RBAC (Role-Based Access Control) di SnapCenter

SnapCenter Software 5.0

NetApp
July 18, 2024

Sommario

RBAC (Role-Based Access Control) di SnapCenter

Tipi di RBAC

Le autorizzazioni RBAC (Role-Based Access Control) e ONTAP di SnapCenter consentono agli amministratori di SnapCenter di delegare il controllo delle risorse SnapCenter a diversi utenti o gruppi di utenti. Questo accesso gestito centralmente consente agli amministratori delle applicazioni di lavorare in modo sicuro all'interno degli ambienti delegati.

È possibile creare e modificare i ruoli e aggiungere l'accesso alle risorse agli utenti in qualsiasi momento, ma quando si imposta SnapCenter per la prima volta, è necessario almeno aggiungere utenti o gruppi Active Directory ai ruoli, quindi aggiungere l'accesso alle risorse a tali utenti o gruppi.

Non è possibile utilizzare SnapCenter per creare account utente o di gruppo. È necessario creare account utente o di gruppo in Active Directory del sistema operativo o del database.

SnapCenter utilizza i seguenti tipi di controllo degli accessi in base al ruolo:

- SnapCenter RBAC
- Plug-in SnapCenter RBAC (per alcuni plug-in)
- RBAC a livello applicativo
- Permessi ONTAP

SnapCenter RBAC

Ruoli e autorizzazioni

SnapCenter viene fornito con ruoli predefiniti con autorizzazioni già assegnate. È possibile assegnare utenti o gruppi di utenti a questi ruoli. È inoltre possibile creare nuovi ruoli e gestire autorizzazioni e utenti.

Assegnazione delle autorizzazioni a utenti o gruppi

È possibile assegnare autorizzazioni a utenti o gruppi per accedere a oggetti SnapCenter come host, connessioni di storage e gruppi di risorse. Non è possibile modificare le autorizzazioni del ruolo SnapCenterAdmin.

È possibile assegnare le autorizzazioni RBAC a utenti e gruppi all'interno della stessa foresta e a utenti appartenenti a foreste diverse. Non è possibile assegnare autorizzazioni RBAC agli utenti appartenenti a gruppi nidificati tra foreste.

Se si crea un ruolo personalizzato, deve contenere tutte le autorizzazioni del ruolo di amministratore di SnapCenter. Se si copiano solo alcune delle autorizzazioni, ad esempio aggiunta host o rimozione host, non è possibile eseguire tali operazioni.

Autenticazione

Gli utenti devono fornire l'autenticazione durante l'accesso, tramite l'interfaccia grafica utente (GUI) o utilizzando i cmdlet PowerShell. Se gli utenti sono membri di più ruoli, dopo aver immesso le credenziali di accesso, viene richiesto di specificare il ruolo che si desidera utilizzare. Gli utenti devono inoltre fornire l'autenticazione per eseguire le API.

RBAC a livello applicativo

SnapCenter utilizza le credenziali per verificare che gli utenti SnapCenter autorizzati dispongano anche delle autorizzazioni a livello di applicazione.

Ad esempio, se si desidera eseguire operazioni di snapshot e protezione dei dati in un ambiente SQL Server, è necessario impostare le credenziali con le credenziali Windows o SQL appropriate. Il server SnapCenter autentica il set di credenziali utilizzando uno dei due metodi. Per eseguire operazioni di Snapshot e data Protection in un ambiente file system Windows sullo storage ONTAP, il ruolo di amministratore SnapCenter deve disporre dei privilegi di amministratore sull'host Windows.

Allo stesso modo, se si desidera eseguire operazioni di protezione dei dati su un database Oracle e se l'autenticazione del sistema operativo (OS) è disattivata nell'host del database, è necessario impostare le credenziali con il database Oracle o con le credenziali ASM Oracle. Il server SnapCenter autentica il set di credenziali utilizzando uno di questi metodi, a seconda dell'operazione.

Plug-in SnapCenter per VMware vSphere RBAC

Se si utilizza il plug-in VMware di SnapCenter per la protezione dei dati coerente con le macchine virtuali, il server vCenter fornisce un livello aggiuntivo di RBAC. Il plug-in VMware di SnapCenter supporta sia vCenter Server RBAC che Data ONTAP RBAC.

Per informazioni, vedere "Plug-in SnapCenter per VMware vSphere RBAC"

Permessi ONTAP

È necessario creare un account vsadmin con le autorizzazioni necessarie per accedere al sistema di storage.

Per informazioni sulla creazione dell'account e l'assegnazione delle autorizzazioni, vedere "Creare un ruolo di cluster ONTAP con privilegi minimi"

Autorizzazioni e ruoli RBAC

Il RBAC (Role-Based Access Control) di SnapCenter consente di creare ruoli e assegnare autorizzazioni a tali ruoli, quindi assegnare utenti o gruppi di utenti ai ruoli. Ciò consente agli amministratori di SnapCenter di creare un ambiente gestito centralmente, mentre gli amministratori delle applicazioni possono gestire i processi di protezione dei dati. SnapCenter viene fornito con alcuni ruoli e autorizzazioni predefiniti.

Ruoli di SnapCenter

SnapCenter viene fornito con i seguenti ruoli predefiniti. È possibile assegnare utenti e gruppi a questi ruoli o creare nuovi ruoli.

Quando si assegna un ruolo a un utente, nella pagina lavori sono visibili solo i lavori pertinenti a tale utente, a

meno che non sia stato assegnato il ruolo Amministratore SnapCenter.

- Backup dell'app e amministratore del clone
- Visualizzatore di backup e cloni
- Amministratore dell'infrastruttura
- SnapCenterAdmin

Plug-in SnapCenter per i ruoli di VMware vSphere

Per la gestione della protezione dei dati coerente con le macchine virtuali di macchine virtuali, VMDK e datastore, i seguenti ruoli vengono creati in vCenter dal plug-in SnapCenter per VMware vSphere:

- Amministratore di SCV
- Vista dei distributori idraulici
- SCV di backup
- Ripristino dei distributori idraulici
- Ripristino del file ospite SCV

Per ulteriori informazioni, vedere "Tipi di plug-in RBAC per SnapCenter per utenti di VMware vSphere"

Best practice: NetApp consiglia di creare un ruolo ONTAP per il plug-in SnapCenter per le operazioni VMware vSphere e assegnargli tutti i privilegi richiesti.

Permessi SnapCenter

SnapCenter fornisce le seguenti autorizzazioni:

- Gruppo di risorse
- Policy
- Backup
- Host
- Connessione storage
- Clonare
- Provisioning (solo per database Microsoft SQL)
- Dashboard
- Report
- Ripristinare
  - Full Volume Restore (solo per plug-in personalizzati)
- Risorsa

  L'amministratore deve disporre dei privilegi del plug-in per consentire ai non amministratori di eseguire l'operazione di rilevamento delle risorse.

- Installazione o disinstallazione del plug-in

Quando si abilitano le autorizzazioni per l'installazione del plug-in, è necessario modificare anche l'autorizzazione host per abilitare le letture e gli aggiornamenti.

- Migrazione
- Montare (solo per database Oracle)
- Smontare (solo per database Oracle)
- Monitoraggio del processo

  L'autorizzazione Job Monitor consente ai membri di diversi ruoli di visualizzare le operazioni su tutti gli oggetti a cui sono assegnati.

Ruoli e autorizzazioni SnapCenter predefiniti

SnapCenter viene fornito con ruoli predefiniti, ciascuno con un set di autorizzazioni già attivate. Quando si imposta e si amministra RBAC (role-based access control), è possibile utilizzare questi ruoli predefiniti o crearne di nuovi.

SnapCenter include i seguenti ruoli predefiniti:

- Ruolo di amministratore di SnapCenter
- Backup dell'app e ruolo di amministratore del clone
- Ruolo di Backup e Clone Viewer
- Ruolo di amministratore dell'infrastruttura

Quando si aggiunge un utente a un ruolo, è necessario assegnare l'autorizzazione StorageConnection per abilitare la comunicazione SVM (Storage Virtual Machine) o assegnare una SVM all'utente per abilitare l'autorizzazione all'utilizzo di SVM. L'autorizzazione connessione storage consente agli utenti di creare connessioni SVM.

Ad esempio, un utente con il ruolo di amministratore SnapCenter può creare connessioni SVM e assegnarle a un utente con il ruolo di backup dell'applicazione e amministratore clone, che per impostazione predefinita non dispone dell'autorizzazione per creare o modificare connessioni SVM. Senza una connessione SVM, gli utenti non possono completare alcuna operazione di backup, clonazione o ripristino.

Ruolo di amministratore di SnapCenter

Il ruolo di amministratore di SnapCenter ha tutte le autorizzazioni attivate. Non è possibile modificare le autorizzazioni per questo ruolo. È possibile aggiungere utenti e gruppi al ruolo o rimuoverli.

Backup dell'app e ruolo di amministratore del clone

Il ruolo App Backup and Clone Admin dispone delle autorizzazioni necessarie per eseguire azioni amministrative per i backup delle applicazioni e le attività correlate ai cloni. Questo ruolo non dispone di autorizzazioni per la gestione degli host, il provisioning, la gestione della connessione dello storage o l'installazione remota.

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
Gruppo di risorse	Non applicabile	Sì	Sì	Sì	Sì
Policy	Non applicabile	Sì	Sì	Sì	Sì
Backup	Non applicabile	Sì	Sì	Sì	Sì
Host	Non applicabile	Sì	Sì	Sì	Sì
Connessione storage	Non applicabile	No	Sì	No	No
Clonare	Non applicabile	Sì	Sì	Sì	Sì
Provisioning	Non applicabile	No	Sì	No	No
Dashboard	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Report	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Ripristinare	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Risorsa	Sì	Sì	Sì	Sì	Sì
Installazione/disinstallazione del plug-in	No	Non applicabile		Non applicabile	Non applicabile
Migrazione	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Montare	Sì	Sì	Non applicabile	Non applicabile	Non applicabile
Smontare	Sì	Sì	Non applicabile	Non applicabile	Non applicabile
Ripristino completo del volume	No	No	Non applicabile	Non applicabile	Non applicabile
Monitoraggio del processo	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Ruolo di Backup e Clone Viewer

Il ruolo Backup and Clone Viewer (Visualizzatore di backup e clonazione) dispone di una vista in sola lettura di tutte le autorizzazioni. Questo ruolo dispone anche di autorizzazioni abilitate per il rilevamento, la creazione di

report e l'accesso al dashboard.

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
Gruppo di risorse	Non applicabile	No	Sì	No	No
Policy	Non applicabile	No	Sì	No	No
Backup	Non applicabile	No	Sì	No	No
Host	Non applicabile	No	Sì	No	No
Connessione storage	Non applicabile	No	Sì	No	No
Clonare	Non applicabile	No	Sì	No	No
Provisioning	Non applicabile	No	Sì	No	No
Dashboard	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Report	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Ripristinare	No	No	Non applicabile	Non applicabile	Non applicabile
Risorsa	No	No	Sì	Sì	No
Installazione/disinstallazione del plug-in	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Migrazione	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Montare	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Smontare	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Ripristino completo del volume	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Monitoraggio del processo	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile

Ruolo di amministratore dell'infrastruttura

Il ruolo Infrastructure Admin (Amministratore dell'infrastruttura) dispone di autorizzazioni abilitate per la gestione degli host, la gestione dello storage, il provisioning, i gruppi di risorse, i report di installazione remota, E l'accesso alla dashboard.

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
Gruppo di risorse	Non applicabile	Sì	Sì	Sì	Sì
Policy	Non applicabile	No	Sì	Sì	Sì
Backup	Non applicabile	Sì	Sì	Sì	Sì
Host	Non applicabile	Sì	Sì	Sì	Sì
Connessione storage	Non applicabile	Sì	Sì	Sì	Sì
Clonare	Non applicabile	No	Sì	No	No
Provisioning	Non applicabile	Sì	Sì	Sì	Sì
Dashboard	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Report	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Ripristinare	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Risorsa	Sì	Sì	Sì	Sì	Sì
Installazione/disinstallazione del plug-in	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Migrazione	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Montare	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Smontare	No	Non applicabile	Non applicabile	Non applicabile	Non applicabile
Ripristino completo del volume	No	No	Non applicabile	Non applicabile	Non applicabile

Permessi	Attivato	Creare	Leggi	Aggiornare	Eliminare
Monitoraggio del processo	Sì	Non applicabile	Non applicabile	Non applicabile	Non applicabile