Privilegi richiesti per le attività VSC

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

Sommario

Privilegi richiesti per le attività VSC . . . 1
Privilegio a livello di prodotto richiesto da VSC per VMware vSphere . . . 1
Controllo degli accessi basato sul ruolo di ONTAP per l'appliance virtuale per VSC, provider VASA e SRA . . . 1
Ruoli ONTAP consigliati quando si utilizza VSC per VMware vSphere . . . 3
Come configurare il controllo degli accessi basato sui ruoli di ONTAP per VSC per VMware vSphere . . . 4
Configurare i ruoli e i privilegi degli utenti . . . 5

Privilegi richiesti per le attività VSC

Le diverse attività di Virtual Storage Console per VMware vSphere richiedono diverse combinazioni di privilegi specifici per (VSC) e i privilegi nativi di vCenter Server.

Informazioni sui privilegi richiesti per le attività VSC sono disponibili nell'articolo della Knowledge base di NetApp 1032542.

"Come configurare RBAC per Virtual Storage Console"

Privilegio a livello di prodotto richiesto da VSC per VMware vSphere

Per accedere alla GUI di Virtual Storage Console per VMware vSphere, è necessario disporre del privilegio View specifico per VSC a livello di prodotto assegnato al livello di oggetto vSphere corretto. Se si effettua l'accesso senza questo privilegio, VSC visualizza un messaggio di errore quando si fa clic sull'icona NetApp e impedisce l'accesso a VSC.

Le seguenti informazioni descrivono il privilegio View a livello di prodotto VSC:

Privilegio	Descrizione	Livello di assegnazione
Visualizza	È possibile accedere alla GUI di VSC. Questo privilegio non consente di eseguire attività all'interno di VSC. Per eseguire qualsiasi attività VSC, è necessario disporre dei privilegi vCenter Server nativi e specifici di VSC corretti per tali attività.	Il livello di assegnazione determina le parti dell'interfaccia utente che è possibile visualizzare. L'assegnazione del privilegio View all'oggetto root (cartella) consente di accedere a VSC facendo clic sull'icona NetApp. È possibile assegnare il privilegio View a un altro livello di oggetto vSphere; tuttavia, ciò limita i menu VSC che è possibile visualizzare e utilizzare. L'oggetto root è la posizione consigliata per assegnare qualsiasi autorizzazione contenente il privilegio View.

Controllo degli accessi basato sul ruolo di ONTAP per l'appliance virtuale per VSC, provider VASA e SRA

Il RBAC (Role-Based Access Control) di ONTAP consente di controllare l'accesso a specifici sistemi storage e le azioni che un utente può eseguire su tali sistemi storage. Nella console di storage virtuale per VMware vSphere, ONTAP RBAC lavora con vCenter

Server RBAC per determinare quali attività possono essere eseguite da un utente specifico sugli oggetti di un sistema storage specifico.

VSC utilizza le credenziali (nome utente e password) impostate in VSC per autenticare ciascun sistema storage e determinare quali operazioni storage possono essere eseguite su tale sistema. VSC utilizza un set di credenziali per ciascun sistema storage. Queste credenziali determinano quali attività VSC possono essere eseguite su quel sistema di storage; in altre parole, le credenziali sono per VSC, non per un singolo utente VSC.

ONTAP RBAC si applica solo all'accesso ai sistemi storage e all'esecuzione di task VSC correlati allo storage, come il provisioning di macchine virtuali. Se non si dispone dei privilegi RBAC ONTAP appropriati per uno specifico sistema di storage, non è possibile eseguire attività su un oggetto vSphere ospitato su tale sistema di storage. È possibile utilizzare ONTAP RBAC insieme ai privilegi specifici di VSC per controllare quali attività di VSC possono essere eseguite da un utente:

- Monitoraggio e configurazione degli oggetti storage o vCenter Server che risiedono su un sistema storage
- Provisioning di oggetti vSphere residenti su un sistema storage

L'utilizzo di ONTAP RBAC con i privilegi specifici di VSC offre un livello di sicurezza orientato allo storage che l'amministratore dello storage può gestire. Di conseguenza, si dispone di un controllo degli accessi più dettagliato rispetto a quello supportato da solo da ONTAP RBAC o da solo da vCenter Server RBAC. Ad esempio, con vCenter Server RBAC, è possibile consentire a vCenterUserB di eseguire il provisioning di un datastore sullo storage, impedendo al contempo a vCenterUserA di eseguire il provisioning dei datastore. Se le credenziali del sistema di storage per un sistema di storage specifico non supportano la creazione di storage, né vCenterUserB né vCenterUserA possono eseguire il provisioning di un datastore su tale sistema di storage.

Quando si avvia un'attività VSC, VSC verifica innanzitutto se si dispone dell'autorizzazione vCenter Server corretta per tale attività. Se l'autorizzazione vCenter Server non è sufficiente per consentire l'esecuzione dell'attività, VSC non deve controllare i privilegi ONTAP per il sistema di storage in quanto non è stato superato il controllo di protezione iniziale di vCenter Server. Di conseguenza, non è possibile accedere al sistema di storage.

Se l'autorizzazione del server vCenter è sufficiente, VSC verifica i privilegi RBAC di ONTAP (il proprio ruolo ONTAP) associati alle credenziali del sistema di storage (nome utente e password) Per determinare se si dispone di privilegi sufficienti per eseguire le operazioni di storage richieste dall'attività VSC sul sistema di storage in questione. Se si dispone dei privilegi ONTAP corretti, è possibile accedere al sistema di storage ed eseguire l'attività VSC. I ruoli ONTAP determinano le attività VSC che è possibile eseguire sul sistema di storage.

A ciascun sistema storage è associato un set di privilegi ONTAP.

L'utilizzo di ONTAP RBAC e vCenter Server RBAC offre i seguenti vantaggi:

- Sicurezza

  L'amministratore può controllare quali utenti possono eseguire le attività a livello di oggetto vCenter Server e a livello di sistema di storage.

- Informazioni di audit

  In molti casi, VSC fornisce un audit trail sul sistema storage che consente di tenere traccia degli eventi all'utente di vCenter Server che ha eseguito le modifiche dello storage.

- Usabilità

  È possibile conservare tutte le credenziali del controller in un'unica posizione.

Ruoli ONTAP consigliati quando si utilizza VSC per VMware vSphere

È possibile impostare diversi ruoli ONTAP consigliati per lavorare con la console di storage virtuale per VMware vSphere e il RBAC (role-based access control). Questi ruoli contengono i privilegi di ONTAP necessari per eseguire le operazioni di storage richieste eseguite dalle attività (VSC).

Per creare nuovi ruoli utente, è necessario accedere come amministratore nei sistemi storage che eseguono ONTAP. È possibile creare ruoli ONTAP utilizzando una delle seguenti opzioni:

- 9.7 o versione successiva

  "Configurare i ruoli e i privilegi degli utenti"

- Tool RBAC User Creator per ONTAP (se si utilizza ONTAP 9.6 o versione precedente)

  "Tool RBAC User Creator per VSC, VASA Provider e Storage Replication Adapter 7.0 per VMware vSphere"

A ciascun ruolo di ONTAP è associata una coppia di nome utente e password, che costituiscono le credenziali del ruolo. Se non si effettua l'accesso utilizzando queste credenziali, non è possibile accedere alle operazioni di storage associate al ruolo.

Come misura di sicurezza, i ruoli ONTAP specifici del VSC sono ordinati gerarchicamente. Ciò significa che il primo ruolo è il ruolo più restrittivo e dispone solo dei privilegi associati al set più semplice di operazioni di storage VSC. Il ruolo successivo include sia i propri privilegi che tutti i privilegi associati al ruolo precedente. Ogni ruolo aggiuntivo è meno restrittivo per quanto riguarda le operazioni di storage supportate.

Di seguito sono riportati alcuni dei ruoli RBAC ONTAP consigliati quando si utilizza VSC. Dopo aver creato questi ruoli, è possibile assegnare i ruoli agli utenti che devono eseguire attività correlate allo storage, ad esempio il provisioning delle macchine virtuali.

1. Discovery (rilevamento)

   Questo ruolo consente di aggiungere sistemi storage.

2. Creare storage

   Questo ruolo consente di creare storage. Questo ruolo include anche tutti i privilegi associati al ruolo Discovery.

3. Modificare lo storage

   Questo ruolo consente di modificare lo storage. Questo ruolo include anche tutti i privilegi associati al ruolo Discovery e al ruolo Create Storage.

4. Distruggere lo storage

Questo ruolo consente di distruggere lo storage. Questo ruolo include anche tutti i privilegi associati al ruolo Discovery, al ruolo Create Storage e al ruolo Modify Storage.

Se si utilizza il provider VASA per ONTAP, è necessario impostare anche un ruolo di gestione basato su policy (PBM). Questo ruolo consente di gestire lo storage utilizzando le policy di storage. Questo ruolo richiede anche la configurazione del ruolo “DDiscovery”.

Come configurare il controllo degli accessi basato sui ruoli di ONTAP per VSC per VMware vSphere

Se si desidera utilizzare il controllo degli accessi basato sui ruoli con la console di storage virtuale per ONTAP vSphere (VSC), è necessario configurare RBAC (Role-Based Access Control) sul sistema storage. È possibile creare uno o più account utente personalizzati con privilegi di accesso limitati con la funzione RBAC di ONTAP.

VSC e SRA possono accedere ai sistemi storage a livello di cluster o di livello. Se si aggiungono sistemi storage a livello di cluster, è necessario fornire le credenziali dell’utente amministratore per fornire tutte le funzionalità richieste. Se si aggiungono i sistemi storage aggiungendo direttamente i dettagli, è necessario tenere presente che l’utente “vsadmin” non dispone di tutti i ruoli e le funzionalità necessari per eseguire determinate attività.

IL provider VASA può accedere ai sistemi storage solo a livello di cluster. Se il provider VASA è richiesto per un controller storage specifico, il sistema storage deve essere aggiunto a VSC a livello di cluster anche se si utilizza VSC o SRA.

Per creare un nuovo utente e connettere un cluster o un a VSC, VASA Provider e SRA, attenersi alla seguente procedura:

- Creare un ruolo di amministratore o amministratore del cluster

  Per creare questi ruoli, è possibile utilizzare una delle seguenti opzioni:

  - Gestore di sistema di ONTAP 9.7 o versione successiva

  "Configurare i ruoli e i privilegi degli utenti"

  - Tool RBAC User Creator per ONTAP (se si utilizza ONTAP 9.6 o versione precedente)

  "Tool RBAC User Creator per VSC, VASA Provider e Storage Replication Adapter 7.0 per VMware vSphere"

- Creare utenti con il ruolo assegnato e il set di applicazioni appropriato utilizzando ONTAP

  Queste credenziali del sistema storage sono necessarie per configurare i sistemi storage per VSC. È possibile configurare i sistemi storage per VSC immettendo le credenziali in VSC. Ogni volta che si accede a un sistema storage con queste credenziali, si disporranno delle autorizzazioni per le funzioni VSC configurate in ONTAP durante la creazione delle credenziali.

- Aggiungere il sistema storage a VSC e fornire le credenziali dell’utente appena creato

Ruoli VSC

VSC classifica i privilegi ONTAP nel seguente set di ruoli VSC:

- Discovery (rilevamento)

  Attiva il rilevamento di tutti i controller di storage collegati

- Creare storage

  Consente la creazione di volumi e LUN (Logical Unit Number)

- Modificare lo storage

  Consente il ridimensionamento e la deduplica dei sistemi storage

- Distruggere lo storage

  Consente la distruzione di volumi e LUN

Ruoli del provider VASA

È possibile creare solo la gestione basata su policy a livello di cluster. Questo ruolo consente la gestione dello storage basata su policy utilizzando i profili delle funzionalità di storage.

Ruoli SRA

SRA classifica i privilegi ONTAP in un ruolo SAN o NAS a livello di cluster o di livello. Ciò consente agli utenti di eseguire operazioni SRM.

> Per configurare manualmente i ruoli e i privilegi utilizzando i comandi di ONTAP, consultare gli articoli della Knowledge base.

- "Configurazione RBAC di VSC, VASA e SRA 7.0 ONTAP"
- "Eseguire il rollup di tutti i comandi per VSC e SRA per il livello di SVM"

Quando si aggiunge il cluster a VSC, VSC esegue una convalida iniziale dei privilegi dei ruoli RBAC di ONTAP. Se è stato aggiunto un IP di storage diretto, VSC non esegue la convalida iniziale. VSC controlla e applica i privilegi in un secondo momento nel flusso di lavoro delle attività.

Configurare i ruoli e i privilegi degli utenti

È possibile configurare nuovi ruoli utente per la gestione dei sistemi storage utilizzando il file JSON fornito con l'appliance virtuale per VSC, provider VASA, SRA e Gestore di sistema ONTAP.

Prima di iniziare

- Il file dei privilegi ONTAP dovrebbe essere stato scaricato dall'appliance virtuale per VSC, provider VASA e SRA utilizzando `https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`.
- È necessario aver configurato Gestore di sistema di ONTAP 9.7.

- Si dovrebbe aver effettuato l'accesso con privilegi di amministratore per il sistema di storage.

fasi

1. Decomprimere il scaricato `https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip` file.
2. Accedere a Gestore di sistema di ONTAP.
3. Fare clic su **CLUSTER › Impostazioni › utenti e ruoli**.
4. Fare clic su **Add User** (Aggiungi utente).
5. Nella finestra di dialogo **Aggiungi utente**, selezionare **prodotti di virtualizzazione**.
6. Fare clic su **Browse** (Sfoglia) per selezionare e caricare il file ONTAP Privileges JSON.

   Il campo DEL PRODOTTO viene compilato automaticamente.

7. Selezionare la funzionalità desiderata dal menu a discesa **PRODUCT CAPABILITY** (FUNZIONALITÀ DEL PRODOTTO).

   Il campo **ROLE** viene compilato automaticamente in base alla funzionalità del prodotto selezionata.

8. Immettere il nome utente e la password richiesti.
9. Selezionare i privilegi (Discovery, Create Storage, Modify Storage, Destroy Storage) richiesti per l'utente, quindi fare clic su **Add** (Aggiungi).

Risultati

Il nuovo ruolo e l'utente vengono aggiunti e i privilegi dettagliati vengono visualizzati sotto il ruolo configurato.