VERITAS

Role Based Access Control (RBAC)
Veritas NetBackup 8.3

Read Me First Guide

Veritas NetBackup 8.3 and new RBAC

Veritas is committed to providing its users flexibility and ease of use by creating simple products and features. The **Role Based Access Control (RBAC)** feature in NetBackup 8.3 is a step forward in that direction. With the release of NetBackup 8.3, the RBAC feature allows more granular access control.

What is RBAC

RBAC uses roles as a way of delegating permissions on objects to users. The NetBackup Web User Interface (web UI) provides users with the ability to configure and apply role-based access control in their NetBackup environment for APIs and the web UI. You can use RBAC to provide access for users who do not usually have access to NetBackup. NetBackup users who would normally require administrator access can now be provided limited access and permissions based on their role within your organization.

Beginning with the NetBackup 8.1.2 release, the NetBackup web UI provided role-based access control for a limited number of security settings and workloads. The RBAC feature is enforced and applicable for web UI and APIs.

With improved infrastructure in the NetBackup 8.3 release, RBAC allows more granular permissions, improved flexibility. and greater control. The design of RBAC is based on Access Control Lists (ACLs), and it closely follows the ANSI INCITS 359-2004. Earlier designs of RBAC enforcement were dynamic in nature; configuration with the improved infrastructure is static.

Fresh install

After the installation of NetBackup 8.3, the administrator can create access definitions and roles. An access rule gives a user permissions and access to the NetBackup environment through the web UI, based on the user's role in the organization.

By default, only the "Administrator" role is created in NetBackup 8.3 has all privileges for RBAC. The "Administrator" needs to login to the web UI to configure additional custom roles such as Workload administrator, Security administrator, Backup Administrator, and other custom roles for different tasks.

RBAC bootstrapping

RBAC bootstrapping allows assignment of RBAC permissions to a user or a user group during NetBackup installation or upgrade on UNIX platforms. The UNIX installer uses the **bpnbaz -AddRBACPrincipal** command to assign the Administrator role to the user or the user group that is specified in the /tmp/NBInstallAnswer.conf file.

After installation or upgrade, the **bpnbaz -AddRBACPrincipal** command can be run on both Windows and UNIX platforms to assign RBAC permissions. The command is available only on the master server.

Upgrade to NetBackup 8.3 - Check for RBAC configuration

While running an upgrade to NetBackup 8.3, some pre-condition checks will run. The installer would need confirmation if any of the roles listed in table 1 below are already implemented.

There are multiple checks needed for RBAC configuration. The presence of any pre-configured principals in RBAC, or whether the user may have configured custom roles or added custom object groups to pre-defined roles all indicate a need to inform the user that RBAC has changed in ways the user must understand this before proceeding.

While there are no error messages, there will be prompts during the upgrade process. Any NetBackup master server that is being upgraded from 8.2 to NetBackup 8.3 runs these checks. The checks performed during the upgrade process determine whether RBAC API keys are found in the NetBackup database. If the database has no entries for API keys, the check will pass. The user must acknowledge the message before proceeding with the upgrade.

After upgrading to NetBackup 8.3, a migration tool called **rbac_user_migration** is available to move previous Backup administrator users to the new elevated Administrator role. A corresponding Perl script of this tool is also accessible from SORT. You can also use the migration tool to create a Security Administrator role in the new RBAC with equivalent permissions and add the principals from the earlier RBAC Security administrator role to the new RBAC Security Administrator role.

RBAC canned roles such as Workload Admin orCustom roles configured in previous NetBackup versions must be reconfigured after upgrading to NetBackup 8.3. After the upgrade, the earlier RBAC configuration remains accessible but cannot be enforced. The GET APIs function can be used to retrieve pre-configured RBAC read only data.

When using API keys, the user must be assigned a role that has permission to call APIs that the user wants to execute. The actual API Key value does not need to be changed, but the underlying principals must be configured using the new RBAC design.

Table 1: Different Roles defined in new RBAC

Role	Definition
VMware Administrator	Provides all permissions necessary to manage protection for VMware VMs through Protection Plans.
RHV Administrator	Provides all permissions necessary to manage protection for RedHat Virtualization VMs through Protection Plans.
Cloud Administrator	Provides all permissions necessary to manage protection of cloud assets using Protection Plans.
MS-SQL Administrator	Provides all permissions necessary to manage protection for Microsoft SQL Server databases using Protection Plans.
Storage Administrator	Provides all permissions necessary to configure and manage disk-based storage and cloud storage for NetBackup.

The above table-1 lists the new roles offered with new RBAC in NetBackup 8.3. These roles are not offered with the installed product but can be generated using a separate utility script. The RBAC role templates can be downloaded from SORT.

Earlier RBAC vs new RBAC

Table 2: Difference/similarity between earlier and new RBAC

Workflow/Support	**Earlier RBAC** *(NetBackup 8.1.2 and 8.2)*	**New RBAC** *(NetBackup 8.3)*
Ability to add, delete, update roles	✓	✓
Ability to create custom roles	✓	✓
On upgrade, recreate custom roles, Workload admin role	✗	✓
Optional User Migration Tool	✗	✓
RBAC configuration protected as part of disaster recovery of Master	✓	✓
Multiple canned roles (Backup Admin, Security Admin)	✓	✗
Closely aligned with Access Control List model	✗	✓
RBAC support for web UI & API only	✓	✓

RBAC and ransomware

RBAC compliments the ransomware resiliency posture for data protection. RBAC ensures that access to resources on NetBackup is restricted. Only the users that are assigned the Administrator role are authorized to configure and manage NetBackup. RBAC configuration is protected in catalog backup of master servers and can be recovered through already established catalog recovery processes.

RBAC and cloud plug-in support

In NetBackup 8.3, cloud plug-in support is provided with named queries for assets, asset-by-id, create-or-update-assets, assets-count, delete-assets and cleanup-assets. There are two named queries implemented by cloud providers: “add-assets-protection” and “remove-assets-protection”. These named queries are consumed by service level objective (SLO) APIs internally when the asset is subscribed to a protection plan. All other workload providers have also implemented these named queries for SLO integration. SLO APIs post the information with the ‘add-assets-protection’ named query to the plug-in and

the plug-in stores basic information such as the protection plan name, policy name, or SLO ID. The same plug-in experience exists for VMware, SQL server and RHV.

Figure 1- RBAC with NetBackup 8.3 – CloudPoint servers and cloud providers

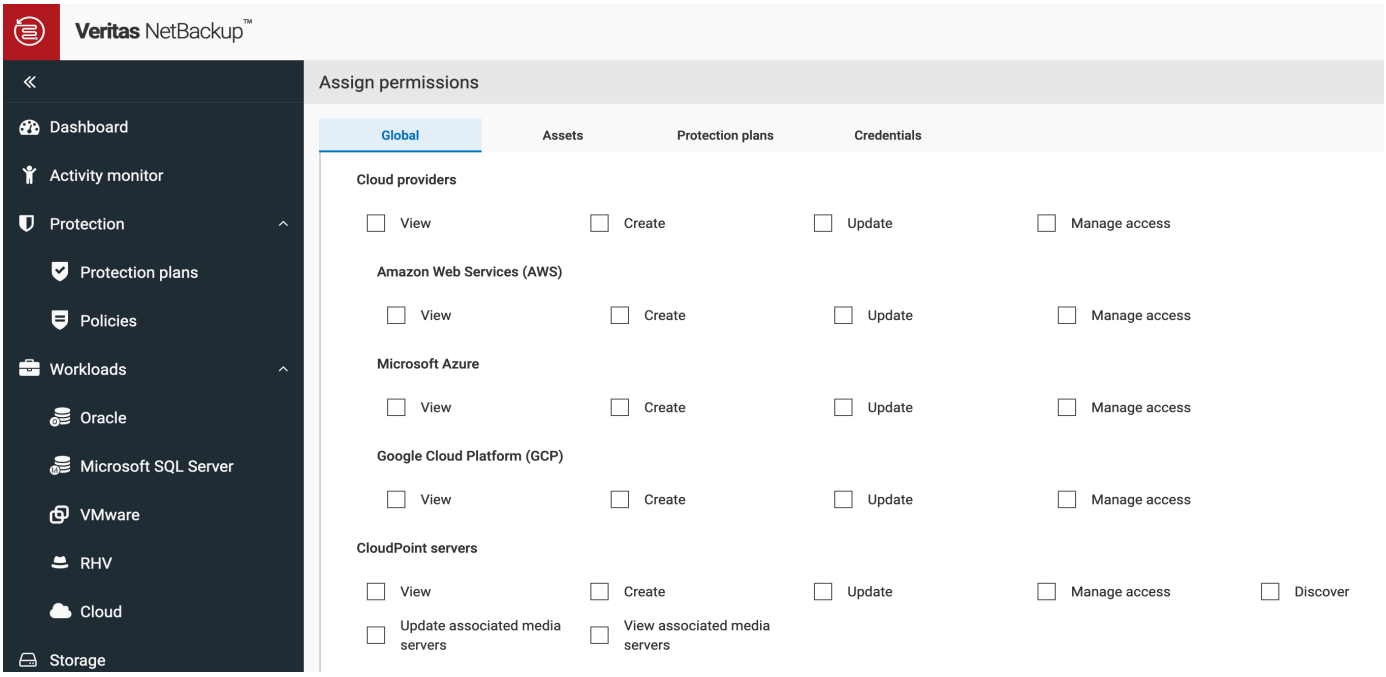
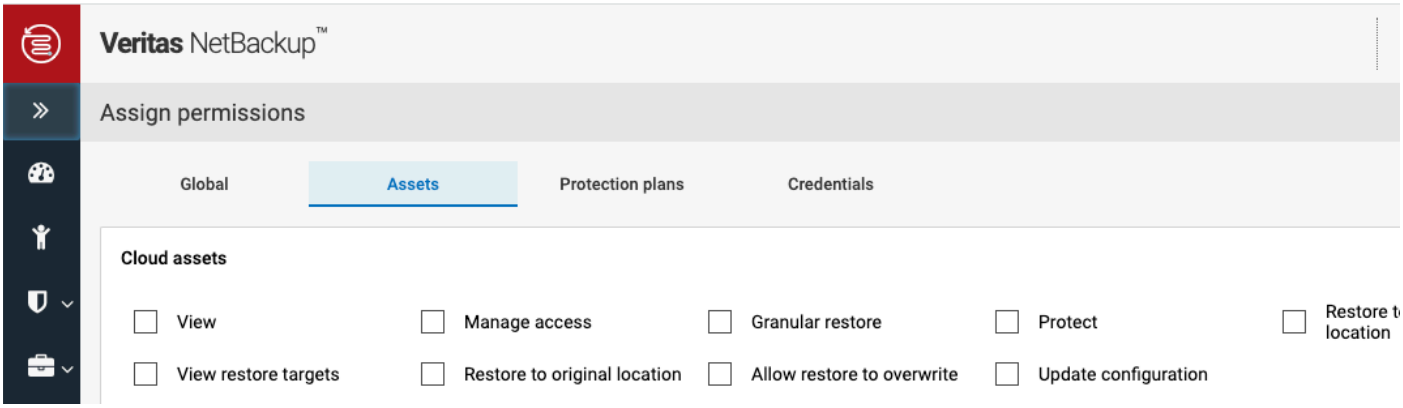


Figure 2- RBAC with NetBackup 8.3 – Cloud Assets Permissions



Best practices for RBAC with NetBackup 8.3

- Take advantage of inheritance wherever possible to grant access at higher level namespaces.
- Perform successful catalog backups before upgrading.
- Run the NetBackup pre-install checker well in advance of an upgrade to NetBackup 8.3. Keep a copy of all information of all roles created in NetBackup 8.1.2/8.2

With NetBackup 8.3, Veritas has further extended the functionality and flexibility of the RBAC solutions for backup and restore administration. With added functionality and more granular controls, customers will see even more value from RBAC in 8.3 that will allow for a greater delegation and distribution of responsibilities to allow storage and backup administrators to put more ownership of data protection in application teams' hands.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For specific country offices
and contact numbers,
please visit our website.