Configurare RBAC (role-based access control)

SnapCenter Software 6.0

NetApp
January 31, 2025

Sommario

Configurare RBAC (role-based access control)

Aggiungere un utente o un gruppo e assegnare ruolo e risorse

Per configurare il controllo degli accessi basato sui ruoli per gli utenti SnapCenter, è possibile aggiungere utenti o gruppi e assegnare un ruolo. Il ruolo determina le opzioni a cui gli utenti SnapCenter possono accedere.

Prima di iniziare

- È necessario aver effettuato l'accesso come ruolo "SnapCenterAdmin".
- È necessario aver creato gli account utente o di gruppo in Active Directory nel sistema operativo o nel database. Non è possibile utilizzare SnapCenter per creare questi account.

  È possibile includere solo i seguenti caratteri speciali nei nomi degli utenti e dei gruppi: Spazio ( ), trattino (-), trattino basso (_) e due punti (:).

- SnapCenter include diversi ruoli predefiniti.

  È possibile assegnare questi ruoli all'utente o crearne di nuovi.

- Gli utenti AD e i gruppi ad aggiunti a RBAC SnapCenter devono disporre dell'autorizzazione DI LETTURA sul container utenti e sul container computer in Active Directory.
- Dopo aver assegnato un ruolo a un utente o a un gruppo che contiene le autorizzazioni appropriate, è necessario assegnare all'utente l'accesso alle risorse SnapCenter, ad esempio host e connessioni storage.

  In questo modo, gli utenti possono eseguire le azioni per le quali dispongono delle autorizzazioni per le risorse ad essi assegnate.

- È necessario assegnare un ruolo all'utente o al gruppo per sfruttare le autorizzazioni e le efficienze RBAC.
- È possibile assegnare risorse come host, gruppi di risorse, policy, connessione allo storage, plug-in, e all'utente durante la creazione dell'utente o del gruppo.
- Le risorse minime che è necessario assegnare a un utente per eseguire determinate operazioni sono le seguenti:

Operazione	Assegnazione delle risorse
Proteggere le risorse	host, policy
Backup	host, gruppo di risorse, policy
Ripristinare	host, gruppo di risorse
Clonare	host, gruppo di risorse, policy
Ciclo di vita dei cloni	host

Operazione	Assegnazione delle risorse
Creare un gruppo di risorse	host

- Quando un nuovo nodo viene aggiunto a un cluster Windows o a una risorsa DAG (Exchange Server Database Availability Group) e se questo nuovo nodo viene assegnato a un utente, è necessario riassegnare la risorsa all'utente o al gruppo per includere il nuovo nodo all'utente o al gruppo.

  È necessario riassegnare l'utente o il gruppo RBAC al cluster o al DAG per includere il nuovo nodo all'utente o al gruppo RBAC. Ad esempio, si dispone di un cluster a due nodi ed è stato assegnato un utente o un gruppo RBAC al cluster. Quando si aggiunge un altro nodo al cluster, è necessario riassegnare l'utente o il gruppo RBAC al cluster per includere il nuovo nodo per l'utente o il gruppo RBAC.

- Se si intende replicare le istantanee, è necessario assegnare la connessione di archiviazione per il volume di origine e di destinazione all'utente che esegue l'operazione.

  Aggiungere le risorse prima di assegnare l'accesso agli utenti.

Se si utilizza il plug-in SnapCenter per le funzioni di VMware vSphere per proteggere macchine virtuali, VMDK o datastore, è necessario utilizzare l'interfaccia utente di VMware vSphere per aggiungere un utente vCenter a un plug-in SnapCenter per il ruolo di VMware vSphere. Per informazioni sui ruoli VMware vSphere, vedere "Ruoli predefiniti in pacchetto con il plug-in SnapCenter per VMware vSphere".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **utenti e accesso** > * *.
3. Nella pagina Add Users/Groups from Active Directory or Workgroup (Aggiungi utenti/gruppi da Active Directory o Workgroup):

Per questo campo…	Eseguire questa operazione…
Tipo di accesso	Selezionare Domain (dominio) o Workgroup (gruppo di lavoro) Per il tipo di autenticazione dominio, specificare il nome di dominio dell'utente o del gruppo a cui si desidera aggiungere l'utente a un ruolo. Per impostazione predefinita, viene compilato con il nome di dominio connesso. È necessario registrare il dominio non attendibile nella pagina **Impostazioni** > **Impostazioni globali** > **Impostazioni dominio**.

Per questo campo…	Eseguire questa operazione…
Tipo	Selezionare User (utente) o Group (Gruppo) SnapCenter supporta solo il gruppo di sicurezza e non il gruppo di distribuzione.
Nome utente	a. Digitare il nome utente parziale, quindi fare clic su **Aggiungi**. Il nome utente fa distinzione tra maiuscole e minuscole. b. Selezionare il nome utente dall'elenco di ricerca. Quando si aggiungono utenti da un dominio diverso o da un dominio non attendibile, è necessario digitare completamente il nome utente, in quanto non esiste un elenco di ricerca per gli utenti di più domini. Ripetere questo passaggio per aggiungere altri utenti o gruppi al ruolo selezionato.
Ruoli	Selezionare il ruolo a cui si desidera aggiungere l'utente.

4. Fare clic su **Assegna**, quindi nella pagina Assegna risorse:
   a. Selezionare il tipo di risorsa dall'elenco a discesa **risorsa**.
   b. Nella tabella Asset, selezionare la risorsa.

      Le risorse vengono elencate solo se l'utente ha aggiunto le risorse a SnapCenter.

   c. Ripetere questa procedura per tutte le risorse richieste.
   d. Fare clic su **Save** (Salva).
5. Fare clic su **Invia**.

Dopo aver aggiunto utenti o gruppi e aver assegnato ruoli, aggiornare l'elenco delle risorse.

Creare un ruolo

Oltre a utilizzare i ruoli SnapCenter esistenti, è possibile creare i propri ruoli e personalizzare le autorizzazioni.

Dovresti aver effettuato l'accesso come ruolo "SnapCenterAdmin".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **ruoli**.
3. Fare clic su .
4. Nella pagina Add role (Aggiungi ruolo), specificare un nome e una descrizione per il nuovo ruolo.

   È possibile includere solo i seguenti caratteri speciali nei nomi degli utenti e dei gruppi: Spazio ( ), trattino (-), trattino basso (_) e due punti (:).

5. Selezionare **tutti i membri di questo ruolo possono visualizzare gli oggetti degli altri membri** per consentire agli altri membri del ruolo di visualizzare risorse come volumi e host dopo l'aggiornamento dell'elenco delle risorse.

   Deselezionare questa opzione se non si desidera che i membri di questo ruolo vedano gli oggetti a cui sono assegnati altri membri.

   Quando questa opzione è attivata, l'assegnazione dell'accesso degli utenti agli oggetti o alle risorse non è necessaria se gli utenti appartengono allo stesso ruolo dell'utente che ha creato gli oggetti o le risorse.

6. Nella pagina autorizzazioni, selezionare le autorizzazioni che si desidera assegnare al ruolo o fare clic su **Seleziona tutto** per concedere tutte le autorizzazioni al ruolo.
7. Fare clic su **Invia**.

Aggiungere un ruolo RBAC ONTAP utilizzando i comandi di accesso di sicurezza

È possibile utilizzare i comandi di accesso di sicurezza per aggiungere un ruolo RBAC ONTAP quando i sistemi storage eseguono Clustered ONTAP.

Prima di iniziare

- Prima di creare un ruolo RBAC ONTAP per i sistemi storage che eseguono Clustered ONTAP, è necessario identificare quanto segue:
  - L'attività (o le attività) che si desidera eseguire
  - I privilegi richiesti per eseguire queste attività
- La configurazione di un ruolo RBAC richiede l'esecuzione delle seguenti azioni:
  - Concedere privilegi alle directory dei comandi e/o dei comandi.

    Esistono due livelli di accesso per ogni directory di comando: All-access e Read-only.

    È sempre necessario assegnare prima i privilegi di accesso completo.

  - Assegnare ruoli agli utenti.
  - Modificare la configurazione a seconda che i plug-in SnapCenter siano collegati all'IP dell'amministratore del cluster per l'intero cluster o direttamente a una SVM all'interno del cluster.

A proposito di questa attività

Per semplificare la configurazione di questi ruoli nei sistemi storage, è possibile utilizzare il tool RBAC User Creator for Data ONTAP, disponibile nel forum delle community NetApp.

Questo strumento gestisce automaticamente la corretta impostazione dei privilegi ONTAP. Ad esempio, lo strumento RBAC User Creator for Data ONTAP aggiunge automaticamente i privilegi nell'ordine corretto in modo che i privilegi di accesso completo vengano visualizzati per primi. Se si aggiungono prima i privilegi di sola lettura e poi i privilegi di accesso completo, ONTAP contrassegna i privilegi di accesso completo come duplicati e li ignora.

Se in seguito si aggiorna SnapCenter o ONTAP, eseguire nuovamente lo strumento RBAC User Creator for Data ONTAP per aggiornare i ruoli utente creati in precedenza. I ruoli utente creati per una versione precedente di SnapCenter o ONTAP non funzionano correttamente con le versioni aggiornate. Quando si esegue di nuovo, lo strumento gestisce automaticamente l'aggiornamento. Non è necessario ricreare i ruoli.

Per ulteriori informazioni sull'impostazione dei ruoli RBAC di ONTAP, vedere "Autenticazione amministratore di ONTAP 9 e guida all'alimentazione RBAC".

Per coerenza, la documentazione di SnapCenter fa riferimento ai ruoli come all'utilizzo dei privilegi. L'interfaccia utente grafica di Gestore di sistema di OnCommand utilizza il termine *attribute* invece di *Privilege*. Quando si impostano i ruoli RBAC di ONTAP, entrambi questi termini significano la stessa cosa.

Fasi

1. Nel sistema di storage, creare un nuovo ruolo immettendo il seguente comando:

   ```
   security login role create <role_name\> -cmddirname "command" -access all
   -vserver <svm_name\>
   ```

   - nome_svm è il nome della SVM. Se si lascia questo campo vuoto, per impostazione predefinita viene visualizzato l'amministratore del cluster.
   - role_name è il nome specificato per il ruolo.
   - Command è la funzionalità ONTAP.

     È necessario ripetere questo comando per ogni autorizzazione. Tenere presente che i comandi all-access devono essere elencati prima dei comandi di sola lettura.

   Per informazioni sull'elenco delle autorizzazioni, vedere "Comandi dell'interfaccia utente di ONTAP per la creazione di ruoli e l'assegnazione delle autorizzazioni".

2. Creare un nome utente immettendo il seguente comando:

   ```
   security login create -username <user_name\> -application ontapi -authmethod
   <password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
   "user_description"
   ```

   - user_name è il nome dell'utente che si sta creando.
   - <password> è la tua password. Se non si specifica una password, il sistema ne richiederà una.

- nome_svm è il nome della SVM.

3. Assegnare il ruolo all'utente immettendo il seguente comando:

```
security login modify username <user_name\> –vserver <svm_name\> -role
<role_name\> -application ontapi -application console -authmethod <password\>
```

   - <user_name> è il nome dell'utente creato al punto 2. Questo comando consente di modificare l'utente per associarlo al ruolo.
   - <svm_name> è il nome della SVM.
   - <role_name> è il nome del ruolo creato nella fase 1.
   - <password> è la tua password. Se non si specifica una password, il sistema ne richiederà una.

4. Verificare che l'utente sia stato creato correttamente immettendo il seguente comando:

```
security login show –vserver <svm_name\> -user-or-group-name <user_name\>
```

   User_name è il nome dell'utente creato nel passaggio 3.

Creare ruoli SVM con privilegi minimi

Quando si crea un ruolo per un nuovo utente SVM in ONTAP, è necessario eseguire diversi comandi dell'interfaccia utente di ONTAP. Questo ruolo è necessario se si configurano le SVM in ONTAP per l'utilizzo con SnapCenter e non si desidera utilizzare il ruolo vsadmin.

Fasi

1. Nel sistema di storage, creare un ruolo e assegnare tutte le autorizzazioni al ruolo.

```
security login role create –vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```

   Ripetere questo comando per ogni autorizzazione.

2. Creare un utente e assegnarne il ruolo.

```
security login create -user <user_name\> -vserver <svm_name\> -application
ontapi -authmethod password -role <SVM_Role_Name\>
```

3. Liberare l'utente.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

Comandi dell'interfaccia utente di ONTAP per la creazione di ruoli SVM e l'assegnazione delle autorizzazioni

Esistono diversi comandi dell'interfaccia utente di ONTAP da eseguire per creare ruoli SVM e assegnare autorizzazioni.

A partire da 5,0, gli utenti amministrativi dei vserver sono supportati solo con API REST. Se si desidera creare ruoli utilizzando un amministratore non vserver, è necessario utilizzare ZAPI.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"volume clone split stop" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname`

"nvme subsystem delete" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

Creare ruoli cluster ONTAP con privilegi minimi

È necessario creare un ruolo di cluster ONTAP con privilegi minimi in modo da non dover utilizzare il ruolo di amministratore di ONTAP per eseguire operazioni in SnapCenter. È possibile eseguire diversi comandi dell'interfaccia utente di ONTAP per creare il ruolo del cluster ONTAP e assegnare privilegi minimi.

Fasi

1. Nel sistema di storage, creare un ruolo e assegnare tutte le autorizzazioni al ruolo.

   ```
   security login role create –vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   Ripetere questo comando per ogni autorizzazione.

2. Creare un utente e assegnarne il ruolo.

   ```
   security login create -user <user_name\> -vserver <cluster_name\> -application
   ontapi -authmethod password -role <role_name\>
   ```

3. Liberare l'utente.

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

Comandi dell'interfaccia utente di ONTAP per la creazione di ruoli cluster e l'assegnazione delle autorizzazioni

Esistono diversi comandi dell'interfaccia utente di ONTAP da eseguire per creare ruoli cluster e assegnare autorizzazioni.

> A partire da SnapCenter 5,0, gli utenti degli amministratori del cluster sono supportati solo con API REST. Se si desidera creare ruoli utilizzando un amministratore non cluster, è necessario utilizzare ZAPI.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"lun igroup modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly

- `security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all`
- `security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"system node show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

"vserver create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all

Configurare i pool di applicazioni IIS per abilitare le autorizzazioni di lettura di Active Directory

È possibile configurare Internet Information Services (IIS) sul server Windows per creare un account pool di applicazioni personalizzato quando è necessario attivare le autorizzazioni di lettura di Active Directory per SnapCenter.

Fasi

1. Aprire Gestione IIS sul server Windows in cui è installato SnapCenter.
2. Nel riquadro di spostamento di sinistra, fare clic su **Application Pools**.
3. Selezionare SnapCenter nell'elenco Pool di applicazioni, quindi fare clic su **Impostazioni avanzate** nel riquadro delle azioni.
4. Selezionare identità, quindi fare clic su **…** per modificare l'identità del pool di applicazioni SnapCenter.
5. Nel campo Custom account (account personalizzato), immettere un nome utente di dominio o un nome account admin di dominio con l'autorizzazione di lettura di Active Directory.
6. Fare clic su OK.

   L'account personalizzato sostituisce l'account ApplicationPoolIdentity incorporato per il pool di applicazioni SnapCenter.

Informazioni sul copyright

Informazioni sul marchio commerciale