Controllo degli accessi in base al ruolo in SnapDrive per UNIX

Snapdrive for Unix

NetApp
October 04, 2023

Sommario

Controllo degli accessi in base al ruolo in SnapDrive per UNIX

RBAC (role-based access control) viene utilizzato per l'accesso utente e le autorizzazioni dei ruoli. RBAC consente agli amministratori di gestire gruppi di utenti definendo i ruoli. Se è necessario limitare l'accesso al database ad amministratori specifici, è necessario impostare account amministratore per tali amministratori. Inoltre, se si desidera limitare le informazioni, che gli amministratori possono visualizzare e le operazioni che possono eseguire, è necessario applicare i ruoli agli account amministratore creati.

RBAC viene utilizzato in SnapDrive per UNIX con l'aiuto della console di Operations Manager. La console di Operations Manager offre un accesso granulare agli oggetti storage come LUN, qtree, volumi, aggregati e unità vFiler.

Informazioni correlate

Controlli obbligatori per SnapRestore basato su volume

Ripristino delle copie Snapshot su un sistema storage di destinazione

Procedura di scollegamento a scatto

Che cos'è il RBAC (role-based access control) in SnapDrive per UNIX

RBAC consente agli amministratori di SnapDrive di limitare l'accesso a un sistema storage per varie operazioni SnapDrive. Questo accesso limitato o completo per le operazioni di storage dipende dal ruolo assegnato all'utente.

SnapDrive 4.0 per UNIX e versioni successive richiede un controllo dell'accesso RBAC per tutte le operazioni di SnapDrive per UNIX. Questo comportamento consente agli amministratori dello storage di limitare le operazioni che gli utenti SnapDrive possono eseguire in base ai ruoli assegnati. RBAC viene implementato utilizzando l'infrastruttura di Operations Manager. Nelle versioni precedenti a SnapDrive 4.0 per UNIX, il controllo degli accessi era limitato e solo l'utente root poteva eseguire operazioni SnapDrive per UNIX. SnapDrive 4.0 per UNIX e versioni successive fornisce supporto per utenti locali non root e utenti NIS (Network Information System) utilizzando l'infrastruttura RBAC della console di Operations Manager. SnapDrive per UNIX non richiede la password root del sistema di storage, ma comunica con il sistema di storage utilizzando un utente sd-<hostname>.

Per impostazione predefinita, la funzionalità RBAC della console di Operations Manager non viene utilizzata. È necessario attivare la funzionalità RBAC impostando la variabile *`rbac-method=dfm`* in `snapdrive.conf` Archiviare e riavviare il daemon SnapDrive per UNIX.

Prima di poter utilizzare questa funzione, è necessario soddisfare i seguenti requisiti:

- Console Operations Manager 3.7 o successiva.
- Il server della console di Operations Manager deve essere presente e configurato nella rete IP che contiene gli host SnapDrive e i sistemi di storage.
- Le impostazioni di comunicazione della console di Operations Manager devono essere configurate durante

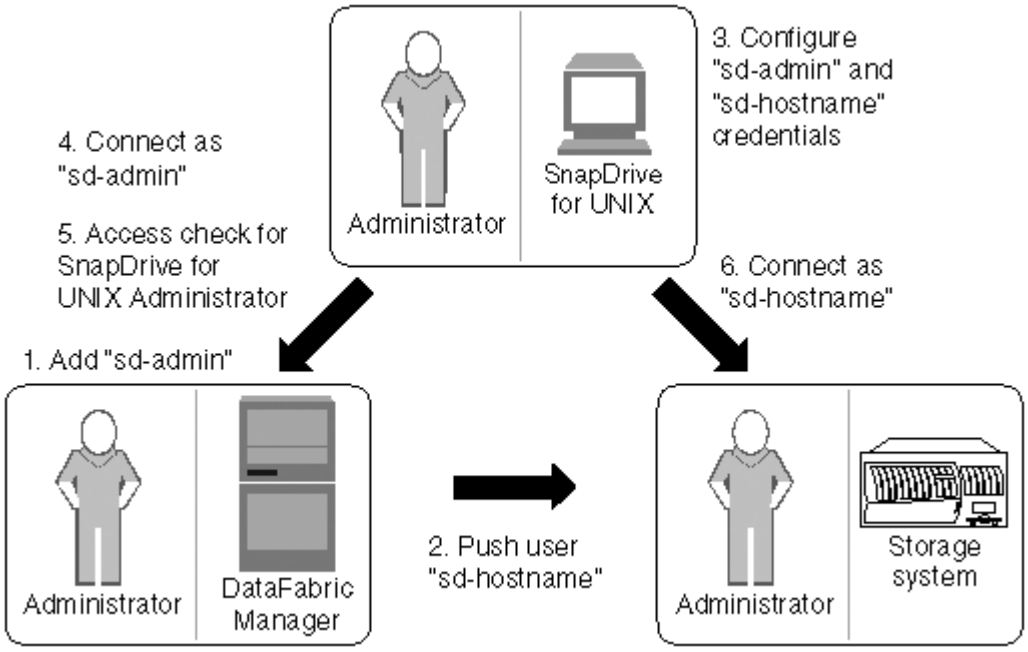
l'installazione di SnapDrive.

- SnapDrive per UNIX daemon dovrebbe essere in esecuzione.

Interazione della console di SnapDrive per UNIX e Operations Manager

L'utilizzo del RBAC (role-based access control) dipende dall'infrastruttura della console di Operations Manager. L'amministratore della console di Operations Manager deve creare nomi utente per l'utilizzo di SnapDrive per UNIX. Tutte le richieste relative alle operazioni di storage vengono prima inviate alla console di Operations Manager per un controllo dell'accesso. Dopo che la console di Operations Manager ha verificato un'operazione di storage da parte di un utente SnapDrive specifico, l'operazione viene completata.

Il seguente diagramma illustra l'intero RBAC per le operazioni di storage.



1. L'amministratore della console di Operations Manager aggiunge l'utente di amministrazione sd alla console di Operations Manager.
2. L'amministratore della console di Operations Manager crea un utente con nome host sd sul sistema di storage.
3. L'amministratore della console di Operations Manager invia le credenziali sd-admin e sd-hostname all'amministratore di SnapDrive per UNIX.
4. L'amministratore di SnapDrive configura SnapDrive con le credenziali utente ricevute.
5. La console di Operations Manager esegue il controllo dell'accesso per l'utilizzo di SnapDrive per UNIX con le credenziali utente aggiunte dall'amministratore di SnapDrive.
6. Dopo l'autenticazione dell'utente SnapDrive, l'utente può connettersi al sistema di storage.

Quando un utente SnapDrive desidera eseguire alcune operazioni di storage, invia il comando corrispondente alla riga di comando. La richiesta viene inviata alla console di Operations Manager per un controllo dell'accesso. La console di Operations Manager verifica se l'utente richiesto dispone delle autorizzazioni

appropriate per eseguire l'operazione SnapDrive. Il risultato della verifica dell'accesso viene restituito a SnapDrive. A seconda del risultato, all'utente è consentito o meno eseguire le operazioni di storage sul sistema di storage.

Se l'utente viene verificato dopo il controllo dell'accesso, si connette al sistema di storage come nome host sd.

> i nomi utente consigliati sono sd-hostname e sd-admin. È possibile configurare SnapDrive per UNIX con altri nomi utente.

Configurazione del controllo degli accessi in base al ruolo in SnapDrive per UNIX

È necessario completare varie attività per configurare RBAC (Role-Based Access Control) per SnapDrive per UNIX. È possibile utilizzare la console di Operations Manager o l'interfaccia della riga di comando per eseguire le attività.

Configurazione di sd-admin nella console di Operations Manager

L'amministratore della console di Operations Manager può creare l'utente di amministrazione sd.

L'amministratore della console di Operations Manager crea un utente denominato sd-admin, con la possibilità di eseguire un controllo degli accessi core su un gruppo globale (globale `DFM.Core.AccessCheck`). Dopo che l'amministratore della console di Operations Manager ha configurato l'utente sd-admin, è necessario inviare manualmente le informazioni sulle credenziali all'amministratore di SnapDrive per UNIX. Per ulteriori informazioni sull'utilizzo della console di Operations Manager per configurare utenti e ruoli, consultare la *Guida all'amministrazione della console di Operations Manager* e la Guida in linea.

> È possibile utilizzare qualsiasi nome al posto di sd-admin; tuttavia, si consiglia di utilizzare sd-admin.

Per creare un ruolo nella console di Operations Manager, selezionare **Setup** > **Roles**. Nella pagina di configurazione di sd-admin, l'amministratore della console di Operations Manager deve assegnare `DFM.Database.Write` Funzionalità del gruppo globale in ruolo di amministratore sd, in modo che SnapDrive per UNIX possa aggiornare le entità di storage nella console di Operations Manager.

Configurazione di sd-admin mediante l'interfaccia della riga di comando

L'amministratore del sistema di storage può configurare l'utente sd-admin utilizzando l'interfaccia della riga di comando.

Fasi

1. Aggiungere un utente denominato sd-admin.

```
# useradd sd-admin
```

```
# passwd sd-admin
Changing password for sd-admin.
New password:
Re-enter new password:
Password changed
```

2. Aggiungere un amministratore denominato sd-admin.

```
# dfm user add sd-admin
Added administrator sd-admin.
```

3. Creare un ruolo denominato sd-admin-role.

```
# dfm role create sd-admin-role
Created role sd-admin-role.
```

4. Aggiungere una funzionalità al ruolo creato nel passaggio 3.

```
# dfm role add sd-admin-role DFM.Core.AccessCheck Global
Added 1 capability to role sd-admin-role.
```

5. L'amministratore di Operations Manager può anche concedere `DFM.Database.Write` capacità sul gruppo globale a. `<sd-admin>` Per consentire a SnapDrive per UNIX di aggiornare le entità del sistema di storage in Gestione operazioni.

```
# dfm role add sd-admin-role DFM.Database.Write Global
Added 1 capability to role sd-admin-role.
```

6. Aggiungere un ruolo di amministratore sd all'utente di amministrazione sd.

```
# dfm user role set sd-admin sd-admin-role
Set 1 role for administrator sd-admin.
```

Aggiunta di un nome host sd al sistema di storage

L'amministratore della console di Operations Manager può creare l'utente del nome host sd sul sistema di storage utilizzando la console di Operations Manager. Una volta completata la procedura, l'amministratore della console di Operations Manager deve inviare manualmente le credenziali all'amministratore di SnapDrive per UNIX. È possibile utilizzare qualsiasi nome al posto di sd-hostname; tuttavia, si consiglia di utilizzare sd-

hostname.

Fasi

1. Ottenere la password root del sistema di storage e memorizzarla.

   Per aggiungere la password per il sistema di storage, selezionare **Gestione** > **sistema di storage**.

2. Creare un nome host sd per ciascun sistema UNIX.
3. Assegnare le funzionalità `api- e. login-` a un ruolo, come il ruolo sd.
4. Includere questo ruolo (ruolo sd) in un nuovo gruppo di utenti, ad esempio sd-usergroup.
5. Associare questo gruppo di utenti (gruppo di utenti sd) all'utente del nome host sd sul sistema di storage.

Aggiunta di un nome host sd al sistema di storage mediante CLI

L'amministratore del sistema di storage può creare e configurare l'utente del nome host sd utilizzando il comando useradmin.

Fasi

1. Aggiungere storage.

```
# dfm host add storage_array1
Added host storage_array1.lab.eng.btc.xyz.in
```

2. Impostare la password per l'host.

```
# dfm host password save -u root -p xxxxxxxx storage_array1
Changed login for host storage_array1.lab.eng.btc.xyz.in to root.
Changed Password for host storage_array1.lab.eng.xyz.netapp
.in
```

3. Creare un ruolo nell'host.

```
# dfm host role create -h storage_array1 -c "api-*,login-*" sd-unixhost-
role
Created role sd-unixhost-role on storage_array1
```

4. Creare un gruppo di utenti.

```
# dfm host usergroup create -h storage_array1 -r sd-unixhost-role sd-
unixhost-ug
Created usergroup sd-unixhost-ug(44) on storage_array1
```

5. Creare un utente locale.

```
# dfm host user create -h storage_array1 -p xxxxxxxx -g sd-unixhost-ug
sd-unixhost
Created local user sd-unixhost on storage_array1
```

Configurazione delle credenziali utente su SnapDrive per UNIX

L'amministratore di SnapDrive per UNIX riceve le credenziali utente dall'amministratore della console di Operations Manager. Queste credenziali utente devono essere configurate su SnapDrive per UNIX per le corrette operazioni di storage.

Fasi

1. Configurare sd-admin sul sistema storage.

```
[root]#snapdrive config set -dfm sd-admin ops_mngr_server
Password for sd-admin:
Retype password:
```

2. Configurare il nome host sd sul sistema di storage.

```
[root]#snapdrive config set sd-unix_host storage_array1
Password for sd-unix_host:
Retype password:
```

3. Verificare i passaggi 1 e 2 utilizzando `snapdrive config list` comando.

```
user name       appliance name          appliance type
-------------------------------------------------------
sd-admin        ops_mngr_server         DFM
sd-unix_host    storage_array1          StorageSystem
```

4. Configurare SnapDrive per UNIX per utilizzare RBAC (role-based access control) della console di Operations Manager impostando la variabile di configurazione `rbac-method="dfm"` in `snapdrive.conf` file.

> Le credenziali dell'utente vengono crittografate e salvate nel file esistente `.sdupw` file. La posizione predefinita del file precedente è `/opt/NetApp/snapdrive/.sdupw`.

Formati dei nomi utente per l'esecuzione dei controlli di accesso con la console di Operations Manager

SnapDrive per UNIX utilizza i formati dei nomi utente per eseguire controlli di accesso con la console di Operations Manager. Questi formati dipendono dal fatto che si tratti di

un NIS (Network Information System) o di un utente locale.

SnapDrive per UNIX utilizza i seguenti formati per verificare se un utente è autorizzato a eseguire determinate attività:

- Se si è un utente NIS che esegue `snapdrive` Command, SnapDrive per UNIX utilizza il formato `<nisdomain>\<username>` (ad esempio, `netapp.com\marc`)
- Se si è utenti locali di un host UNIX come lnx197-141, SnapDrive per UNIX utilizza il formato `<hostname>\<username>` formato (ad esempio, `lnx197-141\john`)
- Se sei un amministratore (root) di un host UNIX, SnapDrive per UNIX considera sempre l'amministratore come un utente locale e utilizza il formato `lnx197-141\root`.

Variabili di configurazione per il controllo degli accessi in base al ruolo

È necessario impostare le varie variabili di configurazione correlate al controllo degli accessi basato sul ruolo in `snapdrive.conf` file.

Variabile	Descrizione
contact-http-dfm-port = 8088	Specifica la porta HTTP da utilizzare per la comunicazione con un server della console di Operations Manager. Il valore predefinito è 8088.
contact-ssl-dfm-port = 8488	Specifica la porta SSL da utilizzare per la comunicazione con un server della console di Operations Manager. Il valore predefinito è 8488.
rbac-method=dfm	Specifica i metodi di controllo dell'accesso. I valori possibili sono `native` e. `dfm`. Se il valore è `native`, il file di controllo degli accessi memorizzato in `/vol/vol0/sdprbac/sdhost-name.prbac` viene utilizzato per i controlli degli accessi. Se il valore è impostato su `dfm`, La console di Operations Manager è un prerequisito. In tal caso, SnapDrive per UNIX invia i controlli di accesso alla console di Operations Manager.

Variabile	Descrizione
rbac-cache=on	SnapDrive per UNIX mantiene una cache di query di controllo degli accessi e i risultati corrispondenti. SnapDrive per UNIX utilizza questa cache solo quando tutti i server della console di Operations Manager configurati non sono attivi. È possibile impostare questo valore su uno dei due `on` per attivare la cache o a. `off` per disattivarlo. Il valore predefinito è Off per consentire a SnapDrive per UNIX di utilizzare la console di Operations Manager e impostare `rbac-method` variabile di configurazione a. `dfm`.
rbac-cache-timeout	Specifica il periodo di timeout della cache rbac ed è applicabile solo quando *rbac-cache* è attivato. Il valore predefinito è `24` ore SnapDrive per UNIX utilizza questa cache solo quando tutti i server della console di Operations Manager configurati non sono attivi.
use-https-to-dfm=on	Questa variabile consente di impostare SnapDrive per UNIX in modo che utilizzi la crittografia SSL (HTTPS) quando comunica con la console di Operations Manager. Il valore predefinito è `on`.

Comandi e funzionalità di SnapDrive

Nel controllo degli accessi basato sul ruolo (RBAC), è necessaria una funzionalità specifica per il successo di ciascuna operazione. Per eseguire le operazioni di storage, l'utente deve disporre del set corretto di funzionalità assegnate.

La seguente tabella elenca i comandi e le funzionalità corrispondenti richieste:

Comando	Funzionalità
`storage show`	SD.Storage.Read sul volume
`storage list`	SD.Storage.Read sul volume
`storage create`	• Per LUN all'interno dei volumi: `SD.Storage.Write` Sul volume • Per LUN all'interno di qtree: `SD.Storage.Write` su qtree
`storage resize`	`SD.Storage.Write` Su LUN

Comando	Funzionalità
`storage delete`	`SD.Storage.Delete` Su LUN
`snap show`	`SD.SnapShot.Read` sul volume
`snap list`	`SD.SnapShot.Read` sul volume
`snap delete`	`SD.Storage.Delete` sul volume
`snap rename`	`SD.Storage.Write` sul volume
`snap connect`	• Per i cloni LUN nel volume: `SD.SnapShot.Clone` sul volume • Per i cloni LUN in qtree: `SD.SnapShot.Clone` su qtree • Per i cloni di volumi tradizionali: `SD.SnapShot.Clone` sul sistema storage • Per il volume FlexClone: `SD.SnapShot.Clone` sul volume padre • Per volumi FlexClone senza restrizioni: `SD.SnapShot.UnrestrictedClone` sul volume padre
`snap connect-split`	• Per i cloni LUN (LUN clonati e suddivisi in volume): `SD.SnapShot.Clone` sul volume e. `SD.Storage.Write` sul volume • Per i cloni LUN (LUN clonati e divisi in qtree): `SD.SnapShot.Clone` su qtree e. `SD.Storage.Write` su qtree • Per i cloni di volume tradizionali suddivisi: `SD.SnapShot.Clone` sul sistema storage e. `SD.Storage.Write` sul sistema storage • Per i cloni di volumi Flex suddivisi: `SD.SnapShot.Clone` sul volume padre.
`clone split start`	• Per i cloni LUN in cui il LUN risiede nel volume o nel qtree: `SD.SnapShot.Clone` contenente volume o qtree • Per i cloni di volume: `SD.SnapShot.Clone` sul volume padre

Comando	Funzionalità
`snap disconnect`	• Per i cloni LUN in cui il LUN risiede nel volume o nel qtree: `SD.SnapShot.Clone` contenente volume o qtree • Per i cloni di volume: `SD.SnapShot.Clone` sul volume padre • Per l'eliminazione di cloni di volumi senza restrizioni: `SD.SnapShot.DestroyUnrestrictedClone` sul volume
`snap disconnect-split`	• Per i cloni LUN in cui il LUN risiede nel volume o nel qtree: `SD.SnapShot.Clone` sul volume o qtree contenente • Per i cloni di volume: `SD.Storage.Delete` sul volume padre • Per l'eliminazione di cloni di volumi senza restrizioni: `SD.SnapShot.DestroyUnrestrictedClone` sul volume
`snap restore`	• Per le LUN presenti in un volume: `SD.SnapShot.Restore` sul volume e. `SD.Storage.Write` Su LUN • Per LUN presenti in un qtree: `SD.SnapShot.Restore` su qtree e. `SD.Storage.Write` Su LUN • Per LUN non presenti nei volumi: `SD.SnapShot.Restore` sul volume e. `SD.Storage.Write` sul volume • Per LUN non presenti in qtree: `SD.SnapShot.Restore` su qtree e. `SD.Storage.Write` su qtree • Per i volumi: `SD.SnapShot.Restore` su sistemi storage per volumi tradizionali, o. `SD.SnapShot.Restore` su aggregato per volumi flessibili • Per il ripristino snap di un singolo file nei volumi: `SD.SnapShot.Restore` sul volume • Per il ripristino snap di un singolo file in qtree: `SD.SnapShot.Restore` qtree • Per eseguire l'override delle copie Snapshot di riferimento: `SD.SnapShot.DisruptBaseline` sul volume

Comando	Funzionalità
`host connect`, `host disconnect`	`SD.Config.Write` Sul LUN
`config access`	`SD.Config.Read` sul sistema storage
`config prepare`	`SD.Config.Write` su almeno un sistema storage
`config check`	`SD.Config.Read` su almeno un sistema storage
`config show`	`SD.Config.Read` su almeno un sistema storage
`config set`	`SD.Config.Write` sul sistema storage
`config set -dfm`, `config set -mgmtpath`,	`SD.Config.Write` su almeno un sistema storage
`config delete`	`SD.Config.Delete` sul sistema storage
`config delete dfm_appliance`, `config delete -mgmtpath`	`SD.Config.Delete` su almeno un sistema storage
`config list`	`SD.Config.Read` su almeno un sistema storage
`config migrate set`	`SD.Config.Write` su almeno un sistema storage
`config migrate delete`	`SD.Config.Delete` su almeno un sistema storage
`config migrate list`	`SD.Config.Read` su almeno un sistema storage

SnapDrive per UNIX non verifica alcuna funzionalità per l'amministratore (root).

Ruoli preconfigurati per semplificare la configurazione del ruolo dell'utente

I ruoli preconfigurati semplificano l'assegnazione dei ruoli agli utenti.

La tabella seguente elenca i ruoli predefiniti:

Nome ruolo	Descrizione
GlobalSDStorage	Gestisci lo storage con SnapDrive per UNIX
GlobalSDConfig	Gestisci le configurazioni con SnapDrive per UNIX

Nome ruolo	Descrizione
GlobalSDSnapshot	Gestisci le copie Snapshot con SnapDrive per UNIX
GlobalSDFullControl	Utilizzo completo di SnapDrive per UNIX

Nella tabella precedente, Global si riferisce a tutti i sistemi storage gestiti da una console di Operations Manager.

Aggiornamento automatico del sistema di storage sulla console di Operations Manager

La console di Operations Manager rileva i sistemi storage supportati dalla rete. Monitora periodicamente i dati raccolti dai sistemi storage rilevati. I dati vengono aggiornati a un intervallo impostato. L'amministratore della console di Operations Manager può configurare l'intervallo di aggiornamento.

L'intervallo di monitoraggio LUN, l'intervallo di monitoraggio qtree e l'intervallo di monitoraggio vFiler sono campi importanti che decidono la frequenza degli aggiornamenti di LUN, qtree e vFiler. Ad esempio, se viene creata una nuova LUN su un sistema di storage, la nuova LUN non viene aggiornata immediatamente sulla console di Operations Manager. Per questo motivo, e il controllo di accesso emesso alla console di Operations Manager per quel LUN alla console di Operations Manager non riesce. Per evitare questa situazione, è possibile modificare l'intervallo di monitoraggio del LUN in base alle proprie esigenze.

1. Selezionare **Setup** > **Options** nella console di Operations Manager per modificare l'intervallo di monitoraggio.
2. L'amministratore della console di Operations Manager può anche fare un refresh forzato della console di Operations Manager eseguendo l'operazione `dfm host discovery filername` nell'interfaccia della riga di comando.
3. L'amministratore della console di Operations Manager può anche concedere `DFM.Database.Write` Funzionalità del gruppo globale di sd-admin per consentire a SnapDrive per UNIX di aggiornare le entità del sistema di storage sulla console di Operations Manager.

   ```
   # dfm role add sd-admin-role DFM.Database.Write Global
   Added 1 capability to role sd-admin-role.
   ```

Server console di Operations Manager multipli

SnapDrive per UNIX supporta più server console di Operations Manager. Questa funzionalità è necessaria quando un gruppo di sistemi storage viene gestito da più di un server console Operations Manager. SnapDrive per UNIX contatta i server della console di Operations Manager nello stesso ordine in cui i server della console di Operations Manager sono configurati in SnapDrive per UNIX. È possibile eseguire `snapdrive config list` per ottenere l'ordine di configurazione.

L'esempio seguente mostra l'output per più server console Operations Manager:

```
# snapdrive config list
username    appliance name     appliance type
----------------------------------------------
root        storage_array1     StorageSystem
root        storage_array2     StorageSystem
sd-admin    ops_mngr_server1   DFM
sd-admin    ops_mngr_server2   DFM
```

Nell'esempio precedente, storage_array1 è gestito da Ops_mngr_server1 e storage_array2 è gestito da Ops_mngr_server2. In questo esempio, SnapDrive per UNIX contatta prima Ops_mngr_server1. Se Ops_mngr_server1 non riesce a determinare l'accesso, SnapDrive per UNIX contatta Ops_mngr_server2.

SnapDrive per UNIX contatta la seconda console di Operations Manager solo alle seguenti condizioni:

- Quando la prima console di Operations Manager non è in grado di determinare l'accesso. Questa situazione potrebbe verificarsi perché la prima console di Operations Manager non gestisce il sistema di storage.
- Quando la prima console di Operations Manager non è attiva.

Console di Operations Manager non disponibile

SnapDrive per UNIX necessita di una console di gestione delle operazioni per i controlli degli accessi. A volte il server della console di Operations Manager potrebbe non essere disponibile per diversi motivi.

Quando il metodo RBAC *`rbac-method = dfm`* È impostato e la console di Operations Manager non è disponibile, SnapDrive per UNIX visualizza il seguente messaggio di errore:

```
[root]# snapdrive storage delete -lun storage_array1:/vol/vol2/qtree1/lun1
0002-333 Admin error: Unable to connect to the DFM ops_mngr_server
```

SnapDrive per UNIX può anche mantenere una cache dei risultati del controllo dell'accesso utente restituiti dalla console di Operations Manager. Questa cache è valida per 24 ore e non è configurabile. Se la console di Operations Manager non è disponibile, SnapDrive per UNIX utilizza la cache per determinare l'accesso. Questa cache viene utilizzata solo quando tutti i server della console Operations Manager configurati non rispondono.

Affinché SnapDrive per UNIX utilizzi la cache per un controllo degli accessi, è necessario attivare *`rbac-cache`* la variabile di configurazione deve essere attivata per mantenere la cache dei risultati di accesso. Il *`rbac-cache`* la variabile di configurazione è disattivata per impostazione predefinita.

Per utilizzare SnapDrive per UNIX anche quando la console di Operations Manager non è disponibile, l'amministratore del server deve reimpostare il metodo RBAC (role-based access control) su *`rbac-method = native`* in `snapdrive.conf` file. Dopo aver modificato il `snapdrive.conf` Riavviare il daemon SnapDrive per UNIX. Quando *`rbac-method = native`* È impostato, solo l'utente root può utilizzare SnapDrive per UNIX.

Esempi di operazioni RBAC e storage

Il controllo degli accessi basato sui ruoli consente di eseguire operazioni di storage in base alle funzionalità assegnate all'utente. Viene visualizzato un messaggio di errore se non si dispone delle funzionalità appropriate per eseguire l'operazione di storage.

Operazioni con un singolo filespec su un singolo oggetto di storage

SnapDrive per UNIX visualizza un messaggio di errore quando non si è autorizzati a creare un filespec su un volume specificato.

Filespec: Filespec può essere un file system, un volume host, un gruppo di dischi o un LUN.

```
[john]$ snapdrive storage create -fs /mnt/testfs -filervol
storage_array1:/vol/vol1 -dgsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mngr_server
```

In questo esempio, John è un utente non root e non è autorizzato a creare un filespec sul volume specificato. John deve chiedere all'amministratore della console di Operations Manager di concedere `SD.Storage.Write` accesso al volume `storage_array1:/vol/vol1`.

Operazioni con un singolo filespec su più oggetti storage

SnapDrive per UNIX visualizza un messaggio di errore quando l'amministratore non dispone dell'autorizzazione necessaria per eseguire le operazioni di storage su più oggetti di storage.

Filespec: Filespec può essere qualsiasi file system, volume host, gruppo di dischi o LUN

```
[root]# snapdrive storage create -fs /mnt/testfs -lun
storage_array1:/vol/vol1/lun2 -lun storage_array1:/vol/vol2/lun2  -lunsize
100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager
server ops_mngr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
unix_host\root on Operations Manager server ops_mngr_server
```

In questo esempio, il filespec si estende su due volumi di sistema storage, vol1 e vol2. L'amministratore (root) di unix_host non dispone di `SD.Storage.Write` accesso su entrambi i volumi. Pertanto, SnapDrive per UNIX visualizza un messaggio di errore per ogni volume. Per procedere con `storage create`, L'amministratore (root) deve chiedere all'amministratore della console di Operations Manager di concedere `SD.Storage.Write` accesso su entrambi i volumi.

Operazioni con più filespec e oggetti di storage

L'esempio seguente mostra il messaggio di errore che si riceve quando non si è un utente autorizzato a eseguire l'operazione specifica.

```
[marc]$ snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6
-lun storage_array1:/vol/vol2/lun2 -lunsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user nis_domain\marc on Operations Manager
server ops_mngr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
nis_domain\marc on Operations Manager server ops_mngr_server
```

In questo esempio, tre LUN risiedono su due volumi di sistema storage, vol1 e vol2. L'utente Marc appartiene a nis_domain e non è autorizzato a creare filespec su vol1 e vol2. SnapDrive per UNIX visualizza i due messaggi di errore dell'esempio precedente. I messaggi di errore indicano che l'utente deve avere `SD.Storage.Write` accesso su vol1 e vol2.

Operazioni con più oggetti di storage

L'esempio seguente mostra il messaggio di errore che si riceve quando non si è un utente autorizzato a eseguire l'operazione specifica.

```
[john]$ snapdrive storage show -all

Connected LUNs and devices:

device filename   adapter  path  size  proto  state  clone  lun path
backing Snapshot
----------------  -------  ----  ----  -----  -----  -----  --------
---------------
/dev/sdao            -     -     200m  iscsi  online  No
storage_array1:/vol/vol2/passlun1           -
/dev/sda1            -     -     200m  fcp    online  No
storage_array1:/vol/vol2/passlun2           -

Host devices and file systems:

dg: testfs1_SdDg                dgtype lvm
hostvol: /dev/mapper/testfs1_SdDg-testfs1_SdHv  state: AVAIL
fs: /dev/mapper/testfs1_SdDg-testfs1_SdHv       mount point: /mnt/testfs1
(persistent) fstype jfs2

device filename   adapter  path  size  proto  state   clone  lun path
backing Snapshot
----------------  -------  ----  ----  -----  -----   -----  --------
---------
/dev/sdn             -      P    108m  iscsi  online   No
storage_array1:/vol/vol2/testfs1_SdLun         -
/dev/sdn1             -      P    108m  fcp  online   No
storage_array1:/vol/vol2/testfs1_SdLun1         -

0002-719 Warning: SD.Storage.Read access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mngr_server
```

John è autorizzato ad elencare le entità di storage su vol2 ma non su vol1. SnapDrive per UNIX visualizza le entità di vol1 e un messaggio di avviso per vol2.

> Per `storage list`, `storage show`, `snap list`, e. `snap show` Commands SnapDrive per UNIX visualizza un avviso invece di un errore.

Funzionamento con più server console Operations Manager che gestiscono i sistemi storage

Il seguente output mostra il messaggio di errore che si riceve quando i sistemi storage sono gestiti dalla console di Multiple Operations Manager.

```
[root]# snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6
-lun storage_array2:/vol/vol1/lun2 -lunsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager
server ops_mngr_server1
SD.Storage.Write access denied on volume storage_array2:/vol/vol1 for user
unix_host\root on Operations Manager server ops_mngr_server2
```

storage_array1 è gestito da ops_mngr_server1 e storage_array2 è gestito da ops_mngr_server2. L'amministratore di unix_host non è autorizzato a creare filespecs su storage_array1 e storage_array2. Nell'esempio precedente, SnapDrive per UNIX visualizza la console di Operations Manager utilizzata per determinare l'accesso.