Controllo degli accessi in base al ruolo

ONTAP tools for VMware vSphere 10.1

NetApp
June 21, 2024

Sommario

Controllo degli accessi in base al ruolo

Panoramica sul role-based access control nei tool ONTAP per VMware vSphere

VCenter Server offre RBAC (role-based access control) che consente di controllare l'accesso agli oggetti vSphere. VCenter Server fornisce servizi di autenticazione e autorizzazione centralizzati a diversi livelli all'interno del proprio inventario, utilizzando i diritti degli utenti e dei gruppi con ruoli e privilegi. VCenter Server è dotato di cinque componenti principali per la gestione di RBAC:

Componenti	Descrizione
Privilegi	Un privilegio abilita o nega l'accesso per eseguire azioni in vSphere.
Ruoli	Un ruolo contiene uno o più privilegi di sistema in cui ogni privilegio definisce un diritto amministrativo per un determinato oggetto o tipo di oggetto nel sistema. Assegnando a un utente un ruolo, l'utente eredita le capacità dei privilegi definiti in quel ruolo.
Utenti e gruppi	Gli utenti e i gruppi vengono utilizzati nelle autorizzazioni per assegnare i ruoli da Active Directory (ad). VCenter Server dispone dei propri utenti e gruppi locali che è possibile utilizzare.
Permessi	Le autorizzazioni consentono di assegnare privilegi a utenti o gruppi per eseguire determinate azioni e apportare modifiche agli oggetti all'interno di vCenter Server. Le autorizzazioni di vCenter Server interessano solo gli utenti che accedono a vCenter Server anziché gli utenti che accedono direttamente a un host ESXi.
Oggetto	Un'entità su cui vengono eseguite le azioni. Gli oggetti VMware vCenter sono data center, cartelle, pool di risorse, cluster, host, e VM

Per completare correttamente un'attività, è necessario disporre dei ruoli vCenter Server RBAC appropriati. Durante un'attività, gli strumenti ONTAP per VMware vSphere controllano i ruoli vCenter Server di un utente prima di controllare i privilegi ONTAP dell'utente.

I ruoli di vCenter Server si applicano agli strumenti ONTAP per gli utenti di VMware vSphere vCenter, non agli amministratori. Per impostazione predefinita, gli amministratori hanno accesso completo al prodotto e non richiedono l'assegnazione di ruoli.

Gli utenti e i gruppi accedono a un ruolo facendo parte di un ruolo vCenter Server.

Punti chiave sull'assegnazione e la modifica di ruoli per vCenter Server

È necessario impostare i ruoli di vCenter Server solo se si desidera limitare l'accesso a oggetti e task vSphere.

In caso contrario, è possibile accedere come amministratore. Questo login consente di accedere automaticamente a tutti gli oggetti vSphere.

L'assegnazione di un ruolo determina gli strumenti ONTAP per le attività di VMware vSphere che un utente può eseguire. È possibile modificare un ruolo alla volta. Se si modificano i privilegi all'interno di un ruolo, l'utente associato a tale ruolo dovrebbe disconnettersi e quindi riconnettersi per abilitare il ruolo aggiornato.

Ruoli standard forniti con strumenti ONTAP per VMware vSphere

Per semplificare l'utilizzo dei privilegi di vCenter Server e RBAC, i tool ONTAP per VMware vSphere forniscono tool ONTAP standard per i ruoli VMware vSphere che consentono di eseguire tool ONTAP chiave per i task VMware vSphere. Esiste anche un ruolo di sola lettura che consente di visualizzare le informazioni, ma non di eseguire attività.

È possibile visualizzare gli strumenti ONTAP per i ruoli standard di VMware vSphere facendo clic su **ruoli** nella home page del client vSphere. I ruoli forniti dai tool ONTAP per VMware vSphere consentono di eseguire le seguenti attività:

Ruolo	Descrizione
Strumenti NetApp ONTAP per l'amministratore di VMware vSphere	Fornisce tutti i privilegi nativi di vCenter Server e i privilegi specifici degli strumenti ONTAP necessari per eseguire alcuni degli strumenti ONTAP per le attività di VMware vSphere.
Tool NetApp ONTAP per VMware vSphere in sola lettura	Fornisce accesso in sola lettura agli strumenti ONTAP. Questi utenti non possono eseguire strumenti ONTAP per le azioni VMware vSphere controllate dall'accesso.
Tool NetApp ONTAP per il provisioning di VMware vSphere	Fornisce alcuni dei privilegi nativi di vCenter Server e dei privilegi specifici degli strumenti ONTAP necessari per il provisioning dello storage. È possibile eseguire le seguenti operazioni: • Creare nuovi datastore • Gestire i datastore

Il ruolo di amministratore di ONTAP Tools Manager non è registrato in vCenter Server. Questo ruolo è specifico del gestore strumenti ONTAP.

Se la tua azienda richiede l'implementazione di ruoli più restrittivi degli strumenti ONTAP standard per i ruoli VMware vSphere, puoi utilizzare gli strumenti ONTAP per i ruoli VMware vSphere per creare nuovi ruoli.

In questo caso, è necessario clonare gli strumenti ONTAP necessari per i ruoli VMware vSphere e quindi modificare il ruolo clonato in modo che disponga solo dei privilegi richiesti dall'utente.

Autorizzazioni per backend di storage ONTAP e oggetti vSphere

Se l'autorizzazione vCenter Server è sufficiente, gli strumenti ONTAP per VMware vSphere controllano quindi i privilegi RBAC di ONTAP (il ruolo ONTAP) associati alle credenziali backend di storage (il nome utente e la password) per determinare se si dispone di privilegi sufficienti per eseguire le operazioni di storage richieste dai tool ONTAP per l'attività VMware vSphere su quel backend dello storage. Se si dispone dei privilegi ONTAP corretti, è possibile accedere a. Lo storage termina ed esegue tool ONTAP per i task VMware

vSphere. I ruoli ONTAP determinano i tool ONTAP per i task VMware vSphere che puoi eseguire sul backend dello storage.

Componenti delle autorizzazioni vCenter Server

VCenter Server riconosce le autorizzazioni e non i privilegi. Ogni autorizzazione vCenter Server è composta da tre componenti.

VCenter Server include i seguenti componenti:

- Uno o più privilegi (il ruolo)

  I privilegi definiscono le attività che un utente può eseguire.

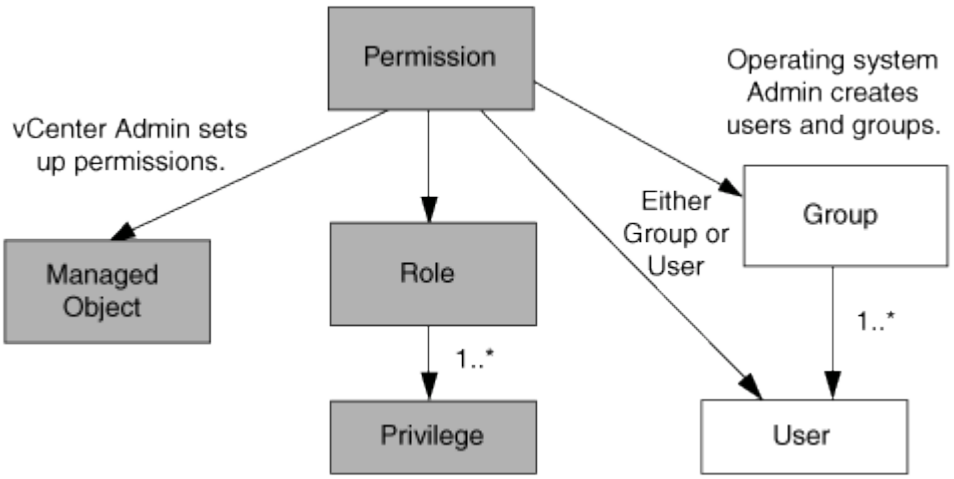
- Un oggetto vSphere

  L'oggetto è la destinazione delle attività.

- Un utente o un gruppo

  L'utente o il gruppo definisce chi può eseguire l'attività.

In questo diagramma, le caselle grigie indicano i componenti presenti in vCenter Server e le caselle bianche indicano i componenti presenti nel sistema operativo in cui è in esecuzione vCenter Server.



Privilegi

Due tipi di privilegi sono associati ai tool ONTAP per VMware vSphere:

- Privilegi vCenter Server nativi

  Questi privilegi vengono forniti con vCenter Server.

- Privilegi specifici per i tool ONTAP

  Questi privilegi sono definiti per strumenti ONTAP specifici per le attività VMware vSphere. Sono esclusivi

dei tool ONTAP per VMware vSphere.

Gli strumenti ONTAP per le attività VMware vSphere richiedono privilegi specifici di ONTAP e privilegi nativi di vCenter Server. Questi privilegi costituiscono “role” per l’utente. Un’autorizzazione può avere più privilegi. Questi privilegi sono riservati a un utente che ha effettuato l’accesso a vCenter Server.

> Per semplificare le operazioni con vCenter Server RBAC, gli strumenti ONTAP per VMware vSphere forniscono diversi ruoli standard che contengono tutti i privilegi nativi e specifici degli strumenti ONTAP necessari per eseguire gli strumenti ONTAP per i task VMware vSphere.

Se si modificano i privilegi all’interno di un’autorizzazione, l’utente associato a tale autorizzazione deve disconnettersi e quindi accedere per attivare l’autorizzazione aggiornata.

Oggetti vSphere

Le autorizzazioni sono associate agli oggetti vSphere, come vCenter Server, host ESXi, macchine virtuali, datastore, data center, e cartelle. È possibile assegnare autorizzazioni a qualsiasi oggetto vSphere. In base all’autorizzazione assegnata a un oggetto vSphere, vCenter Server determina chi può eseguire le attività su tale oggetto. Per gli strumenti ONTAP per attività specifiche di VMware vSphere, le autorizzazioni vengono assegnate e convalidate solo a livello di cartella principale (vCenter Server) e non su altre entità. Ad eccezione del funzionamento del plug-in VAAI, in cui le autorizzazioni vengono convalidate per l’host ESXi interessato.

Utenti e gruppi

È possibile utilizzare Active Directory (o la macchina vCenter Server locale) per configurare utenti e gruppi di utenti. È quindi possibile utilizzare le autorizzazioni di vCenter Server per concedere l’accesso a questi utenti o gruppi per consentire loro di eseguire strumenti ONTAP specifici per i task di VMware vSphere.

> Queste autorizzazioni di vCenter Server si applicano agli strumenti ONTAP per gli utenti di VMware vSphere vCenter, non agli strumenti ONTAP per gli amministratori di VMware vSphere. Per impostazione predefinita, gli strumenti ONTAP per gli amministratori di VMware vSphere dispongono dell’accesso completo al prodotto e non richiedono le autorizzazioni assegnate.

Gli utenti e i gruppi non hanno ruoli assegnati. Ottengono l’accesso a un ruolo facendo parte di un’autorizzazione vCenter Server.

Assegnare e modificare le autorizzazioni per vCenter Server

Esistono diversi punti chiave da tenere a mente quando si utilizzano le autorizzazioni di vCenter Server. Il successo di un’attività di ONTAP Tools per VMware vSphere dipende dalla posizione in cui è stata assegnata un’autorizzazione o dalle azioni intraprese da un utente dopo la modifica di un’autorizzazione.

Assegnazione delle autorizzazioni

È necessario impostare le autorizzazioni di vCenter Server solo se si desidera limitare l’accesso agli oggetti e alle attività di vSphere. In caso contrario, è possibile accedere come amministratore. Questo login consente di accedere automaticamente a tutti gli oggetti vSphere.

Il punto in cui si assegna l’autorizzazione determina gli strumenti ONTAP per le attività di VMware vSphere che un utente può eseguire.

A volte, per garantire il completamento di un'attività, è necessario assegnare un'autorizzazione a un livello superiore, ad esempio l'oggetto root. Questo accade quando un'attività richiede un privilegio che non si applica a un oggetto vSphere specifico (ad esempio, il monitoraggio dell'attività) o quando un privilegio richiesto si applica a un oggetto non vSphere (ad esempio, un sistema storage).

In questi casi, è possibile impostare un'autorizzazione in modo che venga ereditata dalle entità figlio. È inoltre possibile assegnare altre autorizzazioni alle entità figlio. L'autorizzazione assegnata a un'entità figlio sovrascrive sempre l'autorizzazione ereditata dall'entità padre. Ciò significa che è possibile assegnare autorizzazioni a un'entità figlio per limitare l'ambito di un'autorizzazione assegnata a un oggetto radice e ereditata dall'entità figlio.

A meno che le policy di sicurezza aziendali non richiedano autorizzazioni più restrittive, è consigliabile assegnare autorizzazioni all'oggetto root (anche noto come cartella root).

Permessi e oggetti non vSphere

L'autorizzazione creata viene applicata a un oggetto non vSphere. Ad esempio, un sistema storage non è un oggetto vSphere. Se un privilegio si applica a un sistema di storage, è necessario assegnare l'autorizzazione contenente tale privilegio agli strumenti ONTAP per l'oggetto root VMware vSphere, poiché non è possibile assegnarlo a un oggetto vSphere.

Ad esempio, qualsiasi autorizzazione che includa un privilegio come gli strumenti ONTAP per il privilegio "Aggiungi/Modifica/Salta sistemi di archiviazione" di VMware vSphere deve essere assegnata a livello dell'oggetto principale.

Modifica delle autorizzazioni

È possibile modificare un'autorizzazione alla volta.

Se si modificano i privilegi all'interno di un'autorizzazione, l'utente associato a tale autorizzazione deve disconnettersi e quindi accedere nuovamente per attivare l'autorizzazione aggiornata.

Privilegi richiesti per gli strumenti ONTAP per le attività VMware vSphere

I diversi strumenti ONTAP per le attività VMware vSphere richiedono diverse combinazioni di privilegi specifici per gli strumenti ONTAP per VMware vSphere e i privilegi nativi di vCenter Server.

Per accedere agli strumenti ONTAP per la GUI di VMware vSphere, è necessario disporre del privilegio View specifico dei tool ONTAP a livello di prodotto assegnato al livello di oggetto vSphere corretto. Se si accede senza questo privilegio, gli strumenti ONTAP per VMware vSphere visualizzano un messaggio di errore quando si fa clic sull'icona NetApp e si impedisce l'accesso agli strumenti ONTAP.

Nel privilegio **View**, è possibile accedere agli strumenti ONTAP per VMware vSphere. Questo privilegio non consente di eseguire attività all'interno degli strumenti ONTAP per VMware vSphere. Per eseguire qualsiasi strumento ONTAP per le attività VMware vSphere, è necessario disporre dei privilegi vCenter Server nativi e specifici per gli strumenti ONTAP per tali attività.

Il livello di assegnazione determina le parti dell'interfaccia utente che è possibile visualizzare. L'assegnazione del privilegio Visualizza all'oggetto principale (cartella) consente di accedere agli strumenti ONTAP per VMware vSphere facendo clic sull'icona NetApp.

È possibile assegnare il privilegio View a un altro livello di oggetto vSphere, tuttavia ciò limita gli strumenti ONTAP per i menu VMware vSphere che è possibile visualizzare e utilizzare.

L'oggetto root è la posizione consigliata per assegnare qualsiasi autorizzazione contenente il privilegio View.

Ruoli ONTAP consigliati per i tool ONTAP per VMware vSphere

È possibile impostare diversi ruoli ONTAP consigliati per lavorare con gli strumenti ONTAP per VMware vSphere e RBAC (role-based access control). Questi ruoli contengono i privilegi di ONTAP necessari per eseguire le operazioni di storage eseguite dai tool ONTAP per i task VMware vSphere.

Per creare nuovi ruoli utente, occorre accedere come amministratore dei sistemi storage che eseguono ONTAP. È possibile creare ruoli ONTAP utilizzando Gestione di sistema di ONTAP 9.8P1 o versioni successive.

Ogni ruolo ONTAP dispone di una coppia di nome utente e password associata, 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, gli strumenti ONTAP per i ruoli ONTAP specifici di VMware vSphere sono ordinati gerarchicamente. Ciò significa che il primo ruolo è il più restrittivo e dispone solo dei privilegi associati al set più elementare di tool ONTAP per le operazioni di storage di VMware vSphere. Il ruolo successivo include i propri privilegi e tutti i privilegi associati al ruolo precedente. Ogni ruolo aggiuntivo è meno restrittivo delle operazioni di storage supportate.

Di seguito sono elencati alcuni dei ruoli RBAC di ONTAP consigliati quando si utilizzano i tool ONTAP per VMware vSphere. Dopo aver creato questi ruoli, è possibile assegnarli agli utenti che devono eseguire attività correlate allo storage, ad esempio il provisioning di macchine virtuali.

Ruolo	**privilegi**
Discovery (rilevamento)	Questo ruolo consente di aggiungere sistemi storage.
Creare storage	Questo ruolo consente di creare storage. Questo ruolo include anche tutti i privilegi associati al ruolo di rilevamento.
Modificare lo storage	Questo ruolo consente di modificare lo storage. Questo ruolo include anche tutti i privilegi associati al ruolo di rilevamento e al ruolo Crea archivio.
Distruggere lo storage	Questo ruolo consente di distruggere lo storage. Questo ruolo include anche tutti i privilegi associati al ruolo di rilevamento, al ruolo Crea archivio e al ruolo Modifica archivio.

Se si utilizzano strumenti ONTAP per VMware vSphere, è necessario impostare anche un ruolo di gestione basata su criteri (PBM, Policy-Based Management). Questo ruolo consente di gestire lo storage utilizzando le policy di storage. Questo ruolo richiede anche la configurazione del ruolo "DDiscovery".