NetBackup™ Web UI Security Administrator's Guide

Release 8.2

VERITAS™

NetBackup Web UI Security Administrator's Guide

Last updated: 2019-06-28

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 user interface

The NetBackup web user interface provides the following features:

- Ability to access the master server from a web browser, including Chrome and Firefox.
  For details on supported browsers for the web UI, see the NetBackup Software Compatibility List.
- A dashboard that displays a quick overview of the information that is important to you.
- Role-based access control (RBAC) that lets the administrator configure user access to NetBackup and to delegate the tasks that are related to security, backup management, or workload protection.
- NetBackup security administrators can manage NetBackup security, certificates, RBAC, API keys, user sessions, and locked NetBackup user accounts.

- Backup administrators provide protection services to satisfy their service level objectives (SLOs). Protection of assets is achieved through protection plans, job management, and visibility of the protection status of assets.
- Workload administrators can subscribe assets to the protection plans that meet the SLO, monitor protection status, and perform self-service recovery of virtual machines. The web UI supports the following workloads:
  - Cloud
  - Red Hat Virtualization (RHV)
  - VMware
- Usage reporting tracks the size of backup data on your master servers. You can also easily connect to Veritas Smart Meter to view and manage NetBackup licensing.

Access control in the NetBackup web UI

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

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

Monitor NetBackup jobs and events

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

- For a NetBackup security administrator, the dashboard lets the administrator see the status of security certificates and of audit events.
- For a backup administrator, the dashboard allows the administrator to see the status of NetBackup jobs. Email notifications can also be configured so they receive notifications when job failures occur. NetBackup supports any ticketing system that can receive inbound email.

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

Protection plans offer the following benefits:

- In addition to schedules for backups, a protection plan can also include a schedule for replication and long-term retention.
- You can easily choose either on-premises or snapshot storage.
- When you select from your available storage, you can see any additional features available for that storage.
- The backup administrator creates and manages protection plans and is therefore responsible for backup schedules and storage.
- The workload administrator primarily selects the protection plans to use to protect assets or intelligent groups. However, the backup administrator can also subscribe assets to protection plans if needed.

Self-service recovery

Terminology

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

Table 1-1 Web user interface terminology and concepts

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

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

Term	Definition
Administrator	A user that has complete access and permissions to NetBackup and all of the interfaces, including the NetBackup web UI. The root, administrator, and Enhanced Auditing user all have complete access to NetBackup. In the *NetBackup Web UI* guides, the term *NetBackup administrator* also refers to a user that has full permissions for NetBackup, usually in reference to a user of the NetBackup Administration Console. Also see *Role*.
Asset group	See *intelligent group*.
Asset	The data to be protected, such as physical clients, virtual machines, and database applications.
Classic policy	In the NetBackup web UI, indicates that a legacy policy protects the asset. Legacy policies are created with the NetBackup Administration Console.
External certificate	A security certificate issued from any CA other than NetBackup.
Intelligent group	Allows NetBackup to automatically select assets for protection based on the criteria (queries) that you specify. An intelligent group automatically stays up-to-date with changes in the production environment. These groups are also referred to as asset groups. For VMware and RHV, these groups appear under the tab **Intelligent VM groups**.
Object group	For RBAC, a collection of assets, protection plans, servers, and other resources that the user is granted access to.
NetBackup certificate	A security certificate issued from the NetBackup CA.
Protection plan	A protection plan defines when backups are performed, how long the backups are retained, and the type of storage to use. Once a protection plan is set up, assets can be subscribed to the protection plan.

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

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

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

After the installation of NetBackup, a root user or an administrator must sign into the NetBackup web UI from a web browser and create RBAC access rules for users. An access rule 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 14.

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 root or the administrator credentials and click **Sign in**.

For this type of user	Use this format	Example
Local user	*username*	**root**
Domain user	*DOMAIN\username*	**WINDOWS\Administrator**

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 access rules for all users that require access to NetBackup.
   - Delegate the task of creating access rules to another user.
     Create an access rule for that user with the role of **Security administrator**. This user can then create rules for all users that require access to the NetBackup web UI.

   See “Configuring RBAC” on page 19.

   Root or administrator access is no longer needed for the web UI once you have delegated one or more users as a NetBackup security administrator.

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 14.
- 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.

Sign in to the NetBackup web UI

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

- Sign in with a user name and password
- Sign in with a certificate or smart card

Sign in with a user name and password

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

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

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

   https://*masterserver*/webui/login

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

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

   For example:

For this type of user	Use this format	Example
Local user	*username*	**root**
Domain user	*DOMAIN\username*	**WINDOWS\Administrator**

Sign in with a certificate or smart card

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

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

To sign in with a certificate or smart card

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

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master server that you want to sign in to.
2. Click **Sign in with certificate or smart card**.
3. When your browser prompts you, select the certificate.

Authorized users

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

Table 1-2 Users that are authorized to use the NetBackup web UI

User	Access
Root, administrator, and Enhanced Auditing users	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 a default or a custom RBAC role	Varies

The NetBackup dashboard

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

Table 1-3 The NetBackup dashboard for the NetBackup security administrator

Dashboard widget	Description
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 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 50.
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.

Chapter 2

Managing role-based access control

This chapter includes the following topics:

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 2-1 RBAC features

Feature	Description
Predefined roles or custom roles allow users to perform specific tasks	Predefined roles in RBAC allow users to perform common tasks for a system administrator, backup administrator, or workload administrator. Or, create custom roles to fit the role of your users. Root users and administrators still have full permissions in all NetBackup interfaces and in the APIs.
Users can access NetBackup areas and 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 successful 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. You cannot use the web UI if you have NetBackup Access Control (NBAC) enabled.

NetBackup default RBAC roles

With the NetBackup RBAC default roles you can delegate for tasks like NetBackup security management, protection plan configuration and job management, and protection and recovery of assets.

NetBackup security administrator

The NetBackup security administrator performs the following tasks in the NetBackup environment:

- Manages role-based access control. This user can delegate access to NetBackup. This task includes managing the users that can access NetBackup, the role or permissions that users have, and the NetBackup assets that users can access.

- Oversees the security management. This task includes managing NetBackup hosts and certificates, global security settings, session management, locked NetBackup user accounts, and API keys. Users with this role can also view security events.

Backup administrator

The backup administrator performs the following tasks in the NetBackup environment:

- Configures cloud providers, application servers, and intelligent groups.
- Configures protection plans for the workload administrator.
- Manages all jobs activity. Monitors all job operations. Able to cancel, suspend, resume, restart, and delete jobs.
  The backup administrator can also configure NetBackup to send email notifications to their ticketing system when certain job failures occur.
- Configures all storage options for the Media Server Deduplication Pool (MSDP) and AdvancedDisk.
- Configures NetBackup to work with Cloud and OpenStorage options.
- Manages recovery points, including the ability to restore, expire, copy, and duplicate recovery points.
- Views the usage reporting details on backup data size for NetBackup master servers.

You can limit access (through object groups) for users with the **Backup administrator** role or with a custom role. However, you cannot limit the jobs that a backup administrator can see. Users with this role can view all job activity.

Workload administrator

The workload administrator performs the following tasks in the NetBackup environment:

- Manages the jobs that they initiate.
- Manages the assets they are granted access to.
- Monitors protection status and subscribes assets to protection plans.
- Performs the recovery for assets they manage.

You can limit access (through object groups) for users with the **Workload administrator** role.

Configuring RBAC

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

Table 2-2

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. Use the `vssat` command to configure the domains in your environment. See "Add AD or LDAP domains" on page 35.
2	Review the RBAC roles.	NetBackup has three default roles: system administrator, backup administrator, and workload administrator. Review the permissions for these roles to determine which role or roles are appropriate for your users. See "NetBackup default RBAC roles" on page 17. If it is needed, you can create a custom role with a custom set of permissions. See "Add a custom role" on page 19.
3	Add object groups.	Create object groups to organize the assets, application servers, or protection plans in your NetBackup environment. Object groups determine, for example, what assets that a user can view or manage. See "Steps to create an object group" on page 25.
4	Grant access for users through access rules.	Create the access rules that include a user, the role a user has, and the object group that they have access to. You can create multiple access rules for a user, which means that a user can have multiple RBAC roles and access to multiple object groups. See "Add access for a user through access rules" on page 32.

Add a custom role

If the default NetBackup roles for RBAC do not meet your needs, you can configure a role with custom role permissions. Note, however, that custom roles do have certain limitations. See Limitations of custom roles.

To add a custom role

1. On the left, select **Security > RBAC**.
2. Select the **Roles** tab and click **Add**.

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 For **Role permissions**, choose the permission or type of access that you want users with that role to have for each permission type.

For example, you may want a user to be able to view, but not manage protection plans. Or you may want to give only some users the ability to perform recovery of assets, but not to configure application servers or asset groups.

See Table 2-3.

5 Click **Add.**

Permissions for custom roles

Table 2-3 describes the individual permissions that you can select for a custom role.

Table 2-3 Description of permissions for custom roles

Permission category	Permission	Action that the permission allows
Job management Allow a user view to jobs or to manage job operations.	Manage Jobs	Manage current or completed jobs. Includes the ability to delete, cancel, restart, and suspend a job.
	View Jobs	View the current or the completed jobs for the master server.
Asset management Allow a user to manage assets, subscribe assets to protection plans, or to view assets. Note that a user can only manage assets for which that user is granted access.	Manage Application Servers and Asset Groups	Add credentials, so NetBackup can discover additional information for the workload. For example, when the user adds VMware credentials, NetBackup discovers more details for the VMware server. The user can then view and select objects within the vCenter. Create and manage asset groups (or “intelligent” groups) and subscribe groups to protection plans. When the backup runs, NetBackup dynamically creates a list of all VMs that meet the conditions for the intelligent group. For example, a user can create an intelligent VM group named “Finance Department”. Then the user can add a condition so the group contains all VMs that have a display name that starts with the specific string “finance”.
	Manage Assets	Manage the assets that are associated with the supported workloads and subscribe assets to protection plans.
	View Assets	View assets that are associated with the supported workloads.

Table 2-3 Description of permissions for custom roles *(continued)*

Permission category	Permission	Action that the permission allows
Storage Management Allow a user to view and manage storage servers and storage units.	Manage Storage	Create, view, edit, or delete storage servers and storage units. **Note:** Users that only have this permission are not able to sign in to the web UI.
	View Storage	View the attributes for storage servers and storage units. **Note:** Users that only have this permission are not able to sign in to the web UI.
Recovery Point Management	Manage Recovery Point Expiration	Expire the recovery points available for an asset. This functionality is currently only available from the NetBackup APIs. **Note:** Users that only have this permission are not able to sign in to the web UI.
	Manage Recovery Points	Manage the recovery points available for an asset. This permission lets the user restore, copy, and duplicate a recovery point and change the primary copy of an image. These functions are currently only available from the NetBackup APIs. **Note:** Users that only have this permission are not able to sign in to the web UI.

Table 2-3 Description of permissions for custom roles *(continued)*

Permission category	Permission	Action that the permission allows
Security management Allow a user to view audit logs or to manage security settings or certificates in NetBackup.	Manage Global Security Settings	Manage security settings for the NetBackup master server. These settings affect communication with 8.0 and earlier hosts, automatic mapping of host names, the security level for certificate deployment, and the disaster recovery passphrase. **Note:** Users that only have this permission are not able to sign in to the web UI.
	Manage API Keys	Add, edit, view, or delete any API keys that are created for NetBackup users.
	Manage Certificates	Manage NetBackup security certificates and view external CA certificate details for hosts. For NetBackup certificates, includes the ability to revoke a certificate, create a resissue token so a certificate can be reissued, or create a new token. Users with this permission can also manage user sessions.
	View Audit Logs	See who has signed in to NetBackup, made changes to security settings, or who has browsed or restored a backup image. Also view the access history for the current user.
	Manage User Authentication	Manage the settings for authenticating users with a smart card or digital certificate. Users with this permission can also manage locked NetBackup user accounts.
	View API Keys	View the API keys that are created for NetBackup users. A NetBackup user is able to view and manage their own key.
Protection plan management Note that a user can only manage or select a protection plan for which that user is granted access.	Manage Protection Plans	Create, edit, or delete protection plans. Also can subscribe assets to protection plans.
	View Protection Plans	View the protection plans that are available and subscribe assets to a protection plan.
Role based access control Allow an administrator to create the access rules that determine the permissions a user has for a specific workload or asset and for specific protection plans.	View Access Rules	View the access rules that are configured.
	Manage Access Rules	Create, manage, or delete access rules. Create custom roles and object groups.

Table 2-3 Description of permissions for custom roles *(continued)*

Permission category	Permission	Action that the permission allows
Recovery Allow a user to perform one or more types of recovery. Note that users can only view and recover assets for which that user is granted access.	Instant Access	Create an instant access image. This permission also enables **View Recovery Points** and **View Assets**.
	Overwrite Asset	Allows the user to restore assets to their original location. Without this permission a user must restore assets to a different location.
	View Recovery Points	View the recovery points that are available for an asset. **Note:** Users that only have this permission are not able to sign in to the web UI.
	Restore Files	Restore individual files from the backup image. This permission also enables **View Recovery Points** and **View Assets**.
	Recover/Restore	Restore the data from a backup image to a different location.
	Download Files	Download individual files from an instant access mount point. This permission also enables **View Recovery Points** and **View Assets**.

Limitations of custom roles

When you create custom roles, note the following:

- Some permissions are only available with default RBAC roles or for a custom role that is configured with the NetBackup APIs.
  - A user can only manage **Hosts** settings if that user has the **Security administrator** role.
  - A user can only manage **Alerts and notifications** and view **Usage reporting** if that user has the **Backup administrator** role.
  - A user with the **Security administrator** role also has certain “view” permissions. This way that user can find and add assets, application servers, and protection plans to an object group. If you want a user with a custom role to create access rules, be sure to select the appropriate view permissions for the custom role.
- 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. When you create custom roles, be sure to enable the minimal number of permissions so the user can sign in to and use the web UI.

Edit or delete a custom role

You can edit or delete a custom role when you want to change or remove permissions for users with that role.

Edit a custom role

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

To edit a role

1. On the left, click **Security > RBAC**.
2. Click on the **Roles** tab.
3. Locate and click on the role that you want to edit.

   Note that searches are case-sensitive.
4. At the bottom left, click the lock icon.
5. Edit the details for the role and click **Save**.

Delete a custom role

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

To delete a role

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

   Note that searches are case-sensitive.
4. Click **Remove > Remove**.

About object groups

An object group defines some combination of assets, application servers, or protection plans. A user's role and object group (which make up the user's access rule) determine the permissions that a user has for the objects in the object group.

To manage or perform recovery of specific assets, a user must have an access rule with those assets. To manage or subscribe assets to certain protection plans,

a user must have an access rule with those plans. To manage credentials for specific application servers, a user must have an access rule that includes those servers. Depending on the role a user has, the user can perform the following tasks.

- A security administrator has permissions for all objects in all object groups. A user with this role can:
  - View all assets.
  - View all application servers.
  - View all protection plans.
- A backup administrator can manage:
  - Protection plans that are included in the object group.
  - Which plans the assets in the object group are subscribed to.
  - Jobs for the assets that are included in the object group.
  - The credentials for application servers in the object group.
  - Asset groups.
- A workload administrator can:
  - View protection plans that are included in the object group.
  - Manage which plans the assets in the object group are subscribed to.
  - Perform recovery of assets in the object group.

Note: Object groups can also limit what the user can create. For example, assume that a backup administrator has only one access rule that gives access to the protection plans that contain the word “finance”. Therefore that user can only create the protection plans that contain the word “finance”.

Steps to create an object group

Create an object group to define the combination of assets, application servers, or protection plans that is available to users that have permissions for that object group.

Table 2-4 How to create an object group

Step	Action	Description
1	On the left, click **Security > RBAC**.	

Table 2-4 How to create an object group *(continued)*

Step	Action	Description
2	Click the **Object groups** tab and click **Add**.	
3	Provide the name and description for the object group.	You may want to include any keywords that describe the type of assets in the group or the region the assets reside in.
4	Configure any assets that you want to add to this object group.	See "Selecting the assets for an object group" on page 26. Add the assets that you want users to be able to view or manage, if users have the appropriate RBAC role or permissions. For example, add the assets that you want a workload administrator to manage protection or recovery for.
5	Configure any application servers that you want to add to this object group.	See "Selecting application servers for an object group" on page 28. Add the application servers that you want users to be able to manage, if users have the appropriate RBAC role or permissions. For example, add the application servers that you want a backup administrator to manage.
6	Configure any protection plans that you want to add to this object group.	See "Selecting protection plans for an object group" on page 30. Add the protection plans that you want users to be able to manage, if users have the appropriate RBAC role or permissions. For example, add the protection plans that you want a backup administrator to manage. Workload administrators can view these plans and subscribe assets to these plans.
7	Preview the assets, application servers, or plans that you configured for the object group.	See "Preview the objects in an object group" on page 30.
8	Click **Save**.	

Selecting the assets for an object group

You can define the assets for this object group in the following ways:

- All workloads
- All Cloud assets that meet one or more conditions

- A specific VMware server or RHV manager and all its VMs
- A specific VMware server or RHV manager and VMs that meet one or more conditions

You can also preview the assets that are included in an object group. See "Preview the objects in an object group" on page 30.

All workloads

To include all assets for all workloads

- Select **Grant access to all** to include all available assets for all workloads.

Cloud assets

To include the cloud assets that meet one or more conditions

1. Under **Assets**, click **Add workload** and select **Cloud**.
2. Click **Add condition** to define one or more conditions. Conditions are case-sensitive.

RHV assets

To include a specific RHV server and all its VMs

1. Under **Assets**, click **Add workload** and select **RHV**.
2. Click **Add RHV manager**.
3. Select the name of the RHV manager that you want to include. Or, click on the RHV manager name to browse for a server, cluster, or datacenter.
4. By default, **Include all VMs** is enabled, so all VMs for that VMware server are included.

VMware assets

To include a specific VMware server and all its VMs

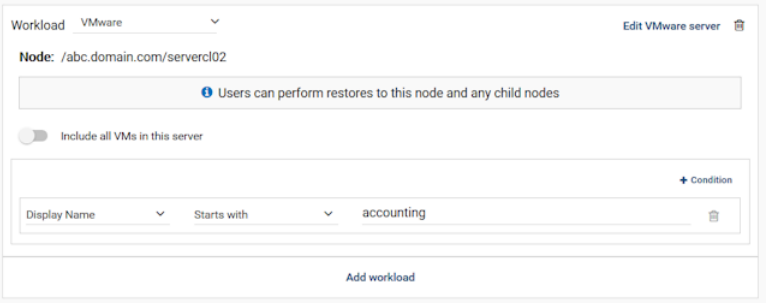
1. Under **Assets**, click **Add workload** and select **VMware**.
2. Click **Add VMware server**.
3. Select the name of the vCenter that you want to include. Or, click on the vCenter name to browse for a server, cluster, or datacenter.
4. By default, **Include all VMs** is enabled, so all VMs for that VMware server are included.

To include a specific VMware server and selected VMs for that server

1. Under **Assets**, click **Add workload** and select **VMware**.
2. Click **Add VMware server**.
3. Select the name of the vCenter that you want to include. Or, click on the vCenter name to browse for a server, cluster, or datacenter.
4. Turn off **Include all VMs**.
5. Click **Add condition** to define one or more conditions. Conditions are case-sensitive.

   For multiple conditions, select the operator (**AND** or **OR**).

   In the following example, the object group includes assets in the VMware workload, from the cluster **servercl02** on the VMware server **abc.domain.com** and with a display name that starts with **accounting**.



Selecting application servers for an object group

The object group defines the application servers that a user can manage. Currently application servers only apply to the VMware and RHV workloads.

You can preview the application servers that are included in an object group.

See “Preview the objects in an object group” on page 30.

To include all application servers, in all workloads

- Under **Application servers**, select **Grant access to all**.

To include all application servers, in a specific workload

- Under **Application servers**, click **Add condition**, then select the workload type that you want to include.

  Select the **Server Type**, the operator, and the workload type.

  For example, select **Server Type** > **Is In** > **RHV** to select all RHV application servers.

To include specific application servers, in a specific workload

1. Under **Application servers**, click **Add condition**, then select the workload type that you want to include.

   Select the **Server Type**, the operator, and the workload type.

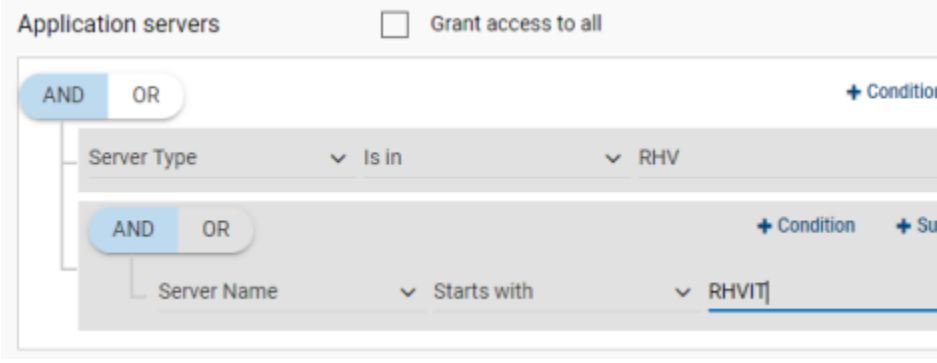
   For example, select **Server Type** > **Is In** > **RHV** to select all RHV application servers.

2. Click **Condition** to add one or more conditions based on the **Server Name**. Conditions are case-sensitive.

   For example, if you want application servers starting with a specific name for a specific workload.

3. For multiple conditions, use the **Sub-query** option and select the operator (**AND** or **OR**).

   In the following example, the object group includes application servers from the RHV workload and with a name that starts with **RHVIT**.



Selecting protection plans for an object group

The protection plans that are included in an object group determine the plans that users can view, add, or manage.

You can preview the plans that an object group includes.

See "Preview the objects in an object group" on page 30.

To include all application servers, in all workloads

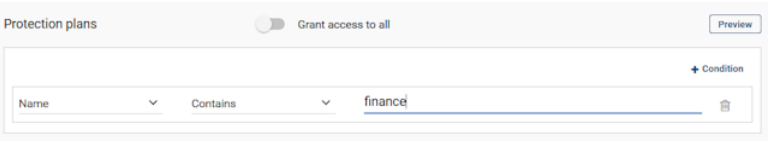
- Under **Protection plans**, select **Grant access to all**.

To include specific protection plans

1. Under **Protection plans**, click **Add condition**.
2. Select the attributes for the condition. Conditions are case-sensitive.

   For multiple conditions, select the operator (**AND** or **OR**).

   In the following example, the object group includes protection plans with a name that contains **finance**.



Note: In this example, users can only view, add, or manage protection plans that contain the word "finance".

Preview the objects in an object group

You can preview what assets, application servers, or protection plans are associated with object group. Users with access to that object group can view or manage those items in the object group. The preview only includes the assets, servers, or plans that are available when you display the preview. As you add or remove items in your environment or plans in the web UI, the object group changes dynamically.

To preview assets or protection plans for an object group

1. On the left, click **Security > RBAC**.
2. Click the **Object groups** tab.
3. Click on the name of the object group that you want to edit.

4 Next to **Assets**, **Application servers**, or **Protection plans**, click **Preview**.

5 Close the preview panel.

Edit or delete an object group

You can edit or delete an object group when you want to change or remove the assets, application servers, or the protection plans in the object group.

Edit an object group

Note: When you change an object group, the changes apply to all access rules (and the associated users) that contain that object group.

To edit an object group

1 On the left, click **Security > RBAC**.

2 Click the **Object groups** tab.

3 Locate and click on the object group that you want to edit.

Note that searches are case-sensitive.

4 At the bottom left, click the lock icon.

5 Edit the name or description for the object group.

6 Edit the assets, application, servers or protection plans,.

7 Click **Save**.

Delete an object group

Note: When you delete an object group, the changes affect all users that are associated with that object group.

To delete an object group

1 On the left, click **Security > RBAC**.

2 Click the **Object groups** tab.

3 Locate the object group that you want to delete and select the check box for it.

Note that searches are case-sensitive.

4 Click **Remove > Remove**.

Add access for a user through access rules

In the NetBackup web UI, you give a user access to NetBackup through one or more access rules. Access rules are composed of:

- A user or a user group. This user or group can be either local or of a domain.
- A role, which defines the permissions that a user has.
  Role permissions only determine what kinds of actions a user can perform. The object group determines what a user can access in the environment.
- An object group, which defines the assets, application servers, or protection plans that a user can view or manage.
  Note: When you create an access rule for a user with the **Security administrator** role, that user has access to all objects or assets.

Before you can create an access rule, you need to do the following:

- To add domain users, you must configure the Active Directory (AD) or LDAP domain with NetBackup.
  Use the `vssat` command to configure the domains in your environment. See "Add AD or LDAP domains" on page 35.
  Local users do not require this configuration.
- Determine which role you want to give a user.
  See "NetBackup default RBAC roles" on page 17.
- Determine which assets or application servers that you want a user to have access to and select the appropriate object groups. Or, create the appropriate object groups.
  See "Steps to create an object group" on page 25.
- The role permissions that a user has can be further limited by the object groups the user is granted access to. See "Steps to create an object group" on page 25.

To add access for a user

1. On the left, click **Security > RBAC**.
2. Click the **Access rules** tab and click **Add**.
3. Type a domain and a user name. Click **+** to validate this user.

   For example:

For this type of user	Use this format	Example
Local user	*username*	**root**
Domain user	*DOMAIN\username*	**WINDOWS\Administrator**

4 Select a role that includes the permissions that you want to assign to the user.

5 Select an object group that includes the assets that you want the user to have access to.

Note that a user with the **Security administrator** role has access to all objects or assets. The only available selection for that role is **All objects**.

6 Provide a description for the access rule and click **Save**.

Edit or remove user access rules

If a user's role in your organization changes or you need to change the user's access to the assets in the environment, you have the following options:

- Edit an access rule for the user and select a different RBAC role or a different object group.
  See the section called “Edit the access rule for a user” on page 33.
- If the user has a custom role, change the permissions for the role. Note that changing the permissions also changes the permissions for any other users that are associated with that role.
  See “Edit or delete a custom role” on page 24.
- Change the object group settings that determine the objects that the user can view or manage. Note that changing these settings also changes access for any other users that are associated with that object group.
  See “Edit or delete an object group” on page 31.
- Remove an access rule for user so that user no longer has those role permissions or object group access that are defined in the access rule.
  See the section called “Remove an access rule for a user” on page 34.

Note: Changes to a user's access rules 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. A NetBackup security administrator can also sign out users.

See “Sign out a NetBackup user session” on page 60.

Edit the access rule for a user

Edit an access rule if you want to change the role permissions for a user or objects that the user can view or manage. Any changes you make to an access rule affect only that user.

To edit the access rule for a user

1. On the left, click **Security > RBAC**.
2. Click the **Access rules** tab.
3. Locate and click on the name of the user (which is the user's associated access rule) that you want to edit.
4. At the bottom left, click the lock icon.
5. Select a different role or object group.
6. Click **Save**.
7. Repeat step 3 through step 6 to edit other access rules for the user.

Remove an access rule for a user

Remove an access rule for a user if you want to revoke the role permissions and object group access of the access rule. Removing an access rule only affects the user that is configured in the rule. The user still retains any permissions and access that is granted from other access rules.

To remove an access rule for a user

1. On the left, click **Security > RBAC**.
2. Click the **Access rules** tab.
3. Locate the name of the user and select the check box for the access rule that you want to remove.
4. Click **Remove > Remove**.

Chapter 3

Adding AD or LDAP domains

This chapter includes the following topics:

Add AD or LDAP domains

NetBackup RBAC in the NetBackup web UI supports domain users of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP). Before you can add access rules for domain users, 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.

Note: Ensure that the user account (in the `-m` option) has the required rights to query the AD or the LDAP server.

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

To add an AD or a LDAP domain

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

```
vssat addldapdomain -d DomainName -s server_URL -u user_base_DN -g group_base_DN
-t rfc2307 | msad -m admin_user_DN
```

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
```

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

```
vssat validateprpl
```

Chapter 4

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 42.

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 41.
`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
```

Chapter 5

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.

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 63.

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**.

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 48.

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.

Chapter 6

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 56.

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 53.

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 supports 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 57.

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 External CA support in NetBackup video 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 7

Managing user sessions

This chapter includes the following topics:

Display a message to users when they sign in

You can display a sign-in message (or banner) to users when they sign in to the NetBackup Administration Console, the NetBackup client, or the NetBackup web UI. A different banner can be configured for any master server, media server, or client. This message can also require the user to agree to the terms of service before the user signs in.

These settings are currently managed in the NetBackup Administration Console, in **Host Properties > *hostname* > Login Banner Configuration**. See the NetBackup Administrator's Guide, Volume I for details.

Enable maximum sign-in attempts and idle time-out settings for user sessions

You can enable and customize when user sessions should time out and the maximum number of NetBackup sign-in attempts. The settings you choose are applied to the NetBackup Administration Console and the NetBackup web UI.

These settings are currently managed in the NetBackup Administration Console, in **Host Properties > *master_server* > User Account Settings**. See the NetBackup Administrator's Guide, Volume I for details.

Sign out a NetBackup user session

For security or maintenance purposes, you can sign out one or more NetBackup user sessions. By default, user sessions are automatically logged out when the session is idle for 10 minutes.

Time-out settings are managed with the NetBackup Administration Console in **Host Properties > *master_server* > User Account Settings**. See the NetBackup Administrator's Guide, Volume I for details. By default a user's account only remains locked for 24 hours. You can change this time by adjusting the **Account lockout duration**.

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.

Account lockout settings are managed with the NetBackup Administration Console in **Host Properties > *master_server* > User Account Settings**. See the NetBackup Administrator's Guide, Volume I for details. Note that a user's account only remains locked for the time that is specified by the **Account lockout duration** setting.

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**.

Chapter 8

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.

Note: During NetBackup certificate deployment on a NAT client, you must provide an authorization token irrespective of the certificate deployment security level that is set on the master server. This is because, the master server cannot resolve the host name to the IP address from which the request is sent.

For more information on NAT support in NetBackup, refer to the NetBackup Administrator's Guide, Volume I.

Table 8-1 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 8-1 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 64.
- 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.

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**.

Chapter 9

Creating and using API keys

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. NetBackup audits operations that are performed with that key with the full identity of the user.

Table 9-1 How users can manage and view API keys using the web UI and the APIs

User	RBAC role or permissions	Create and manage API keys	View API keys	Interfaces
NetBackup security administrator	Security administrator role	All users	All users	Web UI, APIs
NetBackup RBAC user	Manage API Keys	All users	All users	Web UI, APIs
NetBackup RBAC user	View API Keys	Self	All users	Web UI, APIs

Table 9-1 How users can manage and view API keys using the web UI and the APIs *(continued)*

User	RBAC role or permissions	Create and manage API keys	View API keys	Interfaces
Other NetBackup authenticated user	No RBAC role or API key permissions	Self	Self	APIs

More information

See "User identity in the audit report" on page 41.

See "Add access for a user through access rules" on page 32.

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

Manage API keys

NetBackup security administrators or NetBackup users with permissions to manage API keys can use the NetBackup web UI to add, edit, delete, or view the keys that are associated with all NetBackup users. A NetBackup-authenticated user can view and manage their own API key using the NetBackup APIs, if that user does not have RBAC permissions.

See "Add access for a user through access rules" on page 32.

Add an API key

You can create API keys 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.

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

To add an API key

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**.

Edit an API key

You can change the expiration date for an active API key. After an API key expires, a user's old key must be deleted and a new key created.

To edit an API key

1 On the left, select **Security > API keys**.

2 Select the API key and click **Edit**.

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

4 Click **Save**.

Delete an API key

You can delete an API key if you do not want a user to have access to the key or when it is no longer used. When you delete an API key, that key is permanently deleted. The associated user can no longer use that key for authentication or with the NetBackup APIs.

To delete an API key

1 On the left, select **Security > API keys**.

2 Select the API key and click **Delete** > **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>'
```

View API keys

NetBackup security administrators or NetBackup users with permissions to view API keys can view the keys that are associated with all NetBackup users. A

NetBackup-authenticated user can view and manage their own API key using the NetBackup APIs, if the user does not have RBAC permissions.

To view API keys

- On the left, select **Security > API keys**.

Chapter 10

Configuring smart card authentication

This chapter includes the following topics:

Configure user authentication with smart cards or digital certificates

NetBackup supports authentication of Active Directory (AD) or LDAP domain users with a 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. You must perform this configuration separately for each master server domain where you want to use this authentication method.

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 35.
- Configure RBAC for the NetBackup users.
  See “Configuring RBAC” on page 19.

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 35.
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.

Chapter 11

Troubleshooting access to the 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 11-1 Solutions when the web user interface does not display

Step	Action	Description
Step 1	Check the network connection.	
Step 2	Verify that the firewall is open for port 443.	Refer to the following article: https://www.veritas.com/docs/100042950

Table 11-1 Solutions when the web user interface does not display *(continued)*

Step	Action	Description
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 11-1.

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.
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 19.

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 user name (or the user name and domain name) that is specified in the user's access rule.
- Review the access rules for the user in **Security > RBAC**. You may need to change the role permissions or object groups that are associated with those access rules. However, be aware that those kinds of changes also affect any other users that are associated with those roles or object groups.
- Any user account changes with the identity provider are not synchronized with the user's access rules. 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 access rule for the user to remove the existing user account and re-add the new account.
- Changes to a user's access rules 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>`