NetBackup™ Web UI Security Administrator's Guide

Release 8.1.2

VERITAS™

NetBackup Web UI Security Administrator's Guide

Last updated: 2019-12-06

Document version: NetBackup 8.1.2

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

https://sort.veritas.com/documents

Documentation feedback

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

Introducing the NetBackup web user interface

This chapter includes the following topics:

About the NetBackup web user interface

NetBackup 8.1.2 introduces a new web user interface that provides the following features:

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

- Backup administrators provide protection services to satisfy their service level objectives (SLOs). Protection of assets is achieved through protection plans, job management, and visibility of the protection status of assets.
- Workload administrators can subscribe assets to the protection plans that meet the SLO, monitor protection status, and perform self-service recovery of virtual machines. In NetBackup 8.1.2, workload administrators can manage and configure VMware and cloud workloads.
- Usage reporting tracks the size of backup data on your master servers. You can also easily connect to Veritas Smart Meter to view and manage NetBackup licensing.

Access control in the NetBackup web UI

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

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

Monitor NetBackup jobs and events

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

- For a NetBackup security administrator, the dashboard lets the administrator see the status of security certificates and of audit events.

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

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

Protection plans offer the following benefits:

- In addition to schedules for backups, a protection plan can also include a schedule for replication and long-term retention.
- You can easily choose either on-premises or snapshot storage.
- When you select from your available storage, you can see any additional features available for that storage. For example, NetBackup Accelerator or Instant Access for backup storage. For long-term storage, the cloud provider, CloudCatalyst, Encryption, or Compression.
- The protection plan wizard helps you select storage for backups, replication, or long-term storage based on the supported storage that is already configured.
- The backup administrator creates and manages protection plans and is therefore responsible for backup schedules and storage.
- The workload administrator primarily selects the protection plans to use to protect assets or asset groups. However, the backup administrator can also subscribe assets to protection plans if needed.

Self-service recovery

The NetBackup web UI makes it easy to recover VMs. You can also use the instant access feature to mount a VM's snapshot for immediate access to its files: you can download the file to your local host or restore the file to its original VM.

Terminology

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

Table 1-1 Web user interface terminology and concepts

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

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

Term	Definition
Administrator	A user that has complete access and permissions to NetBackup and all of the interfaces, including the NetBackup web UI. The root, administrator, and Enhanced Auditing user all have complete access to NetBackup. In the *NetBackup Web UI* guides, the term *NetBackup administrator* also refers to a user that has full permissions for NetBackup, usually in reference to a user of the NetBackup Administration Console. Also see *Role*.
Asset group	See *intelligent group*.
Asset	The data to be protected, such as physical clients, virtual machines, and database applications.
Classic policy	In the NetBackup web UI, indicates that a legacy policy protects the asset. Legacy policies are created with the NetBackup Administration Console.
Intelligent group	Allows NetBackup to automatically select assets for protection based on the criteria (queries) that you specify. An intelligent group automatically stays up-to-date with changes in the production environment. These groups are also referred to as asset groups. For VMware, these groups appear under the tab **Intelligent VM groups**.
Instant access	An instant access VM created from a NetBackup backup image is available almost instantaneously, achieving a near-zero recovery time objective. NetBackup mounts the VM's snapshot directly on the backup storage device to allow your ESXi host or cluster to treat the snapshot as a normal VM.
Object group	For RBAC, a collection of assets, protection plans, servers, and other resources that the user is granted access to.
Protection plan	A protection plan defines when backups are performed, how long the backups are retained, and the type of storage to use. Once a protection plan is set up, assets can be subscribed to the protection plan.

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

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

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.

Note the following:

- Enhanced Auditing users also have administrator access.
- The default admin user for the NetBackup appliance does not have access to the web UI.

- The appliance **nbasecadmin** user and the Flex Appliance **appadmin** user have the NetBackup security administrator role and can grant access to other appliance users.

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 15.

   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

- 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 a third-party certificate, see the instructions for configuring a third-party certificate for the web server.

- See other tips for accessing the web UI.

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

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

   https://*masterserver*/webui/login

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

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

   For example:

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

The NetBackup dashboard

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

Table 1-2 The NetBackup dashboard for the NetBackup security administrator

Dashboard widget	Description
Certificates	Displays information about the host ID-based security certificates in your environment.
Tokens	Displays the information about the authorization tokens in your environment.
Security events	The **Access history** view includes a record of login events. The **Audit events** view includes events that are related to tokens, certificates, and the certificate revocation list (CRL).

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, managing global security settings, and viewing security events.

Backup administrator

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

- 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 protection plans for the workload administrator.
- 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. Configure assets in the NetBackup environment including cloud providers, application servers, and asset groups.
- 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.
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 14. If needed, you can create a custom role with a custom set of permissions. See "Add a custom role" on page 16.
3	Add object groups.	Organize your assets into object groups. See "Add an object group" on page 20.
4	Grant access for users through access rules.	Create 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 26.

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 customer roles do have certain limitations. See the section called "Limitations of custom roles" on page 17.

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.**

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.

Permissions for custom roles

See Table 2-3 on page 18. 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
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.	Recover/Restore	Restore the data from a backup image to its original location or 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.
	Download Files	Download individual files from an instant access mount point. This permission also enables **View Recovery Points** and **View Assets**.
	Instant Access	Create an instant access image. This permission also enables **View Recovery Points** and **View Assets**.
	Restore Files	Restore individual files from the backup image to an ESXi server or cluster. This permission also enables **View Recovery Points** and **View Assets**.
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.
Security management Allow a user to view audit logs or to manage security settings or certificates in NetBackup.	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 Global Security Settings	Manage global security in NetBackup. 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 Certificates	Manage security certificates for hosts. Includes the ability to revoke a certificate, create a resissue token so a certificate can be reissued, or create a new token.
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.

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

Permission category	Permission	Action that the permission allows
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 Appservers and Asset Groups	Add VMware vCenter credentials, which allow NetBackup to discover additional information for the server so administrator can view and select objects within the vCenter. Create and manage asset groups and subscribe groups to protection plans.
	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.
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.	Manage Access Rules	Create, manage, or delete access rules. Create custom roles and object groups.
	View Access Rules	View the access rules that are configured.

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**.

Add an object group

Object groups can define the assets, application servers, or protection plans that users can view or manage. You can create an object group that grant access to specific workloads or objects. For example, you can grant access to all objects in the VMware workload or to specific VMware servers. Or, you can grant access to all assets, application servers, or protection plans. For example, a backup administrator that has access for all protection plans can manage any protection plan in NetBackup.

To manage or perform recovery of assets or application servers, a user must have one or more access rules with an object group that includes those objects. To manage or subscribe assets to certain protection plans, a user must have one or more access rules with an object group that includes those plans.

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 protection plans that contain the word “finance”. Therefore that user can only create protection plans that contain the word “finance”.

To add an object group

1. On the left, click **Security > RBAC**.
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 Select any assets that you want to add to this object group.

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

- All assets in a specific workload
- A specific VMware server and all its VMs
- A specific VMware server and selected VMs for that server
- Turn on **Grant access to all** to include all available assets

See the section called “Selecting the assets for an object group” on page 22.

Users granted access to these assets can view or manage these assets, according to the role that they are assigned.

5 Select any application servers that you want to add to this object group.

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

- All application servers, in a specific workload
- Specific application servers
- Turn on **Grant access to all** to include all available application servers

See the section called “Selecting the application servers for an object group” on page 23.

Users granted access to these assets can view or manage these application servers, according to the role that they are assigned.

6 Select the protection plans that you want to add to this object group.

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

- Specific protection plans
- Turn on **Grant access to all** to include all protection plans

See the section called “Selecting the protection plans for an object group” on page 24.

Users granted access to these protection plans can view or manage these plans, according to the role that they are assigned. Users with “view” permissions can also subscribe assets to the protection plans in the object group.

7 Click **Save**.

Selecting the assets for an object group

You can preview the assets that are included in an object group. See the section called “Preview the assets, application servers, or protection plans that are in an object group” on page 25.

To include all assets in a specific workload

- Click **Add workload**, then select the workload type that you want to include.

  For example, select **VMware** to include all VMware assets.

To include a specific VMware server and all its VMs

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

   For example, select **VMware** to include all VMware assets.
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. Click **Save**.

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

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

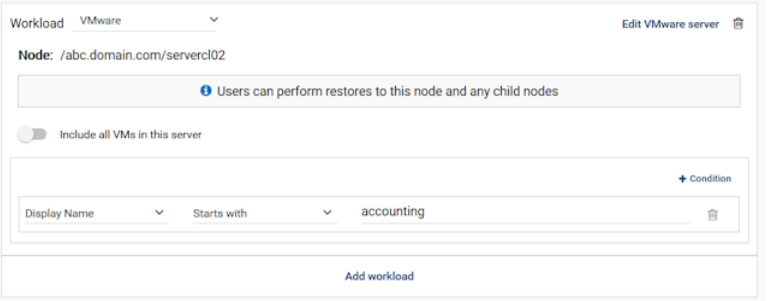
   For example, select **VMware** to include all VMware assets.
2. Click **Add VMware server**.
3. Select the name of the vCenter that you want to include. Or, click on the vCenter name to browse for a server, cluster, or datacenter.
4. Click **Save**.

5 Turn off **Include all VMs in this server**.

6 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 the application servers for an object group

You can preview the assets that are included in an object group. See the section called “Preview the assets, application servers, or protection plans that are in an object group” on page 25.

To include all application servers, in a specific workload

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

  For example, select **VMware** to include all VMware application servers.

To include specific application servers, in a specific workload

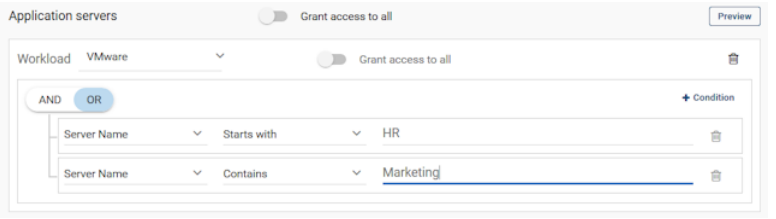
1. Under **Application servers**, click **Add workload**, then select the workload type that you want to include.

   For example, select **VMware** to include all VMware application servers.

2. Add 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 application servers from the VMware workload with a server name that starts with **HR** or with a name that contains **Marketing**.



Selecting the protection plans for an object group

You can preview the assets that are included in an object group. See the section called “Preview the assets, application servers, or protection plans that are in an object group” on page 25.

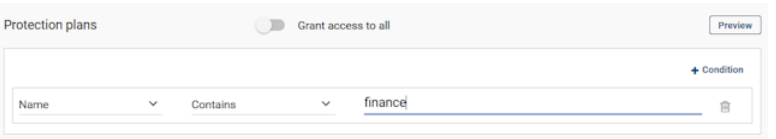
To include specific protection plans

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**.



Preview the assets, application servers, or protection plans that are in an object group

You can preview the objects that are included in an object group. Note that an object group changes dynamically as objects are added and removed from the NetBackup environment. When backups run, the object group updates at run-time to reflect the objects available at the time of backup.

To preview the assets, application servers, or protection plans that are in an object group

1. On the left, click **Security > RBAC**.
2. Click the **Object groups** tab and the object group that you want to edit.
3. To the right of **Assets**, **Application Servers**, or **Protection Plans**, click **Preview**.
4. NetBackup displays a real-time view of the objects that meet the criteria that you configured. You can sort or search the objects in the preview. Note that searches are case-sensitive.
5. When you are finished with the preview, at the top right-click the **Close** icon.

Previewing the assets, application servers, or protection plans for 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 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. What a user can access in the environment is determined by the object group.

- 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 or LDAP domain with NetBackup.
  Use the `vssat` command to configure the domains in your environment. See the *NetBackup Security and Encryption Guide*.
  Local users do not require this authentication.
- Determine which role you want to give a user.
  See "NetBackup default RBAC roles" on page 14.
- 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 "Add an object group" on page 20.
- The role permissions that a user has can be further limited by the object groups the user is granted access to. See "How can I limit role permissions to specific objects or assets?" on page 29.

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 28.
- If you use a custom role, change the permissions for an RBAC 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 19.
- Change the object group settings that determine the assets, application servers, or protection plans 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 25.
- 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 29.
  If the user is currently signed in, use the API `Gateway DELETE /user-sessions` to sign out all users.

Edit the access rule for a user

Edit an access rule if you want to change the role permissions for a user or the assets, application servers, or protection plans 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.

   Note that searches are case-sensitive.

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 inherited 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.

   Note that searches are case-sensitive.

4 Click **Remove > Remove**.

How can I limit role permissions to specific objects or assets?

Security-related permissions and job permissions cannot be limited to certain hosts or assets. For example, a user that has the view or manage job permission is able to view or manage all jobs. Other permissions related to the backup administrator and permissions for the workload administrator can be limited by the object group criteria.

Table 2-4 Role permissions and how to use object groups to limit permissions

Permission	Can filter and limit object groups by
Recover/Restore	VMWare recovery points: Display name VM absolute path Cloud asset recovery points: Display name, vendor, config ID
View Recovery Points	VMWare recovery points: Display name VM absolute path Cloud asset recovery points: Display name, vendor, config ID
Download Files	VMWare recovery points: Display name VM absolute path Cloud asset recovery points: Display name, vendor, config ID
Instant Access	VMWare recovery points: Display name VM absolute path Cloud asset recovery points: Display name, vendor, config ID
Restore Files	VMWare recovery points: Display name VM absolute path Cloud asset recovery points: Display name, vendor, config ID
Manage Protection Plans	Name, description
View Protection Plans	Name, description
View audit logs	All logs or no logs
Manage global security settings	All settings or no settings
Manage Certificates	All certificates or no certificates
Manage Jobs	All jobs or no jobs
View Jobs	All jobs or no jobs
Manage Appservers and Asset Groups	Protection plans that user can view: Name, description Application servers: Server name, server type

Table 2-4 Role permissions and how to use object groups to limit permissions *(continued)*

Permission	Can filter and limit object groups by
Manage Assets	Protection plans that user can view and subscribe assets to: Name, description Application servers: Server name, server type
View Assets	VMware: Display name, VM absolute path Cloud: Display name, vendor, config ID
Manage Access Rules	All objects or no objects
View Access Rules	All objects or no objects

Chapter 3

Security events and audit logs

This chapter includes the following topics:

About NetBackup auditing

An audit trail is a record of user-initiated actions in a NetBackup environment. Essentially, auditing gathers the information to help answer who changed what and when they changed it. Auditing NetBackup operations can help provide information in the following areas:

General tracking	Customers can gain insight from audit trails while they investigate unexpected changes in a NetBackup environment. For example, it might be found that the addition of a client or a backup path has caused a significant increase in backup times. The audit report can indicate that an adjustment to a schedule or to a storage unit configuration might be necessary to accommodate the policy change.
Regulatory compliance	Auditing creates a record of who changed what and when it was changed. The record complies with guidelines such as those required by the Sarbanes-Oxley Act (SOX).
Corporate change management	For customers who must adhere to internal change management policies, NetBackup auditing offers a method to adhere to such policies.
Troubleshooting	The information from NetBackup auditing helps NetBackup Support to troubleshoot problems for customers.

You can view the actions NetBackup audits in the Security events in the NetBackup web user interface or in the NetBackup Administration Console. You can see full audit event details with the `nbauditreport` command or in NetBackup OpsCenter.

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. By default, auditing is enabled.

The Audit Manager provides the mechanism to query and report on auditing information. For example, an administrator can search specifically for information based on the following:

- 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

The audit manager behaves in the following manner when it creates audit records:

- The audit record limits the details of an entry to a maximum of 4096 characters. (For example, the Policy name.) The remaining characters are truncated while stored in the audit database.
- The audit record limits the restore image IDs to a maximum of 1024 characters. The remaining characters are truncated while stored in the audit database.
- Rollback operations are not audited.
  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.

Actions that NetBackup audits

NetBackup records the following user-initiated actions.

Policies actions	Adding, deleting, or updating policy attributes, clients, schedules, and backup selections lists.
Activity monitor actions	Canceling, suspending, resuming, restarting, or deleting any type of job creates an audit record.

Storage units actions	Adding, deleting, or updating storage units. **Note:** Actions that are related to storage lifecycle policies are not audited.
Storage servers actions	Adding, deleting, or updating storage servers.
Disk pools and Volume pools actions	Adding, deleting, or updating disk or volume pools.
Catalog information	This information includes: ■ Verifying and expiring images. ■ Read the requests sent for the front-end usage data.
Certificate management	Creating, revoking, renewing, and deploying of certificates and specific certificate failures.
Certificate Verification Failures (CVFs)	Any failed connection attempts that involve SSL handshake errors, revoked certificates, or host name validation failures.
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.
Hold operations	Creating, modifying, and deleting hold operations.
Host database	NetBackup host database related operations.
Login attempts	Any successful or failed login attempts for the NetBackup Administration Console, the NetBackup web UI or the NetBackup APIs.
Security configuration	Information related to changes 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.
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.
Authorization failure	Authorization failure is audited when you use the NetBackup web UI, the NetBackup APIs, or Enhanced Auditing .

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.

NetBackup also does not audit the following actions unless NetBackup Access Control (NBAC) is enabled. Note, however that you cannot use the NetBackup web UI when NBAC is enabled.

- Changes to the `bp.conf` file (UNIX) or the registry (Windows). Manual changes to the `bp.conf` file or the registry are not audited.
- Host properties actions.

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 additional details on NetBackup auditing, see the NetBackup Security and Encryption Guide. For a full audit report, use the `nbauditreport` command.

To view security events and audit logs

- On the left, select **Security > Security events**.
  - 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. For each audit category, 1000 events are displayed at maximum.

Chapter 4

Managing host mappings and certificates

This chapter includes the following topics:

About security management and certificates in NetBackup

NetBackup uses security certificates to authenticate the NetBackup hosts. The security certificates conform to the X.509 Public Key Infrastructure (PKI) standard. A master server acts as the Certificate Authority (CA) and issues digital certificates to hosts. NetBackup uses Transport Layer Security (TLS) protocol for host communication where each host needs to present its security certificate and validate the peer host's certificate against the Certificate Authority (CA) certificate.

The NetBackup 8.1 and later hosts can communicate with each other only in a secure mode. These hosts must have a Certificate Authority (CA) certificate and a host ID-based certificate for successful communication.

Security certificates for NetBackup 8.0 and earlier hosts

Any security certificates that NetBackup generated for 8.0 and earlier 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 system randomly generates Host IDs; these IDs not tied to any property of the hardware. The host ID remains the same even when the host name changes. The host ID is used in many certificate management operations to identify the host.

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.

The master server is the Certificate Authority (CA), which maintains a list of all of the host IDs that have certificates (or revoked certificates). It assigns host ID-based certificates to NetBackup 8.1 and later hosts and stores the host information in the `nbdb` database.

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 47.

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 NetBackup host ID to hostnames** 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**.

Reissue a certificate when a host's certificate is no longer valid

In some cases a host's 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 certificate. When you reissue a certificate, the host gets the host ID same as the original certificate.

Reissue a certificate, with a token

If you need to reissue a host's 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 certificate for a host

1. On the left, select **Security > Hosts**.
2. Select the host and click **Generate reissue token**.
3. Enter a token name and indicate how long the token should be valid for.
4. Click **Create**.

5 Click **Copy to clipboard** and click **Close**.

6 Share the authorization token so the host's administrator can obtain a new certificate.

Allow a 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 certificate reissue, without a token

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

2 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.

Revoke the ability to reissue a certificate without a token

After you allow a 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 certificate without a token

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

2 Select the host and click **Revoke auto reissue certificate > Revoke**.

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 host's communication status. See "Reset a host's attributes" on page 42.

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 **Enable insecure communication with 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.

You can view and revoke certificates and view information on the Certificate Authority (CA). More detailed information about certificate management, certificate deployment, and the Certificate Management utility is available in the NetBackup Security and Encryption Guide. To reissue a token for a host, see:

See “Reissue a certificate when a host’s certificate is no longer valid” on page 40.

View a certificate

To view a certificate

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

   The list of certificates displays for the master server.

2. To view additional certificate details for a host, click on a host name.

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 can 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.

See “About revoking host ID-based certificates” in the NetBackup Security and Encryption Guide.

Security best practices suggest that the NetBackup security administrator explicitly revoke the certificates for any host that is no longer active, 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 cease.

---

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

For secure communication with the master server or Certificate Authority, 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 Certificate Authority details and fingerprint

1. On the left, select **Security > Hosts**.
2. At the top, click **View Certificate Authority**.

3 Find the **Fingerprint** information and click **Copy to clipboard**.

4 Provide this fingerprint information to the host's administrator.

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

Create a token

Depending on the security level, an authorization token may be required for a non-master NetBackup host to obtain a host ID-based 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.

To create a 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 a token value

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

To find and copy a 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** 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.

Chapter 5

Managing global security settings

This chapter includes the following topics:

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 OpsCenter server, the insecure communication 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 **Enable insecure 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 NetBackup host ID to hostnames** 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 NetBackup host ID to hostnames**.
3. Click **Save**.

Select a security level for certificate deployment

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

For more details on security levels, certificate deployment, and the CRL, see the NetBackup Security and Encryption Guide.

To select a security level for certificate deployment

1. At the top, click **Settings > Global security**.
2. Click **Secure communication**.

3 Certificates 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 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. See "About certificate deployment security levels" in the NetBackup Security and Encryption Guide.
Medium	NetBackup issues 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 "About 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 6

Troubleshooting the web UI

This chapter includes the following topics:

Tips for accessing the NetBackup web UI

When NetBackup is properly configured, you 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 6-1 Solutions when the web user interface does not display

Step	Action	Description
Step 1	Check your 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 6-1 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 third-party certificate is accessible and has not expired.	Use the java keytools command to validate the `nbwebservice.jks` file. 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.

Try carrying out all steps from Table 6-1.

Certificate warning displays when you try to access the web UI

The certificate warning is displayed if the NetBackup web server is using a certificate issued by a CA that is not trusted by the web browser. The default NetBackup web server certificate is issued by the NetBackup CA that is not trusted by web browsers.

To resolve a certificate warning from the browser when you access the web UI

1. Configure the third-party certificate on the NetBackup web server.

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

2. If the problem persists, contact Veritas Technical Support.

Certificate warning displays after a failover in a clustered setup

To resolve a certificate warning from the browser when you access the web UI

1. Run the `configureTPCerts` command on all cluster nodes.

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

2. After you run the `configureTPCerts` command, be sure to restart the `nbwmc` and `vnetd` services.

If a user doesn't have the correct permissions or access to workload assets 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 15.

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 name or user name and domain name that are specified in the access rule match the user's credentials.
- 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.