



Controllo degli accessi in base al ruolo

ONTAP tools for VMware vSphere 10

NetApp

September 30, 2025

This PDF was generated from https://docs.netapp.com/it-it/ontap-tools-vmware-vsphere-100/concepts/concept_vcenter_server_role_based_access_control_features_in_vsc_for_vmware_vsphere.html on September 30, 2025. Always check docs.netapp.com for the latest.

Sommario

- Controllo degli accessi in base al ruolo 1
 - Panoramica del controllo degli accessi basato sui ruoli negli strumenti ONTAP 1
 - Punti chiave sull'assegnazione e la modifica di ruoli per vCenter Server 1
 - Ruoli standard forniti con gli strumenti ONTAP 2
 - Autorizzazioni per backend di storage ONTAP e oggetti vSphere 2
 - Ruoli ONTAP consigliati quando si utilizzano gli strumenti ONTAP per VMware vSphere 3

Controllo degli accessi in base al ruolo

Panoramica del controllo degli accessi basato sui ruoli negli strumenti ONTAP

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) o anche da utenti/gruppi Windows potenzialmente locali (sconsigliato)
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 controllano i ruoli vCenter Server di un utente prima di controllare i privilegi ONTAP dell'utente.



I ruoli vCenter Server si applicano agli utenti vCenter degli strumenti ONTAP, 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.

Quando si assegna un ruolo, vengono determinate le attività degli strumenti ONTAP 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 gli strumenti ONTAP

Per semplificare le operazioni con i privilegi di vCenter Server e RBAC, gli strumenti ONTAP forniscono ruoli standard degli strumenti ONTAP che consentono di eseguire attività chiave degli strumenti ONTAP. Esiste anche un ruolo di sola lettura che consente di visualizzare le informazioni, ma non di eseguire attività.

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

Ruolo	Descrizione
NetApp ONTAP Tools Amministratore	Fornisce tutti i privilegi nativi di vCenter Server e i privilegi specifici degli strumenti ONTAP necessari per eseguire alcune delle attività degli strumenti ONTAP.
Strumenti NetApp ONTAP di sola lettura	Fornisce accesso in sola lettura agli strumenti ONTAP. Questi utenti non possono eseguire alcuna azione di ONTAP Tools controllata dall'accesso.
Provisioning degli strumenti di NetApp ONTAP	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: <ul style="list-style-type: none">• Creare nuovi datastore• Gestire i datastore

Il ruolo di amministratore dell'interfaccia utente di Manager non è registrato in vCenter. Questo ruolo è specifico dell'interfaccia utente del manager.

Se l'azienda richiede l'implementazione di ruoli più restrittivi rispetto ai ruoli standard degli strumenti ONTAP, è possibile utilizzare i ruoli degli strumenti ONTAP per creare nuovi ruoli.

In questo caso, clonare i ruoli degli strumenti ONTAP necessari e 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 controllano 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 dall'attività degli strumenti ONTAP su quel backend dello storage. Se si dispone dei privilegi ONTAP corretti, è possibile accedere a. Lo storage termina ed esegue l'attività degli strumenti ONTAP. I ruoli ONTAP determinano le attività degli strumenti ONTAP che puoi eseguire sul backend dello storage.

Ruoli ONTAP consigliati quando si utilizzano gli strumenti 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 necessarie eseguite dalle attività degli strumenti ONTAP.

Per creare nuovi ruoli utente, è necessario accedere come amministratore nei sistemi storage che eseguono ONTAP. È possibile creare ruoli ONTAP utilizzando Gestione di sistema di ONTAP 9.8P1 o versioni successive. Vedere ["Elenco dei privilegi minimi richiesti per gli utenti cluster con ambito globale non amministratori"](#) per ulteriori informazioni.

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 degli strumenti ONTAP vengono 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 degli strumenti ONTAP. 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 utilizzano gli strumenti ONTAP. 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".

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.