NetBackup™ Web UI Administrator's Guide

Release 9.0

VERITAS™

NetBackup Web UI Administrator's Guide

Last updated: 2021-01-05

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1

Introducing the NetBackup web user interface

This chapter includes the following topics:

About the NetBackup web UI

The NetBackup web user interface provides the following features:

- Ability to access the master server from a web browser, including Chrome and Firefox. For details on supported browsers for the web UI, see the NetBackup Software Compatibility List.
  Note that the NetBackup web UI may behave differently for different browsers. Some functionality, for example a date picker, may not be available on all browsers. These inconsistencies are due to the capabilities of the browser and not because of a limitation with NetBackup.
- A dashboard that displays a quick overview of the information that is important to you.
- Role-based access control (RBAC) that lets the administrator configure user access to NetBackup and to delegate the tasks such as security, storage management, or workload protection.
- Management of NetBackup security settings, certificates, API keys, and user sessions.

- Protection of assets is achieved through protection plans, job management, and visibility of the protection status of assets. Alternatively, policy management is also available for a limited number of policy types.
- Workload administrators can create protection plans, subscribe assets to the protection plans that meet the SLO, monitor protection status, and perform self-service recovery of virtual machines. The web UI supports the following workloads:
  - Cloud
  - Microsoft SQL Server
  - Oracle
  - Red Hat Virtualization (RHV)
  - VMware
- Usage reporting tracks the size of backup data on your master servers. You can also easily connect to Veritas NetInsights Console to view and manage NetBackup licensing.

Note: The NetBackup web UI is best viewed at a 1280x1024 or higher screen resolution.

Access control in the NetBackup web UI

NetBackup uses role-based access control to grant access to the web UI. Access control is accomplished through roles.

- A role defines the operations that a user can perform and the access that the user has to any workload assets, protection plans, or credentials. A user can have multiple roles, allowing for full and for flexible customization of user access.
- RBAC is only available for the web UI and the APIs.
  Other access control methods for NetBackup are not supported for the web UI and APIs, with the exception of Enhanced Auditing (EA). .

Monitor NetBackup jobs and events

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

- The dashboard displays an overview of NetBackup jobs, certificates, tokens, security events, and usage reporting.
  The dashboard widgets that display depend on a user's RBAC role and permissions.

- Email notifications can be configured so administrators receive notifications when job failures occur. NetBackup supports any ticketing system that can receive inbound email.

Protection plans: One place to configure schedules, storage, and storage options

Protection plans offer the following benefits:

- In addition to schedules for backups, a protection plan can also include a schedule for replication and long-term retention.
- When you select from your available storage, you can see any additional features available for that storage.
- A default workload administrator can create and manage protection plans, including the backup window and retention.
  See "Role permissions" on page 52.
- A default workload administrator can select the protection plans to use to protect assets or intelligent groups.

Self-service recovery

The NetBackup web UI makes it easy for a workload administrator to recover VMs or databases. For the workloads that support the instant access feature, users can mount a snapshot for immediate access to a VM's files or to a database.

Terminology

The following table describes the concepts and terms that are introduced with the new web user interface.

Table 1-1 Web user interface terminology and concepts

Term	Definition
Administrator	A user that has complete access and permissions to NetBackup and all of the interfaces, including the NetBackup web UI. The root, administrator, and Enhanced Auditing user all have complete access to NetBackup. In the *NetBackup Web UI* guides, the term *NetBackup administrator* also refers to a user that has full permissions for NetBackup. Usually in reference to a user of the NetBackup Administration Console. Also see *role*.
Asset group	See *intelligent group*.

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

Term	Definition
Asset	The data to be protected, such as physical clients, virtual machines, and database applications.
Backup now	An immediate backup of an asset. NetBackup performs a one-time, full backup of an asset using the selected protection plan. This backup does not affect any scheduled backups.
Classic policy	In the NetBackup web UI, indicates that a legacy policy protects the asset. Legacy policies are created with the NetBackup Administration Console.
External certificate	A security certificate that is issued from any CA other than NetBackup.
Intelligent group	Allows NetBackup to automatically select assets for protection based on the criteria (queries) that you specify. An intelligent group automatically stays up-to-date with changes in the production environment. These groups are also referred to as asset groups. For VMware and RHV, these groups appear under the tab **Intelligent VM groups**.
Instant access	An instant access VM or database that is created from a NetBackup backup image is available almost instantaneously, achieving a near-zero recovery time objective. NetBackup mounts the snapshot directly on the backup storage device and the snapshot is treated as a normal VM or database.
NetBackup certificate	A security certificate that is issued from the NetBackup CA.
Protection plan	A protection plan defines when backups are performed, how long the backups are retained, and the type of storage to use. Once a protection plan is set up, assets can be subscribed to the protection plan.
RBAC	Role-based access control. Administrators can delegate or limit access to the NetBackup web UI through the roles that are configured in RBAC. **Note:** The roles that you configure in RBAC do not control access to the NetBackup Administration Console or the CLIs.

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

Term	Definition
Role	For RBAC, defines the operations that a user can perform and the assets or objects that they can access. For example, you can configure a role to mange recovery of specific databases and the credentials that are needed for backups and restores.
Storage	The storage to which the data is backed up, replicated, or duplicated (for long-term retention).
Subscribe, to a protection plan	The action of selecting an asset or an asset group to subscribe to a protection plan. The asset is then protected according to the schedule in the plan. The web UI also refers to *Subscribe* as *Add protection*.
Unsubscribe, from a protection plan	*Unsubscribe* refers to the action of removing protection or removing an asset or asset group from a plan.
Workload	The type of asset. For example, VMware, RHV, or Cloud.

Sign in to the NetBackup web UI

Authorized users can sign in to a NetBackup master server from a web browser, using the NetBackup web UI. The following sign-in options are available:

- Sign in with a username and password
- Sign in with a certificate or smart card
- Sign in with single sign-on (SSO)

Sign in with a username and password

Only authorized users can sign in to NetBackup web UI. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup master server using a username and password

1. Open a web browser and go to the following URL.

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master server that you want to sign in to.

2. Enter your credentials and click **Sign in**.

   For example:

For this type of user	Use this format	Example
Local user	*username*	**jane_doe**
Windows user	*DOMAIN\username*	**WINDOWS\jane_doe**
UNIX user	*username@domain*	**john_doe@unix**

Sign in with a certificate or smart card

You can sign in to NetBackup web UI with a smart card or digital certificate if you are an authorized user. Contact your NetBackup security administrator for more information.

To use a digital certificate that is not on a smart card, you must first upload the certificate to the browser's certificate manager. See the browser documentation for instructions or contact your certificate administrator for more information.

To sign in with a certificate or smart card

1. Open a web browser and go to the following URL.

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master server that you want to sign in to.

2. Click **Sign in with certificate or smart card**.

3. When your browser prompts you, select the certificate.

Sign in with single sign-on (SSO)

You can sign in to NetBackup web UI with the single sign-on (SSO) option if SAML is configured as an identity provider in your NetBackup environment. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup master server using SSO

1. Open a web browser and go to the following URL.

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master server that you want to sign in to.

2. Click **Sign in with single sign-on**.

3. Follow the steps as provided by your administrator.

   On subsequent logons, NetBackup signs you in automatically to the master server.

Sign out of the NetBackup web UI

Note that NetBackup automatically signs you out of the web UI after 24 hours, which is the maximum time that is allowed for a user session. After that time NetBackup requires that you sign in again. You can also sign out if you want to change the sign-in option that you want to use (username and password, smart card, or single sign-on (SSO)).

To sign out of the NetBackup web UI

- On the top right, click the profile icon and click **Sign out**.

Section 1

Monitoring and notifications

Chapter 2

Monitoring NetBackup

This chapter includes the following topics:

The NetBackup dashboard

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

Table 2-1 The NetBackup dashboard

Dashboard widget	Description
Jobs	Lists job information, including the number of active and queued jobs and the status of attempted and completed jobs.
Certificates	Displays the information about the NetBackup host ID-based security certificates or the external certificates in your environment. For external certificates, the following information is shown for NetBackup 8.2 and later hosts: ■ Total hosts. The total number hosts. The hosts most be online and able to communicate with NetBackup master server. ■ Missing. The number hosts that do not have an external certificate enrolled. ■ Valid. The number of hosts that have an external certificate enrolled. ■ Expired. The number of hosts with expired external certificates. More details are available in **Certificates > External certificates**. See "About security management and certificates in NetBackup" on page 106.
Tokens	Displays the information about the authorization tokens in your environment.
Security events	The **Access history** view includes a record of logon events. The **Audit events** view includes the events that users initiate on the NetBackup master server.

Table 2-1 The NetBackup dashboard *(continued)*

Dashboard widget	Description
Usage reporting	Lists the size of the backup data for the NetBackup master servers in your organization. This reporting is useful to track capacity licensing. Use the drop-down lists in the top right to select the time period and the view that you want to display. Click on a server name to see specific details for that server. 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 187.

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. On the left, click **Activity monitor > Jobs**.

   You can perform the following actions:

   - Click the job name that you want to view.
   - Select the check box for a job and perform a particular action on that job, such as restarting the job.
     See "Jobs: canceling, suspending, restarting, resuming, deleting" on page 21.

2. Click on a job name that you want to view.

   On the **Overview** tab you can view information about a job.

   - The **File List** contains the files that are included in the backup image.
   - The **Status** section shows the status and the status codes that are related to the job. Click the status code number to view information about this status code in the Veritas Knowledge Base.

See the NetBackup Status Codes Reference Guide.

3 Click the **Details** tab to view the logged details about a job. You can filter the logs by error type using the drop-down menu.

See "Filter jobs in the job list" on page 21.

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

Notifications

This chapter includes the following topics:

About notifications

To make NetBackup administrators aware of important system events, NetBackup regularly queries system logs and displays notifications about the events.

Note: Job events are not included with these notifications. See job details in the **Activity Monitor** for information about job events.

A **Notifications** icon is located at the top right in the web UI. You can click the icon to open the **Notifications** window and view a list of critical notifications 10 at a time. If a number is displayed with the icon, it indicates how many unseen critical messages exist. After you have opened the window, the number is reset.

From the window, you can choose to see a more comprehensive list of all notifications. Each event has a category for its NetBackup or external component and is assigned a severity level:

- Error
- Critical
- Warning

- Information
- Debug

You can sort, filter, and search the list. The comprehensive list also lets you review details about each event. The details include the full description as well as any appropriate extended attributes.

NetBackup notifications are not available if the NetBackup Messaging Broker (`nbmqbroker`) is not running. See the *NetBackup Troubleshooting Guide* for information about restarting the service.

Viewing notifications

To view notifications

1. At the top right, click the **Notifications** icon to view a list of critical notifications 10 at a time.

   Note: If a number is displayed with the icon, it indicates how many unseen critical messages exist. After you have opened the **Notifications** window, the number is reset.

   Click **Load 10 more** to view the next 10 notifications. After you have viewed 30 notifications, click **Show all** to view any remaining messages.

   Use **Refresh** to load the most recent notifications again.

2. To view all notifications, click **Show all** to open the **Notifications** page. On the page, you can do the following:

   - Click a notification to view its details. The details include the full description as well as extended attributes.
   - To sort the list, click any of the column headings except **Description**. Notifications are sorted by default by the date received.
   - To filter notifications, click the **Filter** icon at the top right. You can filter by **Severity** and **Timeframe**.
     In the **Filter** window, select the parameter values you want to filter by, and then click **Apply filters**.
     To remove all filters, click **Clear all**.
   - To search for notifications, enter the search string in the **Search...** field. You can search for values in all columns except **Description** and **Received**.

Modify or disable NetBackup event notifications in the web UI

You can disable specific types of NetBackup event notifications that appear in the web UI, or modify their severity and priority, by making changes to the `eventlog.properties` file on the NetBackup master server:

- Windows:
  install_path\var\global\wmc\h2Stores\notifications\properties
- UNIX:
  /usr/openv/var/global/wmc/h2Stores/notifications/properties

To disable event notifications

- Add a `DISABLE` entry in the `eventlog.properties` file in one of the following formats:

  `DISABLE.`*`NotificationType`* `= true`

  Or `DISABLE.`*`NotificationType.Action`* `= true`

  Or `DISABLE.`*`namespace`*

  See Table 4-1 for valid *NotificationType* and *Action* values.

  For example:

  - To disable notifications about all storage unit events:
    `DISABLE.StorageUnit = true`
  - To disable only notifications about create storage unit events:
    `DISABLE.StorageUnit.CREATE = true`
  - To disable only notifications about update to storage unit events using a namespace:
    `DISABLE.eventlog.vrts.nbu.emm.storageunit.update = true`

To modify the priority or severity of event notifications

- Add or change an entry in the `eventlog.properties` file in one of the following formats:

  `NotificationType.Action.priority = value`

  Or *`NotificationType.Action.severity = value`*

  Valid `priority` values are: `LOW, MEDIUM, HIGH`

  Valid `severity` values are: `CRITICAL, ERROR, WARNING, INFO, DEBUG`

  For example:

- To set priority and severity for create storage unit events:

```
StorageUnit.CREATE.priority = LOW
StorageUnit.CREATE.severity = INFO
```

Note: It can take up to one minute for the events of type Policy, SLP, and Catalog to generate after the corresponding action has been performed.

Table 4-1 NetBackup event types supported with notifications

Event type and notification type value	Action	Severity	Sample notification message
Policy `Policy` **Note:** When possible, an aggregated policy event for two or more policy actions is created.	Create	INFO	The policy *{Policy_Name}* was created. Event for Policy received. No additional details found.
	Update	INFO or CRITICAL	The policy *{Policy_Name}* was activated. The policy *{Policy_Name}* was deactivated. The policy *{Policy_Name}* was updated. The client *{Policy_Name}* was added to the policy ${policyName}. The client *{Policy_Name}* was removed from the policy *{Policy_Name}*. The schedule *{Policy_Name}* was added to the policy $*{Policy_Name}*. The schedule *{Policy_Name}* was removed from the policy *{Policy_Name}*.
	Delete	CRITICAL	The policy *{Policy_Name}* was deleted.
Client `ClientEvent`	CREATE	INFO	The client *{Client_Name}* was created.
	DELETE	CRITICAL	The client *{Client_Name}* was deleted.
	UPDATE	INFO	The client *{Client_Name}* was updated.

Table 4-1 NetBackup event types supported with notifications *(continued)*

Event type and notification type value	Action	Severity	Sample notification message
Storage Unit `StorageUnit` **Note:** Any change to a basic disk staging schedule (DSSU), such as adding, deleting, or modifying, generates relevant storage unit notifications. With those notifications, some additional policy notifications are also generated with policy name `__DSSU_POLICY_{`*`Storage_Unit_Name`*`}`.	CREATE	INFO	The storage unit *{Storage_Unit_Name}* was created.
	DELETE	CRITICAL	The storage unit *{Storage_Unit_Name}* was deleted.
	UPDATE	INFO	The storage unit *{Storage_Unit_Name}* was updated.
Storage Unit Group `StorageUnitGroup`	CREATE	INFO	The storage unit group *{Storage_Unit_Group_Name}* was created.
	DELETE	CRITICAL	The storage unit group *{Storage_Unit_Group_Name}* was deleted.
	UPDATE	INFO	The storage unit group *{Storage_Unit_Group_Name}* was updated.
	UPDATE	INFO	The storage service *{Storage_Service_Name}* was updated.
Storage life cycle policy `SLP`	Create	INFO	Event for Storage Lifecycle Policy received. No additional details found. The Storage Lifecycle Policy *{Policy_Name}* was created.
	Delete	CRITICAL	The Storage Lifecycle Policy *{Policy_Name}* was deleted. The Storage Lifecycle Policy *{Policy_Name}* with version *Version_Number* was deleted.
Storage life cycle policy state change `SlpVersionActInactEvent`	UPDATE	INFO	The SLP version *{Version}* was changed.

Table 4-1 NetBackup event types supported with notifications *(continued)*

Event type and notification type value	Action	Severity	Sample notification message
cDOT Client `cDOTClientEvent`	CREATE	INFO	*{Cluster_Data_ONTAP_Client_Name}* was added as a cDOT client.
	DELETE	CRITICAL	*{Cluster_Data_ONTAP_Client_Name}* was deleted as a cDOT client.
Isilon Client `IsilonClientEvent`	CREATE	INFO	*{Isilon_Filer_Client_Name}* was added as an Isilon client.
	DELETE	CRITICAL	*{Isilon_Filer_Client_Name}* was deleted as an Isilon client.
Machine [Master/Media/Cluster] `Machine` **Note:** If you add a VMware server, an RHV server, or a Cloud server with valid credentials, then a `Machine Create` notification is generated. If you try to add a VMware server, an RHV server, or a Cloud server with invalid credentials, then `Machine Create` and `Machine Delete` notifications are generated. During an agentless VMware restore, NetBackup requires the credentials for the virtual machine where the files are to be restored. These credentials are stored in the database, in a similar manner as vCenter credentials. Machine-type notifications are generated when these credentials are added, updated, or deleted in the database with UUID as the host value.	CREATE	INFO	The host *{Host_Name}* was created.
	DELETE	CRITICAL	The host *{Host_Name}* was deleted.
Drive `DriveChange`	CREATE	INFO	The drive *{Drive_Name}* was created for host *{Host_Name}*.

Table 4-1 NetBackup event types supported with notifications *(continued)*

Event type and notification type value	Action	Severity	Sample notification message
	DELETE	CRITICAL	The drive *{Drive_Name}* was deleted for host *{Host_Name}*.
	UPDATE	INFO	The drive *{Drive_Name}* was updated for host *{Host_Name}*. **Note:** A notification message like this one is generated when a drive is updated for a particular host or when a drive state is changed to UP or DOWN.
Library Event - Robot `Library`	CREATE	INFO	The library *{Library_Name}* was created for host *{Host_Name}*.
	DELETE	CRITICAL	The library *{Library_Name}* was deleted for host *{Host_Name}*.
	UPDATE	INFO	The library *{Library_Name}* was updated for host *{Host_Name}*.
Media `Media`	CREATE	INFO	The media *{Media_ID}* was created.
	DELETE	CRITICAL	The media *{Media_ID}* was deleted.
	UPDATE	INFO	The media *{Media_ID}* was updated.
Media Group `MediaGroup`	CREATE	INFO	The media group *{Media_Group_ID}* was created.
	DELETE	CRITICAL	The media group *{Media_Group_ID}* was deleted.
	UPDATE	INFO	The media group *{Media_Group_ID}* was updated.
Media Pool `MediaPool`	CREATE	INFO	The media pool *{Media_Pool_ID}* was created.
	DELETE	CRITICAL	The media pool *{Media_Pool_ID}* was deleted.
	UPDATE	INFO	The media pool *{Media_Pool_ID}* was updated.
Retention Event `RetentionEvent`	UPDATE	INFO	Retention level has been changed.

Table 4-1 NetBackup event types supported with notifications *(continued)*

Event type and notification type value	Action	Severity	Sample notification message
VMware Discovery `TAGSDISCOVERYEVENT`	no actions	INFO	VMware tags cannot be retrieved.
Autodiscovery and Discover Now `AutoDiscoveryEvent`	no actions	INFO	**Note:** An appropriate notification is generated when an autodiscovery action or a Discover Now action is performed for VMWare, RHV, Nutanix, or Cloud servers.
	no actions	CRITICAL	**Note:** An appropriate notification is generated when an autodiscovery action or a Discover Now action fails for VMWare, RHV, Nutanix, or Cloud servers.
KMS Certificate Expiration `KMSCredentialStatus`	EXPIRY	WARNING	The certificate that is used to communicate with the KMS server *{KMS_Server_Name}*${server} is about to expire in *{days_to_expiration}*. If the certificate is not renewed on time, communication with the KMS server fails.
Message Broker Service Status `ServiceStatus`	RUNNING	INFO	The NetBackup Messaging Broker service is running. NetBackup internal notifications are now enabled.
	STOPPED	INFO	The NetBackup Messaging Broker service is stopped. NetBackup internal notifications are now disabled.
Protection Plan `ProtectionPlan`	Create	INFO	Received an event for protection plan. The protection plan *Protection_Plan_Name* is created. The protection plan *Protection_Plan_Name* is created from existing NetBackup policy.
	Update	INFO	The protection plan *Protection_Plan_Name* is updated.
	Delete	CRITICAL	The protection plan *Protection_Plan_Name* is deleted.
Protection Plan Subscription `ProtectionPlanSubscription`	Create	INFO	Received an event for protection plan subscription. The *Asset_Class Asset_Display_Name* is subscribed to protection plan *Protection_Plan_Name*.

Table 4-1 NetBackup event types supported with notifications *(continued)*

Event type and notification type value	Action	Severity	Sample notification message
	Update	INFO	The *Asset_Class Asset_Display_Name* subscription with protection plan *Protection_Plan_Name* is updated.
	Delete	CRITICAL	The *Asset_Class Asset_Display_Name* is unsubscribed from protection plan *Protection_Plan_Name*.
Catalog Image Expiration `Catalog` **Note:** Also applicable for manual image expiration.	Not applicable	CRITICAL	Event for Catalog Image received. No additional details found. Catalog Image *Image_Name* was modified. Catalog Image *Image_Name* expired.

About configuring automatic notification cleanup tasks

By default, NetBackup runs event notification cleanup tasks every 4 hours. Up to 10,000 event records are stored for up to 3 days in the event database. During the cleanup tasks, NetBackup removes the older notifications from the database.

You can change how often the cleanup tasks run, how many event records are kept at one time, and the number of days a record is retained.

From a command line, use `bpsetconfig` or `bpgetconfig` to change the parameter values listed in Table 4-2. See the *NetBackup Command Reference Guide* for more information about these commands.

You can also change the parameter values with the following APIs:

- `GET/config/hosts/{hostId}/configurations`
- `POST/config/hosts/{hostId}/configurations`
- `GET/config/hosts/{hostId}/configurations/configurationName` (for a specific property)
- `PUT/config/hosts/{hostId}/configurations/configurationName`
- `DELETE/config/hosts/{hostId}/configurations/configurationName`

See the *NetBackup 9.0 API Reference* on SORT for more information about these APIs.

Table 4-2 Configurable parameters for automatic notification cleanup tasks

Parameter and description	Minimum value	Default value	Maximum value
EVENT_LOG_NOTIFICATIONS_COUNT The maximum number of records that are stored, after which the cleanup process removes the oldest record, overriding the retention value.	1000	10000	100000
EVENT_LOG_NOTIFICATIONS_RETENTION_IN_HOURS The number of hours for which the events are stored in the database.	24 (hours)	72 (hours)	168 (hours)
EVENT_LOG_NOTIFICATIONS_CLEANUP_INTERVAL_IN_HOURS The frequency at which the event cleanup service runs.	1 (hour)	4 (hours)	24 (hours)

Send email notifications for job failures

You can configure NetBackup to send email notifications when job failures occur. This way administrators spend less 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.

See "Status codes that generate alerts" on page 34.

NetBackup generates alerts based on certain job failure conditions or NetBackup status codes. 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 a notification cannot be sent, NetBackup retries every 2 hours, up to three 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. See "About NetBackup auditing" on page 97.

Prerequisites

Review the following requirements before you configure email notifications using a 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 the inbound emails that NetBackup sends.

To configure email notifications

1. At the top right, click **Settings > Email notifications**.
2. Go to the **Email notifications** tab.
3. Select **Send email notifications**.
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 username and password if you have specified the credentials earlier on the SMTP server.
6. Click **Save**.
7. Log on to the ticketing system to view the tickets that were created based on NetBackup alerts.

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 > Email notifications**.
2. Locate **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
```

Status codes that generate alerts

The NetBackup web UI 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 information for alert notification status codes in the NetBackup Status Codes Reference Guide.

Table 4-3 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 4-3 Examples of status codes that generate alerts

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

Table 4-3 Examples of status codes that generate alerts *(continued)*

Status code	Error message
7625	SSL socket connection failed

Section 2

Managing security

Chapter 5

Managing role-based access control

This chapter includes the following topics:

First-time sign in to a NetBackup master server from the NetBackup web UI

After the installation of NetBackup, an administrator must sign into the NetBackup web UI from a web browser and create RBAC roles for users. A role gives a user permissions and access to the NetBackup environment through the web UI, based on the user's role in your organization. Some users have access to the web UI by default.

See "Authorized users" on page 39.

If you do not have access to root or to administrator credentials you can use the `bpnbaz -AddRBACPrincipal` command to add an administrator user.

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.

   If you are not able to access the web UI, refer to Support and additional configuration.

2. Enter the administrator credentials and click **Sign in**.

For this type of user	Use this format	Example
Local user	*username*	**jane_doe**
Windows user	*DOMAIN\username*	**WINDOWS\jane_doe**
UNIX user	*username@domain*	**john_doe@unix**

3. On the left, select **Security > RBAC**.

4. You can give users access to the NetBackup web UI in one of the following ways:

   - Create roles for all users that require access to NetBackup.
   - Delegate the task of creating roles to another user.
     Create a role that has permissions to add RBAC roles. This user can then create roles for all users that require access to the NetBackup web UI.

   See “Configuring RBAC ” on page 40.

   Root or administrator access is no longer needed for the web UI once you have delegated one or more users with permissions to create RBAC roles.

Support and additional configuration

Refer to the following information for help with accessing the web UI.

- Ensure that you are an authorized user.
  See “Authorized users” on page 39.
- For details on supported browsers for the web UI, see the NetBackup Software Compatibility List.
- If port 443 is blocked or in use, you can configure and use a custom port.
- If you want to use an external certificate with the web browser, see the instructions for configuring an external certificate for the web server.

- See other tips for accessing the web UI.

Authorized users

The following users are authorized to sign in to and use the NetBackup web UI.

Table 5-1 Users that are authorized to use the NetBackup web UI

User	Access
Root, administrator, Enhanced Auditing users, and users with RBAC **Administrator** role	Full
nbasecadmin Appliance user **appadmin** Flex Appliance user	NetBackup security administrator role, can grant access to other appliance users **Note:** The default admin user for the NetBackup appliance does not have access to the web UI.
User that has an RBAC role that gives access to the web UI	Varies See "Configuring RBAC " on page 40.

About role-based access control (RBAC) in NetBackup

The NetBackup web user interface provides the ability to apply role-based access control in your NetBackup environment. Use RBAC to provide access for the users that do not currently have access to NetBackup. Or, for current NetBackup users with administrator access you can provide limited access and permissions, based on their role in your organization.

For information on access control methods for the NetBackup Administration Console and access control and auditing information for root users and administrators, refer to the NetBackup Security and Encryption Guide.

Table 5-2 RBAC features

Feature	Description
Roles allow users to perform specific tasks	Add users to one or more default RBAC roles or create custom roles to fit the role of your users. Add a user to the Administrator role to give full NetBackup permissions to that user. See "Default RBAC roles" on page 41.

Table 5-2 RBAC features *(continued)*

Feature	Description
Users can access NetBackup areas and the features that fit their role	RBAC users can perform common tasks for their business role, but are restricted from accessing other NetBackup areas and features. RBAC also controls the assets that users can view or manage.
Auditing of RBAC events	NetBackup audits RBAC events.
DR ready	RBAC settings are protected with the NetBackup catalog.
Enhanced Auditing or authorization (`auth.conf`) configurations still available for older interfaces	Enhanced Auditing is supported across all interfaces. You can continue to use the authorization (`auth.conf`) configurations with the NetBackup Administration Console and the CLIs. With these older interfaces you can manage access to workflows that are not yet supported in the NetBackup web UI and NetBackup APIs. Note that the `auth.conf` file does not restrict access to the NetBackup web UI or the NetBackup APIs.

Configuring RBAC

To configure role-based access control for the NetBackup web UI, perform the following steps.

Table 5-3 Steps to configure role-based access control

Step	Action	Description
1	Configure any Active Directory or LDAP domains.	Before you can add domain users, Active Directory or LDAP domains must be authenticated with NetBackup. See “Add AD or LDAP domains” on page 41.
2	Determine the permissions that your users need.	Determine the permissions that your users need to perform their daily tasks. See “Role permissions” on page 52.
3	Select the roles you want users to have.	You can add users directly to a default RBAC role or use a default role as a template to create a new role. Or, you can create a completely custom role to fit your needs. See “Add a user to a role (non-SAML)” on page 51. See “Add a user to a role (SAML)” on page 51. See “Default RBAC roles” on page 41. See “Add a custom RBAC role” on page 48.

Add AD or LDAP domains

Role-based access in the NetBackup web UI supports domain users of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP). Before you can add domain users to RBAC roles, you must add the AD or the LDAP domain. A domain also must be added before you can configure that domain for smart card authentication.

You can use the `POST /security/domains/vxat` API or the `vssat` command to configure domains.

To add an AD or an LDAP domain with the `vssat` command

1. Ensure that the user account (that you specify in the `-m` option in step 3) has the required rights to query the AD or the LDAP server.
2. Log on to the master server as root or administrator.
3. Run the `vssat` command.

   For example, to add an LDAP domain:

```
vssat addldapdomain -d nbudomain -s ldap://example.com -u "OU=Users,DC=example,DC=com"
-g "OU=Groups,DC=example,DC=com" -m "CN=TestUser,OU=Users,DC=example,DC=com" -t msad
```

   For example, to add an AD domain:

```
vssat addldapdomain -d nbudomain -s ldap://domaincontroller.example.com
-u "cn=Users,dc=example,dc=com" -g "cn=Users,dc=example,dc=com"
-m "CN=TestUser,OU=Users,DC=example,DC=com" -t msad
```

   Note that if `domaincontroller.example.com`, then authentication cannot be completed.

4. Verify that the specified AD or LDAP domain was successfully added.

```
vssat validateprpl -p username -d ldap:DomainName -b
localhost:1556:nbatd
```

For more information on the `vssat` command and more of its options, see the NetBackup Command Reference Guide.

Default RBAC roles

The NetBackup web UI provides several default RBAC roles with preconfigured permissions and settings.

Note: Veritas reserves the right to update the RBAC permissions for default roles in future releases. Any revised permissions are automatically applied to users of these roles when NetBackup is upgraded. If you have copies of default roles (or any custom roles that are based on default roles), these roles are not updated automatically. If you want these custom roles to include changes to default roles, you must manually apply the changes or recreate the custom roles.

Administrator

The Administrator role has full permissions for NetBackup and can manage all aspects of NetBackup, including security, storage, protection plans, policies, jobs, and credentials.

Default Cloud Administrator

This role has all the permissions that are necessary to manage cloud assets and to back up those assets with protection plans.

Table 5-4 RBAC permissions for Default Cloud Administrator role

Type	Permissions
Global permissions > NetBackup management	
NetBackup backup images	View Contents, View
Jobs	View
Media server	View
Trusted master servers	View
Snapshot management server plug-ins	View, Create, Update, Manage access
Snapshot management servers	Full permissions
Global permissions > Storage	
Storage units	View
Replication-capable target storage servers	View
Workloads	
Cloud assets	Full permissions
Protection plans	
	Full permissions

Default Microsoft SQL Server Administrator

This role has all the permissions that are necessary to manage SQL Server databases and to back up those assets with protection plans. In addition to this role, the NetBackup user must meet the following requirements:

- Member of the Windows administrator group.
- Have the SQL Server “sysadmin” role.

Table 5-5 RBAC permissions for Default Microsoft SQL Server Administrator role

Type	Permissions
Global permissions > NetBackup management	
Jobs	View
Trusted master servers	View
Global permissions > Storage	
Storage units	View
Replication-capable target storage servers	View
Workloads	
SQL Server assets	Full permissions
Protection plans	
	Full permissions
Credentials	
	Full permissions

Default Resiliency Administrator

This role has all the permissions to protect Veritas Resiliency Platform (VRP) for VMware assets.

Table 5-6 RBAC permissions for Default Resiliency Administrator role

Type	Permissions
Global permissions > NetBackup management	
Resiliency domain	Full permissions

Table 5-6 RBAC permissions for Default Resiliency Administrator role *(continued)*

Type	Permissions
Credentials	
	Full permissions

Default RHV Administrator

This role has all the permissions that are necessary to manage Red Hat Virtualization machines and to back up those assets with protection plans.

Table 5-7 RBAC permissions for Default RHV Administrator role

Type	Permissions
Global permissions > NetBackup management	
Access hosts	View, Create, Delete
Hosts	Update, View
Jobs	View
Resource limits	View, Create, Update, Delete
Trusted master servers	View
Global permissions > Storage	
Storage units	View
Replication-capable target storage servers	View
Workloads	
RHV assets	Full permissions
Protection plans	
	Full permissions

Default Security Administrator

This role has permissions to manage NetBackup security including role-based access control (RBAC), certificates, hosts, identity providers and domains, global security settings, and other permissions. This role can also view settings and assets

in most areas of NetBackup, including workloads, storage, licensing, and other areas.

Table 5-8 RBAC permissions for Default Security Administrator role

Type	Permissions
Global permissions > NetBackup management	
Access hosts	View, Manage access
Data classifications	View, Manage access
Credentials	View, Manage access
Email notifications	View, Manage access
Event logs: Messages, Notifications	View, Manage access
NetBackup hosts	Full permissions
Image sharing: Amazon Machine Image (AMI) Cloud images, Cloud VM IDs	View, Manage access
NetBackup backup images	View, Manage access
Jobs	View, Manage access
Licensing	View, Manage access
Media server	Full permissions
Remote master server certificate authority	Full permissions
Resiliency domain	View, Manage access
Resource limits	View, Manage access
Retention levels	View, Manage access
Trusted master servers	Full permissions
Cloud providers	View, Manage access
Cloud providers: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)	View, Manage access
CloudPoint servers	View, Manage access
WebSocket servers	View, Manage access

Table 5-8 RBAC permissions for Default Security Administrator role *(continued)*

Type	Permissions
Global permissions > Protection	
Policies	View, Manage access
Storage lifecycle policies (SLPs)	View, Manage access
Global permissions > Security	
Security events	View, Manage access
Certificate management: Certificate authorities, ECA, NetBackup certificates, Tokens	Full permissions
Disaster recovery passphrase	Full permissions
Identity provider configuration	Full permissions
Key Management Services	Full permissions
Passphrase constraints	Update (Full permissions)
Global security settings	Full permissions
Trust versions	View, Manage access
User sessions and authentication: API keys, User certificates, User sessions	Full permissions
Global permissions > Storage	
Cloud storage, Disk pools, Storage Key Management Services, Storage servers, Disk volumes, Storage units	View, Manage access
Tape media: Tape media server groups, Tape media volume pools	View, Manage access
Replication-capable target storage servers	View, Manage access
Workloads	
Cloud, SQL Server, RHV, VMware	View, Manage access
Protection plans	

Table 5-8 RBAC permissions for Default Security Administrator role *(continued)*

Type	Permissions
View, Manage access	
Credentials	
View, Manage access	

Default Storage Administrator

This role has permissions to configure and manages disk-based storage and cloud storage.

Table 5-9 RBAC permissions for Default Storage Administrator role

Type	Permissions
Global permissions > NetBackup management	
Media server	View
Remote master server certificate authority	View
Trusted master servers	View, Create, Update, Delete
Global permissions > Security	
NetBackup security tokens	View, Create
Key Management Services	View, View key details
Global permissions > Storage	
Cloud storage	View
Disk pools	View, Create, Update, Delete
Storage servers	View, Create, Update, Delete
Disk volumes	View, Create, Update
Storage units	View, Create, Update, Delete
Replication-capable target storage servers	View

Default VMware Administrator

This role has all the permissions that are necessary to manage VMware virtual machines and to back up those assets with protection plans.

Table 5-10 RBAC permissions for Default VMware Administrator role

Type	Permissions
Global permissions > NetBackup management	
Access hosts	View, Create, Delete
Hosts	View, Update
Host properties	View, Create, Update
NetBackup images	View, View contents
Jobs	View
Resource limits	View, Create, Update, Delete
Trusted master servers	View
Global permissions > Storage	
Storage units	View
Replication-capable target storage servers	View
Workloads	
VMware assets	Full permissions
Protection plans	
Full permissions	

Add a custom RBAC role

Create a custom RBAC role if you want to manually define the permissions and the access that users have to workload assets, protection plans, or credentials.

Note: You can only use the web UI to configure access to workloads, protection plans, and credentials when you first create the custom role. If you want to change those settings after the role is created, you must recreate the role. Or, add an additional role that has the necessary permissions. You can also use the NetBackup APIs to update the custom role.

Note: Veritas reserves the right to update the RBAC permissions for default roles in future releases. Any revised permissions are automatically applied to users of these roles when NetBackup is upgraded. Any copies of default roles (or any custom roles that are based on default roles) are not automatically updated.

To add a custom RBAC role

1. On the left, select **Security > RBAC** and click **Add**.
2. Select the type of role that you want to create.

   You can make a copy of a default role that contains all the preconfigured permissions and settings for that type of role. Or, select **Custom role** to manually configure all the permissions for a role.
3. Provide a **Role name** and a description.

   For example, you may want to indicate that role is for any users that are backup administrators for a particular department or region.
4. On the **Permissions** card, click **Assign**.

   See "Role permissions" on page 52.

   The permissions that you select determine the other settings that you can configure for the role.

   If you select a default role type, certain permissions are enabled only if they are required for that type of role. (For example, the Storage Administrator does not require permissions for protection plans. The Microsoft SQL Server Administrator requires credentials.)

   - The **Workloads** card is enabled when you select **Asset** permissions.
   - The **Protection plans** card is enabled when you select **Protection plans** permissions.
   - The **Credentials** card is enabled when you select **Credentials** permissions.
5. Configure the permissions for the role.

   See "Role permissions" on page 52.
6. On the **Select users** card, click **Assign**.
7. When you are done configuring the role, click **Save**.

Edit or remove a role a custom role

You can edit or remove a custom role when you want to change or remove permissions for users with that role. Note that settings for **Assets**, **Protection plans**, and **Credentials** only can be edited when you add a role. Default roles cannot be edited or removed. You can only add or remove users from default roles.

Edit a custom role

Note: When you change permissions for a custom role, the changes affect all users that are assigned to that role.

To edit a custom role

1. On the left, click **Security > RBAC**.
2. Click on the **Roles** tab.
3. Locate and click on the custom role that you want to edit.
   - To edit the role description, click **Edit description**.
   - The role name cannot be changed after you create the role.
   - To edit permissions for the role, click **Edit**.
   - To add or remove users for the role, click the **Users** tab.
     See "Add a user to a role (non-SAML)" on page 51.
     See "Remove a user from a role" on page 52.

Remove a custom role

Note: When you remove a role, any users that are assigned to that role lose the permissions that the role provided.

To remove a custom role

1. On the left, click **Security > RBAC**.
2. Click the **Roles** tab.
3. Locate the custom role that you want to remove and select the check box for it.
4. Click **Remove > Yes**.

View users in RBAC

You can view the users that have been added to RBAC and the roles that they are assigned to. The **Users** list is view-only. To edit the users that are assigned to a role, you must edit the role.

To view the users in RBAC

1. On the left, click **Security > RBAC**.
2. Click on the **Users** tab.
3. The **Roles** column indicates each role to which the user is assigned.

Add a user to a role (non-SAML)

This procedure describes how to add a non-SAML user or group to a role so the user has the permissions that the role provides. Non-SAML users use one of the following sign-in methods: **Sign in with username and password** or **Sign in with smart card**. After a user is added to a role, the user must sign out and sign in again before the user's permissions are updated.

To add a user to a role (non-SAML)

1. On the left, click **Security > RBAC**.
2. Click the **Roles** tab.
3. Click on the role name, then click on the **Users** tab.
4. (Conditional) From the **Sign-in type** list, select **Default sign-in or smart card**.

   Note: The **Sign-in type** list is only available if there is an IDP configuration available for NetBackup.
5. Enter the user or the group name that you want to add.

For this type of user	Use this format	Example
Local user or group	*username*	**jane_doe**
	groupname	**admins**
Windows user or group	*DOMAIN**username*	**WINDOWS\Admins**
	DOMAIN\groupname	**WINDOWS\jane_doe**
UNIX user or group	*username@domain*	**john_doe@unix**
	groupname@domain	**admins@unix**

6. Click **Add to list**.

Add a user to a role (SAML)

This procedure describes how to add a SAML user or group to a role so the user has the permissions that the role provides. SAML users use one of the following

sign-in methods: **SAML user** or **SAML group**. After a user is added to a role, the user must sign out and sign in again before the user's permissions are updated.

To add a user to a role (SAML)

1. On the left, click **Security > RBAC**.
2. Click the **Roles** tab.
3. Click on the role name, then click on the **Users** tab.
4. From the **Sign-in type** list, select the sign-in method **SAML user** or **SAML group**.
5. Enter the user or the group name that you want to add.

Format	Example
username@domain	**john_doe@unix**
groupname@domain	**admins@unix**

6. Click **Add to list**.

Remove a user from a role

You can remove a user from a role when you want to remove permissions for that user.

If a user is removed from a role, the user must sign out and sign in again before the user's permissions are updated.

To remove a user from a role

1. On the left, click **Security > RBAC**.
2. Click the **Roles** tab.
3. Click on the role that you want to edit, select the **Users** tab.
4. Locate the user you want to remove and click **Actions > Remove > Remove**.

Role permissions

Role permissions define the operations that roles users have permission to perform.

Table 5-11 Role permissions for NetBackup RBAC

Category	Description
Global	Global permissions apply to all assets or objects. For example, currently **Jobs** or **Hosts** permissions cannot be applied to specific jobs or hosts. A role with **Jobs** or **Hosts** permissions apply to all jobs or hosts.
■ **NetBackup management**	Configuration and management of NetBackup. See "Global > NetBackup management" on page 54.
■ **Protection**	NetBackup backup policies and storage lifecyle policies. See "Global > Protection" on page 66.
■ **Security**	NetBackup security settings. See "Global > Security" on page 67.
■ **Storage**	Manage backup storage settings. See "Global > Storage" on page 76.
Assets	Manage assets Cloud, SQL Server, RHV, Universal shares, and VMware. See "Assets" on page 81. **Note:** Assets can only be added when you create a role and cannot be added to an existing role.
Protection plans	Manage how backups are performed with protection plans. See "Protection plans" on page 88. **Note:** Protection plans can only be added when you create a role and cannot be added an existing role.
Credentials	Manage credentials for SQL Server and external KMS. See "Credentials" on page 89. **Note:** Credentials can only be added when you create a role and cannot be added to an existing role.

Notes for using NetBackup RBAC

Note the following when you configure the permissions for RBAC roles:

- RBAC only controls access to the web UI and not the NetBackup Administration Console.

- When you create roles, be sure to enable the minimal number of permissions so the user can sign in to and use the web UI. Some individual permissions do not have a direct correlation with a screen in the web UI. Users that attempt to sign in but that only have a permission of this kind receive an "Unauthorized" message.
- If a user is added to or removed from a role, the user must sign out and sign in again before the user's permissions are updated.
- Most permissions are not implicit.
  In most cases a **Create** permission does not give a user **View** permission. A **Recovery** permission does not give a user **View** permission or other recovery options like **Overwrite**.
- Not all RBAC-controlled operations can be used from the NetBackup web UI. (For example, NetBackup backup images can only be viewed and managed from the APIs or the NetBackup Administration Console.) These types of operations are included in RBAC so a role administrator can create roles for API users as well as web UI users.
- Some tasks require a user to have permissions in multiple RBAC categories. For example, to establish a trust relationship with a remote master server, a user must have permissions for both **Remote master servers** and **Trusted master servers**.

Global > NetBackup management

NetBackup Web Management Console Administration

With guidance from Veritas Support, a user with these permissions can create diagnostic files to troubleshoot NetBackup and perform JVM garbage collection. These operations are only available from the NetBackup APIs. Refer to the following guides for information on JVM tuning options.

NetBackup Installation Guide

NetBackup Upgrade Guide

Table 5-12 RBAC permissions for NetBackup Web Management Console administration

Operation	Description
Dump diagnostics	Take a thread dump or heap dump and write it to a file. Returns the file path to the created thread dump file on the master server.

Table 5-12 RBAC permissions for NetBackup Web Management Console administration *(continued)*

Operation	Description
Garbage collection	Request that the NetBackup Web Service JVM perform a garbage collection. This API is a private API.

Access hosts

An access host acts as a channel to establish an indirect communication between the NetBackup master server and the RHV manager or the VMware server. This host is the “backup host” during backups and the “recovery host” when it performs a restore.

Table 5-13 RBAC permissions for access hosts

Operation	Description	Additional required operations
View	View the access hosts that are configured for VMware or RHV.	
Create	Add an access host for VMware or RHV.	View
Delete	Delete an access host that is configured for VMware or RHV.	View
Manage access	See “Manage access” on page 90.	View

Data classification

The data classification policy attribute specifies the classification of the policy that stores the backup. These levels can be created and edited from the NetBackup Administration Console in **Host Properties > Data Classification**.

Table 5-14 RBAC permissions for data classifications

Operation	Description	Additional required operations
View	View and select the data classification level in the NetBackup policy attributes.	View
Manage access	See “Manage access” on page 90.	

Email notifications

These permissions allow a user to view and manage the settings for the email notifications that are created for use with a ticketing system. In the NetBackup web UI these settings are found in **Settings > Email notifications**. Configuration that is available in the NetBackup Administration Console for other notification types (backup administrator or host administrator) are not yet available for the NetBackup web UI.

Table 5-15 RBAC permissions for NetBackup email notifications

Operation	Description	Additional required operations
View	View the settings for email notifications for job failures.	
Update	Update the settings for email notifications for job failures.	View
Manage access	See "Manage access" on page 90.	View

Event logs

Permissions for event log messages allow users to view and manage message resource bundles from external services. Permissions for event log notifications allow users to view and manage NetBackup notifications. .

Note: A user that has only these permissions cannot sign into the web UI.

Event log messages

Note: These operations are only available from the NetBackup APIs.

Table 5-16 RBAC permissions for event log messages

Operation	Description
View	View messages from external services. (For example, VRP or Picasso.)
Create	Create event log messages for external services.
Update	Update event log messages for external services.
Delete	Delete event log messages for external services.

Table 5-16 RBAC permissions for event log messages *(continued)*

Operation	Description
Manage access	See "Manage access" on page 90.

Event log notifications

Table 5-17 RBAC permissions for event log notifications

Operation	Description
View	Display the bell icon in the toolbar, NetBackup notifications, and any notifications for external services.
Create	Create event log notifications for external services. This operation is only available from the NetBackup APIs.
Manage access	See "Manage access" on page 90.

NetBackup hosts

Note: Though the **Hosts** settings appear under the **Security** node in the NetBackup web UI, giving a user all RBAC "Security" permissions does not give the user "Hosts" permissions.

The **NetBackup hosts** permissions allow a user to view and manage hosts and host mappings.

Minimally the **View** permission is also required to enable the following settings and functionality in the NetBackup web UI: **User sessions**, **Processes** and **Daemons** in the Activity monitor, **Jobs**, notifications in the toolbar, and **Auto discovery** settings for RHV and VMware.

Table 5-18 RBAC permissions for NetBackup hosts

Operation	Description	Additional operation requirements
View	View the NetBackup hosts for the master server.	To see the daemons running on a media server: NetBackup management > Servers > Media server > View See "Media server" on page 61.

Table 5-18 RBAC permissions for NetBackup hosts *(continued)*

Operation	Description	Additional operation requirements
Create	Add a host record to an external certificate authority. This operation is only available from the APIs.	
Update	Allow or revoke auto reissue certificate.	View
Manage access	See "Manage access" on page 90.	View
Comment hosts	Add a comment that provides additional information about a NetBackup host.	View
Delete host mappings	Delete a host mapping or a shared or a cluster mapping.	View
Reset host properties	Reset the host properties, including the host mapping information and communication status for a host.	View
Update host mappings	Add a host mapping or a shared or a cluster mapping. Approve or reject automatic host mappings.	View
View host mappings	View the host mappings for the hosts on the master server. This operation is only available from the APIs and is not required for any functionality with the web UI.	

Host properties

The **Host properties** permissions allow a user to manage the configuration settings for NetBackup hosts. These operations are only available from the NetBackup APIs.

Table 5-19 RBAC permissions for host properties

Operation	Description	Additional operation requirements
View	View the configuration settings for a host.	
Create	Add a configuration setting for a host.	
Update	Update a configuration setting for a host.	
Delete	Delete a configuration setting for a host or return the setting to its default value.	
Manage access	See "Manage access" on page 90.	

Image sharing

These permissions allow a user to find and restore backup images that are stored in cloud storage.

Table 5-20 RBAC permissions for image sharing

Operation		Description
Amazon Machine Images (AMI)		
	View	View Amazon Machine Images (AMI) in the Amazon Web Service.
	Manage access	See "Manage access" on page 90.
Cloud images		
	View	View the shared cloud images.
	Manage access	See "Manage access" on page 90.
	Import shared cloud images	Import the shared cloud images to the NetBackup catalog.
Cloud VM IDs		
	View	View the cloud VM IDs that are generated by cloudrecover API.
	Manage access	See "Manage access" on page 90.

NetBackup backup images

Note: The **View** and **View content** permission for NetBackup backup images is also required to restore files and folders from a VMware image or an instant access image.

View and manage NetBackup images, including changing the image expiration and manage copies.

Table 5-21 RBAC permissions for NetBackup backup images

Operation	Description
View	View the attributes of the backup images. This operation is only available from the NetBackup APIs.
Manage access	See "Manage access" on page 90.

Table 5-21 RBAC permissions for NetBackup backup images *(continued)*

Operation	Description
Change expiration	Update the expiration date of the backups in the image catalog and media in the media catalog. This operation is only available from the NetBackup APIs.
Manage copies	Manage duplicate copies of a backup image. This operation is only available from the NetBackup APIs.
View contents	View the contents of the backup image, including the files in the image. This operation is only available from the NetBackup APIs.

Jobs

Note: The ability to view daemons and processes in the Activity monitor requires **NetBackup hosts** and, optionally, **Media servers**.

Table 5-22 RBAC permissions for Jobs

Operation	Description
View	View jobs in the Activity monitor and on the NetBackup web UI dashboard.
Update	Perform jobs operations including cancel, suspend, restart, and resume.
Delete	Delete a job.
Manage access	See "Manage access" on page 90.

Licensing

These permissions allow a user to view trend data (usage) for the master server and to view and manage registration keys for Veritas Usage Insights.

Table 5-23 RBAC permissions for licensing

Operation	Description
View	View front-end data usage for the master server or master servers. Retrieve the Usage Insights registration keys from the customer registration key file. Retrieve the active registration key information from the customer registration key file. In the NetBackup web UI, trend data displays in the **Usage** widget on the **Dashboard** and on the **Usage** node.

Table 5-23 RBAC permissions for licensing *(continued)*

Operation	Description
Update	Overwrite the existing customer registration key file for Usage Insights with registration keys and active registration key information. Add the active registration key information to the customer registration key file.
Manage access	See "Manage access" on page 90.

Media server

These permissions allow a user to view the configured media servers for the master server and their supported storage (MSDP, CloudCatalyst, etc.).

Table 5-24 RBAC permissions for media servers

Operation	Description
View	View the configured media server and the storage for the media servers. This operation is only available from the NetBackup APIs.
Manage access	See "Manage access" on page 90.

Remote master server certificate authority

This permission allows a user to view the CA certificates for a remote master servers in other domains.

Table 5-25 RBAC permissions for remote master server certificate authority

Operation	Description	Additional required operations
View	View the CA certificates for remote master servers.	This permission is also needed to add a trust relationship with a remote master server. NetBackup management > Servers > Trusted master servers > View NetBackup management > Servers > Trusted master servers > Create See "Servers > Trusted master servers" on page 63.
Manage access	See "Manage access" on page 90.	

Resiliency

These permissions allow a user to view and manage the Veritas Resiliency Platform.

Table 5-26 RBAC permissions for **Resiliency domain**

Operation	Description	Additional required operations
View	View the details of the Veritas Resiliency Platform.	
Create	Add a Resiliency Platform.	Credentials > View Credentials > Create
Update	Edit a Resiliency Platform.	View Credentials > View Credentials > Update
Delete	Delete a Resiliency Platform.	View Credentials > View Credentials > Delete
Discover	Refresh the Resiliency Platform.	View
Manage access	See "Manage access" on page 90.	

Resource limits

Resource limits control the number of simultaneous backups that can be performed on a VMware or RHV resource type.

To view and manage resource limits, users must have permissions to view the workload and the workload assets. Those settings are only available when you create a role in the web UI or from the APIs.

Table 5-27 RBAC permissions for resource limits

Operation	Description	Additional required operations
View	View the resource limits that are configured for all workload types.	
Create	Add or edit resource limits.	View
Update	Reset the values to the default settings. (In the web UI, this permission enables the **Reset default settings** button.)	View

Table 5-27 RBAC permissions for resource limits *(continued)*

Operation	Description	Additional required operations
Delete	Delete any override settings in the resource limits.	View Create
Manage access	See "Manage access" on page 90.	View

Retention levels

In a policy, the retention level determines how long NetBackup retains the backups or the archives that are created according to the schedule. This setting applies to the master server.

Note: These operations are only available when you create NetBackup policies. If you do not choose a specific level, the default level of 2 weeks is used.

Table 5-28 RBAC permissions for retention levels

Operation	Description	Additional required operations
View	View the **Retention** level in a policy schedule.	
Update	Update the **Retention** level in a policy schedule.	View
Manage access	See "Manage access" on page 90.	View

Servers > Trusted master servers

These permissions allow a user to view and manage the trusted master servers for the master server. To perform replication operations across NetBackup domains (master servers), both master servers must have a trust relationship set up with the other master.

Table 5-29 Trusted master servers RBAC permissions

Operation	Description	Additional required operations
View	Display the remote master servers that have a trust relationship with the current master server.	

Table 5-29 Trusted master servers RBAC permissions *(continued)*

Operation	Description	Additional required operations
Create	Add a trust relationship with a remote master server.	View NetBackup management > Remote master server certificate authority > View
Update	Update the trust relationship with the remote master server. API only.	
Delete	Remove a trust relationship with a target master server.	View NetBackup management > Remote master server certificate authority > View
Manage access	See "Manage access" on page 90.	

Cloud providers

These permissions allow a user to view and manage cloud plug-ins. These plug-ins include Amazon Web Services (AWS) configuration, Microsoft Azure configuration, and Google Cloud Platform (GCP) configuration.

Table 5-30 RBAC permissions for cloud providers

Operation	Description	Additional required operations
View	View the configured cloud plug-ins.	
Create	Add a cloud configuration.	View
Update	Update a cloud configuration.	View
Manage access	See "Manage access" on page 90.	

Table 5-31 RBAC permissions for Amazon Web Services (AWS) configurations

Operation	Description	Additional required operations
View	View the configured Amazon Web Services (AWS) configurations.	
Create	Add an AWS configuration.	View
Update	Update an AWS configuration.	View
Manage access	See "Manage access" on page 90.	

Table 5-32 RBAC permissions for Microsoft Azure configurations

Operation	Description	Additional required operations
View	View the Azure configurations.	
Create	Add an Azure configuration.	View
Update	Update an Azure configuration.	View
Manage access	See "Manage access" on page 90.	

Table 5-33 RBAC permissions for Google Cloud Platform (GCP) configurations

Operation	Description	Additional required operations
View	View the configured GCP configurations.	
Create	Add a GCP configuration.	View
Update	Update a GCP configuration.	View
Manage access	See "Manage access" on page 90.	

CloudPoint servers

These permissions allow a user to view and manage CloudPoint servers for the master server and to associate the media servers with the CloudPoint server.

Table 5-34 RBAC permissions for CloudPoint servers

Operation	Description	Additional required operations
View	View a CloudPoint server.	
Create	Add a CloudPoint server.	
Update	Update a CloudPoint server.	View
Discover	Manually start discovery for a CloudPoint server.	View
Update associated media servers	Associate a media server or update the media servers that are associated with the CloudPoint server.	View Update View associated media servers

Table 5-34 RBAC permissions for CloudPoint servers *(continued)*

Operation	Description	Additional required operations
View associated media servers	View the media servers that are associated with the CloudPoint server.	View Update Global > NetBackup management > Media server > View
Manage access	See "Manage access" on page 90.	

WebSocket servers

These permissions manage the NetBackup WebSocket Service (NBWSS), which allows applications in the cloud to communicate with a NetBackupmaster server that is behind a firewall. NBWSS uses the WebSocket protocol to create a secure connection to the application's server in the cloud. On that connection, the application can interact with NetBackup by invoking REST APIs and can receive notifications from NetBackup.

The operations for WebSocket servers are only available from the NetBackup APIs and the NetBackup Administration Console.

Table 5-35 RBAC permissions for WebSocket servers

Operation	Description	Additional required operations
View	List all the WebSocket servers. Allows a user to validate the WebSocket server with the `validateHost` and `validateUrl` APIs.	
Create	Add a WebSocket server.	View
Update	Update the state of a host in WebSocket servers list.	View
Delete	Remove a WebSocket server.	View
Manage access	See "Manage access" on page 90.	

Global > Protection

Policies

Users that have protection permissions can view or perform operations on NetBackup policies with the web UI and APIs. Policy types are limited to MS-Windows, Standard, Oracle, and MS-SQL-Server.

Note: It is recommended that only users with the **Administrator** role manage policies. A user may not have sufficient permissions to perform all policy management operations unless the user is a member of the **Administrator** role.

Table 5-36 RBAC permissions for policies

Operation	Description
View	View policies.
Create	Create policies.
Update	Update policies.
Delete	Delete policies.
Manual backup	Start a manual backup for a policy.
Manage access	See "Manage access" on page 90.

Storage lifecycle policies

Users that have protection permissions can view or perform operations on storage lifecycle policies, using the NetBackup APIs.

Table 5-37 RBAC permissions for storage lifecycle policies

Operation	Description
View	View the details of the storage lifecycle policies or of an individual storage lifecycle policy.
Create	Create a storage lifecycle policy.
Update	Update a storage lifecycle policy.
Delete	Delete a storage lifecycle policy.
Manage access	See "Manage access" on page 90.

Global > Security

Access control

Access control permissions allow a user to view or manage RBAC users and RBAC roles.

Note: In the NetBackup web UI, a user must have permissions in both **Users** and **Roles** to be able to view users or to add or remove users from a role.

Users

Table 5-38 RBAC permissions for users

Operation	Description	Additional required operations
View	API only. View users or groups in RBAC. This permission is granted automatically when the administrator uses the web UI to create a role.	N/A
Manage access	See "Manage access" on page 90.	
Assign access to role	Assign users or groups to or remove them from RBAC roles.	View

Roles

Table 5-39 Roles

Operation	Description	Additional required operations
View	View RBAC roles.	One or more of the following permissions are also required: Create Update Delete
Create	Add RBAC roles.	View Note: If you want a role administrator to be able to grant access to certain RBAC categories in the NetBackup web UI (or namespaces), that administrator must also have **View** and **Manage access** on those namespaces. For example, a role administrator can only create a role for a VMware administrator if that administrator has **View** and **Manage access** on VMware assets (`|ASSETS|VMWARE|`) or on a parent-level namespace.

Table 5-39 Roles *(continued)*

Operation	Description	Additional required operations
Update	Edit the permissions that are related to an RBAC role.	View In the NetBackup web UI, an administrator can grant access for the namespaces on which the administrator has **Manage access**.
Delete	Delete an RBAC role.	View
Manage access	See "Manage access" on page 90.	
Assign access to role	API only. Allow a role to have access to objects in RBAC. This permission is granted automatically when the administrator uses the web UI to create a role.	N/A

Security events

These permissions allow a user to view and manage access to user access history and the audit events that log any user-initiated changes that are made to NetBackup.

Table 5-40 Security events

Operation	Description	Additional required operations
View	View the access history and the audit events for the master server.	
View	Manage the **Audit event** settings. These settings allow the user to select the audit event categories that display in the **Audit events**.	NetBackup management > NetBackup hosts > View NetBackup management > NetBackup hosts > Create NetBackup management > NetBackup hosts > Update NetBackup management > NetBackup hosts > Delete
Manage access	See "Manage access" on page 90.	

Certificate management

The certificate management permissions allow users to manage the NetBackupcertificate authorities and certificates and to manage how NetBackup uses any external certificate authorities.

NetBackup certificate authority

The NetBackup certificate authority permissions allow users to manage the process of migrating the NetBackup Root CA to a higher key strength.

Table 5-41 NetBackup certificate authority

Operation	Description
Manage access	See "Manage access" on page 90.
Migrate CA	View and migrate the NetBackup Root CA to 2048-bit key strength or higher.
View hosts migrate CA	View the NetBackup hosts that are not yet migrated (pending) to the 2048-bit key strength or higher NetBackup Root CA.

External certificates

The external certificates permissions allow users to manage how NetBackup uses certificates from an external certificate authority. Configuration for external certificates is only available from the NetBackup APIs. See the NetBackup Security APIs.

Note: To view external certificates in the NetBackup web UI, a user must have **NetBackup certificates > View**.

Table 5-42 RBAC permissions for external certificates

Operation	Description
Create	Associate the external certificate details with the host ID of the host.
Delete	Removes the association of the host ID to the external certificate.
Manage access	See "Manage access" on page 90.
Reset certificate	Resets the values of the external certificate except the subject. The certificate fields are populated again during certificate enrollment.

NetBackup certificates

NetBackup certificates permissions allow users to view and manage NetBackup security certificates. Note that permissions for NetBackup tokens are separate.

Table 5-43 NetBackup certificates

Operation	Description
View	View the details of the NetBackup security certificates and view any external certificates that NetBackup hosts use.
Manage access	See "Manage access" on page 90.
Dissociate NetBackup security certificates	Dissociates the NetBackup host name from the certificate it is currently associated with.
Revoke	Revoke NetBackup security certificates.

NetBackup security tokens

Permissions for NetBackup security tokens allow users to view and manage NetBackup security tokens. Note that permissions for NetBackup certificates are separate.

Table 5-44 RBAC permissions for NetBackup security tokens

Operation	Description
View	View all NetBackup security tokens.
Create	Create a NetBackup security token.
Delete	Delete a NetBackup security token or cleanup expired tokens.
Manage access	See "Manage access" on page 90.

Disaster recovery passphrase

These permissions allow a user to view and manage the passphrase for NetBackup disaster recovery. The passphrase constraints can be changed using the NetBackup APIs or CLIs.

Table 5-45 RBAC permissions for the disaster recovery passphrase

Operation	Description
View	View the **Disaster recovery** tab in the NetBackup web UI. View if the disaster recovery passphrase is set.
Create	Add or change the disaster recovery passphrase.
Manage access	See "Manage access" on page 90.

Identity provider configuration

These permissions provide access control on NetBackup authentication service (VxAT) domains and on the identity provider configurations (Single Sign-On or SSO authentication using a SAML server).

Note: Configuration for VxAT and identity providers must be done from the command line or APIs. These configurations are not currently available from the web UI.

Table 5-46 Identity provider configuration

Operation	Description
View	View and validate the configured VxAT domains. View all the configured SAML identity provider configurations.
Create	Add a domain to NetBackup through VxAT. Add a SAML identity provider configuration.
Update	Update a SAML identity provider configuration.
Delete	Delete a configured VxAT domain. Delete a SAML identity provider configuration.
Manage access	See "Manage access" on page 90.

Key Management Services (KMS)

With KMS permissions a user can view and manage NetBackup KMS, external KMS, or configure encryption for a storage server or a disk volume. These operations are only available from the NetBackup APIs.

Table 5-47 Key Management Service

Operation	Description
View	View the KMS configuration details.
Create	Add a KMS configuration in NetBackup.
Update	Update a KMS configuration in NetBackup.
Delete	Delete a KMS configuration in NetBackup.
Manage access	See "Manage access" on page 90.
Create key	Create a key on the key management server.
Validate KMS details	Validate that NetBackup can communicate with the key management server, based on the server details and credentials in the configuration.
View key details	View the key details.

Passphrase constraints

These permissions allow a user to change the constraints for the disaster recovery passphrase. This operation is only available from the NetBackup APIs and CLI (`nbseccmd -setpassphraseconstraints`).

Table 5-48 Passphrase constraints

Operation	Description
Update	Update the constraints for the disaster recovery passphrase. The disaster recovery passphrase is configured in the **Settings > Global security settings > Disaster recovery** settings.

Global security settings

These permissions manage access control on the **Global security** settings for the NetBackup master server.

Table 5-49 Security properties

Operation	Description
Update	Manage security settings for the NetBackup master server. These settings affect communication with 8.0 and earlier hosts, automatic mapping of host ID to host names, and the security level for certificate deployment. See "Certificate authority for secure communication" on page 119. **Note:** Permissions for trusted master servers are located in the **NetBackup management > Trusted master servers** RBAC settings.
Manage access	See "Manage access" on page 90.

Trust versions

These permissions allow a user to view the trust version and its details for the master server. The trust version defines the certificate authority (CA) in the domain that hosts must trust. These operations are only available from the NetBackup APIs.

Table 5-50 RBAC permissions for trust versions

Operation	Description
View	View the trust version details of the trust version, including which CA must be part of trust store.
Manage access	See "Manage access" on page 90.

User sessions and authentication

API keys

These permissions allow a user to view and manage NetBackup API keys.

A NetBackup-authenticated user can view and manage their own API key using the web UI. If a user is not assigned to a role, the user can use the NetBackup APIs to manage their API.

Table 5-51 RBAC permissions for API keys

Operation	Description	Additional required operations
View	View API keys.	

Table 5-51 RBAC permissions for API keys *(continued)*

Operation	Description	Additional required operations
Create	Create API keys.	**View**
Update	Change the expiration date for an active API key.	**View**
Delete	Delete API keys.	**View**
Manage access	See "Manage access" on page 90.	

User certificates

These permissions allow a user to view and manage the configuration that allows NetBackup authentication with user certificates or smart cards. Note: Authentication domains must be configured for the master server before you can configure and enable smart card authentication.

Table 5-52 User certificates

Operation	Description	Additional required operations
View	View settings for smart card authentication.	Global > Security > Global security settings > Update
Create	Upload external CA certificates to the smart card authentication trust-store.	Global > Security > Global security settings > Update
Delete	Delete external CA certificates from the smart card authentication trust-store.	Global > Security > Global security settings > Update
Manage access	See "Manage access" on page 90.	

User sessions

Note: Users also need **Hosts** permissions to view the **User account settings** in User sessions. See "NetBackup hosts" on page 57.

These permissions allow a user to view and manage user sessions and user account settings.

Table 5-53 RBAC permissions for user sessions

Operation	Description	Additional required operations
View	View active user sessions.	
Update	Enable, update, or disable sign-in banner configuration in the **User account settings**.	View NetBackup management > Hosts > View
	Enable, update, or disable the following settings in the **User account settings**. ■ Maximum concurrent sessions ■ User account lockout ■ Sign-in banner configuration	Update NetBackup management > Hosts > View NetBackup management > Hosts > Create NetBackup management > Hosts > Update
Delete		
Close user session	Close the selected user sessions.	View
Close all user sessions	Close all user sessions. Without this permission, the administrator can only close the selected user sessions.	View
Unlock	Unlock a user that has an account that is locked out of NetBackup.	View locked
View locked	View any users that are locked out of NetBackup.	
Manage access	See "Manage access" on page 90.	View

Global > Storage

Storage permissions include the following categories:

- See "Cloud storage" on page 77.
- See "Disk pools" on page 77.
- See "Storage Key Management Services" on page 78.
- See "Storage servers" on page 78.
- See "Storage units" on page 79.
- See "Replication-capable target storage servers " on page 80.

The storage permissions allow a user to administer storage for backups, replication, and long-term retention.

Cloud storage

These permissions allow users to view the configurations for cloud “Storage as a Service” (STaaS) vendors that NetBackup supports.

Table 5-54 RBAC permissions for cloud storage

Operation	Description	Additional required operations
View	View the NetBackup-supported configurations of a cloud storage vendor.	
Manage access	API only. See “Manage access” on page 90.	**View**

Disk pools

These permissions allow a user to view and manage disk pools for use with AdvancedDisk, cloud, MSDP, OpenStorage, and replication.

Table 5-55 RBAC permissions for disk pools

Operation	Description	Additional required operations
View	View disk pools.	Global > Storage > Storage servers > View Global > Storage > Replication-capable target storage servers > View
Create	Create disk pools.	View Global NetBackup management > Servers > Trusted master servers > View Global > Storage > Replication-capable target storage servers > View
Update	Inventory and update the configuration for disk pools.	View Global > Servers > Trusted master servers > View Global > Storage > Replication-capable target storage servers > View
Delete	Delete disk pools.	View
Manage access	API only. See “Manage access” on page 90.	View

Storage Key Management Services

Permissions for Storage Key Management Services (KMS) allow a user to encrypt a storage server or a disk volume with NetBackup KMS or with external KMS. These operations are only available from the NetBackup APIs.

Permissions for KMS are managed in **Security**. See "Key Management Services (KMS)" on page 72.

Table 5-56 RBAC permissions for Storage Key Management Services

Operation	Description	Additional required operations
View	View the key management services that are available in NetBackup.	
Manage access	See "Manage access" on page 90.	**View**

Storage servers

Note: In NetBackup 8.3 and 9.0, universal shares are only supported with Media Server Deduplication Pool (MSDP).

Permissions for storage servers allow user to view and manage storage servers and universal shares.

Permissions to view and create instant access mounts from universal shares backups are in **RBAC > Assets > Universal shares**. See "Assets" on page 81.

Table 5-57 RBAC permissions for storage servers

Operation	Description	Additional required operations
View	View storage servers or universal shares.	To view cloud storage servers: Global > NetBackup management > Cloud providers > View
Create	Add storage servers or universal shares.	View Global > NetBackup management > Media server > View If you want to encrypt the storage server: Global > Security > Key Management Services > View

Table 5-57 RBAC permissions for storage servers *(continued)*

Operation	Description	Additional required operations
Update	Edit the settings for storage servers or universal shares.	View
Delete	Delete a storage server or universal share.	View
Manage access	API only. See "Manage access" on page 90.	View

Disk volumes

These permissions allow users to view and manage disk volumes on a storage server.

Table 5-58 Permissions for disk volumes

Operation	Description	Additional required operations
View	View the disk volumes for a storage server.	Global > Storage > Storage servers > View Global > Storage > Disk pools > View
Create	Create a disk volu me for a storage server.	View If you want to encrypt the disk volume, you also need the following permission: Global > Security > Key Management Services > View
Update	Modify the attributes of the disk volumes for a storage server.	View
Manage access	API only. See "Manage access" on page 90.	View

Storage units

These permissions allow a user to view and manage storage units.

Table 5-59 Storage units

Operation	Description	Additional required operations
View	View storage units.	View Global > Storage > Disk pools > View Global > Storage > Storage servers > View
Create	Create storage units.	View Global > Storage > Disk pools > View
Update	Modify storage units.	View Global > Storage > Disk pools > View
Delete	Delete storage units.	View
Manage access	API only. See "Manage access" on page 90.	

Tape media

These permissions allow a user to view and manage access to tape media server groups and to tape media volume pools.

Table 5-60 Tape media server groups

Operation	Description
View	View tape media server groups.
Manage access	API only. See "Manage access" on page 90.

Table 5-61 Tape media volume pools

Operation	Description
View	View tape media volume pools.
Manage access	API only. See "Manage access" on page 90.

Replication-capable target storage servers

These permissions allow a user to view and manage the replication relationship for MSDP and CloudCatalyst.

Table 5-62 RBAC permissions for replication-capable target storage servers

Operation	Description	Additional required operations
View	View target storage servers that are available for replication.	Global > Servers > Trusted masters > View
Manage access	API only. See "Manage access" on page 90.	View

Assets

Assets permissions include permissions for the following workloads:

See the section called "Cloud assets" on page 81.

See the section called "Microsoft SQL Server assets" on page 82.

See the section called "RHV assets" on page 83.

See the section called "Universal shares" on page 85.

See the section called "VMware assets" on page 86.

Cloud assets

Permissions for cloud assets allow users to view, protect, and restore in-cloud workload assets using CloudPoint.

Table 5-63 Permissions for cloud assets

Operation	Description	Additional required operations
View	View cloud assets.	
Manage access	See "Manage access" on page 90.	View
Granular restore	Restore individual files or folders from a cloud asset.	View
Protect	Add Cloud assets to a protection plan.	View
Restore to alternate location	Restore to an alternate location. This permission is required on the source asset.	View On the target asset: Allow restore to overwrite On the target location: View restore targets

Table 5-63 Permissions for cloud assets *(continued)*

Operation	Description	Additional required operations
View restore targets	View the available destinations to which to restore an asset. This permission is required on the target asset.	View
Restore to original location	Restore the cloud asset to its original location.	View On the target location: View restore targets If the original VM exists: Allow restore to overwrite
Allow restore to overwrite	Overwrite an asset if it exists.	View On the target location: View restore targets
Update configuration	Connect to or disconnect from a virtual machine. Add, update, or remove a cloud configuration. Edit VM credentials. Generate a token from CloudPoint to establish communication with the agent on the host.	View

Microsoft SQL Server assets

Permissions for Microsoft SQL Server assets allow users to view, protect, and restore SQL Server assets using the NetBackup for SQL Server agent.

Note: To perform discovery, backups, and restores, valid credentials must exist for an availability group or an instance.

Table 5-64 Permissions for SQL Server assets

Operation	Description	Additional required operations
View	View availability groups, instances, and databases.	
Create	Manually add instances.	View
Update	Update asset details. Add or update credentials for availability replicas or instances.	View

Table 5-64 Permissions for SQL Server assets *(continued)*

Operation	Description	Additional required operations
Delete	Delete availability replicas or instances.	View
Manage access	See “Manage access” on page 90.	View
Restore to alternate location	Restore a database to an alternate server. This permission is required for all SQL Server “MOVE” operations.	View Restore
Discover availability groups	Manually discover availability groups. To perform discovery, valid credentials must be added to one of the availability group replicas.	View
Discover databases	Manually discover databases. To perform discovery, valid credentials must be added to the instance.	View
Instant access	Create an instant access database.	View Restore
Allow restore to overwrite	Overwrite a SQL Server database if it exists.	View Restore
Protect	Add SQL Server assets to or remove them from protection plans.	View
Restore	Restore databases to the original location, a different database, or a different instance.	View
Validate credentials	Validate credentials when they are added (assigned) to an instance or a replica. This permission is required on the asset.	On the asset these additional permissions are needed: View Update On the credential the following permissions are needed: Credentials > View Credentials > Assign credentials

RHV assets

Permissions for RHV assets allow users to view, protect, and restore RHV assets.

Table 5-65 Permissions for RHV assets

Operation	Description	Additional required operations
View	View configured RHV managers and RHV assets.	
	View VM intelligent groups.	On the RHV manager that corresponds to the VM group: View
Create	Add RHV managers.	View
	Add VM intelligent groups.	View
		On the RHV manager that corresponds to the VM group: View
Update	Update asset details. Update VM intelligent group contents. Validate credentials	View
	Update VM intelligent groups.	View
		On the RHV manager that corresponds to the VM group: View
Delete	Delete RHV managers.	View
	Delete VM intelligent groups.	View
		On the RHV manager that corresponds to the VM group: View
Manage access	See "Manage access" on page 90.	View
Protect	Add VMs to or remove them from a protection plan.	View
	Add VM intelligent groups to or remove them from protection plans.	On the RHV manager that corresponds to the VM group: View Protect

Table 5-65 Permissions for RHV assets *(continued)*

Operation	Description	Additional required operations
Restore	Restore to original or to an alternate location.	View Global > NetBackup management > NetBackup backup images > View
		On the target location: View restore targets Global > NetBackup management > Access hosts > View
View restore targets	View the available destinations to which to restore an asset.	View
Allow restore to overwrite	Overwrite an asset if it exists.	View Restore

Universal shares

Note: In NetBackup 8.3 and 9.0, the ability to restore from universal share backups is only available from the NetBackup CLI or the Backup, Archive, and Restore interface. Instant access recovery is only available through the NetBackup APIs.

Permissions for universal share assets allow users to view and create instant access mounts from universal share backups images. Permissions to create and manage universal shares are in **Global > Storage > Storage servers**.

See "Global > Storage" on page 76.

Table 5-66 Permissions for universal shares

Operation	Description
Instant access	View and create instant access mount points on a universal share. Restore from a universal share. Note: When you create a role you can choose whether or not to apply permissions for universal share assets to all and to future universal share assets. If the option is enabled, a role has access to all mount points. Access cannot be provided for individual mount points. Users with this permission can also view the storage server that is associated with the universal share.
Manage access	See "Manage access" on page 90.

VMware assets

Permissions for VMware assets allow users to view, protect, and restore VMware assets.

Table 5-67 RBAC permissions for VMware assets

Operation	Description	Additional required operations
View	View VMs, vCenter servers, and ESX hosts.	
	View VM intelligent groups.	On the vCenter that corresponds to the VM group: View
Create	Add ESX hosts or vCenter hosts. Validate credentials.	View
	Add VM intelligent groups.	View
		On the vCenter that corresponds to the VM group: View
Update	Update ESX hosts or vCenter hosts and their credentials. Validate credentials.	View
	Update VM intelligent groups.	View
		On the vCenter that corresponds to the VM group: View
Delete	Delete ESX hosts or vCenter hosts.	View
	Delete VM intelligent groups.	View
		On the vCenter that corresponds to the VM group: View
Manage access	See “Manage access” on page 90.	View
Restore to cloud	Restore a VM to the cloud.	View

Table 5-67 RBAC permissions for VMware assets *(continued)*

Operation	Description	Additional required operations
Granular restore	Restore individual files or folders from a VM. This permission is required on the source and the target VM.	View Global > NetBackup management > NetBackup backup images > View Global > NetBackup management > NetBackup backup images > View contents
Instant access - Download files	Download individual files using instant access technology.	View Global > NetBackup management > NetBackup backup images > View
Instant access - Restore files	Restore individual files using instant access technology.	View Global > NetBackup management > NetBackup backup images > View Global > NetBackup management > NetBackup backup images > View contents
Instant access	Create an instant access VM.	View Global > NetBackup management > NetBackup backup images > View
Protect	Add VMware assets to or remove them from protection plans.	View
	Add VMware intelligent groups to or remove them from protection plans.	On the vCenter that corresponds to the VM group: View Protect
Restore	Restore to the original or to an alternate location.	View Global > NetBackup management > NetBackup backup images > View Global > NetBackup management > Access hosts > View
		On the target location: View restore targets
View restore targets	View the available destinations to which to restore an asset.	View

Table 5-67 RBAC permissions for VMware assets *(continued)*

Operation	Description	Additional required operations
Allow restore to overwrite	Allow a restore to overwrite an existing asset. Without this permission a user must restore an existing asset to a different location.	View Restore

Protection plans

Permissions for protection plans allow a user to view and manage protection plans and to add assets to a protection plan.

Protecting assets

To view the storage that is associated with a protection plan, a user must also have **View** permission for the **Storage**. This permission is necessary to view the storage when you subscribe an asset to a plan. See "Global > Storage" on page 76.

To add assets to a protection plan or select **Backup now** for an immediate backup, the user needs to have permissions **View** and **Subscribe** on the protection plan. Additionally, the user needs permissions to **View** and **Protect** the assets. See "Assets" on page 81.

Table 5-68 Permissions for protection plans

Operation	Description	Additional required operations
View	View protection plans.	
Create	Create protection plans.	**View** For RHV and VMware: **NetBackup management > Access hosts > View**
Update	Edit protection plans.	**View**
Delete	Delete protection plans.	**View**
Manage access	See "Manage access" on page 90.	**View**
Edit attributes	Edit the protection plan attributes. The attributes that are available to edit depend on the workload.	**View** Subscribe

Table 5-68 Permissions for protection plans *(continued)*

Operation	Description	Additional required operations
Edit full and incremental schedules	Allows users that subscribe assets to the plan to edit the backup start window for any full or any incremental schedules. Note: You cannot edit any exclude dates from the web UI.	**View** Subscribe
Edit transaction log schedules	Allows users that subscribe assets to the plan to edit certain settings for transaction log schedules. These settings can be edited: backup start window, the recurrence (frequency), and the retention. Note: You cannot edit any exclude dates from the web UI.	**View** Subscribe
Subscribe	Allow assets to be subscribed to the plan.	**View**

Credentials

Credential permissions allow a user to view and manage the credentials that are used for the following workloads: Microsoft SQL Server and external Key Management Services (KMS).

When user creates a credential, that user is given full permissions on that credential.

Table 5-69 RBAC permissions for credentials

Operation	Description	Additional required operations
View	View a credential in credential management. Note: If you select **Apply permissions to new and existing credentials** when you create a role, the role has permissions to view all credentials.	
Create	Add a credential to credential management.	View
Update	Update the details of a credential.	View
Delete	Delete a credential from credential management.	View

Table 5-69 RBAC permissions for credentials *(continued)*

Operation	Description	Additional required operations
Manage access	See “Manage access” on page 90.	View
Assign credentials	Allows a credential to be assigned to an asset. This permission is needed on the credential.	On the credential the following permission is also needed: View On the asset the following permissions are needed: View Update To validate credentials, the following permission is needed: Validate credentials

Manage access

The **Manage access** permission allows a user to manage the roles and role permissions for a specific permission category. For example, a user that has **View** and **Manage access** for **User sessions** can view and manage the roles that have access to the **User sessions** settings and the permissions that those roles have. The user must also have **View** on the roles they want to select and give access to **User sessions**.

This permission is available for each permission category. However, for some categories the **Manage access** functionality is only available from the NetBackup APIs and not the NetBackup web UI (indicated with “API only”).

Grant a role the manage access permissions

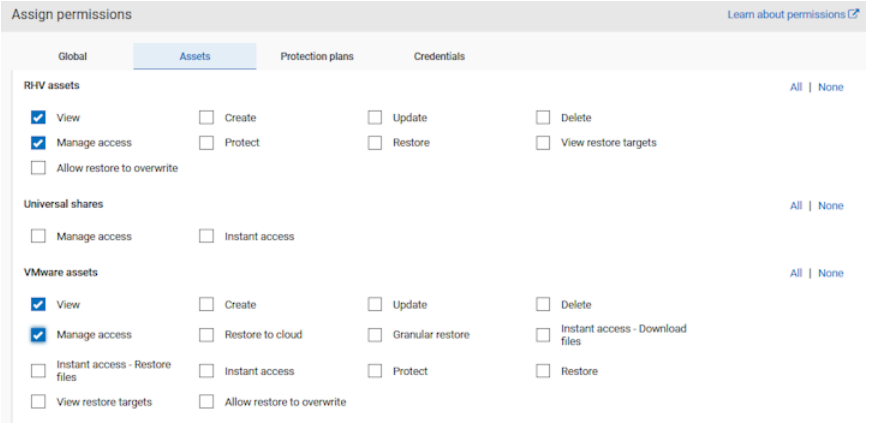
To grant a role manage access permissions

1. On the left, select **RBAC** node and click on the **Roles** tab.
2. Select one of the following:

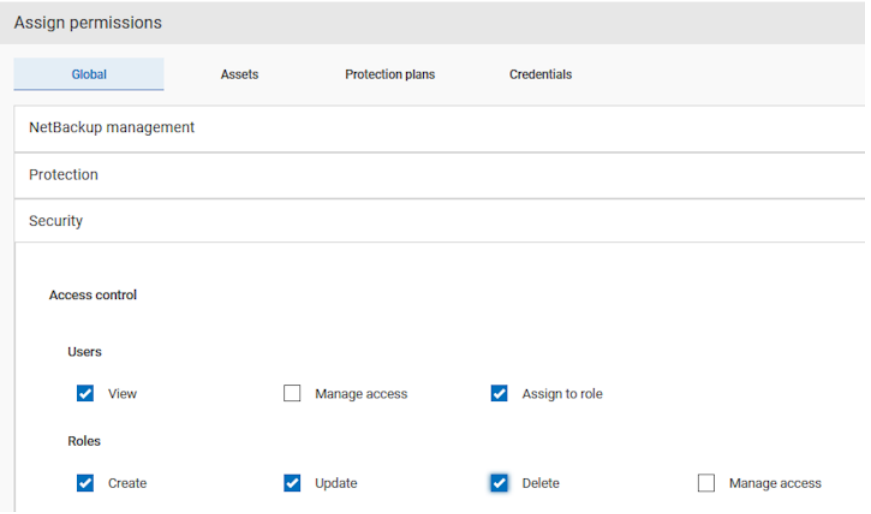
Add a role	Click **Add**. Enter a role name and under **Select permissions**, click **Assign**.
Update a role	Note: Permissions for **Assets**, **Protection plans**, and **Credentials** can only be edited when you add a role. Select the role that you want to edit.

3. For each category that you want the role to have manage access permissions, select the **Manage access** permission.

   For example, you can create a role that can manage access to VMware assets, RHV assets, credentials, and protection plans.



4. Users that manage access also need **Access control** permissions.



Manage the permissions for an area of the web UI

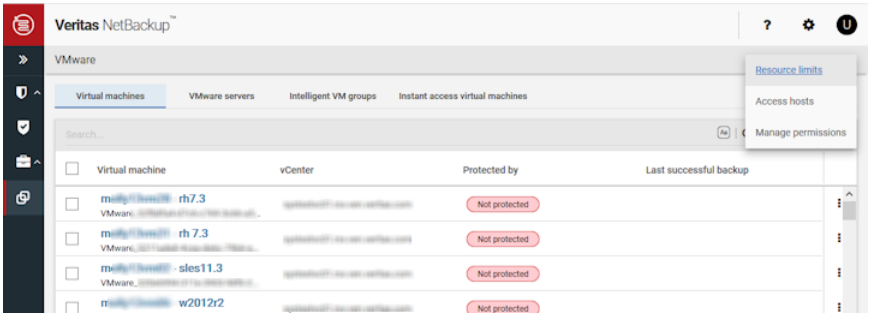
The **Manage access** permission allows a user to manage the roles and role permissions for a specific area of the web UI. For example, a user that has **View** and **Manage access** for **User sessions** can view and manage the roles that have access to the **User sessions** settings and the permissions that those roles have.

Add a role and give access to an area of the web UI

To add a role and give access to an area of the web UI

1. On the left, select the node for which you want to manage access.
2. On the top right, click **Manage permissions**.

   For some categories, the option is available from a menu of options at the top right. For example, for VMware select **VMware settings > Manage permissions**.



3. Click **Add**.
4. Select the role you want to add and select the permissions that you want the role to have.
5. Click **Save**.

Edit the permissions for a role that has access to an area of the web UI

To edit the permissions for a role that has access to an area of the web UI

1. On the left, select the node for which you want to manage access.
2. On the top right, click **Manage permissions**.

   For some categories, the option is available from a menu of options at the top right. For example, for VMware select **VMware settings > Manage permissions**.

3. Select the role that you want to edit and click **Actions > Edit**.
4. Select or remove the permissions for the role and click **Save**.

Remove a role that has access to an area of the web UI

To remove a role that has access to an area of the web UI

1. On the left, select the node for which you want to manage access.
2. On the top right, click **Manage permissions**.

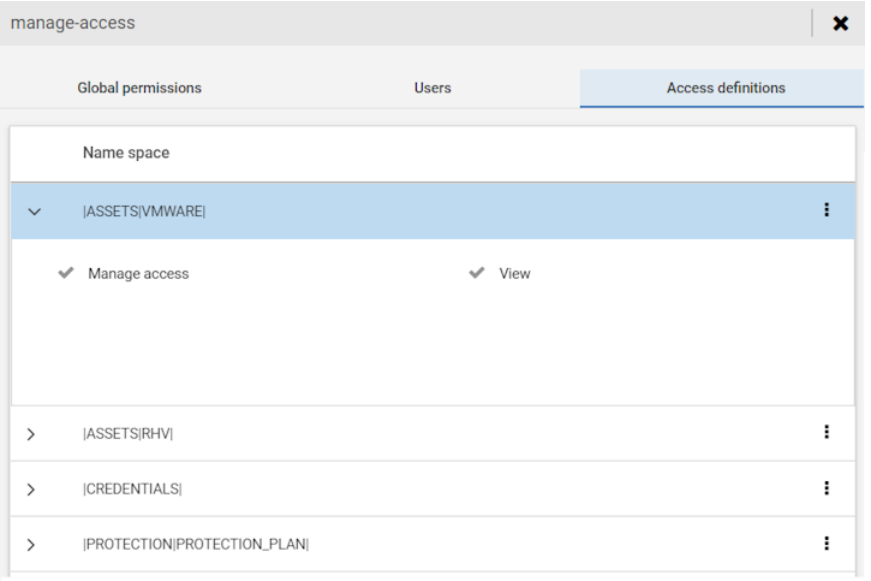
   For some categories, the option is available from a menu of options at the top right. For example, for VMware select **VMware settings > Manage permissions**.
3. Select the role that you want to remove and click **Remove > Remove**.

View access definitions

The **Manage access** permission allows a user to view the access definitions that are related to a role. A user must have **Manage access** specifically on the permission category that they need to manage. For example, VMware or specific VMware objects.

To view access definitions

1. On the left, select **RBAC** node and click on the **Roles** tab.
2. Click on the role.
3. Click on the **Access definitions** tab.



Configure an external certificate for the NetBackup web server

By default, NetBackup uses the security certificates that the NetBackup CA has issued. If you have a certificate that an external CA has issued, you can configure the NetBackup web server to use it for secure communication.

Note: Windows certificate store is not supported as certificate source for the NetBackup web server.

To configure an external certificate for the web server

1. Ensure that you have valid certificate, private key of the certificate, and trusted CA bundle.
2. Run the following command:

   `configureWebServerCerts -addExternalCert -nbHost -certPath` *`certificate path`* `-privateKeyPath` *`private key path`* `-trustStorePath` *`CA bundle path`* `[-passphrasePath` *`passphrase file path`*`]`

   The `configureWebServerCerts` command does not support use of Windows certificate store paths.

   Refer to the NetBackup Commands Reference Guide for more details on the command-line options.

   - In a clustered setup, to avoid a failover run the following command on the active node:

     `install_path``/netbackup/bin/bpclusterutil -freeze`
3. Restart the NetBackup Web Management Console service to reflect the changes.

   On UNIX, run the following commands:

   - *`install_path`*`/netbackup/bin/nbwmc -terminate`
   - *`install_path`*`/netbackup/bin/nbwmc start`

   On Windows, use the **Services** application in the **Windows Control Panel**.

   Location of the commands:

Windows	*`install_path`*`\NetBackup\wmc\bin\install\`
UNIX	*`install_path`*`/wmc/bin/install`

- In a clustered setup, unfreeze the cluster using the following command on the active node:

  install_path/netbackup/bin/bpclusterutil -unfreeze

4. Verify that you can access the NetBackup web user interface using a browser, without a certificate warning message.

Update or renew the external certificate for the web server

You can update or renew the external certificate that you configured for the web server.

To update or renew the external certificate for the web server

1. Ensure that you have the latest external certificate, the matching private key, and the CA bundle file.
2. Run the following command (in a clustered setup, run the command on the active node):

   configureWebServerCerts -addExternalCert -nbHost -certPath *certificate path* -privateKeyPath *private key path* -trustStorePath *CA bundle path*

Remove the external certificate configured for the web server

You can remove the external certificate that is configured for the web server. NetBackup then uses the NetBackup CA-signed certificate for secure communication.

To remove the external certificate configured for the web server

1. Run the following command (in a clustered master server setup, run this command on the active node):

   configureWebServerCerts -removeExternalCert -nbHost

   - In a clustered master server setup, run the following command on the active node to freeze the cluster to avoid a failover:

     install_path/netbackup/bin/bpclusterutil -freeze

2. Restart the NetBackup Web Management Console service.

   - In a clustered master server setup, run the following command on the active node to unfreeze the cluster:

     install_path/netbackup/bin/bpclusterutil -unfreeze

Chapter 6

Security events and audit logs

This chapter includes the following topics:

View security events and audit logs

NetBackup audits user-initiated actions in a NetBackup environment to help answer who changed what and when they changed it. For a full audit report, use the `nbauditreport` command. See "Viewing the detailed NetBackup audit report" on page 102.

To view security events and audit logs

1. On the left, select **Security > Security events**.
2. The following options are available.
   - Click **Access history** to view the users that accessed NetBackup.
   - Click **Audit events** to view the events that NetBackup audited. These events include changes to security settings, certificates, and users who browsed or restored backups images.

About NetBackup auditing

Auditing is enabled by default in new installations. NetBackup auditing can be configured directly on a NetBackup master server.

Auditing of NetBackup operations provides the following benefits:

- Customers can gain insight from audit trails while they investigate unexpected changes in a NetBackup environment.
- Regulatory compliance.
  The record complies with guidelines such as those required by the Sarbanes-Oxley Act (SOX).
- A method for customers to adhere to internal change management policies.
- Help for NetBackup Support in troubleshooting problems for customers.

About the NetBackup Audit Manager

The NetBackup Audit Manager (`nbaudit`) runs on the master server and audit records are maintained in the Enterprise Media Manager (EMM) database.

An administrator can search specifically for:

- When an action occurred
- Failed actions in certain situations
- The actions that a specific user performed
- The actions that were performed in a specific content area
- Changes to the audit configuration

Note the following:

- The audit record truncates any entries greater than 4096 characters. (For example, policy name.)
- The audit record truncates any restore image IDs greater than 1024 characters.

Actions that NetBackup audits

NetBackup records the following user-initiated actions.

Activity monitor actions	Canceling, suspending, resuming, restarting, or deleting any type of job creates an audit record.
Alerts and email notifications	If an alert cannot be generated or an email notification cannot be sent for NetBackup configuration settings. For example, SMTP server configuration and the list of excluded status codes for alerts.
Asset actions	Deleting an asset, such as a vCenter server, as part of the asset cleanup process with the Asset Database API is audited and logged. Creating, modifying, or deleting an asset group as well any action on an asset group for which a user is not authorized is audited and logged.

Authorization failure	Authorization failure is audited when you use the NetBackup web UI, the NetBackup APIs, or Enhanced Auditing.
Catalog information	This information includes: ■ Verifying and expiring images. ■ Read the requests that are sent for the front-end usage data.
Certificate management	Creating, revoking, renewing, and deploying of NetBackup certificates and specific NetBackup certificate failures.
Certificate Verification Failures (CVFs)	Any failed connection attempts that involve SSL handshake errors, revoked certificates, or host name validation failures. For certificate verification failures (CVFs) that involve SSL handshakes and revoked certificates, the timestamp indicates when the audit record is posted to the master server. (Rather than when an individual certificate verification fails.) A CVF audit record represents a group of CVF events over a time period. The record details provide the start and the end times of the time period as well as the total number of CVFs that occurred in that period.
Disk pools and Volume pools actions	Adding, deleting, or updating disk or volume pools.
Hold operations	Creating, modifying, and deleting hold operations.
Host database	NetBackup host database-related operations.
Logon attempts	Any successful or any failed logon attempts for the NetBackup Administration Console, the NetBackup web UI or the NetBackup APIs.
Policies actions	Adding, deleting, or updating policy attributes, clients, schedules, and backup selections lists.
Restore and browse image user actions	All the restore and browse image content (`bplist`) operations that a user performs are audited with the user identity.
Security configuration	Information that is related to changes that are made to the security configuration settings.
Starting a restore job	NetBackup does not audit when other types of jobs begin. For example, NetBackup does not audit when a backup job begins.
Starting and stopping the NetBackup Audit Manager (`nbaudit`).	Starting and stopping of the `nbaudit` manager is always audited, even if auditing is disabled.
Storage lifecycle policy actions	Attempts to create, modify, or delete a storage lifecycle policy (SLP) are audited and logged. However, activating and suspending an SLP using the command `nbstlutil` are not audited. These operations are audited only when they are initiated from a NetBackup graphical user interface or API.
Storage servers actions	Adding, deleting, or updating storage servers.

Storage units actions	Adding, deleting, or updating storage units. **Note:** Actions that are related to storage lifecycle policies are not audited.
Token management	Creating, deleting, and cleanup of tokens and specific token issuing failures.
User management	Adding and deleting Enhanced Auditing users in the Enhanced Auditing mode.
User action that fails to create an audit record	If auditing is enabled but a user action fails to create an audit record, the audit failure is captured in the `nbaudit` log. NetBackup status code 108 is returned (`Action succeeded but auditing failed`). The **NetBackup Administration Console** does not return an exit status code 108 when auditing fails.

Actions that NetBackup does not audit

The following actions are not audited and do not display in the audit report:

Any failed actions.	NetBackup logs failed actions in NetBackup error logs. Failed actions do not display in audit reports because a failed attempt does not bring about a change in the NetBackup system state.
The effect of a configuration change	The results of a change to the NetBackup configuration are not audited. For example, the creation of a policy is audited, but the jobs that result from its creation are not.
The completion status of a manually initiated restore job	While the act of initiating a restore job is audited, the completion status of the job is not audited. Nor is the completion status of any other job type, whether initiated manually or not. The completion status is displayed in the Activity Monitor (Administration Console) and in the Jobs (web UI).
Internally initiated actions	NetBackup-initiated internal actions are not audited. For example, the scheduled deletion of expired images, scheduled backups, or periodic image database cleanup is not audited.
Rollback operations	Some operations are carried out as multiple steps. For example, creating an MSDP-based storage server consists of multiple steps. Every successful step is audited. Failure in any of the steps results in a rollback, or rather, the successful steps may need to be undone. The audit record does not contain details about rollback operations.
Host properties actions	Changes made using the `bpsetconfig` or the `nbsetconfig` commands, or the equivalent property in the Host Properties utility, are not audited. Changes that are made directly to the `bp.conf` file or to the registry are not audited.

User identity in the audit report

The audit report indicates the identity of the user who performed a specific action. The full identity of the user includes the user name and the domain or the host name that is associated with the authenticated user. A user's identity appears in the audit report as follows:

- Audit events always include the full user identity. Root users and administrators are logged as "root@hostname" or "administrator@hostname".
- In NetBackup 8.1.2 and later, image browse and image restore events always include the user ID in the audit event. NetBackup 8.1.1 and earlier log these events as "root@hostname" or "administrator@hostname".
- For any operations that do not require credentials or require the user to sign in, operations are logged without a user identity.

Audit retention period and catalog backups of audit records

The audit records are kept as part of the NetBackup database, for as long as the retention period indicates. The records are backed up as part of the NetBackup catalog backup. The NetBackup Audit Service (`nbaudit`) deletes expired audit records once every 24 hours at 12:00 A.M. (local time).

By default, audit records are kept for 90 days. Use an audit retention period value of `0` (zero) if you do not want to delete the audit records.

To configure the audit retention period

1. Log on to the master server.
2. Open the following directory:

   Windows: *install_path*\NetBackup\bin\admincmd

   UNIX: /usr/openv/netbackup/bin/admincmd
3. Enter the following command:

   ```
   nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD
   number_of_days -machinename masterserver
   ```

   Where *number_of_days* indicates (in days) how long audit records are to be retained for the audit report.

   In the following example, the records of user actions are retained for 30 days and then deleted.

   ```
   nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD 30
   -machinename server1
   ```

   To ensure that audit records are not missed from a catalog backup, configure the catalog backup frequency to be less frequent or equal to the -AUDIT_RETENTION_PERIOD.

Viewing the detailed NetBackup audit report

You can see detailed NetBackup audit event information with the nbauditreport command.

To view the full audit report

1. Log on to the master server.
2. Enter the following command to display the audit report in the summary format.

   Windows: *install_path*\NetBackup\bin\admincmd\nbauditreport

   UNIX: /usr/openv/netbackup/bin/admincmd\nbauditreport

   Or, run the command with the following options.

-sdate <"MM/DD/YY [HH:[MM[:SS]]]">	The start date and time of the report data you want to view.

`-edate` `<"MM/DD/YY [HH:[MM[:SS]]]">`	The end date and time of the report data you want to view.
`-ctgy` *category*	The category of user action that was performed. Categories such as `POLICY` may contain several sub-categories such as schedules or backup selections. Any modifications to a sub-category are listed as a modification to the primary category. See the NetBackup Commands Guide for `-ctgy` options.
`-user` `<`*username*`[:`*domainname*`]>`	Use to indicate the name of the user for whom you'd like to display audit information.
`-fmt DETAIL`	The `-fmt DETAIL` option displays a comprehensive list of audit information. For example, when a policy is changed, this view lists the name of the attribute, the old value, and the new value. This option has the following sub-options: ■ `[-notruncate]` . Display the old and new values of a changed attribute on separate lines in the details section of the report. ■ `[-pagewidth <NNN>]` . Set the page width for the details section of the report.
`-fmt PARSABLE`	The `-fmt PARSABLE` option displays the same set of information as the `DETAIL` report but in a parsable format. The report uses the pipe character (`|`) as the parsing token between the audit report data. This option has the following sub-options: ■ `[-order <DTU|DUT|TDU|TUD|UDT|UTD>]`. Indicate the order in which the information appears. `D` (Description) `T` (Timestamp) `U` (User)

3 The audit report contains the following details:

`DESCRIPTION`	The details of the action that was performed.
`USER`	The identity of the user who performed the action. See "User identity in the audit report" on page 101.
`TIMESTAMP`	The time that the action was performed.

The following information only displays if you use the `-fmt DETAIL` or the `-fmt PARSABLE` options.

`CATEGORY`	The category of user action that was performed.
`ACTION`	The action that was performed.
`REASON`	The reason that the action was performed. A reason displays if a reason was specified for the operation that created the change.
`DETAILS`	An account of all of the changes, listing the old values and the new values.

Example of the audit report:

```
[root@server1 admincmd]# ./nbauditreport
TIMESTAMP            USER           DESCRIPTION
04/20/2018 11:52:43  root@server1   Policy 'test_pol_1' was saved but no changes were detected
04/20/2018 11:52:42  root@server1   Schedule 'full' was added to Policy 'test_pol_1'
04/20/2018 11:52:41  root@server1   Policy 'test_pol_1' was saved but no changes were detected
04/20/2018 11:52:08  root@server1   Policy 'test_pol_1' was created
04/20/2018 11:17:00  root@server1   Audit setting(s) of master server 'server1' were modified

Audit records fetched: 5
```

Send audit events to system logs

You can send NetBackup audit events to system logs. Ensure that you have the following permissions to carry out this task:

- View permission on the **Security > Security events** UI

- View, Create, Update, and Delete permissions on the **NetBackup management > NetBackup hosts** UI

To send audit events to system logs

1. On the left, select **Security > Security events**.
2. On the top right, click **Audit event settings**.
3. Enable **Send the audit events to the system logs** option.
4. In the **Audit event categories** dialog box, select the audit categories for which you want to send the audit events to the system logs.

   To send audit events for all audit categories to the system logs, select the **Audit event categories** check box.
5. Click **Save**.

   You can view NetBackup audit events in the system logs. For example:

   On a Windows system, use **Windows Event Viewer** to view NetBackup audit events.

   On a Linux system, you can view the system logs on the configured location.

Chapter 7

Managing security certificates

This chapter includes the following topics:

About security management and certificates in NetBackup

NetBackup uses security certificates to authenticate the NetBackup hosts. These certificates must conform to the X.509 public key infrastructure (PKI) standard. With NetBackup 8.1, 8.1.1, and 8.1.2, NetBackup certificates are used for secure communication. In NetBackup 8.2 and later you can use NetBackup certificates or external certificates.

NetBackup certificates are issued to hosts by default and the NetBackup master server acts as the CA and manages the Certificate Revocation List (CRL). The **NetBackup certificate deployment security level** determines how certificates are deployed to NetBackup hosts and how often the CRL is updated on each host. If a host needs a new certificate (the original certificate is expired or revoked), you can use an NetBackup authorization token to reissue the certificate.

External certificates are those that a trusted external CA signed. When you configure NetBackup to use external certificates, the master server, media servers, and clients in the NetBackup domain use the external certificates for secure communication.

Additionally, the NetBackup web server uses these certificates for communication between the NetBackup web UI and the NetBackup hosts. Deployment of external certificates, updating or replacing external certificates, and CRL management for the external CA are managed outside of NetBackup.

For more information on external certificates, see the NetBackup Security and Encryption Guide.

Security certificates for NetBackup 8.1 and later hosts

NetBackup 8.1 and later hosts can communicate with each other only in a secure mode. Depending on the NetBackup version, these hosts must have a certificate that the NetBackup CA issued or that another trusted CA issued. A NetBackup certificate that is used for secure communications over a control channel is also referred to as host ID-based certificate.

Security certificates for NetBackup 8.0 hosts

Any security certificates that NetBackup generated for 8.0 hosts are referred to as host name-based certificates. For more details on these certificates, refer to the NetBackup Security and Encryption Guide.

NetBackup host IDs and host ID-based certificates

Each host in a NetBackup domain has a unique identity, which is referred to as a host ID or a Universally Unique Identifier (UUID). The host ID is used in many operations to identify the host. NetBackup creates and manages host IDs as follows:

- Maintains a list on the master server of all of the host IDs that have certificates.
- Randomly generates host IDs. These IDs are not tied to any property of the hardware.
- By default, assigns NetBackup 8.1 and later hosts a host ID-based certificate that is signed by the NetBackup certificate authority.
- The host ID remains the same even when the host name changes.

In some cases a host can have multiple host IDs:

- If a host obtains certificates from multiple NetBackup domains, it has multiple host IDs that correspond to each NetBackup domain.
- When the master server is configured as part of a cluster, each node in the cluster receives a unique host ID. An additional host ID is assigned for the virtual name. For example, if the master server cluster is composed of *N* nodes, the number of host IDs that are allocated for the master server cluster is *N* + 1.

Managing NetBackup security certificates

Note: The information here only applies to the security certificates that are issued by the NetBackup certificate authority (CA). More information is available for external certificates.

See "Using external security certificates with NetBackup" on page 112.

You can view and revoke NetBackup certificates and view information about the NetBackup CA. More detailed information about NetBackup certificate management and certificate deployment is available in the NetBackup Security and Encryption Guide.

View a NetBackup certificate

You can view details of all host ID-based NetBackup certificates that are issued to NetBackup hosts. Note that only 8.1 and later NetBackup hosts have host ID-based certificates. The **Certificates** list does not include any NetBackup 8.0 or earlier hosts.

To view a NetBackup certificate

1. On the left, select **Security > Certificates**.
2. Click **NetBackup certificates**.
3. To view additional certificate details for a host, click on a host name.

Revoke a NetBackup CA certificate

When you revoke a NetBackup host ID-based certificate, NetBackup revokes any other certificates for that host. NetBackup ceases to trust the host, and it can no longer communicate with the other NetBackup hosts.

You may choose to revoke a host ID-based certificate under various conditions. For example, if you detect that client security has been compromised, if a client is decommissioned, or if NetBackup is uninstalled from the host. A revoked certificate cannot be used to communicate with master server web services.

Security best practices suggest that the NetBackup security administrator explicitly revoke the certificates for any host that is no longer active. This action should be taken regardless of whether the certificate is still deployed on the host, or whether it has been successfully removed from the host.

Note: Do not revoke a certificate of the master server. If you do, NetBackup operations may fail.

To revoke a NetBackup CA certificate

1. On the left, select **Security > Certificates**.
2. Click **NetBackup certificates**.
3. Click on the host name that is associated with the certificate that you want to revoke.
4. Click **Revoke Certificate > Yes**.

View the NetBackup certificate authority details and fingerprint

For secure communication with the NetBackup certificate authority (CA) on the master server, a host's administrator must add the CA certificate to an individual host's trust store. The master server administrator must give the fingerprint of the CA certificate to the administrator of the individual host.

To view the NetBackup certificate authority details and fingerprint

1. On the left, select **Security > Certificates**.
2. Click **NetBackup certificates**.
3. In the toolbar, click **Certificate authority**.
4. Find the **Fingerprint** information and click **Copy to clipboard**.
5. Provide this fingerprint information to the host's administrator.

Reissue a NetBackup certificate

Note: The information here only applies to the security certificates that are issued by the NetBackup certificate authority (CA). External certificates must be managed outside of NetBackup.

In some cases a host's NetBackup certificate is no longer valid. For example, if a certificate is expired, revoked, or is lost. You can reissue a certificate either with or without a reissue token.

A reissue token is a type of authorization token that is used to reissue a NetBackup certificate. When you reissue a certificate, the host gets the host ID same as the original certificate.

Reissue a NetBackup certificate, with a token

If you need to reissue a host's NetBackup certificate and want a more secure method to do so, you can create an authorization token that the host administrator must use to obtain a new certificate. This reissue token retains the same host ID as the

original certificate. The token can only be used once. Because it is associated to a specific host, the token cannot be used to request certificates for other hosts.

To reissue a NetBackup certificate for a host

1. On the left, select **Security > Hosts**.
2. Click **NetBackup certificates**.
3. Select the host and click **Generate reissue token**.
4. Enter a token name and indicate how long the token should be valid for.
5. Click **Create**.
6. Click **Copy to clipboard** and click **Close**.
7. Share the authorization token so the host's administrator can obtain a new certificate.

Allow a NetBackup certificate reissue, without a token

In certain scenarios, like BMR client restore, you need to reissue a certificate without a reissue token. The **Allow auto reissue certificate** option enables you to reissue a certificate without requiring a token.

To allow a NetBackup certificate reissue, without a token

1. On the left, select **Security > Hosts**.
2. Click **NetBackup certificates**.
3. Select the host and click **Allow auto reissue certificate > Allow**.

   Once you set the **Allow auto reissue certificate** option, a certificate can be reissued without a token within the next 48 hours, which is the default setting. After this window to reissue expires, the certificate reissue operation requires a reissue token.
4. Notify the host's administrator that you allowed a NetBackup certificate reissue without a token.

Revoke the ability to reissue a NetBackup certificate without a token

After you allow a NetBackup certificate reissue without a token, you can revoke this ability before the window to reissue expires. By default, the window is 48 hours.

To revoke the ability to reissue a NetBackup certificate without a token

1. On the left, select **Security > Hosts**.
2. Click **NetBackup certificates**.
3. Select the host and click **Revoke auto reissue certificate > Revoke**.

Managing NetBackup certificate authorization tokens

Note: The information here only applies to the security certificates that are issued by the NetBackup certificate authority (CA). External certificates must be managed outside of NetBackup.

Depending on the security level for NetBackup certificate deployment, you may need an authorization token to issue a new NetBackup certificate to a host. You can create a token when it is required or find and copy a token if it is needed again. Tokens can be cleaned up or deleted if they are no longer needed.

To reissue a certificate, a reissue token is required in most cases. A reissue token is associated with the host ID.

Create an authorization token

Depending on the NetBackup certificate deployment security level, an authorization token may be required for a non-master NetBackup host to obtain a host ID-based NetBackup certificate. The NetBackup administrator of the master server generates the token and shares it with the administrator of the non-master host. That administrator can then deploy the certificate without the presence of the master server administrator.

Do not create an authorization token for a NetBackup host whose current certificate is not in a valid state because it is lost, corrupt, or expired. In these cases, a reissue token must be used.

See "Reissue a NetBackup certificate" on page 109.

To create an authorization token

1. On the left, select **Security > Tokens**.
2. In the upper-right corner, click **Add**.
3. Enter the following information for the token:
   - Token name
   - The maximum number of times you want the token to be used
   - How long the token is valid for
4. Click **Create**.

To find and copy an authorization token value

You can view the details of the tokens that you have created and copy the token value for future use.

To find and copy an authorization token value

1. On the left, select **Security > Tokens**.
2. Select the name of the token for which you want to view the details.
3. At the top right, click **Show Token** and then click the **Copy to clipboard** icon.

Cleanup tokens

Use the Cleanup tokens utility to delete tokens from the token database that are expired or that have reached the maximum number of uses allowed.

To cleanup tokens

1. On the left, select **Security > Tokens**.
2. Click **Cleanup > Yes**.

Delete a token

You can delete a token can be deleted before it is expired or before the **Maximum Uses Allowed** is reached.

To delete a token

1. On the left, select **Security > Tokens**.
2. Select the name of the tokens that you want to delete.
3. Click **Delete** in the upper-right corner.

Using external security certificates with NetBackup

NetBackup 8.2 and later versions support the security certificates that are issued by an external CA. External certificates and the certificate revocation list for an external certificate authority must be managed outside of NetBackup. The **External certificates** tab displays details for the NetBackup 8.1 and later hosts in the domain and whether or not they use external certificates.

See “View external certificate information for the NetBackup hosts in the domain” on page 113.

Before you can see external certificate information in **Certificates > External certificates**, you must first configure the master server and the NetBackup web server to use external certificates. See the NetBackup Security and Encryption Guide for details.

See the video *External CA support in NetBackup* for details.

Video link

View external certificate information for the NetBackup hosts in the domain

Note: Before you can see external certificate information, you must configure NetBackup for external certificates. See the NetBackup Security and Encryption Guide for details.

As you add external certificates to the hosts in the NetBackup domain, use the **External certificates** dashboard to track which hosts need attention. To support an external certificate, a host must be upgraded and enrolled with an external certificate.

To view external certificate information for the hosts

1. On the left, select **Security > Certificates**.
2. Click **External certificates**.

In addition to hosts information and details for the hosts' external certificates, the following information is also included:

- The **NetBackup certificate status** column indicates if a host also has a NetBackup certificate.
- The **External certificate** dashboard contains the following information for NetBackup 8.1 and later hosts:
  - Total hosts. The total number hosts. The hosts most be online and able to communicate with NetBackup master server.
  - Hosts with certificates. The number of hosts that have a valid external certificate enrolled with the NetBackup master server.
  - Host missing certificates. Either the host supports external certificates, but does not have one enrolled. Or, an upgrade to NetBackup 8.2 is required for the host (applies to versions 8.1, 8.1.1, or 8.1.2). The **NetBackup upgrade required** total also includes any hosts that were reset or any hosts for which the NetBackup version is unknown. NetBackup 8.0 and earlier hosts do not use security certificates and are not reflected here.
  - Certificate expiry. The hosts that have an expired or expiring external certificate.

View details for a host's external certificate

You can view details of a host's certificate that was issued by an external certificate authority.

To view details for a host's external certificate

1. On the left, select **Security > Certificates**.
2. Click **External certificates**.

   The list of external certificates displays for the master server.
3. To view additional certificate details for a host, click on a host name.

Chapter 8

Managing user sessions

This chapter includes the following topics:

Sign out a NetBackup user session

For security or maintenance purposes, you can sign out one or more NetBackup user sessions. To configure NetBackup to automatically sign out any idle user sessions, see the following topic.

See "Configure when idle sessions should time out" on page 116.

Note: Changes to a user's roles are not immediately reflected in the web UI. An administrator must terminate the active user session before any changes take effect. Or, the user must sign out and sign in again.

To sign out a user session

1. On the left, select **Security > User sessions**.
2. Click **Active sessions**.
3. Select the user session that you want to sign out.
4. Click **Terminate session**.

To sign out all user sessions

1. On the left, select **Security > User sessions**.
2. Click **Active sessions**.
3. Click **Terminate all sessions**.

Unlock a NetBackup user

You can view the user accounts that are currently locked out of NetBackup and unlock one or more users.

By default a user's account only remains locked for 24 hours. You can change this time by adjusting the **User sessions > User account settings > User account lockout** setting.

See "Configure the maximum of failed sign-in attempts" on page 117.

To unlock out a locked user account

1. On the left, select **Security > User sessions**.
2. Click **Locked users**.
3. Select the user account that you want to unlock.
4. Click **Unlock**.

To unlock all locked user accounts

1. On the left, select **Security > User sessions**.
2. Click **Locked users**.
3. Click **Unlock all users**.

Configure when idle sessions should time out

You can customize when user sessions should time out and a user is automatically signed out. The setting you choose is applied to the NetBackup Administration Console and the NetBackup web UI. To configure this setting from the command line, use `nbsetconfig` to set the `GUI_IDLE_TIMEOUT` option.

To configure when idle sessions should time out

1. Select **Security > User sessions**.
2. Click **User account settings**.

3 Turn on **Session idle timeout** and click **Edit**.

4 Select the number of minutes and click **Save**.

Configure the maximum of concurrent user sessions

This setting limits the number of concurrent API sessions that a user can have active. API sessions are used for some applications in the NetBackup Administration Console. This setting does not apply to API key sessions or to other applications like the NetBackup Backup, Archive, and Restore interface. To configure this setting from the command line, use `nbsetconfig` to set the `GUI_MAX_CONCURRENT_SESSIONS` option.

To configure the maximum of concurrent user sessions

1 Select **Security > User sessions**.

2 Click **User account settings**.

3 Turn on **Maximum concurrent sessions** and click **Edit**.

4 Select the **Number of concurrent sessions per user** and click **Save**.

Configure the maximum of failed sign-in attempts

You can customize the maximum number of NetBackup failed sign-in attempts. The setting you choose applies only to the NetBackup web UI. To configure this setting from the command line, use `nbsetconfig` to set the `GUI_MAX_LOGIN_ATTEMPTS` and `GUI_ACCOUNT_LOCKOUT_DURATION` options.

To configure the maximum of failed sign-in attempts

1 Select **Security > User sessions**.

2 Click **User account settings**.

3 Turn on **User account lockout** and click **Edit**.

4 Select the number of failed sign-in attempts that you want to allow before an account is locked.

5 To unlock a locked account after a period of time, select the number of minutes for **Unlock locked accounts after**.

6 Click **Save**.

Display a banner to users when they sign in

You can configure a sign-in banner that displays each time that any user signs in to the NetBackup web UI. A different banner can be configured for any master server. This banner can also require the user to agree to the terms of service before the user signs in.

To configure the banner for the NetBackup Administration Console and the Backup, Archive, and Restore client, see the NetBackup Administrator's Guide, Volume I. To migrate the banner that is used for the NetBackup Administration Console to the NetBackup web UI, see the `nbmlb` command in the NetBackup Commands Reference Guide.

To display a banner to users when they sign in

1. Select **Security > User sessions**.
2. Click **User account settings**.
3. Turn on **Sign-in banner configuration** and click **Edit**.
4. Enter the text you want to use for the heading and the body of the message.
5. If you want to require the user to agree to the terms of service, select **Include "Agree" and "Disagree" buttons on the sign-in banner**.
6. Click **Save**.

   For active users, the updates are applied the next time the user signs in.

Chapter 9

Managing master server security settings

This chapter includes the following topics:

Certificate authority for secure communication

In the global security settings, the **Certificate authority** information indicates the type certificate authorities that the NetBackup domain supports. Open **Security > Global security** to view these settings.

NetBackup hosts in the domain can use certificates as follows:

- NetBackup certificates.
  By default, NetBackup certificates are deployed on the master server and its clients.
- External certificates.
  You can configure NetBackupto only communicate with the hosts that use an external certificate. Requires that a host is upgraded to 8.2 or later and has an external certificate that is installed and enrolled. In this case, NetBackup does

not communicate with any hosts that use NetBackup certificates. However, you can enable **Allow communication with NetBackup 8.0 and earlier hosts** to communicate with any hosts that use NetBackup 8.0 or earlier.

- Both NetBackup certificates and external certificates.
  With this configuration, NetBackup communicates with the hosts that use a NetBackup certificate or an external certificate. If a host has both types of certificates, NetBackup uses the external certificate for communication.

Disable communication with NetBackup 8.0 and earlier hosts

By default, NetBackup allows communication with NetBackup 8.0 and earlier hosts that are present in the environment. However, this communication is insecure. For increased security, upgrade all your hosts to the current NetBackup version and disable this setting. This action ensures that only secure communication is possible between NetBackup hosts. If you use Auto Image Replication (A.I.R.), you must upgrade the trusted master server for image replication to NetBackup 8.1 or later.

To communicate with an OpsCenter server, this setting must be enabled.

To disable communication with NetBackup 8.0 and earlier hosts

1. At the top right, select **Security > Global security** .
2. Turn off **Allow communication with NetBackup 8.0 and earlier hosts**.
3. Click **Save**.

Disable automatic mapping of NetBackup host names

For successful communication between NetBackup hosts, all relevant host names and IP addresses need to be mapped to the respective host IDs. Use the **Automatically map host names to their NetBackup host ID** option to automatically map the host ID to the respective host names (and IP addresses) or disable it to allow the NetBackup security administrator to manually verify the mappings before approving them.

To disable automatic mapping of NetBackup host names

1. At the top right, click the **Settings > Global security** .
2. Turn off **Automatically map host names to their NetBackup host ID**.
3. Click **Save**.

About NetBackup certificate deployment security levels

Security levels for certificate deployment are specific to NetBackup CA-signed certificates. If the NetBackup web server is not configured to use NetBackup certificates for secure communication, the security levels cannot be accessed.

The NetBackup certificate deployment level determines the checks that are performed before the NetBackup CA issues a certificate to a NetBackup host. It also determines how frequently the NetBackup Certificate Revocation List (CRL) is refreshed on the host.

NetBackup certificates are deployed on hosts during installation (after the host administrator confirms the master server fingerprint) or with the `nbcertcmd` command. Choose a deployment level that corresponds to the security requirements of your NetBackup environment.

Table 9-1 Description of NetBackup certificate deployment security levels

Security level	Description	CRL refresh
Very High	An authorization token is required for every new NetBackup certificate request.	The CRL that is present on the host is refreshed every hour.

Table 9-1 Description of NetBackup certificate deployment security levels *(continued)*

Security level	Description	CRL refresh
High (default)	No authorization token is required if the host is known to the master server. A host is considered to be known to the master server if the host can be found in the following entities: **1** The host is listed for any of the following options in the NetBackup configuration file (Windows registry or the `bp.conf` file on UNIX): ■ APP_PROXY_SERVER ■ DISK_CLIENT ■ ENTERPRISE_VAULT_REDIRECT_ALLOWED ■ MEDIA_SERVER ■ NDMP_CLIENT ■ SERVER ■ SPS_REDIRECT_ALLOWED ■ TRUSTED_MASTER ■ VM_PROXY_SERVER For more details on the NetBackup configuration options, refer to the NetBackup Administrator's Guide, Volume I. **2** The host is listed as a client name in the `altnames` file (ALTNAMESDB_PATH). **3** The host appears in the EMM database of the master server. **4** At least one catalog image of the client exists. The image must not be older than 6 months. **5** The client is listed in at least one backup policy. **6** The client is a legacy client. This is a client that was added using the **Client Attributes** host properties.	The CRL that is present on the host is refreshed every 4 hours.
Medium	The certificates are issued without an authorization token if the master server can resolve the host name to the IP address from which the request was originated.	The CRL that is present on the host is refreshed every 8 hours.

Select a security level for NetBackup certificate deployment

NetBackup offers several security levels for the NetBackup certificate deployment. The security level determines what security checks the NetBackup certificate authority (CA) performs before it issues a certificate to a NetBackup host. The level also determines how frequently the Certificate Revocation List (CRL) for the NetBackup CA is refreshed on the host.

More details are available for security levels, NetBackup certificate deployment, and the NetBackup CRL:

- See "About NetBackup certificate deployment security levels" on page 121.
- See the NetBackup Security and Encryption Guide.

To select a security level for NetBackup certificate deployment

1. At the top, click **Settings > Global security**.
2. Click **Secure communication**.
3. For **Security level for NetBackup certificate deployment**, select a security level.

   If you choose to use NetBackup certificates, they are deployed on hosts during installation, after the host's administrator confirms the master server fingerprint. The security level determines if an authorization token is required or not for a host.

Very high	NetBackup requires an authorization token for every new NetBackup certificate request.
High (Default)	NetBackup does not require an authorization token if the host is known to the master server, which means the host appears in a NetBackup configuration file, the EMM database, a backup policy, or the host is a legacy client.
Medium	NetBackup issues NetBackup certificates without an authorization token if the master server can resolve the host name to the IP address from which the request was originated.

4. Click **Save**.

Set a passphrase for disaster recovery

During a catalog backup, NetBackup creates a disaster recovery package and encrypts the backup with a passphrase that you set. The constraints for the passphrase can be changed with the NetBackup APIs or the CLIs (`nbseccmd -setpassphraseconstraints`).

See the information for disaster recovery settings in the NetBackup Security and Encryption Guide.

To set a passphrase for disaster recovery

1. At the top, click **Settings > Global security**.
2. Click **Disaster recovery**.
3. Enter and confirm a passphrase.
4. Click **Save**.

About trusted master servers

A trust relationship between NetBackup domains lets you do the following:

- Select specific domains as a target for replication. This type of Auto Image Replication is known as targeted A.I.R.
  Without a trust relationship, NetBackup replicates to all defined target storage servers. A trust relationship is optional for Media Server Deduplication Pool and PureDisk Deduplication Pool as a target storage. To use a Cloud Catalyst storage server, a trust relationship is required.
- Include usage reporting for multiple master servers.

Master servers can use a NetBackup certificate authority (CA) certificate or an external CA certificate. NetBackup determines the CAs used by the source and the target domains and selects the appropriate CA to use for communication between the servers. If the target master server is configured for both CA types, NetBackup prompts you to select the CA that you want to use. To establish trust with a remote master server using the NetBackup CA, the current master and the remote master must have NetBackup version 8.1 or later. To establish trust with a remote master server using an external CA, the current master and the remote master must have NetBackup version 8.2 or later.

Table 9-2 Determining the certificate authority (CA) to use for a trust relationship between servers

Source master server CA or CAs	Target master server CA or CAs	Certificate authority that is selected
NetBackup CA and external CA	External CA	External CA
	NetBackup CA	NetBackup CA
	External CA and NetBackup CA	
NetBackup CA	External CA	No trust is established.
	NetBackup CA	NetBackup CA
	External CA and NetBackup CA	NetBackup CA

Add a trusted master server

Note: The NetBackup web UI does not support adding a trusted master that uses version 8.0 or earlier.

You can create a trust relationship between the master servers that use the NetBackup CA or an external CA.

To add a trusted master server

1. For the servers that use the NetBackup certificate authority (CA), first obtain an authorization token for each server and the fingerprint for each server.
2. At the top, select **Settings > Global security**.
3. Select **Trusted master servers**.
4. Click the **Add** button.
5. Follow the prompts in the wizard.
6. Repeat these steps on the remote master server.

More information

For more information on using an external CA with NetBackup, see the NetBackup Security and Encryption Guide.

Remove a trusted master server

Note: Any trusted master servers at NetBackup version 8.0 or earlier must be removed using the NetBackup Administration Console.

You can remove a trusted master server, which removes the trust relationship between master servers. Note the following implications:

- Any replication operations fail that require the trust relationship.
- A remote master server is not included in any usage reporting after you remove the trust relationship.

To remove a trusted master server

1. Ensure that all replication jobs to the target master server are complete.
2. Delete all storage lifecycle policies (SLPs) that use the trusted master as a destination. Before deleting an SLP, ensure that there are no backup policies or protection plans that use the SLP for storage.
3. At the top, select **Settings > Global security**.
4. Select **Trusted master servers**.
5. Select **Actions > Remove**.
6. Click **Remove trust**.
7. Repeat step 3 through step 6 on the remote master server.

Chapter 10

Creating and managing API keys for users (Administrators)

This chapter includes the following topics:

About API keys

A NetBackup API key is a pre-authenticated token that identifies a NetBackup user to NetBackup RESTful APIs. The user can use the API key in an API request header when a NetBackup API requires authentication. API keys can be created for authenticated NetBackup users (groups are not supported). A specific API key is only created one time and cannot be recreated. Each API key has a unique key value and API key tag. NetBackup audits operations that are performed with that key with the full identity of the user.

The following actions are available for administrators and API key users.

- Administrators with the applicable role or RBAC permissions can manage API keys for all users. These roles are the Administrator or the Security Administrator or a role with RBAC permissions for API keys.
- In NetBackup 9.0, administrators can view key details and delete keys for SAML users, but not add keys.

- An authenticated NetBackup user can add and manage their own API key in NetBackup web UI. If a user does not have access to the web UI, they can use the NetBackup APIs to add or manage a key.

More information

See "User identity in the audit report" on page 101.

See the NetBackup Security and Encryption Guide for information on using API keys with the `bpnbat` command.

Add an API key or view API key details

The API key administrator can manage the keys that are associated with all NetBackup users.

Add an API key for a non-SAML user

In NetBackup 9.0, administrators can only add API keys for non-SAML users.

Note: Only one API key can be associated with a specific user at a time. If a user requires a new API key, the user or administrator must delete the key for that user.

To add an API key for a non-SAML user

1. On the left, select **Security > API keys**.
2. In the upper-right corner, click **Add**.
3. Enter a **User name** for which you want to create the API key.
4. Indicate how long you want the API key to be valid, from today's date.

   NetBackup calculates the expiration date and displays it below.
5. Click **Add**.
6. To copy the API key, click **Copy to clipboard**.

   Store this key in a safe place until you can deliver the key to the user. After you click **Close**, the key cannot be retrieved again. If this API key replaces a previous key for the user, the user must update any scripts, etc. to reflect the new API key.
7. Click **Close**.

View API key details

An API key administrator can view the API key details that are associated with all NetBackup users.

To view API key details

1. On the left, select **Security > API keys**.
2. Locate the API key that you want to view.
3. From the **Actions** menu, click **Edit**.

Edit or delete API keys

As an API key administrator, you can edit API key details for non-SAML users and delete API keys.

Edit the expiration date or description for an API key (non-SAML users)

Note: In NetBackup 9.0, administrators can only edit API key details for non-SAML users.

You can change the expiration date of an active API key for a non-SAML user.

To edit the expiration date or description for an API key

1. On the left, select **Security > API keys**.
2. Locate the API key that you want to view.
3. Click the **Actions** menu. Then select **Edit**.

   Note: If the API key is expired, the old key must be deleted and a new key created.
4. Note the current expiration date for the key and extend the date as wanted.
5. Make any wanted changes to the description.
6. Click **Save**.

Expired keys

If a key expires, the user must obtain a new API key. The existing expired key must be deleted before a new key can be created for the user.

Delete an API key

You can delete an API key to remove access for the user or when the key is no longer used. The key is permanently deleted, meaning that the associated user can no longer use that key for authentication.

To delete an API key

1. On the left, select **Security > API keys**.
2. Locate the API key that you want to view.
3. Click the **Actions** menu. Then click **Delete** > **Delete**.

Chapter 11

Adding and managing your API key (Users)

This chapter includes the following topics:

Add an API key or view your API key details

As NetBackup web UI user you can use the web UI to add or view the details for your own API key.

Add an API key

You can create an API key to authenticate your NetBackup user account when using NetBackup RESTful APIs.

To add an API key

1. For non-SAML users, if your API key has expired you must first delete that key.
2. On the top right, click the profile icon and click **Add API key**.
3. (Non-SAML users) Indicate how long you want the API key to be valid, from today's date.

   NetBackup calculates the expiration date and displays it below.
4. (SAML users) After NetBackup validates the token from the SAML session, then the expiration date for the API key can be determined.
5. Click **Add**.

6 To copy the API key, click **Copy to clipboard**.

Store this key in a safe place. After you click **Close**, the key cannot be retrieved again. If this API key replaces a previous key for your account, you must update any scripts, etc. to reflect the new API key.

7 Click **Close**.

View your API key details

To view your API key details

- On the top right, click the profile icon and select **View my API key details**.

Edit or delete your API key

You can manage your own API key from the NetBackup web UI.

Edit the expiration date or description for your API key (non-SAML users)

Non-SAML users can change the expiration date for an active API key. After an API key expires, you must delete the old key and add a new key.

To edit your API key details

1 On the top right, click the profile icon and click **View my API key details**.

2 From the **Actions** menu, select **Edit**.

3 Click the **Actions** menu. Then select **Edit**.

Note: If your API key is expired, delete the expired key and create a new key.

4 Note the current expiration date for the key and extend the date as wanted.

5 Make any wanted changes to the description.

6 Click **Save**.

Delete your API key

You can delete an API key if you no longer have access to the key or no longer use it. When you delete an API key, that key is permanently deleted. You can no longer use that key for authentication or with the NetBackup APIs.

To delete your API key

1. On the top right, click the profile icon and click **View my API key details**.
2. Perform one of the following, based on your authentication method.
   - (Non-SAML users) Click the **Actions** menu. Then click **Delete** > **Delete**.
   - (SAML users) On the right, click **Delete**, then **Delete**.

Use an API key with NetBackup REST APIs

After a key is created, the user can pass the API key in the API request headers. For example:

```
curl -X GET https://masterservername.domain.com/netbackup/admin/jobs/5 \
     -H 'Accept: application/vnd.netbackup+json;version=3.0'     \
     -H 'Authorization: <API key value>'
```

Chapter 12

Configuring authentication options

This chapter includes the following topics:

Sign-in options for the NetBackup web UI

NetBackup supports authentication of local domain users and Active Directory (AD) or LDAP domain users. AD and LDAP domains, smart card, and Single Sign-On (SSO with SAML) requires separate configuration for each master server domain where you want to use the authentication method.

NetBackup supports the following types of user authentication:

- User name and password
- Digital certificate or smart card, including CAC and PIV
  This authentication method only supports one AD or LDAP domain for each master server domain and is not available for local domain users.
  See "Configure user authentication with smart cards or digital certificates" on page 135.
- Single sign-on, with SAML

  Note the following requirements and limitations.

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Only one AD or LDAP domain is supported for each master server domain. This feature is not available for local domain users.
- Configuration of the IDP requires the NetBackup APIs or the NetBackup command `nbidpcmd`.
- API keys are used to authenticate a user or a group and cannot be used with SAML-authenticated users or groups.
- Global logout is not supported.

See "Configure NetBackup for Single Sign-On (SSO)" on page 140.

Configure user authentication with smart cards or digital certificates

If not already completed as part of role-based access control (RBAC) configuration, ensure that you complete the following steps before you configure certificate authentication:

- Add the AD or the LDAP domains that are associated with your NetBackup users.
  See "Add AD or LDAP domains" on page 41.
- Configure RBAC for the NetBackup users.
  See "Configuring RBAC " on page 40.

To configure NetBackup to authenticate users with a smart card or digital certificate

1. At the top right, select **Settings > Smart card authentication**.
2. Turn on **Smart card authentication**.
3. Select a **User authentication domain**.
4. Select a **Certificate mapping attribute**.
5. Optionally, enter the **OCSP URI**.

   If you do not provide the OCSP URI, the URI in the user certificate is used.
6. Click **Save**.
7. To the right of **CA certificates**, click **Add**.

8 Browse for or drag and drop the **CA certificates** and click **Add**.

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

Certificate file types must be `.crt`, `.cer`, `.der`, `.pem`, or `PKCS #7` format and less than 64KB in size.

9 On the **Smart card authentication** page, verify the configuration information.

10 Before users can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager.

See the browser documentation for instructions or contact your certificate administrator for more information.

11 When users sign in, they now see an option to **Sign in with certificate or smart card**.

If you do not want users to have this sign-in option yet, turn off **Smart card authentication**. (For example, if all users do not yet have their certificates configured on their hosts.). The settings that you configured are retained even if you turn off smart card authentication.

Edit the configuration for smart card authentication

If the configuration changes for smart card authentication, you can edit the configuration details.

To edit user authentication configuration

1 At the top right, select **Settings > Smart card authentication**.

2 Click **Edit**.

3 Select a **User authentication domain**.

Only the domains that are configured for NetBackup display in this list.

See "Add AD or LDAP domains" on page 41.

4 Edit the **Certificate mapping attribute**.

5 Leave the **OCSP URI** field empty if you want to use the **URI** value from the user certificate. Or, provide the URI that you want to use.

Add or delete a CA certificate that is used for smart card authentication

Add a CA certificate

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

To add a CA certificate

1. At the top right, select **Settings > Smart card authentication**.
2. Click **Add**.
3. Browse for or drag and drop the **CA certificates**. Then click **Add**.

   Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

   Certificate file types must be in `DER`, `PEM`, or `PKCS #7` format and no more than 1 MB in size.

Delete a CA certificate

You can delete a CA certificate if it is no longer used for smart card authentication. Note that if a user attempts to use the associated digital certificate or smart card certificate, they are not able to sign in to NetBackup.

To delete a CA certificate

1. At the top right, select **Settings > Smart card authentication**.
2. Select the CA certificates that you want to delete.
3. Click **Delete > Delete**

Disable or temporarily disable smart card authentication

You can disable smart card authentication if you no longer want to use that authentication method for the master server. Or, if you need to complete other configuration before users can use smart cards.

To disable smart card authentication

1. At the top right, select **Settings > Smart card authentication**.
2. Turn off **Smart card authentication**.

   The settings that you configured are retained even if you turn off smart card authentication.

About Single Sign-On (SSO) configuration

You can configure Single Sign-On (SSO) with any identity provider (IDP) that uses the SAML 2.0 protocol for exchanging authentication and authorization information. Note that you can configure an IDP with more than one Veritas product. For example, the same IDP can be configured with NetBackup and with APTARE.

Note the following requirements and limitations:

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Only identity providers that use AD or LDAP directory services are supported.
- Configuration of the IDP requires the NetBackup APIs or the NetBackup command `nbidpcmd`.
- SAML users cannot use the APIs. API keys are used to authenticate a user and therefore cannot be used with a SAML-authenticated user.
- Global logout is not supported.

Figure 12-1 Example NAT configuration: Identity provider in a private network

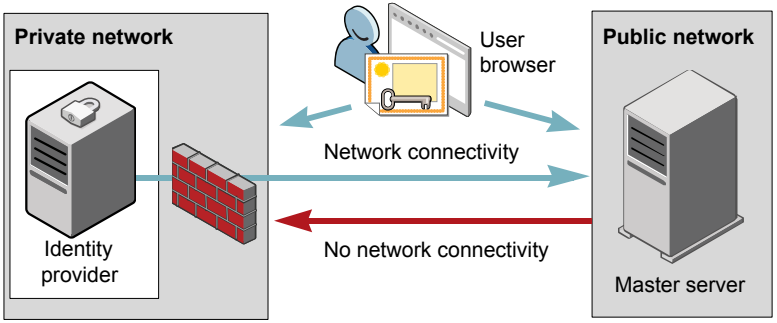


Figure 12-2 Example NAT configuration: Master server in a private network

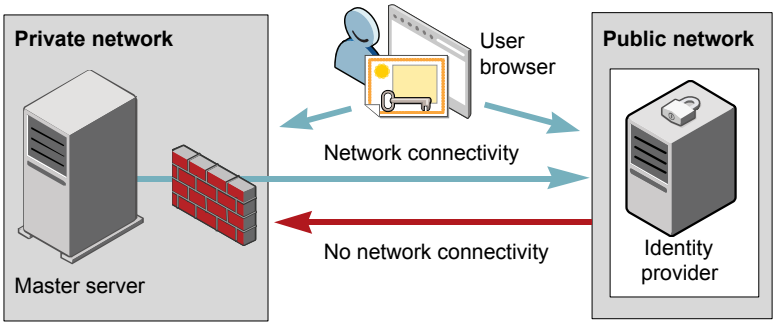


Figure 12-3 Example configuration: Master server and identity provider in same network

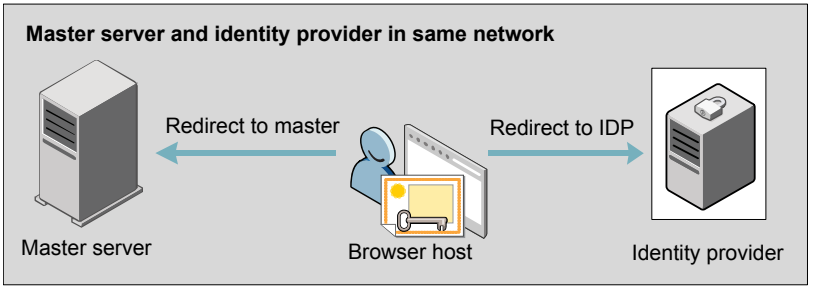
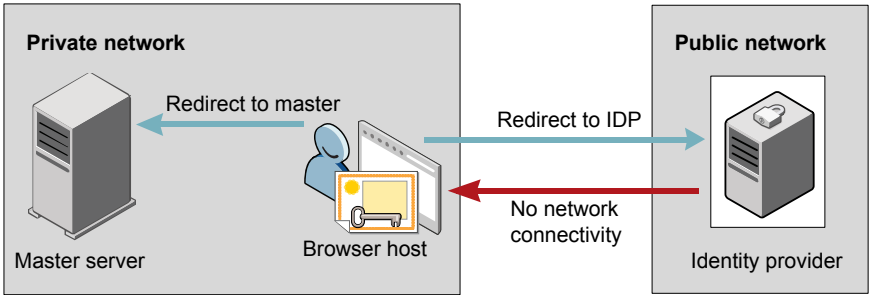


Figure 12-4 Example configuration: Master server in private network and identity provider in public network



Configure NetBackup for Single Sign-On (SSO)

This section provides steps to set up trust and exchange configuration information between the IDP and the NetBackup master server. Before proceeding with the steps, ensure that the following prerequisites are met in your environment:

- An IDP is set up and deployed in your environment.
- The IDP is configured to authenticate domain users of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP).

Table 12-1 Steps to configure NetBackup for Single Sign-On

Step	Action	Description
1.	Configure the Java keystore	To establish a trust between the NetBackup master server and the IDP, add a SAML Java keystore (JKS) on the NetBackup master server. See "Configure the Java KeyStore" on page 141.
2.	Download the IDP metadata XML file	Download and save the IDP metadata XML file from the IDP. SAML metadata that is stored in XML files is used to share configuration information between the IDP and the NetBackup master server. The IDP metadata XML file is used to add the IDP configuration to the NetBackup master server.
3.	Add and enable the IDP configuration on the NetBackup master server	See "Add and enable the IDP configuration" on page 143.
4.	Download the service provider (SP) metadata XML file	The NetBackup master server is the SP in the NetBackup environment. You can access the SP metadata XML file from the NetBackup master server by entering the following URL in your browser: `https://masterserver/netbackup/sso/saml2/metadata` Where *masterserver* is the IP address or host name of the NetBackup master server.
5.	Enroll the NetBackup master server as a service provider (SP) with the IDP	See "Enroll the NetBackup master server with the IDP" on page 144.

Table 12-1 Steps to configure NetBackup for Single Sign-On *(continued)*

Step	Action	Description
6.	Add SAML users and the SAML groups that use SSO to the necessary RBAC roles	SAML users and SAML user groups are available in RBAC only if the IDP is configured and enabled on the NetBackup master server. For steps on adding RBAC roles, see the following topic. See "Add a user to a role (non-SAML)" on page 51.

After the initial setup, you can choose to enable, update, disable, or delete the IDP configuration.

See "Manage an IDP configuration" on page 145.

Configure the Java KeyStore

To establish a trust between the NetBackup master server and the IDP server, you must configure an SAML Java KeyStore (JKS) on the NetBackup master server. Depending on whether you are using the NetBackup CA or an external certificate authority (ECA), refer to either of the following sections:

Note: If you are using a combination of an ECA and NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server.

Configure a NetBackup CA JKS

If you are using the NetBackup CA, create the NetBackup CA JKS on the NetBackup master server.

To create a NetBackup CA JKS

1. Log on to the NetBackup master server as root or administrator.
2. Depending on whether you are on a Windows or Linux operating system, run the `configureCerts` script as follows:
   - On Windows: *`install_path`*`\wmc\bin\install\configureCerts.bat -configure_saml_cert_jks`
   - On Linux: *`install_path`*`/wmc/bin/install/configureCerts -configure_saml_cert_jks`

   Where *`install_path`* is the path where NetBackup is installed.

Once the NetBackup CA JKS is created, ensure that you update the NetBackup CA JKS every time the NetBackup CA certificate is renewed.

To renew the NetBackup CA JKS

1. Log on to the NetBackup master server as root or administrator.
2. Depending on whether you are on a Windows or Linux operating system, run the `configureCerts` script as follows:
   - On Windows: *`install_path`*`\wmc\bin\install\configureCerts.bat -renew_saml_cert_jks`
   - On Linux: *`install_path`*`/wmc/bin/install/configureCerts -renew_saml_cert_jks`

   Where *`install_path`* is the path where NetBackup is installed.
3. Download the new SP metadata XML file from the NetBackup master server by entering the following URL in your browser:

   https://*masterserver*/netbackup/sso/saml2/metadata

   Where *masterserver* is the IP address or host name of the NetBackup master server.
4. Upload the new SP metadata XML file to the IDP.

   See "Enroll the NetBackup master server with the IDP" on page 144.

Configure an ECA JKS

If you are using an ECA, import the ECA JKS to the NetBackup master server.

Note: If you are using a combination of an ECA and the NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server. To use the NetBackup CA, you must first remove the ECA JKS.

To import an ECA JKS

1. Log on to the master server as root or administrator.
2. Depending on whether you are on a Windows or Linux operating system, run the `configureSAMLECACert` script as follows:
   - On Windows: :
     `install_path``\wmc\bin\install\configureSAMLECACert.bat -addExternalCert -keystorefile <External JKS path> -keystorepassfile <Path to JKS password file>`
   - On Linux: *`install_path`*`/wmc/bin/install/configureSAMLECACert -addExternalCert -keystorefile External JKS path -keystorepassfile JKS password file path`

Replace the variables as described below:

- *install_path* is the path where the product is installed.
- *External JKS path* is the path to the ECA JKS file.
- *JKS password file path* is the path to a file containing the password for the ECA JKS.

To remove the ECA JKS

1. Log on to the master server as root or administrator.
2. Depending on whether you are on a Windows or Linux operating system, run the `configureSAMLECACert` script as follows:
   - On Windows: : *Installation_Path*`\wmc\bin\install\configureSAMLECACert.bat -removeExternalCert`
   - On Linux: *Installation_Path*`/wmc/bin/install/configureSAMLECACert - removeExternalCert`

   Where *Installation_Path* is the path where the product is installed.
3. Download the new SP metadata XML file from the NetBackup master server by entering the following URL in your browser:

   https://*masterserver*/netbackup/sso/saml2/metadata

   Where *masterserver* is the IP address or host name of the NetBackup master server.
4. Upload the new SP metadata XML file to the IDP.

   See "Enroll the NetBackup master server with the IDP" on page 144.

Add and enable the IDP configuration

Before proceeding with the following steps, ensure that you have downloaded the IDP metadata XML file and saved it on the NetBackup master server.

To add and enable an IDP configuration

1. Log on to the master server as root or administrator.
2. Run the following command.

   `nbidpcmd -ac -n` *IDP configuration name* `-mxp` *IDP XML metadata file* `[-t SAML2] [-e true | false] [-u` *IDP user field*`] [-g` *IDP user group field*`] [-M` *Master Server*`]`

   Replace the variables as described below:

- *IDP configuration name* is a unique name provided to the IDP configuration.
- *IDP XML metadata file* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.
- -e true | false enables or disables the IDP configuration. An IDP configuration must be added and enabled, otherwise users cannot sign in with the Single Sign-On (SSO) option. Even though you can add multiple IDP configurations on a NetBackup master server, only one IDP configuration can be enabled at a time.
- *IDP user field* and *IDP user group field* are the SAML attribute names, which are mapped to the userPrincipalName and the memberOf attributes of the AD or LDAP.

  Note: Ensure that the SAML attribute names are defined in the format of ***username@domainname*** and **(CN=*group name*, DC=*domainname*)** respectively.

- *Master Server* is the host name or IP address of master server to which you want to add or modify the IDP configuration. The NetBackup master server where you run the command is selected by default.

Fore example: `nbidpcmd -ac -n veritas_configuration -mxp file.xml -t SAML2 -e true -u username -g group-name -M master_server.abc.com`

Enroll the NetBackup master server with the IDP

The NetBackup master server must be enrolled with the IDP as a service provider (SP). For step-by-step procedures that are specific to a particular IDP, see the following table:

Table 12-2 IDP-specific steps for enrolling the NetBackup master server

IDP name	Link to steps
ADFS	https://www.veritas.com/docs/100047744
Okta	https://www.veritas.com/docs/100047745
PingFederate	https://www.veritas.com/docs/100047746
Azure	https://www.veritas.com/docs/100047748

Table 12-2 IDP-specific steps for enrolling the NetBackup master server *(continued)*

IDP name	Link to steps
Shibboleth	https://www.veritas.com/docs/00047747

Enrolling an SP with an IDP typically involves the following operations:

Uploading the SP metadata XML file to the IDP

The SP metadata XML file contains the SP certificate, the entity ID, the Assertion Consumer Service URL (ACS URL), and a log out URL (SingleLogoutService). The SP metadata XML file is required by the IDP to establish trust, and exchange authentication and authorization information with the SP.

Mapping the SAML attributes to their AD or LDAP attributes

Attribute mappings are used to map SAML attributes in the SSO with its corresponding attributes in the AD or LDAP directory. The SAML attribute mappings are used for generating SAML responses, which are sent to the NetBackup master server. Ensure that you define SAML attributes that map to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP directory. The SAML attributes must adhere to the following formats:

Table 12-3

Corresponding AD or LDAP attribute	SAML attribute format
`userPrincipalName`	***username@domainname***
`memberOf`	**(CN=*group name*, DC=*domainname*)**

Note: While adding the IDP configuration to the NetBackup master server, the values entered for the user (`-u`) and user group (`-g`) options must match the SAML attribute names that are mapped to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP.

See "Add and enable the IDP configuration" on page 143.

Manage an IDP configuration

You can manage the identity provider (IDP) configurations on the NetBackup master server by using the enable (`-e true`), update (`-uc`), disable (`-e false`). and delete (`-dc`) options of the `nbidpcmd` command.

Enable an IDP configuration

By default, an IDP configuration is not enabled in the product environment. If you did not enable the IDP when you added it, you can use the `-uc -e true` options to update and enable the IDP configuration.

To enable an IDP configuration

1. Log on to the master server as root or administrator.
2. Run the following command:

   `nbidpcmd -uc -n` *`IDP configuration name`* `-e true`

   Where *`IDP configuration name`* is a unique name provided to the IDP configuration.

Note: Even though you can configure multiple IDPs on a NetBackup master server, only one IDP can be enabled at a time.

Update an IDP configuration

You can update the XML metadata file associated with an IDP configuration.

To update the IDP XML metadata file in an IDP configuration

1. Log on to the master server as root or administrator.
2. Run the following command:

   `nbidpcmd -uc -n` *`IDP configuration name`* `-mxp` *`IDP XML metadata file`*

   Replace the variables as described below:

   - *`IDP configuration name`* is a unique name provided to the IDP configuration.
   - *`IDP XML metadata file`* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.

If you want to update the IDP user or IDP user group values in an IDP configuration, you must first delete the configuration. The Single Sign-On (SSO) option is not available for users until you re-add the configuration with the updated IDP user or IDP user group values.

To update IDP user or IDP user group in an IDP configuration

1. Log on to the master server as root or administrator.
2. Delete the IDP configuration.

   `nbidpcmd -dc -n` *`IDP configuration name`*

   Where *`IDP configuration name`* is a unique name provided to the IDP configuration.
3. To add and enable the configuration again, run the following command:

   `nbidpcmd -ac -n` *`IDP configuration name`* `-mxp` *`IDP XML metadata file`* `[-t SAML2] [-e true | false] [-u` *`IDP user`*`] [-g` *`IDP user group field`*`] [-M` *`Master Server`*

   Replace the variables as described below:

   - *`IDP configuration name`* is a unique name provided to the IDP configuration.
   - *`IDP XML metadata file`* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.
   - `-e true | false` enables or disables the IDP configuration. An IDP must be available and enabled otherwise users cannot sign in with the Single Sign-On (SSO) option. Even though you can add multiple IDP configurations on a NetBackup master server, only one IDP configuration can be enabled at a time.
   - *`IDP user field`* and *`IDP user group field`* are the SAML attribute names, which are mapped to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP.

     Note: Ensure that the SAML attribute names are defined in the format of ***username@domainname*** and **(CN=*group name*, DC=*domainname*)** respectively.

   - *`Master Server`* is the host name or IP address of the master server to which you want to add or modify the IDP configuration. The NetBackup master server where you run the command is selected by default.

Disable an IDP configuration

If an IDP configuration is disabled in the product environment, the Single Sign-On (SSO) option of that IDP is not available for users when they sign in.

To disable an IDP configuration

1. Log on to the master server as root or administrator.
2. Run the following command:

   ```
   nbidpcmd -uc -n IDP configuration name -e false
   ```

   Where *IDP configuration name* is a unique name provided to the IDP configuration.

Delete an IDP configuration

If an IDP configuration is deleted, the Single Sign-On (SSO) option of that IDP is not available for users when they sign in.

To delete an IDP configuration

1. Log on to the master server as root or administrator.
2. Run the following command:

   ```
   nbidpcmd -dc -n IDP configuration name
   ```

   Where *IDP configuration name* is a unique name provided to the IDP configuration.

Video: Configure Single Sign-On in NetBackup

In this video, you will see an overview of how to configure Single Sign-On (SSO) in NetBackup.

Video link

Depending on which IDP you are using, see the following articles for steps on downloading the IDP metadata XML file and enrolling the NetBackup master server with the IDP:

- ADFS: https://www.veritas.com/support/en_US/article.100047744
- Okta: https://www.veritas.com/support/en_US/article.100047745
- PingFederate: https://www.veritas.com/support/en_US/article.100047746
- Azure: https://www.veritas.com/support/en_US/article.100047748
- Shibboleth: https://www.veritas.com/support/en_US/article.100047747

Troubleshooting SSO

This section provides steps for troubleshooting issues related to SSO.

Redirection issues

If you are facing issues with redirection, check the error messages in web services log files to narrow down the cause of the issue. NetBackup creates logs for the NetBackup web server and for the web server applications. These logs are written to the following location:

- UNIX: `/usr/openv/logs/nbwebservice`
- Windows:*`install_path`*`\NetBackup\logs\nbwebservice`

NetBackup web UI does not redirect to the IDP sign in page

The IDP metadata XML file contains the IDP certificate, the entity ID, the redirect URL, and the logout URL. The NetBackup web UI can fail to redirect to the IDP sign in page, if the IDP XML metadata file is outdated or corrupted. The following message is added to the web service log:

```
Failed to redirect to the IDP server.
```

To ensure that the latest configuration details are available to the NetBackup master server, download the latest copy of the XML metadata file from the IDP. Use the IDP XML metadata file to add and enable the latest IDP configuration on the NetBackup master server. See "Add and enable the IDP configuration" on page 143.

IDP sign in page does not redirect to the NetBackup web UI

When you enter your credentials in the IDP sign in page, your browser might display an **Authentication failed** error, instead of redirecting to the NetBackup web UI. Refer to the following table for resolution steps based on the error found in the web service log.

Table 12-4

Web Service Log Error message	Explanation and recommended action
`userPrincipalName not found in response.`	While adding the IDP configuration to the NetBackup master server, the value entered for the user (`-u`) option must match the SAML attribute name, which is mapped to the `userPrincipalName` attribute in AD or LDAP. For more information, See "Add and enable the IDP configuration" on page 143.

Table 12-4 *(continued)*

Web Service Log Error message	Explanation and recommended action
`userPrincipalName is not in expected format`	The IDP sends SAML responses to the NetBackup master server, which contains SAML user and SAML user group information. To enable the IDP to successfully send this information, ensure the value of `userPrincipalName` attribute sent by the IDP is defined in the format of ***username@domainname***. For more information, See "Enroll the NetBackup master server with the IDP" on page 144.
`Authentication issue instant is too old or in the future`	This error can occur because of the following reasons: ■ The date and time of IDP server and the NetBackup master server is not synchronized. ■ By default, the NetBackup master server allows a user to remain authenticated for a period of 24 hours. You might encounter this error, If an IDP allows a user to remain authenticated for a period longer than 24 hours. To resolve this error, you can update the SAML authentication lifetime of the Netbackup master server to match that of the IDP. Specify the new SAML authentication lifetime in the `<installpath>\var\global\wsl\config\web.conf` file on the NetBackup master server. For example, If your IDP has an authentication lifetime as 36 hours, update the entry in the `web.conf` file as follows: `SAML_ASSERTION_LIFETIME_IN_SECS=129600`

Table 12-4 *(continued)*

Web Service Log Error message	Explanation and recommended action
`Response is not success`	This error can occur because of the following reasons: ■ The IDP metadata XML file contains an IDP certificate. If you are using a NetBackup CA, ensure that the IDP certificate is updated with latest NetBackup CA certificate information. For more information, See "Configure the Java KeyStore" on page 141. ■ The Certificate Revocation List (CRL) must be disabled in the IDP if you are using a NetBackup CA keystore.

Unable to sign in due to authorization-related issues

To sign in with SSO, you must add SAML users and the SAML user groups to the necessary RBAC roles. If the RBAC roles are not correctly assigned, you might encounter the following error while signing into NetBackup web UI.

```
You are not authorized to access this application. Contact your
NetBackup security administrator to request RBAC permissions for the
NetBackup web user interface.
```

Refer to the table below to troubleshoot authorization-related issues:

Table 12-5

Cause	Explanation and recommended action
RBAC roles are not assigned to the SAML users and the SAML groups.	After an IDP configuration is added and enabled on the NetBackup master server, ensure that necessary RBAC roles are assigned to SAML users and SAML user groups that use SSO. Note that SAML users and SAML user groups are available in RBAC only after the IDP configuration is added and enabled on the NetBackup master server. For steps on adding users, See "Add a user to a role (non-SAML)" on page 51.

Table 12-5 *(continued)*

Cause	Explanation and recommended action
RBAC roles are assigned to SAML users and SAML user groups associated with an IDP configuration that is not currently added and enabled.	When you add a SAML users or SAML user group in RBAC, the SAML user or SAML user group entry is associated with the IDP configuration that is added and enabled at that time. If you add and enable a new IDP configuration, ensure that you also add another entry for the SAML user or SAML user group. The new entry is associated with the new IDP configuration. For example, **NBU_user** is added to RBAC and assigned the necessary permissions, while an ADFS IDP configuration is added and enabled. If you add and enable an Okta IDP configuration, you must add a new user entry for **NBU_user**. Assign the necessary RBAC roles to the new user entry, which is associated with the Okta IDP configuration. For steps on adding users, See "Add a user to a role (non-SAML)" on page 51.
RBAC roles are assigned to local domain users or Active Directory (AD) or LDAP domain users (instead of SAML users and SAML user groups).	SAML user or SAML user group records might appear similar to corresponding local domain users or AD or LDAP domain users already added in the RBAC. After an IDP configuration is added and enabled on the NetBackup master server, ensure that you add SAML users and SAML user groups in RBAC and assign the necessary permissions. Note that SAML users and SAML user groups are available in RBAC only after the IDP configuration is added and enabled on the NetBackup master server. For steps on adding SAML users and user groups, See "Add a user to a role (non-SAML)" on page 51.

Table 12-5 *(continued)*

Cause	Explanation and recommended action
The NetBackup master server is unable to retrieve user group information from the IDP	The IDP sends SAML responses to the NetBackup master server, which contains SAML user and SAML user group information. To enable the IDP to successfully send this information, ensure the following: ■ The IDP is configured to authenticate domain users from AD or LDAP. ■ The value of `memberOf` attribute sent by the IDP is in the X.500 distinguished format, that is, **{cn=groupname,dc=domain}**. ■ While adding the IDP configuration to the NetBackup master server, the values entered for the user group (`-g`) option matches the SAML attribute name, which is mapped to the `memberOf` attribute in AD or LDAP. For more information, See "Add and enable the IDP configuration" on page 143.

Chapter 13

Managing hosts

This chapter includes the following topics:

View NetBackup host information

The **Hosts** application contains details about the NetBackup hosts in your environment, including the master server, media servers, and clients. Only hosts with a host ID are displayed in this list. The **Host** name reflects the NetBackup client name of a host, also referred to as the primary name of the host.

Note: NetBackup discovers any dynamic IP addresses (DHCP or Dynamic Host Configuration Protocol hosts) and adds these addresses to a host ID. You should delete these mappings.

For host name-based certificates for 8.0 and earlier NetBackup hosts, refer to the respective version of the NetBackup Security and Encryption Guide.

To view NetBackup host information

1. On the left, select **Security > Hosts**.

   Review the security status and any other host names mapped to this host.

2. For additional details for this host, click the name of the host.

Approve or add mappings for a host that has multiple host names

A NetBackup host can have multiple host names. For example, both a private and a public name or a short name and a fully qualified domain name (FQDN). A NetBackup host may also share a name with other NetBackup host in the environment. NetBackup also discovers cluster names, including the host name and fully qualified domain name (FQDN) of the virtual name of the cluster.

See the section called “Examples of auto-discovered mappings for a cluster” on page 157.

See the section called “Example of auto-discovered mappings for a cluster in a multiple NIC environment” on page 157.

See the section called “Examples of auto-discovered mappings for SQL Server environments” on page 158.

The NetBackup client name of a host (or the primary name) is automatically mapped to its host ID during certificate deployment. For successful communication between NetBackup hosts, NetBackup also automatically maps all hosts to their other host names. However, that method is less secure. Instead, you can choose to disable this setting and choose to manually approve the individual host name mappings that NetBackup discovers.

See “Disable automatic mapping of NetBackup host names” on page 120.

Approve the host mappings that NetBackup discovers

NetBackup automatically discovers many shared names or cluster names that are associated with the NetBackup hosts in your environment. Use the **Mappings to approve** tab to review and accept the relevant host names. When **Automatically map host names to their NetBackup host ID** is enabled, the **Mappings to approve** list shows only the mappings that conflict with other hosts.

Note: You must map all available host names with the associated host ID. If you deploy a certificate on a host using a host name that is not mapped with the associated host ID, NetBackup deploys a new certificate and issues a new host ID to the host as NetBackup considers it as a different host.

To approve the host names that NetBackup discovers

1. On the left, select **Security > Hosts**.
2. Click the **Mappings to approve** tab.
3. Click the name of the host.

4 Review the mappings for the host and click **Approve** if you want to use the discovered mapping.

Click **Reject** if you do not want to associate the mapping with the host.

The rejected mappings do not appear in the list until NetBackup discovers them again.

5 Click **Save**.

Map other host names to a host

You can manually map the NetBackup host to its host names. This mapping ensures that NetBackup can successfully communicate with the host using the other name.

To map a host name to a host

1 On the left, select **Security > Hosts**.

2 Select the host and click **Manage mappings**.

3 Click **Add**.

4 Enter the host name or IP address and click **Save**.

5 Click **Close**.

Map shared or cluster names to multiple NetBackup hosts

Add a shared or a cluster name mapping if multiple NetBackup hosts share a host name. For example, a cluster name.

Note the following before you create a shared or a cluster name mapping:

- NetBackup automatically discovers many shared names or cluster names. Review the **Mappings to approve** tab.
- If a mapping is shared between an insecure and a secure host, NetBackup assumes that the mapping name is secure. However, if at run-time the mapping resolves to an insecure host, the connection fails. For example, assume that you have a two-node cluster with a secure host (node 1) and an insecure host (node 2). In this case, the connection fails if node 2 is the active node.

To map shared or cluster names to multiple NetBackup hosts

1 On the left, select **Security > Hosts**.

2 Select the host and click **Add shared or cluster mappings**.

3 Enter a **Shared host name or cluster name** that you want to map to two or more NetBackup hosts.

For example, enter a cluster name that is associated with NetBackup hosts in your environment.

4 On the right, click **Add**.

5 Select the NetBackup hosts that you want to add and click **Add to list**.

For example, if you entered a cluster name in step 3 select the nodes in the cluster here.

6 Click **Save**.

Examples of auto-discovered mappings for a cluster

For a cluster with hosts `client01.lab04.com` and `client02.lab04.com`, you may see the following entries. For each host, approve the mappings that are valid.

Host	Auto-discovered mapping
client01.lab04.com	client01
client01.lab04.com	clustername
client01.lab04.com	clustername.lab04.com
client02.lab04.com	client02
client02.lab04.com	clustername
client02.lab04.com	clustername.lab04.com

When you have approved all valid mappings, you see the **Mapped host or IP address** settings that are similar to the following entries.

Host	Mapped Host Names/IP Addresses
client01.lab04.com	client01.lab04.com, client01, clustername, clustername.lab04.com
client02.lab04.com	client02.lab04.com, client02, clustername, clustername.lab04.com

Example of auto-discovered mappings for a cluster in a multiple NIC environment

To perform backups of a cluster in a multi-NIC environment you must map the cluster node names to the virtual name of the cluster on the private network.

Table 13-1 Mapping host names for a cluster in a multi-NIC environment

Host	Mapped Host Names
Private name of *Node 1*	Virtual name of the cluster on the private network
Private name of *Node 2*	Virtual name of the cluster on the private network

For example, for a cluster in a multi-NIC environment with hosts `client01-bk.lab04.com` and `client02-bk.lab04.com`, you may see the following entries. For each host, approve the mappings that are valid.

Host	Auto-discovered Mapping
client01-bk.lab04.com	clustername-bk.lab04.com
client02-bk.lab04.com	clustername-bk.lab04.com

When you have approved all valid mappings, you see the **Mapped host or IP address** settings that are similar to the following entries.

Host	Mapped Host Names/IP Addresses
client01-bk.lab04.com	clustername-bk.lab04.com
client02-bk.lab04.com	clustername-bk.lab04.com

Examples of auto-discovered mappings for SQL Server environments

In Table 13-2, FCI is a SQL Server failover cluster instance. WSFC is Windows Server Failover Cluster.

Table 13-2 Example mapped host names for SQL Server environments

Environment	Host	Mapped Host Names
FCI (cluster with two nodes)	Physical name of *Node 1*	Virtual name of the SQL Server cluster
	Physical name of *Node 2*	Virtual name of the SQL Server cluster

Table 13-2 Example mapped host names for SQL Server environments *(continued)*

Environment	Host	Mapped Host Names
Basic or advanced availability group (primary and secondary)	Primary name	WSFC name
	Secondary name	WSFC name
Basic or advanced availability group, with an FCI (primary FCI and secondary FCI)	Primary FCI name	WSFC name
	Secondary FCI name	WSFC name
	Physical name of *Node 1*	Virtual name of the SQL Server cluster
	Physical name of *Node 2*	Virtual name of the SQL Server cluster

Remove mappings for a host that has multiple host names

You can remove any host name mappings that NetBackup added automatically or any host name mappings that you added manually for a host. Note that if you remove a mapping, the host is no longer recognized with that mapped name. If you remove a shared or a cluster mapping, the host may not be able to communicate with other hosts that use that shared or cluster name.

If you have issues with a host and its mappings, you can reset the host attributes. However, that resets other attributes like a host's communication status.

See "Reset a host's attributes" on page 160.

To remove a host name that NetBackup discovers

1. On the left, select **Security > Hosts**.
2. Select the name of the host.
3. Click **Manage mappings**.
4. Locate the mapping you want to remove and click **Delete > Save**.

Reset a host's attributes

In some cases you need to reset a host's attributes to allow successful communication with the host. A reset is most common when a host is downgraded to a 8.0 or earlier version of NetBackup. After the downgrade, the master server cannot communicate with the client because the communication status for the client is still set to the secure mode. A reset updates the communication status to reflect the insecure mode.

When you reset a host's attributes:

- NetBackup resets the host ID to host name mapping information, the host's communication status and so on. It does not reset the host ID, host name, or security certificates of the host.
- The connection status is set to the insecure state. The next time the master server communicates with the host, the connection status is updated appropriately.

To reset the attributes for a host

1. On the left, select **Security > Hosts**.
2. Select the host and click **Reset attributes > Reset**.
3. Choose if you want to communicate insecurely with 8.0 and earlier hosts.

   NetBackup can communicate with a 8.0 or earlier host when the **Allow communication with NetBackup 8.0 and earlier hosts** option is enabled in the **Global Security Settings**. This option is enabled by default.

Note: If you unintentionally use the **Reset Host Attributes** option, you can undo the changes by restarting the `bpcd` service. Otherwise, the host attributes are automatically updated with the appropriate values after 24 hours.

Section 3

Managing storage and backups

Chapter 14

Configuring storage

This chapter includes the following topics:

About storage configuration

NetBackup lets you configure storage options for all protection plans and policies. You can configure storage options for the Media Server Deduplication Pool (MSDP), AdvancedDisk, Cloud storage, and OpenStorage options. You can also configure NetBackup to work with your universal shares.

You can set up the storage options using the storage option wizard. Access the wizard by clicking on **Storage** on the left side. The wizard guides you through the options for AdvancedDisk, Cloud storage, MSDP, and OpenStorage.

Note: If you use Key Management Service (KMS), it must be configured before you can select the KMS option in the storage server setup. Refer to NetBackup Security and Encryption Guide for more information.

To ensure that A.I.R and other storage capabilities are displayed accurately for the storage servers on the NetBackup web UI, upgrade the media server. You must upgrade the media server that has NetBackup versions 8.2 or earlier. After you upgrade the media server then use the command line to update the storage server.

Use the following command to update the storage server:

```
/usr/openv/netbackup/bin/admincmd/nbdevconfig -updatests
-storage_server <storage server name> -stype PureDisk
```

For more information, refer to the NetBackup Deduplication Guide.

See "Create a Media Server Deduplication Pool (MSDP) storage server" on page 163.

See "Create a Cloud (Cloud Catalyst), OpenStorage, or AdvancedDisk storage server " on page 164.

See "Create a universal share" on page 169.

See "Create a disk pool" on page 166.

See "Create a storage unit" on page 168.

Create a Media Server Deduplication Pool (MSDP) storage server

Use this procedure to create a Media Server Deduplication Pool (MSDP) storage server. You have the option to create a disk pool (local storage or cloud storage) and storage unit after you create a storage server. The recommendation is that you create the disk pool and storage unit if they do not exist in NetBackup.

To add an MSDP storage server

1. On the left, click **Storage** and then click **Add**.
2. Select **Media Server Deduplication Pool (MSDP)** from the list.
3. In **Basic properties**, enter all required information and click **Next**.

   You must select your media server by clicking on the field. If you do not see the media server you want use, you can use **Search** to find it.
4. In **Storage server options**, enter all required information and click **Next**.

   If you use Key Management Service (KMS), it must be configured before you can select the **KMS** option.

5 (Optional) In **Media servers**, click **Add** to add any additional media servers you want to use.

Click **Next** after selecting additional media servers or if you want to continue without selecting additional media servers.

6 On the **Review** page, confirm that all options are correct and click **Save**.

If the MSDP storage server creation is unsuccessful, follow the prompts on the screen to correct the issue.

To configure MSDP to use cloud storage, use the following procedure (drop-down in **Volumes** step) to select an existing disk pool volume or create a new one.

See "Create a disk pool" on page 166.

7 (Optional) At the top, click on **Create disk pool**.

8 (Optional) To create a cloud logical storage unit and disk pool with replication, click on **Create disk pool**.

Enter the required information to create a disk pool.

In the next tab, select and add the required cloud volume. Select the cloud storage provider and the required details of the storage provider. Enter the credentials to access the cloud storage provider and then define the advanced settings.

Note: Currently, AWS S3 and Azure storage API types are supported.

For more information, refer to the NetBackup *Cloud Administrator's Guide* and *NetBackup Deduplication Guide*.

See "Create a disk pool" on page 166.

See "Create a storage unit" on page 168.

See "Create a Cloud (Cloud Catalyst), OpenStorage, or AdvancedDisk storage server " on page 164.

See "Create a protection plan" on page 177.

Create a Cloud (Cloud Catalyst), OpenStorage, or AdvancedDisk storage server

Use the following procedures to create Cloud (Cloud Catalyst), OpenStorage, or an AdvancedDisk storage server.

Create a Cloud storage server

Follow this procedure to create a Cloud storage server.

To create a Cloud storage server

1. On the left, click **Storage** and then click **Add**.
2. Select **Cloud storage** from the list.
3. In **Basic properties**, enter all required information and click **Next**.

   You must select your **Cloud storage provider** by clicking on the field. If you do not see the cloud storage provider you want use, you can use **Search** to find it.

   If the **Region** information that you want to select does not appear in the table, use **Add** to manually add the required information. This option does not appear for every cloud storage provider.

   The **Deduplication** option is enabled when you select a cloud storage provider that supports Cloud Catalyst.

   You must select your media server by clicking on the field. If you do not see the media server you want use, you can use **Search** to find it.
4. In **Access settings** enter the required access details for the selected cloud provider and click **Next**.

   If you use `SOCKS4`, `SOCKS5`, or `SOCKS4A`, some of the options in the **Advanced** section are not available.

   If you create a Cloud Catalyst storage server, you have the option of encrypting data using MSDP KMS encryption.
5. In **Storage server options**, you can adjust the **Object size**, enable compression, or encrypt data and then click **Next**.
6. (Optional) In **Media servers**, click **Add** to add any additional media servers you want to use.

   For Cloud and Cloud Catalyst storage servers, media servers with a NetBackup version older than master server are not listed.

   Click **Next** after selecting additional media servers or if you want to continue without selecting additional media servers.
7. On the **Review** page, confirm that all options are correct and click **Save**.
8. (Optional) At the top, click on **Create disk pool**.

Create an OpenStorage storage server

Follow this procedure to create an OpenStorage storage server.

To create an OpenStorage storage server

1. On the left, click **Storage** and then click **Add**.
2. Select **OpenStorage** from the list.
3. In **Basic properties**, enter all required information and click **Next**.

   You must select your media server by clicking on the field. If you do not see the media server you want use, you can use **Search** to find it.

   Use the drop-down to select the correct **Storage server type**.
4. (Optional) In **Media servers**, click **Add** to add any additional media servers you want to use.

   Click **Next** after selecting additional media servers or if you want to continue without selecting additional media servers.
5. On the **Review** page, confirm that all options are correct and click **Save**.

   After you click **Save**, the credentials you entered are validated. If the credentials are invalid, click **Change** and you can correct the issue with the credentials.
6. (Optional) At the top, click on **Create disk pool**.

Create an AdvancedDisk storage server

Follow this procedure to create an AdvancedDisk storage server.

To create an AdvancedDisk storage server

1. On the left, click **Storage** and then click **Add**.
2. Select **AdvancedDisk** from the list.
3. Select a media server list and enter a **Storage server name** click **Select**.

See "Create a disk pool" on page 166.

See "Create a storage unit" on page 168.

See "Create a Media Server Deduplication Pool (MSDP) storage server" on page 163.

See "Create a protection plan" on page 177.

Create a disk pool

Use this procedure to create a disk pool after you create any type of storage server. You can create a disk pool at any time, but disk pool creation requires that you have an existing storage server created.

You can configure MSDP storage server to use cloud storage. To configure, you can select an existing cloud volume or create a new one when you create a disk

pool. Use the drop-down in **Volumes** step to select an existing cloud volume or create a new volume for the MSDP storage server.

When you view the **Disk pools** tab, the **Available space** column can be empty for a disk pool that uses a cloud storage provider. NetBackup cannot retrieve the information because the cloud provider does not supply an API for that information.

To create a disk pool

1. On the left, click **Storage**, click the **Disk pools** tab, and then click **Add**.

   Another way to create a disk pool is to click **Create disk pool** at the top of the screen after you have created a storage server.

2. In **Disk pool options**, enter all required information and click **Next**.

   Click **Change** to select a storage server.

   If **Limit I/O streams** is left cleared, the default value is **Unlimited** and may cause performance issues.

3. In **Volumes**, use the **Volume** drop down to select a volume or add a new volume. Enter all required information based on the selection and click **Next**.

   If you want to add a new disk pool volume, use the **Add volume** option.

4. In **Replication**, click **Add** to add replication targets to the disk pool.

   This step lets you select a trusted master server or add a trusted master server. You can add a trusted master server that supports NetBackup Certificate Authority (NBCA), ECA, and ECA together with NBCA.

   Replication is supported only on MSDP and Cloud Catalyst.

   Review all the information that is entered for the replication targets and then click **Next**.

5. On the **Review** page, verify that all settings and information are correct. Click **Finish**.

   The disk pool creation and replication configuration continue in the background if you close the window. If there is an issue with validating the credentials and configuration of the replication, you can use the **Change** option to adjust any settings.

See “Create a storage unit” on page 168.

See “Create a Media Server Deduplication Pool (MSDP) storage server” on page 163.

See “Create a Cloud (Cloud Catalyst), OpenStorage, or AdvancedDisk storage server ” on page 164.

See “Create a protection plan” on page 177.

Create a storage unit

Use this procedure to create a storage unit. You should create a storage unit after you create any type of storage server and disk pool. The steps in this procedure also work if you create a new storage unit without creating a storage server and disk pool.

When you view the **Storage units** tab, the **Used space** column can be empty for a storage unit that uses a cloud storage provider. NetBackup cannot retrieve the information because the cloud provider does not supply an API for that information.

To create a storage unit

1. On the left, click **Storage**, click the **Storage units** tab, and then click **Add**.

   Another way to create a storage unit is to click **Create storage unit** at the top of the screen after you have created a disk pool.

2. Select the storage unit from the list and click **Start**.
3. In **Basic properties**, enter all required information and click **Next**.
4. In **Disk pool**, select the disk pool you want to use in the storage unit and then click **Next**.

   The **Enable WORM** option is activated when you select a disk pool that supports WORM (Write Once Read Many) storage.

   For more information about WORM properties, refer to *Configuring immutability and indelibility of data in NetBackup* in the NetBackup Administrator's Guide, Volume I guide.

   The **On demand only** option specifies whether the storage unit is available exclusively on demand. A policy or schedule must be explicitly configured to use this storage unit

5. In the **Media server** tab, select the media servers you want to use and then click **Next**.

   You can have NetBackup select your media server automatically or you can select your media servers manually using the radio buttons.

6. Review the setup of the storage unit and then click **Save**.

See "Create a disk pool"on page 167 on page 167.

See "Create a Media Server Deduplication Pool (MSDP) storage server" on page 163.

See "Create a Cloud (Cloud Catalyst), OpenStorage, or AdvancedDisk storage server " on page 164.

See "Create a protection plan" on page 177.

Create a universal share

A universal share offers the ability to ingest data directly into a space efficient SMB (CIFS) or NFS share. Space efficiency is achieved by storing the ingested data directly to an existing NetBackup deduplication pool (MSDP). No NetBackup software needs to be installed on the client that is mounting the share. Any operating system that is running a POSIX-compliant file system and can mount an SMB (CIFS) or NFS network share can write data to a universal share.

For more information about universal shares, see the NetBackup Deduplication Guide

With the NetBackup web UI, you can:

- Create, modify, view, and delete universal shares and manage them across appliances and build-your-own (BYO) servers.

  Note: Universal shares created through NetBackup Appliance web GUI cannot be managed through NetBackup web UI. For NetBackup 8.3 and later, it is recommended to use the NetBackup web UI to manage universal shares on a NetBackup appliance.

- Change the quota settings, Active Directory (AD) user and group names, and target hosts that pertain to the universal share.

Note: To create a policy for a universal share, use the NetBackup Java GUI. See the NetBackup Deduplication Guide for more information about universal share policies.

To create a universal share in the NetBackup web UI

1. On the left, click **Storage > Universal Share** and then click **Add**.

   If there are no storage servers, then configure an MSDP storage server:

   See "Create a Media Server Deduplication Pool (MSDP) storage server" on page 163.

   After you create the MSDP storage server, return to Universal Shares tab and click **Add** to add a universal share.

2. Provide the following required information:

   - Enter a **Display name**. This name does not need to be unique. Multiple universal shares can use the same display name.
   - Select the **Storage Server**.

- Select the **Protocol**: NSF or SMB (CIFS)
- Specify a **Host** that is allowed to mount the share and then click **Add to list**. You can use the host name, IP address, short name, or the FQDN to specify the Host. You can enter multiple hosts for each share.

3 At this point, continue to enter values in the remaining fields or click **Save** to save the universal share. You can update the remaining fields later from the universal share's details page:

- Select a **Quota** type: Unlimited or Custom. If you select Custom, also specify the quota in MB, GB, or TB units.

  The Custom quota value limits the amount of data that is ingested into the share. Quotas are enforced using the front-end terabyte (FETB) calculation method. They are Implemented per share and can be modified at any time. You do not need to remount the share for the change to a take effect.

  To update the quote type or value from the universal share's details page, click **Edit** in the Quota section.
- Specify **Active Directory usernames** and **Active Directory group names**. Only the specified users or groups can access the share. You can add and update the **Active Directory usernames** and **Active Directory group names** later from the details page of an existing universal share.

  Note: Currently **Active Directory usernames** and **Active Directory group names** are supported only for the SMB (CIFS) protocol.

4 To view details about a universal share, click its name in the **Universal Shares** table.

5 To delete a universal share, select one or more and click **Delete** or select **Delete** from the action menu.

  Deleting a universal share also deletes all data in the share. This action is irreversible and may take some time if the amount of data is large. Any active data transfers are immediately terminated, and any mounted shares are immediately removed.

Using image sharing from the NetBackup Web UI

You can use the NetBackup Web UI to share images from an on-premises location to the cloud. You can set up a cloud recovery host on demand and share the images to that server.

Use the information from the following topics from the NetBackup Deduplication Guide to set up a cloud recovery host:

About image sharing in cloud using Cloud Catalyst

About image sharing using MSDP cloud

Steps to complete from the NetBackup web UI after setting up the cloud recovery host

Before you begin, ensure that you have the required permissions in the web UI to import the image, restore, convert, and access the AMI ID.

Importing the images.

1. On the left, select **Storage** and then **Disk pool**.
2. Select the volume pools that contain the images that you want to share.
3. In the Disk pool options, click the hamburger menu beside the disk pool name and click **Fast Import**.

   Note: The fast import option is an import operation that is specific to image sharing. You can import the backed-up images from the cloud storage to the cloud recovery host that is used for image sharing. After a fast import, you can restore the images. For AWS cloud provider, you can also convert the VM image to an AWS AMI.

4. In the **Fast import images** page, select the backup images that you want to import and click **Import**.
5. Verify the activity completion status in the **Activity Monitor**.

Converting the VM images to Amazon EC2 instance.

1. On the left select **VMware** and then select the imported VMware image to convert.
2. On the **Recovery point** tab, select the recovery date.
3. For the recovery point date, choose the required recovery point, click the hamburger menu, and select **Convert**.
4. Once the conversion is complete, an AMI ID is generated. In the **Activity** tab, look for the **AMI ID** column for the ID.
5. Use the AMI ID to locate the image in AWS and then use the AWS console to start the EC2 instance.

Troubleshooting storage configuration

The following table describes multiple issues that might occur when you configure storage:

Table 14-1 Storage configuration troubleshooting

Error message or cause	Explanation and recommended action
The following error is displayed when you create a disk pool for a cloud LSU: Disk is full	Workaround: Even if the disk is not full and you get the error, ensure that there is enough space available for creating the cloud LSU. By default the cloud LSU requires approximately 1 TB of free space. To reduce the cloud LSU size, open the `contentrouter.cfg` file from `/msdp/etc/puredisk/` and change the values. After changing the values, restart the MSDP services and then create the cloud LSU.
The local MSDP storage does not display the compression and the encryption values correctly.	In the **Select long-term retention storage** configuration page for protection plans, the local MSDP storage does not display the compression and the encryption values correctly.

Troubleshooting universal share configuration issues

For more information about universal shares, see the NetBackup Deduplication Guide

How to troubleshoot a failed installation or configuration

To configure a universal share, ensure that instant access is enabled on the storage server. For more information about instant access, see the following guides:

- NetBackup Web UI VMware Administrator's Guide
- NetBackup Web UI Microsoft SQL Administrator's Guide

To ensure that instant access is enabled on the storage server

1. Log in to the storage server and run the following command:

   `/usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh`

2. Review the pre-condition checking results and the configuration results:

   `/var/log/vpfs/ia_byo_precheck.log` (for build your own (BYO) instant access only)

   `/usr/openv/pdde/vpfs/vpfs-config.log` (for both instant access and BYO)

   In the following example, several required services are not running:

```
[root@rhelnbu06 ~]# /usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh
Mon Apr 13 12:42:14 EDT 2020 Try to get storagepath
Mon Apr 13 12:42:14 EDT 2020 Storage ContentRouter config path is
   /msdp/etc/puredisk/contentrouter.cfg
Mon Apr 13 12:42:14 EDT 2020 Storagepath is /msdp
Mon Apr 13 12:42:14 EDT 2020 File system for partition /msdp is
   ext2/ext3
Mon Apr 13 12:42:14 EDT 2020 File system for partition /msdp/data
   is ext2/ext3
Mon Apr 13 12:42:14 EDT 2020 **** Hardware Virtualization not
   supported, Instant Access browse may be slow ****
Mon Apr 13 12:42:14 EDT 2020 **** system memory support 50 vpfs
   livemounts ****
Mon Apr 13 12:42:14 EDT 2020 **** nginx service required by
   Instant Access is not running ****
Mon Apr 13 12:42:14 EDT 2020 **** smb service required by
   Instant Access is not running ****
Mon Apr 13 12:42:14 EDT 2020 **** docker service required by
   VMware Instant Access is not running ****
```

3. Resolve the issues that are identified in the log. For example, restart any services that are required for instant access.

How to check for universal share capability

To ensure that the storage server has universal share capability

1. Make sure that the storage service is running NetBackup 8.3 or later.
2. Log on to the storage server and run the following command:

   ```
   nbdevquery -liststs -U
   ```

   Make sure that the `InstantAcess` flag is listed in the command's output.

   If the flag is not listed, see one of the guides mentioned above to enable instant access on the storage server.
3. Run the following command:

   ```
   nbdevconfig -getconfig -stype PureDisk -storage_server
   storage_server_name
   ```

   Make sure that the `UNIVERSAL_SHARE_STORAGE` flag is listed in the command's output.

   If the flag is not listed, create a universal share on the storage server:

   See "Create a universal share" on page 169.

How to restart a universal share

Whenever a universal share is created, a script is also created on the storage server. This script (`/<msdp storage data path>/vpfs.mnt`) can be used later to restart a universal share.

For example:

```
[root@rsvlmvc01vm309 vpfs.mnt]# mount | grep vpfs
vpfsd on /mnt/vpfs type fuse.vpfsd (rw,nosuid,nodev,relatime,user_id=0,
   group_id=0,default_permissions,allow_other)
vpfsd on /mnt/vpfs_shares/aa7e/aa7e83e5-93e4-57ea-a4a8-81ddbf5f819e
   type fuse.vpfsd (rw,nosuid,nodev,relatime,user_id=0,group_id=0,
   default_permissions,allow_other)
```

In this example, `aa7e/aa7e83e5-93e4-57ea-a4a8-81ddbf5f819e` is the universal share's ID. This ID is found on the details page of the universal share in the NetBackup web UI: On the left, click **Storage > Universal Share** and then select the universal share to view its details.

Creating a cloud recovery host for image sharing

Use this topic to create a cloud recovery host for image sharing. Use the information from the following topics from the *NetBackup Deduplication Guide* about a cloud recovery host:

About image sharing using MSDP cloud

To configure cloud recovery host:

1. On the left, click **Storage** and then click **Add**. If you deleted a storage server, refresh this page.
2. Select **Media Server Deduplication Pool (MSDP) for image sharing** from the list.
3. In the basic properties, enter all the required information and click **Next**.

   You must select your media server by clicking on the field. If you do not see the media server you want use, use the search option.
4. In the storage server options, enter all the required information except for **Encryption options** and **Encryption for local storage** and click **Next**.

   If KMS encryption is enabled for the on-premises side, Key Management Service (KMS) must be configured before you can configure cloud recovery host. Then the KMS options from the on-premises side are checked and configured automatically in the cloud recovery host.
5. (Optional) In Media servers, click **Next**. As the cloud recovery host is an all-in-one NetBackup server, no additional media servers are added.
6. On the **Review** page, confirm that all options are correct and click **Save**.

   If the MSDP with image sharing creation is unsuccessful, follow the prompts on the screen to correct the issue.
7. At the top, click on **Create disk pool**.

   Another way: On the left, click **Storage**, click the **Disk pools** tab, and then click **Add**.
8. In **Disk pool** options, enter all the required information and click **Next**.

   Click **Change** to select a storage server.
9. In **Volumes**, use the **Volume** drop down to add a new volume. Enter all the required information based on the selection and click **Next**.

   The volume name must be same as the volume name that is on the on-premises side or the sub bucket name.

10 In **Replication**, click **Next** to continue without adding any master server.

11 On the **Review** page, verify that all settings and information are correct. Click **Save**.

Chapter 15

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. You can also configure access to the protection plan for your workload administrators before or after you configure the protection plan. To set up access, you need to configure roles in RBAC and then assign those roles to the protection plan.

Before you create a protection plan, you must configure all storage options. You can use the web UI to configure the OpenStorage, AdvancedDisk, Cloud storage, and MSDP storage options. Also, the web UI lets you configure a disk pool and a storage unit as well.

See “About storage configuration” on page 162.

Note: After upgrade, the protection plans may not appear in the web UI. The conversion process may not have run but should run within 5 minutes of performing the upgrade.

To create a protection plan

1. On the left, click **Protection** > **Protection plans** and then click **Add**.
2. In **Basic properties**, enter a **Name**, **Description**, and select a **Workload** from the drop-down list.

   Optional selection:

   - **Policy name prefix**:
     Use this option for policy names. A prefix is appended to the policy name when NetBackup automatically creates a policy when users subscribe assets to this protection plan.
3. In **Schedules and retention**, click **Add**.

   You can set up a daily, weekly, or monthly backup and then set retention and replication of that backup. Also depending on workload, you can set up the following backup schedules: a **Automatic**, **Full**, **Differential incremental**, **Cumulative Incremental**, or **Snapshot only**.

   If you select **Monthly** as a frequency, you can select between **Days of the week** (grid view) or **Days of the month** (calendar view).

   Note: If you select **Automatic** for the schedule type, then all schedules for this protection plan are **Automatic**. If you select a **Full**, **Differential incremental**, or **Cumulative Incremental** for the schedule type, then all schedules for this protection plan must be one of these options.

   If you select **Automatic** for the schedule type, NetBackup automatically sets the schedule type for you. NetBackup calculates when to do a **Full** or **Differential incremental** based on frequency you specify.

   In the **Attributes** tab:

   - Select the **Backup type**, how often it runs, and how long to keep the backup for this schedule.
     - The selections in the **Backup type** are dependent on workload that is selected and any other backup schedules that are currently active in this protection plan.
   - (Optional) To replicate the backup, select **Replicate this backup**.

- To use the **Replicate this backup** option, the backup storage must be a source in a targeted A.I.R. environment. The **Replication target** is configured in step 5.
- For more information about replication, review *About NetBackup Auto Image Replication* in the NetBackup Administrator's Guide, Volume I.

- (Optional) To keep a copy in long-term storage, turn on **Duplicate a copy immediately to long-term retention**.
  - NetBackup immediately duplicates a copy to long-term storage after the backup completes.
  - The schedule options that are available for long-term storage are based on the frequency and the retention levels for the regular backup schedules that you created.

In the **Start window** tab:

- Define a **Start day**, **Start time**, **End day**, and **End time** for this schedule using the options available on the screen. Or you can drag your cursor over the time boxes to create the schedule.
- Use the options on the right to duplicate, remove, or undo changes to a schedule.

Click **Save** after all options are selected in the **Attributes** and the **Start window** tabs.

Review the **Backup schedule preview** window and verify that all schedules are set correctly.

4 (Optional) If you have selected the **Cloud** workload, you can configure snapshot replication after you have configured a schedule and retention. For more information about cloud snapshot replication, see the NetBackup Web UI for Cloud Administrator's Guide.

In the **Additional copies** column:

- Click **Configure Snapshot replication**.
- In the **Configure snapshot replica dialog**, click **Add**.
- Configure the **Retention** and select the **Destination** for the replicated snapshots.

Note: You can only create one additional cloud replication copy per protection plan.

If you selected **Cloud** as a workload, proceed to step 8.

5 In **Storage options**, configure the storage type per schedule you configured in step 3.

The options vary depending on storage options currently setup to work with NetBackup.

A protection plan can only use 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 6.
Perform snapshot backups	Microsoft SQL Server is required for this option.	For instructions on configuring protection plans for Microsoft SQL Server, see the following topic: ▪
Backup storage	OpenStorage is required for this option. Tape, storage unit groups, and Replication Director not supported.	Click **Edit** 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 recovery points to support the creation of instant access VMs or databases.
Replication target	The backup storage must be a source in a targeted A.I.R. environment.	Click **Edit** 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. If the replication target master server is not in the list, you must add one in NetBackup. For more information on how to add a replication target master server, review *Adding a trusted master server* in the NetBackup Deduplication Guide.

Storage option	Requirements	Description
Long-term retention storage	OpenStorage is required for this option. Tape, storage unit groups, and Replication Director not supported.	Click **Edit** to select the cloud storage provider. Click **Use selected storage** after selecting the cloud provider target.
Transaction log options	Microsoft SQL Server is required for this option.	If you use the option **Select custom storage options**, click **Edit** to select the backup storage.

6 In **Backup options**, configure all options based on your workload type. The options in this area change depending on workload, schedule, or storage options selected.

7 In **Permissions**, review the roles that have access to protection plans.

To give another role access to this protection plan, click **Add**. Select the **Role** in the table and customize the role by adding or removing permissions in the **Select permissions** section.

See the NetBackup Web UI Administrator's Guide.

8 In **Review**, verify that the protection plan details are correct and click **Finish**.

Edit or delete a protection plan

Edit a protection plan

You can make changes to the **Description** and the **Storage options** in a protection plan.

Note: You cannot edit the **Schedules**, **Protected assets**, or **Advanced** options after a protection plan is created. If you want to use different protection settings, you must create a new protection plan or customize the plan.

See "Create a protection plan" on page 177.

To edit a protection plan

1 On the left, click **Protection** > **Protection plans**.

2 Click on the protection plan name that you want to edit.

3 Click **Edit description** to edit the description.

4 (Optional) In the **Storage options** section, click **Edit** to change the storage options.

Delete a protection plan

You cannot delete a protection plan unless all assets have been removed from the protection plan. If you want to maintain protection on the assets, you must move them to another protection plan before you delete the current protection plan.

See "Unsubscribe an asset from a protection plan" on page 183.

See "Subscribe an asset or an asset group to a protection plan" on page 182.

To delete a protection plan

1. On the left, click **Protection** > **Protection plans**.
2. Select the check box next to the protection plan name.
3. On the top right, click **Delete**. Then click **Yes**.

See "Create a protection plan" on page 177.

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.

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

1. On the left, click **Workloads** then the workload type (for example: **VMware**).
2. Select an asset type (for example: **Virtual machines**, **Intelligent VM groups**).
3. Select one or more assets.
4. Click **Add protection**.

   If you selected a Cloud workload asset or asset group, proceed to step 7
5. In **Choose a protection plan**, select the name of the protection plan and click **Next**.
6. (Optional) Adjust any options in the **Backup options** or **Advanced sections**.
   - **Schedules**
     Change the backup start window for full or incremental schedules.
     For SQL Server transaction log schedules you can change the start window, the recurrence, and the retention period.
   - **Backup options**
     Adjust the backup options that were set up in the original protection plan. The options in this area change depending on workload.

- **Advanced**
  Change or add any options that were set up in the original protection plan.

You need the following permissions to make these changes:

- **Edit attributes**, to edit **Backup options** and **Advanced** options.
- **Edit full and incremental schedules**, to edit the start window for these schedule types.
- **Edit transaction log schedules**, to edit the settings for SQL Server transaction log schedules.

7 Click **Protect**.

See "Create a protection plan" on page 177.

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 **Workloads** then the workload type (for example: **VMware**).

2 Select a single asset type (for example: **Virtual machines**).

3 Click on the specific asset name.

4 Click **Remove protection** and click **Yes**.

To unsubscribe a group of assets from the protection plan

1 On the left, click **Workloads** then 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 **Remove protection** and click **Yes**.

See "Create a protection plan" on page 177.

See "Edit or delete a protection plan" on page 181.

View protection plan overrides

When you set permissions for protection plans, you can set the permissions to allow your workload administrator to customize assets a protection plan covers. The workload administrator can apply overrides to certain areas of schedules and backup options for an asset.

To view protection plan overrides

1. On the left, click **Protection** > **Protection plans** and then click the name of the protection plan.
2. In the **Protected assets** tab, click on **Applied** in the **Custom settings** column.
3. Review the original and the new settings in the **Schedules** and **Backup options** tabs.
   - **Original**: The setting when the protection plan was first created.
   - **New**: The last change that was made to the protection plan for that setting.

About Backup Now

With Backup Now, workload administrators can back up an asset immediately. For example, you may use Backup Now to prepare for upcoming events that are outside scheduled backups, such as system maintenance. This type of backup is independent of scheduled backups and does not affect future backups. You can manage and monitor a Backup Now job in the same way you manage and monitor other NetBackup jobs.

Backup Now is supported for the following workloads:

- VMware
- RHV
- Cloud
- Microsoft SQL

Note: You can select only one asset at a time for each Backup Now operation. Also, you must have permissions to subscribe to least one protection plan to use Backup Now.

To use Backup Now from the web UI

1. Select the workload from the left.
2. Select the asset that you want to back up.

3 Click **Backup now** at the top of the table or select **Backup now** from the action menu in the asset's row.

4 Choose a protection plan for the backup.

All protection plans to which the asset is subscribed are listed.

If you want to back up an asset that is not subscribed to any protection plan, you can select **Backup now** and choose from existing protection plans. You can also create a new protection plan and then use it with a **Backup now** operation.

5 Start the backup.

To use Backup Now from an asset's Details page

- When you view an asset's details, you can see all of the protection plans to which the asset is subscribed. You can choose **Backup now** from any one of the protection plans that are listed.

  If you want to back up an asset that is not subscribed to any protection plan, you can select **Backup now** and choose from existing protection plans. You can also create a new protection plan and then use it with a **Backup now** operation.

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 15-1 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 15-1 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.

About policy management in the NetBackup web UI

The NetBackup web UI uses protection plans to protect the assets in your NetBackup environment. To manage classic policies you must use the NetBackup Administration Console. However, some policy types can also be managed in the NetBackup web UI:

- MS-Windows
- Standard
- Oracle
- MS-SQL-Server
- NDMP

See the following guides for details on these policies.

NetBackup Administrator's Guide, Volume I

NetBackup for Oracle Administrator's Guide

NetBackup for Microsoft SQL Server Administrator's Guide

NetBackup for NDMP Administrator's Guide

Chapter 16

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 provides the following benefits:

- Ability to plan for capacity licensing.
- On a weekly basis, NetBackup gathers and reports usage and trend information. The `nbdeployutil` utility has scheduled runs to gather data for the report (enabled by default). For more information, see Scheduling capacity licensing reports.
- A link to Usage Insights. This tool allows NetBackup customers to proactively manage their license use through near real-time visibility of consumption patterns.
- Reporting for the following policy types.

BigData	Informix	NDMP	Sybase
MS-Exchange-Server	MS-SQL-Server	Oracle	VMware

Hyper-V	MS-Windows	Standard	Hypervisor

Requirements

NetBackup automatically collects data for the usage reporting, provided the following requirements are met:

- The master server (or master servers) are at NetBackup 8.1.2 or later.
- You use capacity licensing.
- You use automatic, scheduled reports. If you manually generate capacity license reports, the data does not display in the usage report in the NetBackupweb UI.
- The following file exists:
  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 the servers list for usage reporting" on page 188.
  See "Track backup data size on your master servers" on page 187.

Additional information

Scheduling capacity licensing reports. Details on capacity licensing, scheduling, and options for capacity licensing reports.

Veritas Usage Insights Getting Started Guide. Details on how to use Usage Insights 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.

Configure the 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.**

Scheduling reports for capacity licensing

By default, NetBackup triggers `nbdeployutil` to run on a specified schedule to incrementally gather data and to generate licensing reports. For the first run, the duration of the report uses the frequency that is specified in the configuration file.

For capacity licensing, the report duration is always for the last 90 days based on the availability of the gathered data. Any data older than 90 days is not considered in the report. Each time `nbdeployutil` runs, it gathers information for the time between the latest run of `nbdeployutil` and the previous successful run.

Licensing report location

The current capacity licensing report resides in the following directory:

On Windows: *`install_path`*`\NetBackup\var\global\incremental`

On UNIX: `/usr/openv/var/global/incremental`

It contains the following files:

- The generated report for the latest `nbdeployutil` result.
- Folders containing incrementally gathered data.
- The archive folder that contains the older generated reports.
- `nbdeployutil` log files.

The older reports are placed in the archive folder. Veritas recommends that you retain at least 90 days of reporting data. Data can be kept longer than 90 days, depending on the requirements of your environment. Older reports can help to show how the capacity usage has changed over time. Delete the reports or the folder when they are no longer required.

Use Case I: Using the default values for the licensing report

The `nbdeployutilconfig.txt` file is not required when you use the default parameters. `nbdeployutil` uses the following default values for capacity licensing:

- FREQUENCY_IN_DAYS=7
- MASTER_SERVERS=*local_server*
- PARENTDIR=*folder_name*
  For Windows: *`install_path`*`\NetBackup\var\global\incremental`
  For UNIX: `/usr/openv/var/global/incremental`
- PURGE_INTERVAL=120 (number of days)
- MACHINE_TYPE_REQUERY_INTERVAL = 90 (number of days)

Use Case II: Using custom values for the licensing report

If the file `nbdeployutilconfig.txt` is not present, create a file using the following format:

```
[NBDEPLOYUTIL_INCREMENTAL]
MASTER_SERVERS=<server_names>
FREQUENCY_IN_DAYS=7
PARENTDIR=<folder_name_with_path>
PURGE_INTERVAL=120
MACHINE_TYPE_REQUERY_INTERVAL=90
```

To use custom values for the licensing report

1. Copy the `nbdeployutilconfig.txt` file to the following location:

   For Windows: *`install_path`*`\NetBackup\var\global`

   For UNIX: `/usr/openv/var/global`

2. Open the `nbdeployutilconfig.txt` file.

3 Edit the `FREQUENCY_IN_DAYS` value to reflect how often you want the report to be created.

Default (recommended)	7
Minimum	1
Value of 0	Disables the incremental reporting and no licensing information is captured.
Parameter deleted	`nbdeployutil` uses the default value.

4 Edit the `MASTER_SERVERS` value to include a comma-separated list of the master servers you want to include in the report.

Note: Veritas Usage Insights requires that master servers be at NetBackup 8.1.2 or later.

No value	`nbdeployutil` uses the default value.
Parameter deleted	`nbdeployutil` uses the default value.

For example:

- MASTER_SERVERS=newserver, oldserver
- MASTER_SERVERS=newserver, oldserver.domain.com
- MASTER_SERVERS=myserver1.somedomain.com, newserver.domain.com

5 Edit the `PARENTDIR` value to include the full path for location where the data is gathered and reported.

No value	`nbdeployutil` uses the default value.
Parameter deleted	`nbdeployutil` uses the default value.

6 Edit the `PURGE_INTERVAL` to indicate the interval (in days) for how often you want to delete the report data. Data that is older than 120 days is automatically purged.

Default	120
Minimum	90
No value	`nbdeployutil` uses the default value.
Parameter deleted	`nbdeployutil` uses the default value.

7 Edit the `MACHINE_TYPE_REQUERY_INTERVAL` to indicate how often to scan physical clients for updates to the machine type.

Default	90
Minimum	1
No value	`nbdeployutil` uses the default value.
Parameter deleted	`nbdeployutil` uses the default value.

Other configuration for incremental reporting

To change the directory of the gathered data and capacity licensing report

1 If you have older gathered data and licensing reports, copy the complete directory to the new location.

2 Edit `nbdeployutilconfig.txt` and change the location of the gathered data and licensing report in the `PARENTDIR=`*`folder_name`* field.

To use the data that was gathered previously to generate a capacity licensing report

1. Locate the folder that was generated for the gathered data after the previous run of `nbdeployutil` and copy it to the following location:

   On Windows: *install_path*\NetBackup\var\global\incremental

   On UNIX: `/usr/openv/var/global/incremental`

2. Create the gather_end.json file inside the copied folder and add the following text:

   ```
   {"success":0}
   ```

   The next incremental run considers the data inside the copied folder to generate a capacity licensing report.

Note: Delete any other gather folders inside the copied folder to avoid gaps for the period in which data is gathered. The missing data is automatically generated during the next incremental run.

To create a custom interval report using existing gathered data for capacity licensing

- To create a report for a time interval that is different than the default interval of 90 days, run the following command:

  On Windows:

  ```
  nbdeployutil.exe --capacity --incremental --report --inc-settings
  "install_dir\netbackup\var\global\nbdeployutilconfig.txt"
  --hoursago <custom-time-interval>
  ```

  On UNIX:

  ```
  nbdeployutil.exe --capacity --incremental --report --inc-settings
  "/usr/openv/var/global/nbdeployutilconfig.txt"
  --hoursago <custom-time-interval>
  ```

  The number of hours specified in `--hoursago` must be fewer than the purge-interval that is specified in the `nbdeployutilconfig.txt` file.

Note: `nbdeployutil` uses existing gathered data to generate the custom interval report. You are not required to use the `--gather` option.

Troubleshooting failures for `nbdeployutil` and incremental reporting

- `nbdeployutil` fails to gather data and generate the report for your environment. Refer to the logs to understand when the task failed and the reason for the failure.
- `nbdeployutil` fails with a bpimagelist error with status 37 after you run the utility manually. Ensure that you added the master servers to the additional servers list.
- For Oracle Real Application Clusters (RAC), protected data size may be reported more than once because the size is reported for the node where data backup happens.
  If the backup operation is initiated from different nodes in the Oracle Real Application Clusters (RAC), the capacity licensing report displays a separate row for every node.
- The following error displays because of internal web service communication failures:
  Report for master server *SERVER_NAME* is generated using the backup image header method instead of accurate licensing method because of web service interruptions during the gather phase.
- For VMware or NDMP, when the backup agent fails to post licensing information to the database, a status code 5930 or 26 displays in the Activity Monitor: For more information, see the NetBackup Status Codes Reference Guide.

Section 4

Veritas Resiliency Platform

Chapter 17

Managing Resiliency Platforms

This chapter includes the following topics:

About Resiliency Platform in NetBackup

You can integrate NetBackup and Veritas Resiliency Platform to manage your disaster recovery operations. Veritas Resiliency Platform provides a single console from which you can proactively maintain business uptime across private, public, and hybrid clouds. Integrating NetBackup and Resiliency Platform lets you leverage the capabilities, such as complete automation, visualizing and monitoring DR specific information for all resiliency operations for the virtual machines in your data center.

Note the following points:

- You can integrate more than one Resiliency Platform with your NetBackup master server.
- You can have more than one data centers for a Resiliency Platform.
- You can use Resiliency Platform with Veritas Resiliency Platform version 3.5 and later in NetBackup.
- After you add a Resiliency Platform, the assets are automatically discovered and displayed on the **Virtual machines** tab.

- You can view detailed information alerts and error messages in the **Notifications** section.

Understanding the terms

The following table explains the key components related to Veritas Resiliency Platform and NetBackup integration.

Term	Description
Resiliency Platform	The Veritas Resiliency Platform integrated with your NetBackup master server. The Resiliency Manager provides the services required for protecting assets, such as virtual machines, within a resiliency domain. It also provides workload automation services.
Resiliency manager	The component that provides resiliency capabilities within a resiliency domain. It is composed of loosely coupled services, a distributed data repository, and a management console.
Infrastructure management server (IMS)	The component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager. The IMS is deployed as a virtual appliance. To achieve scale, multiple IMSs can be deployed in the same data center.
Data center	The location that contains source data center and a target data center. Each data center has one or more IMSs.
Resiliency group	The unit of management and control in Resiliency Platform. You organize related assets into a resiliency group and manage and monitor them as a single entity.
Automated virtual machines	The assets that are a part of a resiliency group and you can perform actions, such as migrate, takeover, rehearse, and restore.
Recovery readiness	Measured based on migrate, takeover, restore or rehearsal operations. ■ Low - If no operations are performed or failed. ■ High - If at least one operation is performed successfully in the past 7 days. ■ Medium - If the recovery readiness does not fall in either high or low category.

Term	Description
Recovery Point Object (RPO)	Recovery Point Objective is the point in time you can recover to in the event of a disaster. For example, if you have an RPO of 4 hours on your critical virtual machines then you lose 4 hours of data, as 4 hours ago is the last point in time to which you can recover data on your VMs.

Configuring a Resiliency Platform

You can add, edit, delete, or refresh a Resiliency Platform. You can add more than one Resiliency Platform in NetBackup.

Add a Resiliency Platform

You can add one or more than one Resiliency Platforms in NetBackup. The Resiliency Platform lets you add virtual machines and automate protection. If the resiliency manager is using a third-party certificate, see the NetBackup Web UI Administrator's Guide.

To add a Resiliency Platform

1. On the left, click **Resiliency**.
2. Click the **Resiliency Platform** tab.
3. Click **Add Resiliency Platform**.
4. Read the instructions on the **Add Resiliency Platform** dialog box and click **Next**.
5. In the **Add credentials** dialog box, enter a value in the following fields and click **Next**:
   - **Resiliency manager host name or IP address**
   - **Resiliency Platform API access key**
   - **NetBackup API access key**
6. In the **Add data center and Infrastructure management** server dialog box, select a data center.
7. In the **Infrastructure management server** section, select a preferred server.
8. Click **Add**.

   After you add the Resiliency Platform in NetBackup, the NetBackup master server will be configured automatically in the Resiliency Platform.

Configuring a third-party CA certificate

You can use a self-signed or a third-party certificate to validate your Resiliency manager.

Consider the following points:

- For Windows, you can give a certificate as a file path or install the third-party certificate in the Trusted root certificates authorities.
- To switch from a self-signed certificate to a third-party certificate for an already added Resiliency Platform, you can edit the Resiliency Platform.

To configure a third-party CA certificate

1. Copy a PKCS #7 or P7B file having certificates of the trusted root certificates authorities that are bundled together. This file may either be PEM or DER encoded.
2. Create a CA file containing the PEM encoded certificates of the trusted root certificate authorities that are concatenated together.
3. In the bp.conf file, create the following entries, where /certificate.pem is the file name:
   - ECA_TRUST_STORE_PATH = /certificate.pem
   - Verify that the `nbwebsvc` account has the permissions to access the path that ECA_TRUST_STORE_PATH refers.

Editing or deleting a Resiliency Platform

After you add a Resiliency Platform, you can edit the Resiliency Platform and NetBackup API access keys. You cannot change or update the Resiliency manager host name or IP address. However, you can delete the Resiliency Platform and add it to NetBackup again. If you refresh the Resiliency Platform, the discovery of assets on the Resiliency Platform is triggered.

To edit a Resiliency Platform

1. On the left, click **Resiliency**.
2. Click the **Resiliency Platform** tab.
3. Click the **Actions** menu for the Resiliency Platform that you want to edit and select **Edit**.
4. Enter the updated **Resiliency Platform API access key** and **NetBackup API access key.**
5. Click **Next**.

6. In the **Edit data center and Infrastructure management server** dialog box, select the **Data center** and then select the preferred infrastructure management server.
7. Click **Save**.
8. To delete a Resiliency Platform, from the **Actions** menu, select **Delete**.

Viewing the automated or not-automated VMs

The virtual machines that belong to a resiliency group in Veritas Resiliency Platform are discovered and displayed on the **Automated** tab and the VMs that don't belong any resiliency group are displayed on the **Not automated** tab. You can view the status of the assets and perform various actions. You can search for a VM or apply filters too.

The following table lists the columns displayed on the **Automated** and **Not automated** tabs:

Table 17-1

Tab	Column	Description
■ Automated ■ Not automated	**Name**	Name of the virtual machine.
■ Automated	**RPO**	Recovery Point Objective is the point in time you can recover to in the event of a disaster. For example, if you have an RPO of 4 hours on your critical virtual machines then you lose 4 hours of data, as 4 hours ago is the last point in time to which you can recover data on your VMs.
■ Automated ■ Not automated	**State**	Whether the VM is switched on or off.

Table 17-1 *(continued)*

Tab	Column	Description
■ Automated	**Recovery readiness**	Measured based on migrate, takeover, restore or rehearsal operations. ■ Low - If no operations are performed or failed. ■ High - If at least one operation is performed successfully in the past 7 days. ■ Medium - If the recovery readiness does not fall in either high or low category.
■ Automated ■ Not automated	**Platform**	The platform that the VM belongs to.
■ Automated ■ Not automated	**Server**	The server name of the VM.
■ Automated	**Protection**	Protection status of the VM.
■ Automated	**Resiliency group**	Name of the resiliency group to which the VM belongs.
■ Not automated	**Recovery action**	Launch the Resiliency Platform to add the VM to a resiliency group.

To view and perform actions on automated VMs

1. On the left, click **Resiliency**.
2. On the **Virtual machines** tab, click **Automated**.
3. To view more details about a VM, in the **Name** column, click a VM.
4. To view all VMs that are a part of the same resiliency group, click the preferred resiliency group.

5 To perform disaster recovery operation, such as rehearse, restore, or recover, click **Launch Resiliency Platform**.

To enable single-sign, same authentication domain must be configured NetBackup and Veritas Resiliency Platform. If not configured, you must login with username and password to access Veritas Resiliency Platform web console.

6 Log on to your Resiliency Platform and perform the preferred action. See the *Veritas™ Resiliency Platform User Guide.*

To view and perform actions on not automated VMs

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

2 On the **Virtual machines** tab, click **Not automated**.

3 To add the VM to a resiliency group, in the **Recovery action** column, click **Automate Recovery**.

4 Perform the preferred action for your Resiliency Platform. See, the *Veritas™ Resiliency Platform User Guide*.

Troubleshooting NetBackup and Resiliency Platform issues

Use the following information to troubleshoot issues.

Table 17-2 Troubleshooting issues

Issue	Action
Failed to configure the current NetBackup master server with the Resiliency Platform.	Check the logs at the following location in Veritas Resiliency Platform's Resiliency manager: ■ /var/opt/VRTSitrp/logs/copydata-service.log ■ /var/opt/VRTSitrp/logs/api-service.log

Failed to establish a persistent connection between the current NetBackup master server and the Resiliency Platform.	■ Verify that the logged in user has permissions in credentials namespace.
	■ Check the logs at the following location on the NetBackup master server:
	  ■ /usr/openv/logs/nbwebservice/ in NetBackup installation directory
	  ■ C:\Program Files\Veritas\NetBackup\logs\nbwebservice in NetBackup windows

Table 17-2 Troubleshooting issues *(continued)*

Issue	Action
Failed to launch the Veritas Resiliency Platform	Verify that same authentication domain is used to configure Veritas Resiliency Platform and NetBackup.

Section 5

Managing credentials

Chapter 18

Managing credentials

This chapter includes the following topics:

About credential management in NetBackup

The Credential management node in the NetBackup web user interface provides the ability to centrally manage credentials that NetBackup uses.

In NetBackup you can create and manage credentials for the following systems:

- An external key management service (KMS) server
- Microsoft SQL Server

Adding credentials comprises the following steps:

- Add the basic credential properties (for example, credential name or tag)
- Assign a category to the credential (for example: Microsoft SQL Server or External KMS server)
- Assign the required permissions to access the credentials

Add a credential in NetBackup

You can add credentials that NetBackup uses to connect to various systems.

To add a credential

1. On the left, click **Credential management**.
2. Click **Add**.
3. Add the following basic properties:
   - Credential name (for example: *sqlserver_cred1*)
   - Tag (for example: *sqlserver*)
   - Description (for example: This credential is used to access *sqlserver*)
4. Click **Next**.
5. Select a credential category and the respective credential details that you want to assign to this credential.

External KMS	Select to assign the credential to the external KMS server that you have configured. Provide the following credential details of the external KMS server that are used to authenticate the communication between the NetBackup master server and the external KMS server: ■ Certificate - Specify the certificate file contents. ■ Private Key - Specify the private key file contents. ■ CA Certificate - Specify the CA certificate file contents. ■ Passphrase - Enter the passphrase of the private key file. ■ CRL Check level - Select the revocation check level for the external KMS server certificate. CHAIN - The revocation status of all the certificates from the certificate chain are validated against the CRL. DISABLE - Revocation check is disabled. The revocation status of the certificate is not validated against the CRL during host communication. LEAF - The revocation status of the leaf certificate is validated against the CRL. See the NetBackup Security and Encryption Guide for more information on external KMS configuration.
Microsoft SQL Server	Select to assign the credential to SQL server that you have configured. Use one of the following options: ■ Use credentials that are defined locally on the client ■ Provide Microsoft SQL Server credentials

6 Click **Next**.

7 Click **Add** to assign permissions to a specific role to access this credential.

See “Credentials” on page 89.

8 Click **Next** and follow the prompts to complete the wizard.

Edit a credential

You can edit a credential when you want to change the credential tag, description, category, or permissions. You cannot change the credential name.

To edit a credential

1 On the left, click **Credential management**.

2 Locate and click on the credential that you want to edit.

3 Click **Edit**.

4 Edit the credential as required.

5 After all the changes are reviewed, click **Finish**.

Delete a credential

You can delete a credential that you no longer need.

To delete a credential

1 On the left, click **Credential management**.

2 Locate and click on the credential that you want to delete.

3 Click **Delete**.

Chapter 19

Troubleshooting the NetBackup Web UI

This chapter includes the following topics:

Tips for accessing the NetBackup web UI

When NetBackup is properly configured, a user can access the master server at the following URL:

https://*masterserver*/webui/login

If the web UI on a master server does not display, follow these steps to troubleshoot the issue.

Browser displays an error that the connection was refused or that it cannot connect to the host

Table 19-1 Solutions when the web user interface does not display

Step	Action	Description
Step 1	Check the network connection.	

Table 19-1 Solutions when the web user interface does not display *(continued)*

Step	Action	Description
Step 2	Verify that the firewall is open for port 443.	Refer to the following article: https://www.veritas.com/docs/100042950
Step 3	If port 443 is in use, configure another port for the web UI.	Refer to the following article: https://www.veritas.com/docs/100042950
Step 4	Verify that the `nbwebservice` is up.	Check the `nbwebservice` logs for more details.
Step 5	Verify that the `vnetd -http_api_tunnel` is running.	Verify that the `vnetd -http_api_tunnel` service is running. For more details, check the `vnetd -http_api_tunnel` logs with OID 491.
Step 6	Ensure that the external certificate for the NetBackup web server is accessible and has not expired.	■ Use the Java Keytool commands to validate the following file: Windows: *install_path*`\var\global\wsl\credentials\nbwebservice.jks` UNIX: `/usr/openv/var/global/wsl/credentials nbwebservice.jks` ■ Check whether the `nbwebgroup` has a permission to access the `nbwebservice.jks` file. ■ Contact Veritas Technical Support.

Cannot access web UI when you use a custom port

- Restart the `vnetd` service.
- Follow the steps in Table 19-1.

Certificate warning displays when you try to access the web UI

The certificate warning displays if the NetBackup web server uses a certificate that is issued by a CA that is not trusted by the web browser. (Including the default NetBackup web server certificate that the NetBackup CA issued.)

To resolve a certificate warning from the browser when you access the web UI

1. Configure the external certificate for the NetBackup web server.

   See "Configure an external certificate for the NetBackup web server" on page 95.

2. If the problem persists, contact Veritas Technical Support.

If a user doesn't have the correct permissions or access in the NetBackup web UI

Note that only administrators, root users, or Enhanced Auditing users automatically have full access to the web UI. Other users must be configured in RBAC to have access and permissions for the web UI.

See "Configuring RBAC " on page 40.

If a user does not have the correct permissions or cannot access the workload assets that they should have access to, do the following:

- Verify that the user's credentials match the username (or the username and the domain name) that is specified in the user's access rule.
- Review the roles for the user in **Security > RBAC**. You may need to change the role permissions. However, be aware that those kinds of changes also affect any other users that belong to those roles.
- Any user account changes with the identity provider are not synchronized with the user's roles. If a user account changes with the identity provider, the user may not have the correct permissions or access. The NetBackup security administrator must edit each role for the user to remove the existing user account and re-add the new account.
- Changes to a user's roles are not immediately reflected in the web UI. A user with an active session must sign out and sign in again before any changes take effect.

Unable to add AD or LDAP domains with the vssat command

After you add an AD or LDAP domain, you can verify the configuration with the `vssat validateprpl` command and for groups with the `vssat validategroup` command. If a domain is not added successfully, the `vssat` validation displays `The principal or group does not exist`. More details are written to the `nbatd` logs.

Validation of an AD or LDAP user can fail for any of the following reasons:

- The connection cannot be established with the AD or LDAP server
- Incorrect user credentials were provided
- An incorrect user base DN or group base DN was provided
- Multiple users or groups exist with the same name under the user base DN or the group base DN

- The user or group does not exist

For information about the `vssat` command, see the NetBackup Commands Reference Guide.

Connection cannot be established with the AD or the LDAP server

If NetBackup could not establish a connection with the AD or the LDAP server, the `nbatd` logs contain the following error:

Example of error message:

```
(authldap.cpp) CAuthLDAP::validatePrpl - ldap_simple_bind_s()
failed for user CN=Test User,OU=VTRSUsers,DC=VRTS,DC=com',
error = -1, errmsg = Can't contact LDAP server,9:debugmsgs,1
```

LDAP server URL validation fails

The LDAP server URL (`-s` option) that is entered using the `vssat addldapdomain` command does not pass the validation test.

Validate the URL:

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd>
-d <debug_level> -o nettimeout=<seconds>
```

Example of validation error message:

```
ldapsearch -H ldaps://example.veritas.com:389 -D
"CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w ********
-d 5 -o nettimeout=60

TLS: can't connect: TLS error -8179:Peer's Certificate issuer
is not recognized. ldap_sasl_bind(SIMPLE):
Can't contact LDAP server (-1)
```

The server certificate issuer is not a trusted certificate authority (CA)

If you use the `ldaps` option you can validate the certificate issuer using the `ldapsearch` command.

Validate the certificate issuer:

```
set env var LDAPTLS_CACERT to cacert.pem

ldapsearch -H <LDAPS_URI> -D "<admin_user_DN>" -w <passwd>
-d <debug_level> -o nettimeout=<seconds>
```

Example of validation message:

```
ldapsearch -H ldaps://example.veritas.com:389 -D
"CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w ********
-d 5 -o nettimeout=60

TLS: can't connect: TLS error -8179:
Peer's Certificate issuer is not recognized..ldap_sasl_bind(SIMPLE):
Can't contact LDAP server (-1)
```

The file path for `cacert.pem` is:

Windows:

```
install_path\NetBackup\var\global\vxss\eab\data
\systemprofile\certstore\trusted\pluggins\ldap\cacert.pem
```

UNIX:

```
/usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile
/certstore/trusted/pluggins/ldap/cacert.pem
```

The certificate authority (CA) that signed the LDAP server's security certificate is not in the `nbatd` trust store

Use the `-f` option of the `vssat addldapdomain` command to add the certificate to the `nbatd` command's truststore.

This option is necessary if the CA that signed the certificate is other than the following:

Certification Services Division	GeoTrust	Symantec Corporation
CyberTrust	GlobalSign	VeriSign Trust Network
DigiCert	RSA Security Inc.	

User credentials are not valid

When you add an LDAP domain using the `vssat addldapdomain` and the user credentials are not valid, the `nbatd` logs contain the following error:

```
CAuthLDAP::validatePrpl - ldap_simple_bind_s() failed for user
'CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com',
error = 49, errmsg = Invalid credentials,9:debugmsgs,1
```

Run the following command to validate the admin user DN and password:

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>"
-w <passwd> -d <debug_level> -o nettimeout=<seconds>
```

Example of message:

```
ldapsearch -H ldap://example.veritas.com:389 -D
"CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w ********
-d 5 –o nettimeout=60 ldap_bind: Invalid credentials (49)
```

An incorrect user base DN or group base DN was provided

If the user base DN (`-u` option) or the group base DN (`-g` option) is not correct, the `nbatd` logs contain the following error:

```
CAuthLDAP::validatePrpl - ldap_search_s() error = 10,
errmsg = Referral,9:debugmsgs,1 CAuthLDAP::validatePrpl-ldap_search_s()
error = 34, errmsg = Invalid DN syntax,9:debugmsgs,1
```

For example, run the following command:

```
ldapsearch -H ldap://example.veritas.com:389 -D
"CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w ******
-b "OU=VRTSUsers,DC=VRTS,DC=con" "(&(cn=test user)(objectClass=user))"
```

```
ldapsearch -H ldap://example.veritas.com:389 -D
"CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w ******
-b "VRTS" "(&(cn=test user)(objectClass=user))"
```

Multiple users or groups exist with the same name under user base DN or group base DN

To troubleshoot the issue

1. Check if the `nbatd` logs contain the following error:

   ```
   CAuthLDAP::validateGroup - search returned '2' entries for group name
   'team_noone', even with referrals set to OFF,9:debugmsgs,1
   ```

2. Validate the number of matching entries for the existing base DN using the `ldapsearch` command:

   ```
   ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd>
   -d <debug_level> -o nettimeout=<seconds> -b <BASE_DN> <search_filter>
   ```

   This is applicable if user search attribute (`-a` option) and group search attribute (`-y` option) do not have unique values for the existing user base DN and group base DN respectively.

Example of validation message:

```
ldapsearch -H ldap://example.veritas.com:389 -D
"CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w ******
-b "DC=VRTS,DC=com" "(&(cn=test user)(objectClass=user))"
# LDAPv3 # base <DC=VRTS,DC=com> with scope subtree # filter:
(cn=Test User) # requesting: ALL # Test User, VRTSUsers,
VRTS.com dn: CN=Test User,OU=VRTSUsers,DC=VRTS,
DC=com # Test User, RsvUsers, VRTS.com dn:
CN=Test User,OU=RsvUsers,DC=VRTS,DC=com # numEntries: 2
```

User or group does not exist

To troubleshoot the issue

1. Check if the `nbatd` logs contain the following error:

   - `CAuthLDAP::validatePrpl - user ‘test user’ NOT found, 9:debugmsgs,4 CAuthLDAP::validateGroup - group 'test group' NOT found, 9:debugmsgs,4`

2. If a user or group exists in the LDAP domain, but the `vssat validateprpl` or the `vssat validategroup` command fails with this error, validate if the user or the group exists in the current base DNs (-u and -g options) using the following command.

- `ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d <debug_level> -o nettimeout=<seconds> -b <BASE_DN> <search_filter>`

Unable to validate the user or group

When the administrator configures the LDAP server, they must specify the `-d DomainName` option. `DomainName` can be the LDAP server name or the domain name. Whatever name is specified for `-d DomainName` is the domain name that an administrator should use when they add users to an RBAC role.

If you specify the incorrect domain, you may see the error `Unable to validate the user or group`. Review the following:

- The username and domain name are typed correctly.
- You specified the correct domain name.
  The domain name that you should specify depends on how the LDAP server is configured in NetBackup. Contact your administrator for help with adding users to RBAC.