



RBAC con VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp

November 17, 2025

This PDF was generated from <https://docs.netapp.com/it-it/ontap-tools-vmware-vsphere-103/concepts/rbac-vcenter-environment.html> on November 17, 2025. Always check docs.netapp.com for the latest.

Sommario

- RBAC con VMware vSphere 1
 - Ambiente vCenter Server RBAC con tool ONTAP per VMware vSphere 10 1
 - Immagine di un'autorizzazione vCenter Server 1
 - Componenti di un'autorizzazione vCenter Server 2
 - USA vCenter Server RBAC con i tool ONTAP per VMware vSphere 10 2
 - Ruoli vCenter e account amministratore 2
 - Gerarchia di oggetti vSphere 3
 - Ruoli inclusi nei tool ONTAP per VMware vSphere 10 3
 - Oggetti vSphere e backend dello storage ONTAP 3
 - Utilizzo di vCenter Server RBAC 3

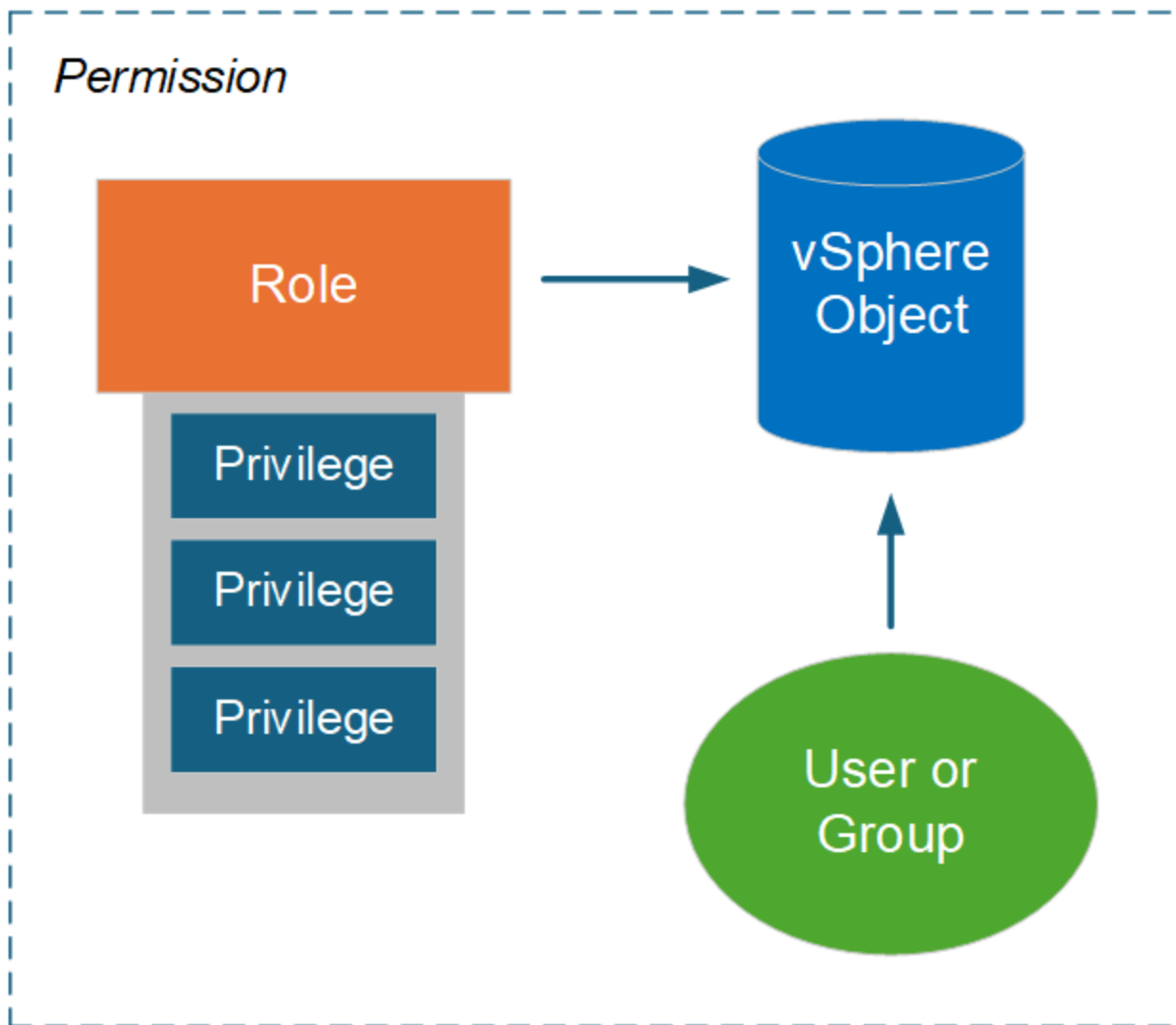
RBAC con VMware vSphere

Ambiente vCenter Server RBAC con tool ONTAP per VMware vSphere 10

VMware vCenter Server offre una funzionalità RBAC che consente di controllare l'accesso agli oggetti vSphere. Si tratta di una parte importante dei servizi di sicurezza per l'autenticazione e l'autorizzazione centralizzati di vCenter.

Immagine di un'autorizzazione vCenter Server

Un'autorizzazione è la base per applicare il controllo degli accessi nell'ambiente vCenter Server. Viene applicato a un oggetto vSphere con un utente o un gruppo incluso nella definizione dell'autorizzazione. Un'illustrazione di alto livello di un'autorizzazione vCenter è riportata nella figura seguente.



Componenti di un'autorizzazione vCenter Server

Un'autorizzazione vCenter Server è un pacchetto di diversi componenti che sono associati insieme quando viene creata l'autorizzazione.

Oggetti vSphere

Le autorizzazioni sono associate agli oggetti vSphere, come vCenter Server, host ESXi, macchine virtuali, datastore, data center e cartelle. In base alle autorizzazioni assegnate all'oggetto, vCenter Server determina quali azioni o attività possono essere eseguite sull'oggetto da ciascun utente o gruppo. Per le attività specifiche degli strumenti ONTAP per VMware vSphere, tutte le autorizzazioni vengono assegnate e convalidate a livello di cartella principale o principale di vCenter Server. Per ulteriori informazioni, vedere ["USA RBAC con server vCenter"](#).

Privileges e ruoli

Esistono due tipi di vSphere Privileges utilizzati con i tool ONTAP per VMware vSphere 10. Per semplificare le operazioni con RBAC in questo ambiente, gli strumenti ONTAP forniscono ruoli che contengono la Privileges nativa e personalizzata richiesta. Il Privileges include:

- Privilegi vCenter Server nativi

Si tratta del Privileges fornito da vCenter Server.

- Privilegi specifici per i tool ONTAP

Si tratta di un'esclusiva di Privileges personalizzata per i tool ONTAP per VMware vSphere.

Utenti e gruppi

È possibile definire utenti e gruppi utilizzando Active Directory o l'istanza locale di vCenter Server. Insieme a un ruolo, è possibile creare un'autorizzazione per un oggetto nella gerarchia degli oggetti vSphere. L'autorizzazione concede l'accesso in base all'Privileges nel ruolo associato. Tenere presente che i ruoli non vengono assegnati direttamente agli utenti in isolamento. Gli utenti e i gruppi ottengono invece l'accesso a un oggetto tramite Role Privileges come parte dell'autorizzazione più grande di vCenter Server.

USA vCenter Server RBAC con i tool ONTAP per VMware vSphere 10

Ci sono diversi aspetti dei tool ONTAP per l'implementazione RBAC di VMware vSphere 10 con vCenter Server che è necessario considerare prima di utilizzarlo in un ambiente di produzione.

Ruoli vCenter e account amministratore

È necessario definire e utilizzare i ruoli vCenter Server personalizzati solo se si desidera limitare l'accesso agli oggetti vSphere e alle attività amministrative associate. Se non è necessario limitare l'accesso, è possibile utilizzare un account amministratore. Ogni account amministratore viene definito con il ruolo Amministratore al livello superiore della gerarchia degli oggetti. In questo modo, si ottiene l'accesso completo agli oggetti vSphere, inclusi quelli aggiunti dai tool ONTAP per VMware vSphere 10.

Gerarchia di oggetti vSphere

L'inventario degli oggetti vSphere è organizzato in una gerarchia. Ad esempio, è possibile spostare la gerarchia in basso come segue:

```
vCenter Server --> Datacenter --> Cluster --> Virtual Machine> ESXi host
```

Tutte le autorizzazioni vengono convalidate nella gerarchia di oggetti vSphere ad eccezione delle operazioni del plug-in VAAI, che vengono convalidate rispetto all'host ESXi di destinazione.

Ruoli inclusi nei tool ONTAP per VMware vSphere 10

Per semplificare le operazioni con vCenter Server RBAC, gli strumenti ONTAP per VMware vSphere offrono ruoli predefiniti personalizzati in base a diverse attività amministrative.



Se necessario, è possibile creare nuovi ruoli personalizzati. In questo caso, è necessario clonare uno dei ruoli degli strumenti ONTAP esistenti e modificarlo secondo necessità. Dopo aver apportato le modifiche alla configurazione, gli utenti del client vSphere interessato devono disconnettersi e riconnettersi per attivare le modifiche.

Per visualizzare gli strumenti ONTAP per i ruoli VMware vSphere, selezionare **Menu** nella parte superiore del client vSphere e fare clic su **Amministrazione**, quindi **ruoli** a sinistra. Esistono tre ruoli predefiniti, come descritto di seguito.

Strumenti NetApp ONTAP per l'amministratore di VMware vSphere

Fornisce tutti gli strumenti vCenter Server Privileges e ONTAP nativi, specifici per Privileges, necessari per eseguire i principali strumenti ONTAP per i task di amministrazione 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

Oggetti vSphere e backend dello storage ONTAP

I due ambienti RBAC lavorano insieme. Quando si esegue un'operazione nell'interfaccia client vSphere, vengono controllati per primi i ruoli degli strumenti ONTAP definiti in vCenter Server. Se l'operazione è consentita da vSphere, viene esaminata la Privileges ruolo ONTAP. Questa seconda fase viene eseguita in base al ruolo ONTAP assegnato all'utente al momento della creazione e della configurazione del backend di storage.

Utilizzo di vCenter Server RBAC

Quando si lavora con vCenter Server Privileges e con le autorizzazioni, è necessario prendere in considerazione alcuni aspetti.

Privilegi richiesti

Per accedere agli strumenti ONTAP per l'interfaccia utente di VMware vSphere 10, è necessario disporre del privilegio *View* specifico di ONTAP tools. Se si accede a vSphere senza questo privilegio e si fa clic sull'icona NetApp, gli strumenti di ONTAP per VMware vSphere visualizzano un messaggio di errore e impediscono l'accesso all'interfaccia utente.

Il livello di assegnazione nella gerarchia degli oggetti vSphere determina le parti dell'interfaccia utente a cui è possibile accedere. L'assegnazione del privilegio *View* all'oggetto root consente di accedere agli strumenti ONTAP per VMware vSphere facendo clic sull'icona NetApp.

È invece possibile assegnare il privilegio *View* a un altro livello di oggetto vSphere inferiore. Tuttavia, ciò limiterà gli strumenti ONTAP per i menu VMware vSphere a cui è possibile accedere e utilizzare.

Assegnazione delle autorizzazioni

Se si desidera limitare l'accesso agli oggetti e ai task vSphere, è necessario utilizzare le autorizzazioni di vCenter Server. Quando si assegna l'autorizzazione nella gerarchia degli oggetti vSphere, gli strumenti ONTAP per le attività di VMware vSphere 10 che gli utenti possono eseguire.



A meno che non sia necessario definire un accesso più restrittivo, in genere è buona norma assegnare autorizzazioni a livello dell'oggetto principale o della cartella principale.

Le autorizzazioni disponibili con i tool ONTAP per VMware vSphere 10 si applicano a oggetti non vSphere personalizzati, come i sistemi storage. Se possibile, è necessario assegnare queste autorizzazioni 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 "Aggiungi/Modifica/Rimuovi sistemi di archiviazione" degli strumenti ONTAP per VMware vSphere deve essere assegnata a livello di oggetto root.

Quando si definisce un'autorizzazione a un livello superiore nella gerarchia degli oggetti, è possibile configurarla in modo che venga trasferita e ereditata dagli oggetti figlio. Se necessario, è possibile assegnare autorizzazioni aggiuntive agli oggetti figlio che sovrascrivono le autorizzazioni ereditate dal padre.

È possibile modificare un'autorizzazione in qualsiasi momento. Se si modifica uno dei Privileges all'interno di un'autorizzazione, gli utenti associati all'autorizzazione devono disconnettersi da vSphere e riconnettersi per abilitare la modifica.

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.