisites" on page 22.
2	Learn about the conditions or status codes for which alerts are generated and are sent to the ticketing system as email notifications.	See "About the status codes supported for alerts" on page 23.
3	Configure email notifications so that the alerts are sent to the ticketing system.	**Note:** You can exclude status codes for which you do not want to send email notifications. See "Configure email notifications" on page 23.
4	View NetBackup alerts (or tickets) in the ticketing system.	Log on to the ticketing system to view the tickets that are generated by NetBackup alerts.

Prerequisites

Ensure the following before you generate the alerts and view them using the ticketing system.

- The ticketing system is up and running.
- The SMTP server is up and running.
- A policy is configured in the ticketing system to create tickets (or incidents) based on inbound emails that NetBackup sends.

About the status codes supported for alerts

NetBackup 8.1.2 supports alerts for VMware job failures and retains the alerts for 90 days. NetBackup generates alerts for the supported status codes for following job types: backup, snapshot, snapshot replication, index from snapshot, and backup from snapshot. For the complete list of status codes for which alerts are generated, refer to the “NetBackup alert notification status codes” section from the NetBackup Status Codes Reference Guide.

Table 4-2 lists some of the conditions or status codes for which alerts are generated. These alerts are sent to the ticketing system through email notifications.

Table 4-2 Examples of the supported status codes

Status code	Error message
10	Allocation failed
196	Client backup was not attempted because backup window closed
213	No storage units available for use
219	The required storage unit is unavailable
2001	No drives are available
2074	Disk volume is down
2505	Unable to connect to the database
4200	Operation failed: Unable to acquire snapshot lock
5449	The script is not approved for execution
7625	SSL socket connection failed

Configure email notifications

You can configure NetBackup to send email notifications when an event that is related to a job failure occurs.

To configure email notifications

1. At the top right, click **Settings > Alerts and notification settings**.
2. Click **Email notifications**.
3. Enable the **Send email notifications** option.

4 Enter the email information including the recipient's email address, the sender's email address, and the email sender's name.

5 Enter the SMTP server details including the SMTP server name and port number.

Provide the SMTP user name and password if you have specified the credentials earlier on the SMTP server.

6 Click **Save**.

Exclude specific status codes from email notifications

You can exclude specific status codes so that email notifications are not sent for these errors.

To exclude specific status codes

1 At the top right, click **Settings > Alerts and notification settings**.

2 Click **Exclude status codes**.

3 Enter the status codes or a range of status codes (separated by commas) for which you do not want to receive email notifications.

4 Click **Save**.

Sample email notification for an alert

An email notification for an alert contains information about master server, job, policy, schedule, and error. Emails may contain other information based on the type of job. For example, for VMware job failures, details such as vCenter Server and ESX host are present in the email notification.

Example email notification:

```
Master Server: master1.example.com

Client Name: client1.example.com

Job ID: 50

Job Start Time: 2018-05-17 14:43:52.0

Job End Time: 2018-05-17 15:01:27.0

Job Type: BACKUP

Parent Job ID: 49

Policy Name: Win_policy

Policy Type: WINDOWS_NT

Schedule Name: schedule1
```

```
Schedule Type: FULL

Status Code: 2074

Error Message: Disk volume is down
```

Chapter 5

Usage reporting and capacity licensing

This chapter includes the following topics:

Track backup data size on your master servers

The Usage reporting application lists the size of the backup data for the NetBackup master servers in your organization. This reporting is useful for planning when you use capacity licensing. NetBackup gathers and reports usage and trend information on a weekly basis by default.

The data for the report is gathered by the scheduled runs of the `nbdeployutil` utility. Scheduled runs of `nbdeployutil` are enabled by default. For more information, see Scheduling capacity licensing reports.

This application also includes a link to the **Veritas Smart Meter**. This portal allows NetBackup customers to proactively manage their license use through near real-time visibility of consumption patterns.

Table 5-1 Policy types supported for usage reporting

BigData	Informix	Oracle	VMware
MS-Exchange-Server	MS-SQL-Server	Standard	
Hyper-V	NDMP	Sybase	

Requirements

Provided the following requirements are met, NetBackup automatically collects data for the usage reporting.

- You use capacity licensing. Usage reporting does not apply to the traditional licensing method.
- Only automatic, scheduled reports display in the web UI. If you manually generate capacity license reports, the data does not display in the usage report in the NetBackupweb UI.

  The following file must exist:

  UNIX: `/usr/openv/var/global/incremental/Capacity_Trend.out`

  Windows: *`install_path`*`\var\global\incremental\Capacity_Trend.out`
- If you want one of your master servers to gather usage reporting data for other remote master servers, additional configuration is required. You must create a trust relationship between the master servers. You must also add the local master server (where you plan to run `nbdeployutil`) to the **Servers** list on each remote master server.

  See "Configure servers list for usage reporting" on page 29.
  See "Adding a trusted master server" on page 27.

Additional information

NetBackup Administrator's Guide, Volume II. Details on capacity licensing, scheduling and options for capacity licensing reports, and for troubleshooting information for `nbdeployutil`.

Veritas Smart Meter Getting Started Guide. Details on using Smart Meter to manage your NetBackup deployment and licensing. This tool provides accurate, near real-time reporting for the total amount of data that is backed up.

Adding a trusted master server

If you want to have usage reporting for multiple master servers in the NetBackup web UI, you need to configure a trust relationship exists between the NetBackup servers in the different domains.

Before you begin

Perform the following steps on both the source and the target server:

- Identify the NetBackup versions that are installed on the source and the target servers.

  Usage reporting and Smart Meter are supported for NetBackup 8.1.2 and later.

- Obtain the authorization tokens of the remote server.
  Use the `bpnbat` command to log on and `nbcertcmd` to get the authorization tokens.
- Obtain the fingerprints for the remote server.
  To obtain the SHA1 fingerprint of root certificate, use the `nbcertcmd -displayCACertDetail` command.
- Ensure that you have one of the following permissions:
  - System administrator permissions with `root` permissions for UNIX, administrator permissions for Windows, or a NetBackupCLI user for a 3.1 NetBackup appliance.
  - Access to the NetBackup Administration Console, where you have **<username> ADMIN=ALL** permissions through `auth.conf`.
  - Enhanced Auditing (EA) user permissions through `authalias.conf`.

Adding a trusted master server, when both the source and the target server are NetBackup version 8.1 or later

To add a trusted master server, when both the source and the target server are NetBackup version 8.1 or later

1. In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers** in the left pane.
2. In the right pane, select the master server and **Actions** > **Properties**.
3. In the properties dialog box left pane, select **Servers**.
4. On the **Trusted Master Servers** tab, click **Add**.
5. Enter the fully-qualified host name of the remote master server and click **Validate Certificate Authority**.
6. In the **Validate Certificate Authority** dialog box, verify if the CA certificate fingerprint of the remote server is correct.

   To proceed, click **Yes**.

   If the fingerprints don't match, click **No**. Contact the remote server admin to provide the correct fingerprints.
7. Enter the trusted master server details using one of the following methods.
   - (Recommended) Select **Specify authentication token of the trusted master server** and enter the token details of the remote master server.
   - Select **Specify credentials of the trusted master server** and enter the user name and password. Note that this method may present a possible

security breach. Only an authentication token can provide restricted access and allow secure communication between both the hosts.

To establish trust with a 3.1 NetBackup master appliance, use the NetBackupCLI credentials.

8 Click **OK**.

9 Perform the same procedure on the remote master server that you added in step 5.

Adding a trusted master server, when both the source and the target server are NetBackup version 8.0 or earlier

To add a trusted master server, when both the source and the target server are NetBackup version 8.0 or earlier

1 Ensure that the **Enable insecure communication with NetBackup 8.0 and earlier hosts** option is enabled in the global security settings.

2 In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers** in the left pane.

3 In the right pane, select the master server and **Actions** > **Properties**.

4 In the properties dialog box left pane, select **Servers**.

5 On the **Trusted Master Servers** tab, click **Add**.

6 Enter the fully-qualified host name of the remote master server and click **Validate Certificate Authority**.

7 Enter the **Username** and **Password** of the remote master server host.

8 Click **OK**.

More information

For details on usage reporting in the web UI, see the *NetBackup Web UI for Backup Administrator's Guide*.

For more information on commands, see the NetBackup Commands Reference Guide. For details on the `authalias.conf`, see the NetBackup Security and Encryption Guide.

Configure servers list for usage reporting

If a you want to add usage reporting information for a master server but that server does not have an internet connection, you need to add the name of the local master

server to the servers list of the remote master server. The local master server is where you plan to run `nbdeployutil`.

To add a server to a list

1. On the remote master server, log on as root or administrator.
2. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Host Properties**.
3. Select **Master Servers**.
4. In the right pane, double-click the master server that you want to modify.
5. In the properties dialog box, in the left pane, click **Servers**.
6. Select the **Additional Severs** tab.
7. Click **Add**.
8. In the **Add a New Server Entry** dialog box, enter the name of the master server where you plan to run `nbdeployutil`.
9. Click **Add**. The dialog box remains open for another entry.
10. Click **Close.**