About role-based access control

SnapManager Oracle

NetApp
April 15, 2021

Table of Contents

About role-based access control

Role-based access control (RBAC) lets you control who has access to SnapManager operations. RBAC allows administrators to manage groups of users by defining roles and assigning users to those roles. You might want to use SnapManager RBAC in environments where RBAC is already in place.

RBAC includes the following components:

- Resources: Volumes and LUNs that hold the datafiles that make up your database.
- Capabilities: Types of operations that can be performed on a resource.
- Users: People to whom you grant capabilities.
- Roles: A set of resources and capabilities allowed on resources. You assign a specific role to a user who should perform those capabilities.

You enable RBAC in SnapDrive. You can then configure specific capabilities per role in the Operations Manager Web graphical user interface or command-line interface. RBAC checks occur in the DataFabric Manager server.

The following table lists some roles and their typical tasks, as set in Operations Manager.

Role	Typical tasks
Oracle database administrator	• Creating, maintaining, and monitoring an Oracle database that resides on a host • Scheduling and creating database backups • Ensuring that backups are valid and can be restored • Cloning databases
Server administrator	• Setting up storage systems and aggregates • Monitoring volumes for free space • Provisioning storage on requests from users • Configuring and monitoring disaster recovery mirroring
Storage architect	• Making architectural decisions on storage • Planning storage capacity growth • Planning disaster recovery strategies • Delegating capabilities to members of the team

If RBAC is in use (meaning that Operations Manager is installed and RBAC is enabled in SnapDrive), the storage administrator needs to assign RBAC permissions on all of the volumes and storage systems for the database files.

Enabling role-based access control

SnapManager role-based access control (RBAC) is enabled using SnapDrive. Upon installation of SnapDrive, RBAC is disabled by default. After you enable RBAC in SnapDrive, SnapManager then performs operations with RBAC enabled.

The snapdrive.config file in SnapDrive sets many options, one of which enables RBAC.

The SnapDrive documentation contains details about SnapDrive.

1. Open the snapdrive.conf file in an editor.
2. Enable RBAC by changing the value of the rbac-method parameter from native to dfm.

   The default value for this parameter is native, which disables RBAC.

Documentation on the NetApp Support Site: mysupport.netapp.com

Setting role-based access control capabilities and roles

After you enable role-based access control (RBAC) for SnapManager using SnapDrive, you can add RBAC capabilities and users to roles to perform SnapManager operations.

You must create a group in the Data Fabric Manager server and add the group to both primary and secondary storage systems. Run the following commands:

- dfm group create smo_grp
- dfm group add smo_grpprimary_storage_system
- dfm group add smo_grpsecondary_storage_system

You can use either the Operations Manager web interface or the Data Fabric Manager server command-line interface (CLI) to modify RBAC capabilities and roles.

The table lists the RBAC capabilities required to perform SnapManager operations:

SnapManager operations	RBAC capabilities required when data protection is not enabled	RBAC capabilities required when data protection is enabled
Profile create or profile update	SD.Storage.Read (smo_grp)	SD.Storage.Read (SMO_profile dataset)

SnapManager operations	RBAC capabilities required when data protection is not enabled	RBAC capabilities required when data protection is enabled
Profile protection	DFM.Database.Write (smo_grp) SD.Storage.Read (smo_grp) SD.Config.Read (smo_grp) SD.Config.Write (smo_grp) SD.Config.Delete (smo_grp) GlobalDataProtection	None
Backup create	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp)	SD.Storage.Read (SMO_profile dataset) SD.Snapshot.Write (SMO_profile dataset) SD.Snapshot.Read (SMO_profile dataset) SD.Snapshot.Delete (SMO_profile dataset)
Backup create (with DBverify)	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp) SD.SnapShot.Clone (smo_grp)	SD.Storage.Read (SMO_profile dataset) SD.Snapshot.Write (SMO_profile dataset) SD.Snapshot.Read (SMO_profile dataset) SD.Snapshot.Delete (SMO_profile dataset) SD.SnapShot.Clone (SMO_profile dataset)

SnapManager operations	RBAC capabilities required when data protection is not enabled	RBAC capabilities required when data protection is enabled
Backup create (with RMAN)	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp) SD.SnapShot.Clone (smo_grp)	SD.Storage.Read (SMO_profile dataset) SD.Snapshot.Write (SMO_profile dataset) SD.Snapshot.Read (SMO_profile dataset) SD.Snapshot.Delete (SMO_profile dataset) SD.SnapShot.Clone (SMO_profile dataset)
Backup restore	SD.Storage.Read (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Delete (smo_grp) SD.SnapShot.Clone (smo_grp) SD.Snapshot.Restore (smo_grp)	SD.Storage.Read (SMO_profile dataset) SD.Snapshot.Write (SMO_profile dataset) SD.Snapshot.Read (SMO_profile dataset) SD.Snapshot.Delete (SMO_profile dataset) SD.SnapShot.Clone (SMO_profile dataset) SD.Snapshot.Restore (SMO_profile dataset)
Backup delete	SD.Snapshot.Delete (smo_grp)	SD.Snapshot.Delete (SMO_profile dataset)
Backup verify	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Clone (smo_grp))	SD.Storage.Read (SMO_profile dataset) SD.Snapshot.Read (SMO_profile dataset) SD.Snapshot.Clone (SMO_profile dataset)

SnapManager operations	RBAC capabilities required when data protection is not enabled	RBAC capabilities required when data protection is enabled
Backup mount	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.Snapshot.Clone (smo_grp)	SD.Storage.Read (SMO_profile dataset) SD.Snapshot.Read (SMO_profile dataset) SD.Snapshot.Clone (SMO_profile dataset)
Backup unmount	SD.Snapshot.Clone (smo_grp)	SD.Snapshot.Clone (SMO_profile dataset)
Clone create	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.SnapShot.Clone (smo_grp)	SD.Storage.Read (SMO_profile dataset) SD.Snapshot.Read (SMO_profile dataset) SD.SnapShot.Clone (SMO_profile dataset)
Clone delete	SD.Snapshot.Clone (smo_grp)	SD.Snapshot.Clone (SMO_profile dataset)
Clone split	SD.Storage.Read (smo_grp) SD.Snapshot.Read (smo_grp) SD.SnapShot.Clone (smo_grp) SD.Snapshot.Delete (smo_grp) SD.Storage.Write (smo_grp)	SD.Storage.Read (SMO_profile dataset) SD.Snapshot.Read (SMO_profile dataset) SD.SnapShot.Clone (SMO_profile dataset) SD.Snapshot.Delete (SMO_profile dataset) SD.Storage.Write (SMO_profile dataset)

For details about defining RBAC capabilities, see the *OnCommand Unified Manager Operations Manager Administration Guide*.

1. Access the Operations Manager console.
2. From the Setup menu, select **Roles**.
3. Select an existing role or create a new one.
4. To assign operations to your database storage resources, click **Add capabilities**.
5. On the Edit Role Settings page, to save your changes to the role, click **Update**.

Related information

OnCommand Unified Manager Operations Manager Administration Guide: mysupport.netapp.com/documentation/productsatoz/index.html