Controllo degli accessi in base al ruolo

ONTAP tools for VMware vSphere 10

NetApp
August 25, 2025

This PDF was generated from https://docs.netapp.com/it-it/ontap-tools-vmware-vsphere-10/concepts/rbac-learn-about.html on August 25, 2025. Always check docs.netapp.com for the latest.

Sommario

Controllo degli accessi in base al ruolo . . . 1
- Scopri i tool ONTAP per VMware vSphere 10 RBAC . . . 1
  - Componenti RBAC . . . 1
  - Due ambienti RBAC . . . 2
- RBAC con VMware vSphere . . . 2
  - Ambiente vCenter Server RBAC con tool ONTAP per VMware vSphere 10 . . . 2
  - USA vCenter Server RBAC con i tool ONTAP per VMware vSphere 10 . . . 4
- RBAC con ONTAP . . . 6
  - Ambiente RBAC ONTAP con tool ONTAP per VMware vSphere 10 . . . 6
  - USA RBAC ONTAP con tool ONTAP per VMware vSphere 10 . . . 7

Controllo degli accessi in base al ruolo

Scopri i tool ONTAP per VMware vSphere 10 RBAC

RBAC (role-based access control) è un framework di sicurezza per controllare l'accesso alle risorse all'interno di un'organizzazione. RBAC semplifica l'amministrazione definendo ruoli con specifici livelli di autorizzazione per eseguire azioni, invece di assegnare autorizzazioni a singoli utenti. I ruoli definiti vengono assegnati agli utenti, riducendo così il rischio di errori e semplificando la gestione del controllo degli accessi all'interno dell'organizzazione.

Il modello standard RBAC è composto da diverse tecnologie di implementazione o fasi di crescente complessità. Il risultato è che le effettive implementazioni RBAC, basate sulle esigenze dei fornitori di software e dei loro clienti, possono differire e variare da relativamente semplice a molto complesso.

Componenti RBAC

Ad un livello elevato, ci sono diversi componenti che sono generalmente inclusi in ogni implementazione RBAC. Questi componenti sono associati in modi diversi come parte della definizione dei processi di autorizzazione.

Privilegi

Un *privilegio* è un'azione o una capacità che può essere consentita o negata. Potrebbe trattarsi di qualcosa di semplice, come la possibilità di leggere un file, o di un'operazione più astratta, specifica di un determinato sistema software. I Privileges possono anche essere definiti per limitare l'accesso agli endpoint dell'API REST e ai comandi della CLI. Ogni implementazione RBAC include privilegi predefiniti e potrebbe anche consentire agli amministratori di creare privilegi personalizzati.

Ruoli

Un *ruolo* è un contenitore che include uno o più Privileges. I ruoli vengono generalmente definiti in base a attività o funzioni lavorative particolari. Quando un ruolo viene assegnato a un utente, all'utente viene concesso tutto il Privileges contenuto nel ruolo. Come per Privileges, le implementazioni includono ruoli predefiniti e in genere consentono la creazione di ruoli personalizzati.

Oggetti

Un *object* rappresenta una risorsa reale o astratta identificata nell'ambiente RBAC. Le azioni definite tramite Privileges vengono eseguite su o con gli oggetti associati. A seconda dell'implementazione, Privileges può essere concesso a un tipo di oggetto o a una specifica istanza di oggetto.

Utenti e gruppi

Users sono assegnati o associati a un ruolo applicato dopo l'autenticazione. Alcune implementazioni RBAC consentono di assegnare un solo ruolo a un utente, mentre altre consentono più ruoli per utente, magari con un solo ruolo attivo alla volta. L'assegnazione di ruoli a *gruppi* può semplificare ulteriormente l'amministrazione della protezione.

Permessi

Un *permesso* è una definizione che associa un utente o un gruppo insieme a un ruolo a un oggetto. Le autorizzazioni possono essere utili con un modello a oggetti gerarchico in cui possono essere eventualmente ereditate dai figli nella gerarchia.

Due ambienti RBAC

Esistono due distinti ambienti RBAC da prendere in considerazione quando si utilizzano i tool ONTAP per VMware vSphere 10.

VMware vCenter Server

L'implementazione RBAC in VMware vCenter Server viene utilizzata per limitare l'accesso agli oggetti esposti tramite l'interfaccia utente del client vSphere. Come parte dell'installazione dei tool ONTAP per VMware vSphere 10, l'ambiente RBAC viene esteso per includere oggetti aggiuntivi che rappresentano le funzionalità dei tool ONTAP. L'accesso a questi oggetti viene fornito tramite il plug-in remoto. Per ulteriori informazioni, vedere ."Ambiente RBAC vCenter Server"

Cluster ONTAP

I tool ONTAP per VMware vSphere 10 si collegano a un cluster ONTAP attraverso l'API REST ONTAP per eseguire operazioni relative allo storage. L'accesso alle risorse di storage viene controllato tramite un ruolo ONTAP associato all'utente ONTAP fornito durante l'autenticazione. Per ulteriori informazioni, vedere "Ambiente RBAC ONTAP" .

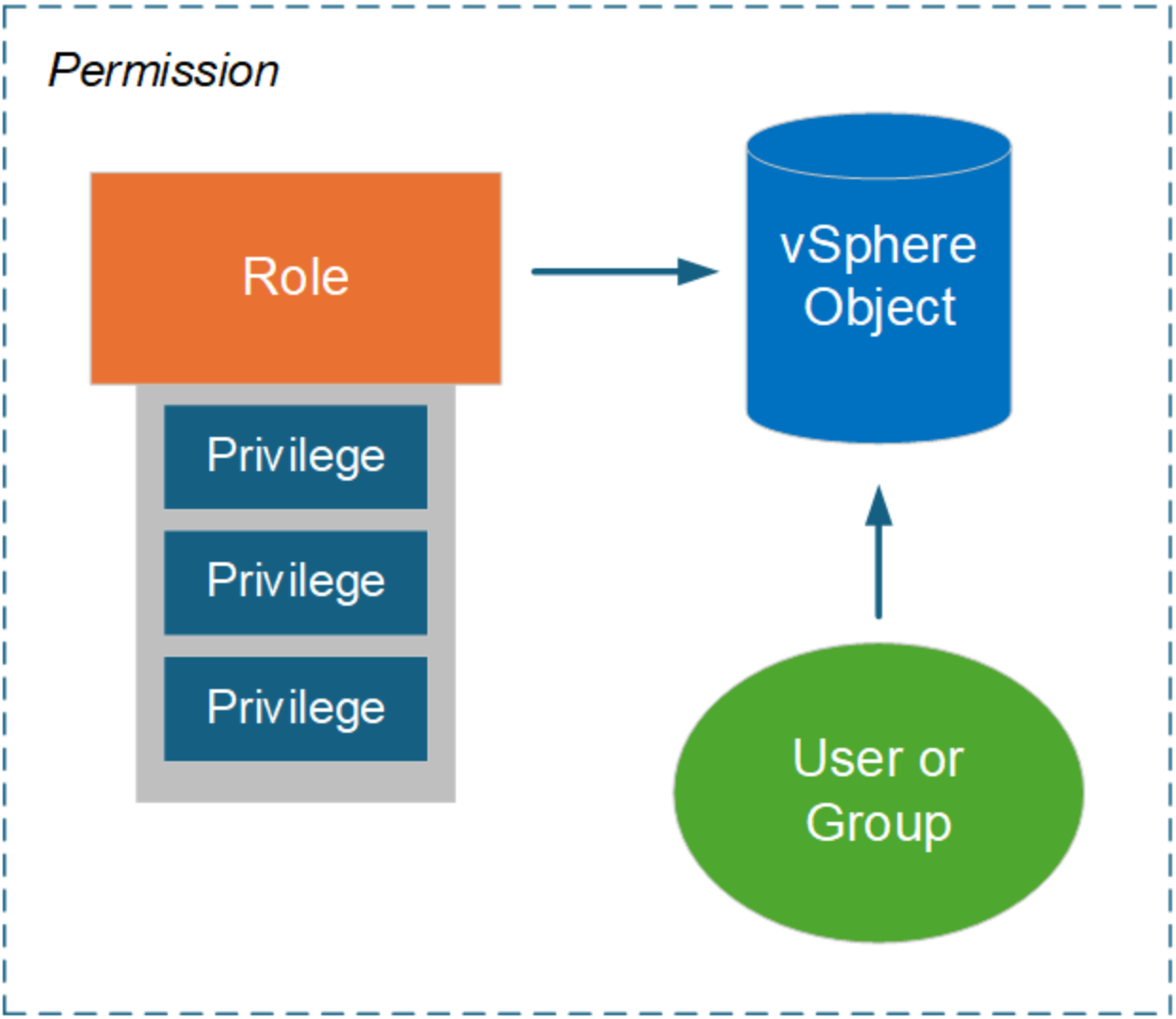
RBAC con VMware vSphere

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. In combinazione con un ruolo, è possibile creare un'autorizzazione su un oggetto nella gerarchia degli oggetti vSphere. L'autorizzazione concede l'accesso in base ai privilegi del ruolo associato. Si noti che i ruoli non vengono assegnati direttamente agli utenti in modo isolato. Invece, utenti e gruppi ottengono l'accesso a un oggetto tramite i privilegi del ruolo, come parte dell'autorizzazione più ampia 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.

RBAC con ONTAP

Ambiente RBAC ONTAP con tool ONTAP per VMware vSphere 10

ONTAP fornisce un ambiente RBAC solido ed estensibile. Puoi utilizzare la funzionalità RBAC per controllare l'accesso alle operazioni di storage e sistema così come esposte attraverso l'API REST e la CLI. È utile acquisire familiarità con l'ambiente prima di utilizzarlo con gli strumenti ONTAP per la distribuzione di VMware vSphere 10.

Panoramica delle opzioni amministrative

Ci sono diverse opzioni disponibili quando si utilizza RBAC ONTAP in base al tuo ambiente e agli obiettivi. Di seguito viene presentata una panoramica delle principali decisioni amministrative. Per ulteriori informazioni, vedere anche "Automazione ONTAP: Panoramica della sicurezza RBAC".

> Il role-based access control ONTAP è personalizzato per un ambiente storage ed è più semplice rispetto all'implementazione RBAC fornita con vCenter Server. ONTAP consente di assegnare un ruolo direttamente all'utente. La configurazione di autorizzazioni esplicite, come quelle utilizzate con vCenter Server, non è necessaria con RBAC di ONTAP.

Tipi di ruoli e Privileges

Quando si definisce un utente ONTAP, è necessario un ruolo ONTAP. Esistono due tipi di ruoli ONTAP:

- RIPOSO

  I ruoli REST sono stati introdotti con ONTAP 9.6 e vengono generalmente applicati agli utenti che accedono a ONTAP tramite l'API REST. Le Privileges incluse in questi ruoli sono definite in termini di accesso agli endpoint delle API REST ONTAP e alle azioni associate.

- Tradizionale

  Questi sono i ruoli legacy inclusi prima di ONTAP 9.6. Essi continuano a essere un aspetto fondamentale del RBAC. Le Privileges sono definite in termini di accesso ai comandi della CLI di ONTAP.

Mentre i ruoli RESTANTI sono stati introdotti più recentemente, i ruoli tradizionali hanno alcuni vantaggi. Ad esempio, è possibile includere facoltativamente parametri di query aggiuntivi in modo che Privileges definisca in modo più preciso gli oggetti a cui vengono applicati.

Scopo

I ruoli ONTAP possono essere definiti con uno dei due ambiti diversi. Possono essere applicati a una SVM dati

specifica (livello SVM) o all'intero cluster ONTAP (livello cluster).

Definizioni dei ruoli

ONTAP offre un set di ruoli predefiniti a livello di cluster e SVM. È inoltre possibile definire ruoli personalizzati.

Utilizzo dei ruoli REST ONTAP

Quando si utilizzano i ruoli REST ONTAP inclusi negli strumenti ONTAP per VMware vSphere 10, è necessario prendere in considerazione diverse considerazioni.

Mappatura dei ruoli

Indipendentemente dall'utilizzo di un ruolo tradizionale o REST, tutte le decisioni relative all'accesso a ONTAP vengono prese in base al comando CLI sottostante. Tuttavia, poiché Privileges in un ruolo REST è definito in termini di endpoint API REST, ONTAP deve creare un ruolo tradizionale *mapped* per ciascuno dei ruoli REST. Pertanto, ogni ruolo REST viene associato a un ruolo tradizionale sottostante. In questo modo, ONTAP può prendere decisioni sul controllo degli accessi in modo coerente, indipendentemente dal tipo di ruolo. Non è possibile modificare i ruoli mappati paralleli.

Definizione di un ruolo REST tramite CLI Privileges

Poiché ONTAP utilizza sempre i comandi CLI per determinare l'accesso a livello base, è possibile esprimere un ruolo REST utilizzando il comando CLI Privileges invece degli endpoint REST. Uno dei vantaggi di questo approccio è la granularità aggiuntiva disponibile con i ruoli tradizionali.

Interfaccia amministrativa per la definizione dei ruoli ONTAP

Puoi creare utenti e ruoli con l'interfaccia a riga di comando e l'API REST di ONTAP. Tuttavia, è più conveniente utilizzare l'interfaccia di Gestione sistema insieme al file JSON disponibile tramite il Gestore strumenti ONTAP. Per ulteriori informazioni, vedere "USA RBAC ONTAP con tool ONTAP per VMware vSphere 10" .

USA RBAC ONTAP con tool ONTAP per VMware vSphere 10

Esistono diversi aspetti dei tool ONTAP per l'implementazione RBAC di VMware vSphere 10 con ONTAP che è necessario prendere in considerazione prima di utilizzarlo in un ambiente di produzione.

Panoramica del processo di configurazione

I tool ONTAP per VMware vSphere 10 includono il supporto per la creazione di un utente ONTAP con un ruolo personalizzato. Le definizioni sono contenute in un file JSON che è possibile caricare nel cluster ONTAP. È possibile creare l'utente e personalizzare il ruolo in base all'ambiente e alle esigenze di protezione.

Le fasi principali della configurazione sono descritte in alto di seguito. Per "Configurare i ruoli e i privilegi degli utenti ONTAP"ulteriori dettagli, fare riferimento a.

1. Preparatevi

È necessario disporre delle credenziali di amministratore per ONTAP Tools Manager e per il cluster ONTAP.

2. Scaricare il file di definizione JSON

Dopo aver effettuato l'accesso all'interfaccia utente di ONTAP Tools Manager, è possibile scaricare il file JSON contenente le definizioni RBAC.

3. Creare un utente ONTAP con un ruolo

Dopo aver effettuato l'accesso a System Manager, è possibile creare l'utente e il ruolo:

1. Selezionare **Cluster** sulla sinistra, quindi **Settings**.
2. Scorrere fino a **utenti e ruoli** e fare clic su −→.
3. Selezionare **Aggiungi** in **utenti** e selezionare **prodotti di virtualizzazione**.
4. Selezionare il file JSON sulla workstation locale e caricarlo.

4. Configurare il ruolo

Come parte della definizione del ruolo, è necessario prendere diverse decisioni amministrative. Per ulteriori informazioni, vedereConfigurare il ruolo utilizzando System Manager.

Configurare il ruolo utilizzando System Manager

Dopo aver iniziato a creare un nuovo utente e ruolo con System Manager e aver caricato il file JSON, è possibile personalizzare il ruolo in base all'ambiente e alle esigenze.

Configurazione principale di utenti e ruoli

Le definizioni dei RBAC sono composte da diverse funzionalità dei prodotti, tra cui combinazioni di VSC, VASA Provider e SRA. Devi selezionare l'ambiente o gli ambienti in cui hai bisogno di supporto RBAC. Ad esempio, se si desidera che i ruoli supportino la funzionalità plug-in remoto, selezionare VSC. È inoltre necessario scegliere il nome utente e la password associata.

Privilegi

Le Privileges del ruolo sono organizzate in quattro serie in base al livello di accesso necessario allo storage ONTAP. Le Privileges su cui si basano i ruoli includono:

- Discovery (rilevamento)

  Questo ruolo consente di aggiungere sistemi storage.

- Creare storage

  Questo ruolo consente di creare storage. Include inoltre tutte le Privileges associate al ruolo di rilevamento.

- Modificare l'archiviazione

  Questo ruolo consente di modificare lo storage. Include inoltre tutta la Privileges associata al rilevamento e alla creazione dei ruoli storage.

- Distruzione dello storage

  Questo ruolo consente di distruggere lo storage. Include inoltre tutta la Privileges associata al rilevamento, la creazione di storage e la modifica dei ruoli storage.

Generare l'utente con un ruolo

Dopo aver selezionato le opzioni di configurazione per il proprio ambiente, fare clic su **Aggiungi** e ONTAP crea l'utente e il ruolo. Il nome del ruolo generato è una concatenazione dei seguenti valori:

- Valore del prefisso costante definito nel file JSON (ad esempio "OTV_10")
- Capacità del prodotto selezionata

- Elenco dei set di privilegi.

Esempio

`OTV_10_VSC_Discovery_Create`

Il nuovo utente verrà aggiunto all'elenco nella pagina "utenti e ruoli". Si noti che sono supportati entrambi i metodi di accesso utente HTTP e ONTAPI.

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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.