Sicurezza RBAC

ONTAP Automation

NetApp
July 11, 2024

Sommario

Sicurezza RBAC

Panoramica della sicurezza RBAC

ONTAP include una funzionalità RBAC (Role-Based Access Control) solida ed estensibile. È possibile assegnare a ciascun account un ruolo diverso per controllare l'accesso dell'utente alle risorse esposte attraverso l'API REST e la CLI. I ruoli definiscono diversi livelli di accesso amministrativo per i vari utenti ONTAP.

La funzionalità RBAC di ONTAP ha continuato a espandersi ed è stata notevolmente migliorata con ONTAP 9.11.1 (e versioni successive). Vedere "Riepilogo dell'evoluzione di RBAC" e. "Novità dell'API REST ONTAP e dell'automazione" per ulteriori informazioni.

Ruoli di ONTAP

Un ruolo è un insieme di privilegi che definiscono collettivamente le azioni che l'utente può intraprendere. Ciascun privilegio identifica un percorso di accesso specifico e il livello di accesso associato. I ruoli vengono assegnati agli account utente e applicati da ONTAP durante le decisioni relative al controllo degli accessi.

Tipi di ruoli

Esistono due tipi di ruoli. Sono stati introdotti e adattati a diversi ambienti con l'evoluzione di ONTAP.

L'utilizzo di ciascun tipo di ruolo comporta vantaggi e svantaggi. Vedere "Confronto dei tipi di ruolo" per ulteriori informazioni.

Tipo	Descrizione
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. La creazione di un ruolo REST crea automaticamente un ruolo *mapping* tradizionale.
Tradizionale	Questi sono i ruoli legacy inclusi prima di ONTAP 9.6. Sono stati introdotti per l'ambiente CLI di ONTAP e continuano ad essere fondamentali per la sicurezza RBAC.

Scopo

Ogni ruolo ha un ambito o un contesto all'interno del quale viene definito e applicato. L'ambito determina dove e come viene utilizzato un ruolo specifico.

Gli account utente di ONTAP hanno anche un ambito simile che determina il modo in cui un utente viene definito e utilizzato.

Scopo	Descrizione
Cluster	I ruoli con un ambito cluster vengono definiti a livello di cluster ONTAP. Sono associati agli account utente a livello di cluster.
SVM	I ruoli con un ambito SVM sono definiti per una SVM di dati specifica. Vengono assegnati agli account utente nella stessa SVM.

Origine delle definizioni dei ruoli

Esistono due modi per definire un ruolo ONTAP.

Fonte del ruolo	Descrizione
Personalizzato	L'amministratore di ONTAP può creare ruoli personalizzati. Questi ruoli possono essere personalizzati in base a un ambiente specifico e a requisiti di sicurezza.
Integrato	Sebbene i ruoli personalizzati offrano maggiore flessibilità, è disponibile anche un set di ruoli integrati sia a livello di cluster che di SVM. Questi ruoli sono predefiniti e possono essere utilizzati per molte attività amministrative comuni.

Mappatura dei ruoli ed elaborazione ONTAP

A seconda della release ONTAP in uso, tutte o quasi tutte le chiamate REST vengono associate a uno o più comandi CLI. Quando si crea un ruolo DI RIPOSO, viene creato anche un ruolo tradizionale o legacy. Questo ruolo tradizionale **mappato** si basa sui comandi CLI corrispondenti e non può essere manipolato o modificato.

La mappatura inversa dei ruoli non è supportata. In altre termini, la creazione di un ruolo tradizionale non crea un corrispondente ruolo DI RIPOSO.

Riepilogo dell'evoluzione di RBAC

I ruoli tradizionali sono inclusi in tutte le release di ONTAP 9. I ruoli RIMANENTI sono stati introdotti in seguito e si sono evoluti come descritto di seguito.

ONTAP 9.6

L'API REST è stata introdotta con ONTAP 9.6. Anche i ruoli RIMANENTI sono stati inclusi in questa release. Inoltre, quando si crea un ruolo DI RIPOSO, viene creato anche un ruolo tradizionale corrispondente.

Da ONTAP 9.7 a 9.10.1

Ogni versione di ONTAP dal 9.7 al 9.10.1 include miglioramenti all'API REST. Ad esempio, ad ogni release sono stati aggiunti ulteriori endpoint REST. Tuttavia, la creazione e la gestione dei due tipi di ruoli sono rimaste separate. Inoltre, ONTAP 9.10.1 ha aggiunto il supporto RBAC REST per l'endpoint REST di Snapshot `/api/storage/volumes/{vol.uuid}/snapshots` che è un endpoint qualificato per le risorse.

ONTAP 9.11.1

Con questa release è stata aggiunta la possibilità di configurare e gestire i ruoli tradizionali utilizzando l'API REST. Sono stati aggiunti anche ulteriori livelli di accesso per i ruoli REST.

Lavorare con ruoli e utenti

Dopo aver compreso le funzionalità di base di RBAC, è possibile iniziare a lavorare con i ruoli e gli utenti di ONTAP.

Vedere "Flussi di lavoro RBAC" Per esempi su come creare e utilizzare ruoli con l'API REST ONTAP.

Accesso amministrativo

È possibile creare e gestire i ruoli ONTAP attraverso l'API REST o l'interfaccia della riga di comando. I dettagli di accesso sono descritti di seguito.

API REST

Esistono diversi endpoint che possono essere utilizzati quando si lavora con i ruoli RBAC e gli account utente. I primi quattro nella tabella vengono utilizzati per creare e gestire i ruoli. Gli ultimi due vengono utilizzati per creare e gestire gli account utente.

È possibile accedere a ONTAP online "Riferimento API" Documentazione per ulteriori informazioni, inclusi esempi di utilizzo dell'API.

Endpoint	Descrizione
`/security/roles`	Questo endpoint consente di creare un nuovo ruolo DI RIPOSO. Inoltre, a partire da ONTAP 9.11.1, è possibile creare un ruolo tradizionale. In questo caso, ONTAP determina il tipo di ruolo in base ai parametri di input. È inoltre possibile recuperare un elenco dei ruoli definiti.
`/security/roles/{owner.UUID}/{name}`	È possibile recuperare o eliminare un cluster specifico o un ruolo con ambito SVM. Il valore UUID identifica la SVM in cui è definito il ruolo (SVM di dati o cluster). Il valore del nome è il nome del ruolo.
`/security/roles/{owner.UUID}/{name}/privileges`	Questo endpoint consente di configurare i privilegi per un ruolo specifico. I ruoli integrati possono essere recuperati ma non aggiornati. Per ulteriori informazioni, consultare la documentazione di riferimento API per la versione ONTAP in uso.
`/security/roles/{owner.UUID}/{name}/privileges/[path]`	È possibile recuperare, modificare ed eliminare il livello di accesso e il valore di query opzionale per un privilegio specifico. Per ulteriori informazioni, consultare la documentazione di riferimento API per la versione ONTAP in uso.
`/security/accounts`	Questo endpoint consente di creare un nuovo cluster o un nuovo account utente con ambito SVM. Prima che l'account sia operativo, è necessario includere o aggiungere diversi tipi di informazioni. È inoltre possibile recuperare un elenco degli account utente definiti.
`/security/accounts/{owner.UUID}/{name}`	È possibile recuperare, modificare ed eliminare un cluster specifico o un account utente con ambito SVM. Il valore UUID identifica la SVM in cui è definito l'utente (SVM di dati o cluster). Il valore del nome corrisponde al nome dell'account.

Interfaccia della riga di comando

Di seguito sono descritti i relativi comandi dell'interfaccia utente di ONTAP. Tutti i comandi sono accessibili a livello di cluster tramite un account amministratore.

Comando	Descrizione
`security login`	Questa è la directory contenente i comandi necessari per creare e gestire un login utente.

Comando	Descrizione
`security login rest-role`	Questa è la directory contenente i comandi necessari per creare e gestire un ruolo DI RIPOSO associato a un login utente.
`security login role`	Questa è la directory contenente i comandi necessari per creare e gestire un ruolo tradizionale associato a un login utente.

Definizioni dei ruoli

I ruoli RIMANENTI e tradizionali vengono definiti attraverso un insieme di attributi.

Proprietario e scopo

Un ruolo può essere di proprietà del cluster ONTAP o di una specifica SVM di dati all'interno del cluster. Il proprietario determina inoltre implicitamente l'ambito del ruolo.

Nome univoco

Ogni ruolo deve avere un nome univoco all'interno del suo ambito. Il nome di un ruolo del cluster deve essere univoco a livello di cluster ONTAP, mentre i ruoli SVM devono essere univoci all'interno della SVM specifica.

> Il nome di un nuovo ruolo DI RIPOSO deve essere unico tra i ruoli DI RIPOSO e quelli tradizionali. Questo perché la creazione di un ruolo DI RIPOSO comporta anche un nuovo ruolo tradizionale *mapping* con lo stesso nome.

Insieme di privilegi

Ogni ruolo contiene un insieme di uno o più privilegi. Ogni privilegio identifica una risorsa o un comando specifico e il livello di accesso associato.

Privilegi

Un ruolo può contenere uno o più privilegi. Ogni definizione di privilegio è una tupla e stabilisce il livello di accesso a una risorsa o a un'operazione specifica.

Percorso delle risorse

Il percorso delle risorse viene identificato come endpoint REST o percorso della directory comando/comando CLI.

Endpoint REST

Un endpoint API ha identificato la risorsa di destinazione per un ruolo DI RIPOSO.

Comando CLI

Un comando CLI identifica la destinazione di un ruolo tradizionale. È inoltre possibile specificare una directory di comandi, che includerà tutti i comandi downstream nella gerarchia CLI di ONTAP.

Livello di accesso

Il livello di accesso definisce il tipo di accesso che il ruolo ha al percorso o al comando di risorsa specifico. I livelli di accesso vengono identificati mediante una serie di parole chiave predefinite. Con ONTAP 9.6 sono stati introdotti tre livelli di accesso. Possono essere utilizzati sia per i ruoli tradizionali che PER QUELLI DI RIPOSO. Inoltre, con ONTAP 9.11.1 sono stati aggiunti tre nuovi livelli di accesso. Questi nuovi livelli di accesso possono essere utilizzati solo con i ruoli REST.

I livelli di accesso seguono il modello CRUD. Con REST, si basa sui metodi HTTP primari (POST, GET, PATCH, DELETE). Le corrispondenti operazioni CLI vengono generalmente associate alle operazioni REST (creazione, visualizzazione, modifica, eliminazione).

Livello di accesso	Primitive REST	Aggiunto	Solo ruolo DI RIPOSO
nessuno	n/a.	9.6	No
readonly	OTTIENI	9.6	No
tutto	OTTIENI, PUBBLICA, PATCH, ELIMINA	9.6	No
read_create	OTTIENI, PUBBLICA	9.11.1	Sì
read_modify	GET, PATCH	9.11.1	Sì
read_create_modify	OTTIENI, PUBBLICA, PATCH	9.11.1	Sì

Query facoltativa

Quando si crea un ruolo tradizionale, è possibile includere facoltativamente un valore **query** per identificare il sottoinsieme di oggetti applicabili per il comando o la directory dei comandi.

Riepilogo dei ruoli integrati

ONTAP include diversi ruoli predefiniti che è possibile utilizzare a livello di cluster o SVM.

Ruoli con ambito del cluster

Nell'ambito del cluster sono disponibili diversi ruoli integrati.

Vedere "Ruoli predefiniti per gli amministratori del cluster" per ulteriori informazioni.

Ruolo	Descrizione
amministratore	Gli amministratori con questo ruolo dispongono di diritti senza restrizioni e possono eseguire qualsiasi operazione nel sistema ONTAP. Possono configurare tutte le risorse a livello di cluster e SVM.
AutoSupport	Si tratta di un ruolo speciale per l'account AutoSupport.
backup	Questo ruolo speciale per il software di backup che deve eseguire il backup del sistema.
SnapLock	Si tratta di un ruolo speciale per l'account SnapLock.
readonly	Gli amministratori con questo ruolo possono visualizzare tutto a livello di cluster, ma non possono apportare modifiche.
nessuno	Non vengono fornite funzionalità amministrative.

Ruoli con ambito SVM

Nell'ambito di SVM sono disponibili diversi ruoli integrati. Il sistema **vsadmin** fornisce l'accesso alle funzionalità più generali e potenti. Sono disponibili diversi ruoli aggiuntivi adattati a specifiche attività amministrative, tra cui:

- volume vsadmin
- protocollo vsadmin
- vsadmin-backup
- vsadmin-snaplock
- vsadmin-readonly

Vedere "Ruoli predefiniti per gli amministratori SVM" per ulteriori informazioni.

Confronto dei tipi di ruolo

Prima di selezionare un ruolo **REST** o **tradizionale**, devi essere consapevole delle differenze. Di seguito sono descritti alcuni dei modi in cui è possibile confrontare i due tipi di ruolo.

Per casi di utilizzo RBAC più avanzati o complessi, è consigliabile utilizzare un ruolo tradizionale.

Modalità di accesso dell'utente a ONTAP

Prima di creare un ruolo, è importante sapere come l'utente accede al sistema ONTAP. In base a ciò, è possibile determinare un tipo di ruolo.

Accesso	Tipo consigliato
Solo API REST	Il ruolo REST è progettato per essere utilizzato con l'API REST.
API REST E CLI	È possibile definire un ruolo DI RIPOSO che crea anche un ruolo tradizionale corrispondente.
Solo CLI	È possibile creare un ruolo tradizionale.

Precisione del percorso di accesso

Il percorso di accesso definito per un ruolo REST si basa su un endpoint REST. Il percorso di accesso per un ruolo tradizionale si basa su un comando CLI o su una directory di comandi. Inoltre, è possibile includere un parametro di query opzionale con un ruolo tradizionale per limitare ulteriormente l'accesso in base ai valori dei parametri del comando.