# Controllo degli accessi in base al ruolo (RBAC)

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

# Sommario

# Controllo degli accessi in base al ruolo (RBAC)

## Scopri RBAC degli strumenti ONTAP

Il controllo degli accessi basato sui ruoli (RBAC) è un framework di sicurezza per il controllo dell'accesso alle risorse all'interno di un'organizzazione. RBAC semplifica l'amministrazione definendo ruoli con specifici livelli di autorità per eseguire azioni, invece di assegnare autorizzazioni ai singoli utenti. I ruoli definiti vengono assegnati agli utenti, il che aiuta a ridurre il rischio di errore e semplifica la gestione del controllo degli accessi in tutta la tua organizzazione.

Il modello standard RBAC si compone di diverse tecnologie o fasi di implementazione di complessità crescente. Di conseguenza, le implementazioni RBAC effettive, in base alle esigenze dei fornitori di software e dei loro clienti, possono variare da relativamente semplici a molto complesse.

### Componenti RBAC

A un livello generale, esistono diversi componenti che sono generalmente inclusi in ogni implementazione RBAC. Questi componenti sono collegati tra loro in vari modi nell'ambito della definizione dei processi di autorizzazione.

#### Privileges

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

#### Ruoli

Un ruolo è un container che include uno o più privilegi. I ruoli sono generalmente definiti in base a compiti o funzioni lavorative specifiche. Quando un ruolo viene assegnato a un utente, l'utente riceve tutti i privilegi contenuti nel ruolo. E come per i privilegi, le implementazioni includono ruoli predefiniti e generalmente permettono di creare ruoli personalizzati.

#### Oggetti

Un *oggetto* rappresenta una risorsa reale o astratta identificata all'interno dell'ambiente RBAC. Le azioni definite tramite i privilegi vengono eseguite sugli oggetti associati o con essi. A seconda dell'implementazione, i privilegi possono essere concessi a un tipo di oggetto o a una specifica istanza di oggetto.

#### Utenti e gruppi

Agli utenti viene assegnato o associato 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 ai gruppi può semplificare ulteriormente l'amministrazione della sicurezza.

#### Autorizzazioni

Un permesso è una definizione che associa un utente o un gruppo insieme a un ruolo a un oggetto. I permessi possono essere utili in un modello a oggetti gerarchico, dove possono essere facoltativamente ereditati dagli elementi figli della gerarchia.

## Due ambienti RBAC

Ci sono due ambienti RBAC distinti che devi considerare quando lavori con ONTAP tools for VMware vSphere 10. ONTAP tools for VMware vSphere 10 richiede privilegi specifici sia in vCenter che in ONTAP per eseguire le sue operazioni. Anche se ONTAP tools automatizza le attività di gestione dello storage, non crea account utente né in vCenter né in ONTAP. Gli account di servizio devono essere creati da un amministratore vSphere quando necessario. Questa documentazione fornisce indicazioni agli amministratori per assegnare i ruoli e le autorizzazioni necessari per una gestione efficace di ONTAP tools.

#### 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 di ONTAP tools for VMware vSphere 10, l'ambiente RBAC viene esteso per includere oggetti aggiuntivi che rappresentano le funzionalità di ONTAP tools. L'accesso a questi oggetti è fornito tramite il plug-in remoto. Vedi "vCenter Server ambiente RBAC" per ulteriori informazioni.

#### cluster ONTAP

ONTAP tools for VMware vSphere 10 si connette a un cluster ONTAP tramite l'ONTAP REST API per eseguire operazioni relative allo storage. L'accesso alle risorse di storage è controllato tramite un ruolo ONTAP associato all'utente ONTAP fornito durante l'autenticazione. Vedi "Ambiente RBAC di ONTAP" per maggiori informazioni.

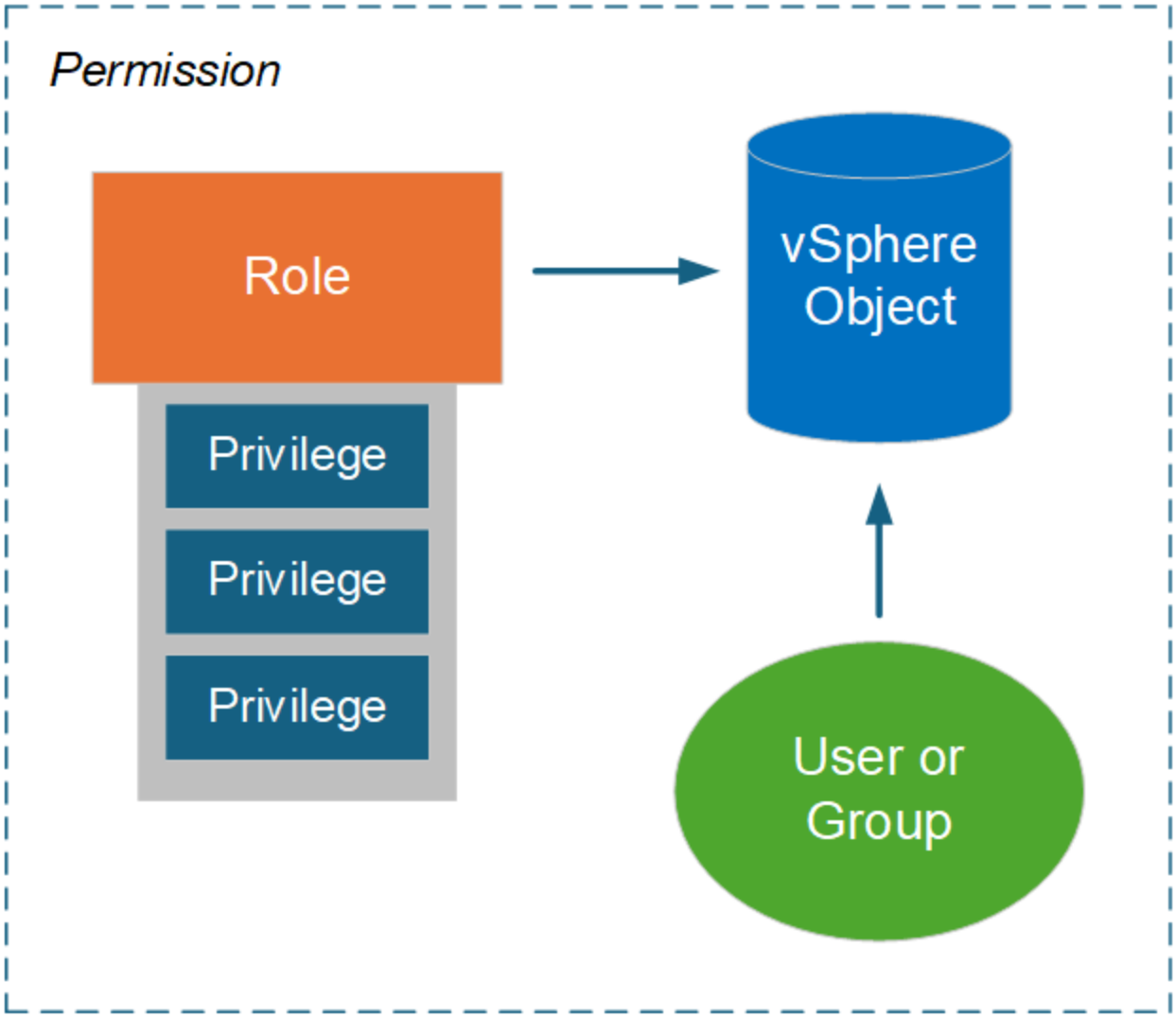
# RBAC con VMware vSphere

## Come funziona RBAC di vCenter Server con ONTAP tools

VMware vCenter Server offre una funzionalità RBAC che ti permette di controllare l'accesso agli oggetti vSphere. È una parte importante dei servizi di sicurezza centralizzati di autenticazione e autorizzazione di vCenter.

#### Illustrazione di un permesso del server vCenter

Un permesso è il fondamento per l'applicazione del controllo degli accessi nell'ambiente vCenter Server. Viene applicato a un oggetto vSphere con un utente o un gruppo incluso nella definizione del permesso. Una rappresentazione high-level di un permesso vCenter è fornita nella figura qui sotto.




### Componenti di un'autorizzazione del server vCenter

Un'autorizzazione del server vCenter è un insieme di diversi componenti che vengono collegati tra loro al momento della creazione dell'autorizzazione stessa.

#### oggetti vSphere

Le autorizzazioni sono associate a oggetti vSphere, come il vCenter Server, host ESXi, macchine virtuali, datastore, data center e cartelle. In base alle autorizzazioni assegnate all'oggetto, il vCenter Server determina quali azioni o attività possono essere eseguite sull'oggetto da ciascun utente o gruppo. Per le attività specifiche di ONTAP tools for VMware vSphere, tutte le autorizzazioni vengono assegnate e convalidate a livello di root o di cartella root del vCenter Server. Vedi "Usa RBAC con il server vCenter" per ulteriori informazioni.

#### Privileges e ruoli

Ci sono due tipi di privilegi vSphere utilizzati con ONTAP tools for VMware vSphere 10. Per semplificare il lavoro con RBAC in questo ambiente, ONTAP tools fornisce ruoli che contengono i privilegi nativi e personalizzati richiesti. I privilegi includono:

- Privilegi nativi del server vCenter

  Questi sono i privilegi forniti da vCenter Server.

- Privilegi specifici degli strumenti ONTAP

  Questi sono privilegi personalizzati unici di ONTAP tools for VMware vSphere.

#### Utenti e gruppi

Puoi definire utenti e gruppi usando Active Directory o l'istanza locale del server vCenter. In combinazione con un ruolo, puoi creare un'autorizzazione su un oggetto nella gerarchia degli oggetti vSphere. L'autorizzazione concede l'accesso in base ai privilegi del ruolo associato. Nota 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 di ruolo come parte dell'autorizzazione del server vCenter.

## vCenter Server: considerazioni RBAC per ONTAP tools

Ci sono diversi aspetti degli ONTAP tools for VMware vSphere 10 nell'implementazione RBAC con vCenter Server che dovresti considerare prima di usarli in un ambiente di produzione.

### vCenter ruoli e l'account amministratore

Devi definire e utilizzare i ruoli server personalizzati di vCenter solo se vuoi limitare l'accesso agli oggetti vSphere e alle attività amministrative associate. Se non è necessario limitare l'accesso, puoi usare un account amministratore. Ogni account amministratore è definito con il ruolo di Administrator al livello superiore della gerarchia degli oggetti. Questo garantisce l'accesso completo agli oggetti vSphere, inclusi quelli aggiunti da ONTAP tools for VMware vSphere 10.

### Gerarchia degli oggetti vSphere

L'inventario degli oggetti vSphere è organizzato in una gerarchia. Ad esempio, puoi scendere nella gerarchia come segue:

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

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

### Ruoli inclusi con ONTAP tools for VMware vSphere 10

Per semplificare il lavoro con il controllo degli accessi basato sui ruoli (RBAC) del server vCenter, ONTAP tools for VMware vSphere fornisce ruoli predefiniti adattati a varie attività amministrative.

> Se necessario, è possibile creare nuovi ruoli personalizzati. Per farlo, clonare uno dei ruoli esistenti di ONTAP tools e modificarlo secondo le proprie esigenze. Dopo aver apportato le modifiche alla configurazione, gli utenti client vSphere interessati dovranno disconnettersi e accedere nuovamente per attivare le modifiche.

Per visualizzare i ruoli di ONTAP tools for VMware vSphere, selezionare **Menu** nella parte superiore del vSphere Client e fare clic su **Amministrazione** e poi su **Ruoli** a sinistra. I seguenti privilegi devono essere inclusi nel ruolo assegnato all'utente vCenter responsabile della distribuzione o dell'onboarding del vCenter

Server. Assicurarsi che questi privilegi siano configurati come prerequisito per il processo di distribuzione o onboarding.

- Allarmi
  - Conferma l’allarme
- Libreria dei contenuti
  - Aggiungi elemento della libreria
  - Verifica in un template
  - Dai un’occhiata a un modello
  - Scarica i file
  - Importa storage
  - Storage di lettura
  - Sincronizza elemento della libreria
  - Sincronizza la libreria sottoscritta
  - Visualizza le impostazioni di configurazione
- Datastore
  - Assegna spazio
  - Esplora datastore
  - Operazioni sui file di basso livello
  - Rimuovi file
  - Aggiornare i file della macchina virtuale
  - Aggiornare i metadati della macchina virtuale
- ESX Agent Manager
  - Visualizza
- Cartella
  - Crea cartella
- Host
  - Configurazione
    - Impostazioni avanzate
    - Modifica impostazioni
    - Configurazione di rete
    - Risorse di sistema
    - Configurazione dell’avvio automatico della macchina virtuale
  - Operazioni locali
    - Crea macchina virtuale
    - Eliminare la macchina virtuale
    - Riconfigurare la macchina virtuale
- Rete

    - Assegna rete
    - Configurare
- OvfManager
    - OvfConsumer Accesso
- Profilo host
    - Visualizza
- Risorsa
    - Assegna la macchina virtuale al pool di risorse
- Attività pianificata
    - Crea attività
    - Modifica attività
    - Esegui attività
- Attività
    - Crea attività
    - Aggiorna attività
- vApp
    - Aggiungi macchina virtuale
    - Assegna pool di risorse
    - Assegna vApp
    - Crea
    - Importare
    - Sposta
    - Spegni
    - Accendi
    - Scarica da URL
    - Visualizza l'ambiente OVF
- Macchina virtuale
    - Modifica configurazione
        - Aggiungi disco esistente
        - Aggiungi nuovo disco
        - Aggiungi o rimuovi dispositivo
        - Configurazione avanzata
        - Modifica il conteggio della CPU
        - Modifica memoria
        - Modifica impostazioni
        - Cambia risorsa
        - Estendi il disco virtuale

        - Modificare le impostazioni del dispositivo
        - Rimuovere il disco
        - Reimposta le informazioni guest
        - Aggiorna la compatibilità della macchina virtuale
    - Modifica inventario
        - Crea da esistente
        - Crea nuovo
        - Sposta
        - Registrati
        - Rimuovi
        - Annulla registrazione
    - Interazione
        - Operazione di backup su macchina virtuale
        - Configura i supporti CD
        - Configura i supporti floppy
        - Collega i dispositivi
        - Interazione con la console
        - Gestione del sistema operativo guest tramite API VIX
        - Spegni
        - Accendi
        - Ripristina
        - Sospendi
    - Provisioning
        - Consenti l'accesso al disco
        - Clona modello
        - Personalizza guest
        - Distribuisci modello
        - Modifica specifica di personalizzazione
        - Leggi le specifiche di personalizzazione
    - Gestione Snapshot
        - Crea snapshot
        - Rimuovi snapshot
        - Rinomina snapshot
        - Ripristina allo snapshot

Ci sono tre ruoli predefiniti, come descritto di seguito.

**Amministratore di NetApp ONTAP tools for VMware vSphere**

Fornisce tutti i privilegi nativi del server vCenter e i privilegi specifici degli ONTAP tools necessari per eseguire

le attività principali di amministratore degli ONTAP tools for VMware vSphere.

**NetApp ONTAP tools for VMware vSphere in sola lettura**

Fornisce accesso in sola lettura agli strumenti ONTAP. Questi utenti non possono eseguire alcuna azione degli strumenti ONTAP per VMware vSphere soggetta a controllo degli accessi.

**Provisioning di NetApp ONTAP tools for VMware vSphere**

Fornisce alcuni dei privilegi nativi del vCenter Server e dei privilegi specifici degli ONTAP tools necessari per il provisioning dello storage. Puoi eseguire le seguenti attività:

- Crea nuovi archivi dati
- Gestisci i datastore

### vSphere oggetti e backend di storage ONTAP

I due ambienti RBAC lavorano insieme. Quando esegui un'attività nell'interfaccia client di vSphere, vengono prima verificati i ruoli degli ONTAP tools definiti per il vCenter Server. Se l'operazione è consentita da vSphere, vengono poi esaminati i privilegi del ruolo ONTAP. Questo secondo passaggio viene eseguito in base al ruolo ONTAP assegnato all'utente quando è stato creato e configurato il backend di storage.

### Lavorare con RBAC del server vCenter

Ci sono alcuni aspetti da considerare quando lavori con i privilegi e le autorizzazioni del server vCenter.

#### Privilegi richiesti

Per accedere all'interfaccia utente di ONTAP tools for VMware vSphere 10, devi avere il privilegio *View* specifico di ONTAP tools. Se accedi a vSphere senza questo privilegio e fai clic sull'icona NetApp, ONTAP tools for VMware vSphere mostra un messaggio di errore e ti impedisce di accedere all'interfaccia utente.

Il livello di assegnazione nella gerarchia degli oggetti vSphere determina a quali parti dell'interfaccia utente puoi accedere. Assegnando il privilegio di visualizzazione all'oggetto radice, puoi accedere a ONTAP tools for VMware vSphere facendo clic sull'icona NetApp.

Puoi invece assegnare il privilegio di visualizzazione a un altro livello di oggetto vSphere inferiore. Tuttavia, questo limiterà i menu di ONTAP tools for VMware vSphere a cui puoi accedere e che puoi usare.

#### Assegnare le autorizzazioni

Devi usare le autorizzazioni del server vCenter se vuoi limitare l'accesso agli oggetti e alle attività di vSphere. Il punto in cui assegni le autorizzazioni nella gerarchia degli oggetti di vSphere determina quali attività di ONTAP tools for VMware vSphere 10 gli utenti possono eseguire.

A meno che tu non abbia bisogno di definire un accesso più restrittivo, di solito è una buona pratica assegnare le autorizzazioni a livello di oggetto radice o di cartella radice.

Le autorizzazioni disponibili con ONTAP tools for VMware vSphere 10 si applicano a oggetti personalizzati non-vSphere, come i sistemi storage. Se possibile, dovresti assegnare queste autorizzazioni all'oggetto radice di ONTAP tools for VMware vSphere perché non esiste un oggetto vSphere a cui puoi assegnarle. Ad esempio, qualsiasi autorizzazione che includa il privilegio "Aggiungi/Modifica/Rimuovi sistemi storage" di ONTAP tools for VMware vSphere dovrebbe essere assegnata a livello dell'oggetto radice.

Quando definisci un'autorizzazione a un livello superiore nella gerarchia degli oggetti, puoi configurarla in modo che venga trasmessa ed ereditata dagli oggetti figlio. Se serve, puoi assegnare autorizzazioni aggiuntive

agli oggetti figlio che sovrascrivono quelle ereditate dal genitore.

Puoi modificare un'autorizzazione in qualsiasi momento. Se cambi uno qualsiasi dei privilegi all'interno di un'autorizzazione, gli utenti associati all'autorizzazione devono disconnettersi da vSphere e accedere di nuovo per rendere effettiva la modifica.

# RBAC con ONTAP

## Come funziona ONTAP RBAC con ONTAP tools

ONTAP offre un ambiente RBAC robusto ed estensibile. Puoi utilizzare la funzionalità RBAC per controllare l'accesso allo storage e alle operazioni di sistema esposte tramite REST API e CLI. È utile conoscere l'ambiente prima di usarlo con una distribuzione di ONTAP tools for VMware vSphere 10.

### Panoramica delle opzioni amministrative

Sono disponibili diverse opzioni per l'utilizzo di ONTAP RBAC, a seconda dell'ambiente e degli obiettivi. Di seguito trovi una panoramica delle principali decisioni amministrative. Vedi anche "Automazione ONTAP: Panoramica della sicurezza RBAC" per ulteriori informazioni.

> ONTAP RBAC è progettato specificamente per un ambiente di storage ed è più semplice rispetto all'implementazione RBAC fornita con vCenter Server. Con ONTAP, assegni un ruolo direttamente all'utente. Non è necessario configurare autorizzazioni esplicite, come quelle utilizzate con vCenter Server, con ONTAP RBAC.

#### Tipi di ruoli e privilegi

È necessario un ruolo ONTAP quando si definisce un utente ONTAP. Esistono due tipi di ruoli ONTAP:

- REST

  I ruoli REST sono stati introdotti con ONTAP 9.6 e vengono generalmente applicati agli utenti che accedono a ONTAP tramite l'API REST. I privilegi inclusi in questi ruoli sono definiti in termini di accesso agli endpoint dell'API REST di ONTAP e alle azioni associate.

- Tradizionale

  Si tratta dei ruoli legacy esistenti prima di ONTAP 9.6. Essi continuano a rappresentare un aspetto fondamentale di RBAC. I privilegi sono definiti in termini di accesso ai comandi CLI di ONTAP.

Sebbene i ruoli REST siano stati introdotti più di recente, i ruoli tradizionali offrono alcuni vantaggi. Ad esempio, è possibile includere parametri di query aggiuntivi per consentire ai Privileges di definire con maggiore precisione gli oggetti a cui si applicano.

#### Ambito

I ruoli ONTAP possono essere definiti con uno dei due diversi ambiti. Possono essere applicati a uno specifico SVM di dati (livello SVM) o all'intero cluster ONTAP (livello cluster).

#### Definizioni dei ruoli

ONTAP offre una serie di ruoli predefiniti sia a livello di cluster che di SVM. Puoi anche definire ruoli personalizzati.

### Lavorare con i ruoli REST di ONTAP

Ci sono diverse considerazioni da tenere presenti quando utilizzi i ruoli REST ONTAP inclusi negli ONTAP tools for VMware vSphere 10.

#### Mappatura dei ruoli

Sia che tu utilizzi un ruolo tradizionale o REST, tutte le decisioni di accesso di ONTAP si basano sul comando CLI sottostante. Ma poiché i privilegi in un ruolo REST sono definiti in termini di endpoint REST API, ONTAP deve creare un ruolo tradizionale *mappato* per ciascuno dei ruoli REST. Quindi, ogni ruolo REST viene associato a un ruolo tradizionale sottostante. Questo permette a ONTAP di prendere decisioni di controllo degli accessi in modo coerente, indipendentemente dal tipo di ruolo. Non puoi modificare i ruoli mappati in parallelo.

#### Definizione di un ruolo REST utilizzando i privilegi CLI

Poiché ONTAP utilizza sempre i comandi CLI per determinare l'accesso a livello base, è possibile esprimere un ruolo REST utilizzando i privilegi dei comandi CLI anziché gli endpoint REST. Un vantaggio di questo approccio è la maggiore granularità disponibile con i ruoli tradizionali.

#### Interfaccia amministrativa durante la definizione dei ruoli ONTAP

Puoi creare utenti e ruoli con la ONTAP CLI e la REST API. Tuttavia, è più comodo usare l'interfaccia di System Manager insieme al file JSON disponibile tramite ONTAP tools Manager. Vedi "Usa ONTAP RBAC con ONTAP tools for VMware vSphere 10" per maggiori informazioni.

## Considerazioni RBAC di ONTAP per ONTAP tools

Ci sono diversi aspetti degli ONTAP tools for VMware vSphere 10 relativi all'implementazione RBAC con ONTAP che dovresti considerare prima di utilizzarli in un ambiente di produzione.

#### Panoramica del processo di configurazione

ONTAP tools for VMware vSphere include il supporto per la creazione di un utente ONTAP con un ruolo personalizzato. Le definizioni sono contenute in un file JSON che puoi caricare sul cluster ONTAP. Puoi creare l'utente e personalizzare il ruolo in base al tuo ambiente e alle tue esigenze di sicurezza.

Di seguito sono descritte a un livello high-level le principali fasi di configurazione. Consulta "Configura i ruoli utente e i privilegi di ONTAP" per maggiori dettagli.

#### 1. Prepara

Devi avere le credenziali amministrative sia per ONTAP tools Manager che per l'ONTAP cluster.

#### 2. Scarica il file di definizione JSON

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

#### 3. Crea un utente ONTAP con un ruolo

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

1. Seleziona **Cluster** a sinistra e poi **Settings**.
2. Scorri verso il basso fino a **Utenti e ruoli** e fai clic su −→.
3. Seleziona **Aggiungi** sotto **Utenti** e seleziona **Prodotti di virtualizzazione**.
4. Seleziona il file JSON sulla tua workstation locale e caricalo.

#### 4. Configura il ruolo

Nell'ambito della definizione del ruolo, devi prendere diverse decisioni amministrative. Vedi Configura il ruolo usando System Manager per maggiori dettagli.

### Configura il ruolo usando System Manager

Dopo aver iniziato a creare un nuovo utente e ruolo con System Manager e aver caricato il file JSON, puoi personalizzare il ruolo in base al tuo ambiente e alle tue esigenze.

#### Configurazione principale di utenti e ruoli

Le definizioni RBAC sono raggruppate in diverse funzionalità di prodotto, incluse combinazioni di VSC, VASA Provider e SRA. Dovresti selezionare l'ambiente o gli ambienti in cui ti serve il supporto RBAC. Ad esempio, se vuoi che i ruoli supportino la funzionalità di plug-in remoto, seleziona VSC. Devi anche scegliere il nome utente e la password associata.

#### Privileges

I privilegi di ruolo sono organizzati in quattro gruppi in base al livello di accesso necessario per lo storage ONTAP. I privilegi su cui si basano i ruoli includono:

- Scoperta

  Questo ruolo ti permette di aggiungere sistemi di archiviazione.

- Crea storage

  Questo ruolo ti consente di creare spazio di archiviazione. Include anche tutti i privilegi associati al ruolo di discovery.

- Modifica lo storage

  Questo ruolo ti consente di modificare lo spazio di archiviazione. Include anche tutti i privilegi associati ai ruoli di individuazione e creazione dello spazio di archiviazione.

- Distruggi storage

  Questo ruolo ti permette di eliminare lo storage. Include anche tutti i privilegi associati ai ruoli di individuazione, creazione e modifica dello storage.

#### Genera l'utente con un ruolo

Dopo aver selezionato le opzioni di configurazione per il tuo ambiente, fai 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")
- Funzionalità 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



## Informazioni sul marchio commerciale