Gestire i ruoli di controllo degli accessi

ONTAP 9

NetApp
September 12, 2024

Sommario

Gestire i ruoli di controllo degli accessi . . . 1
Panoramica sui ruoli di controllo degli accessi . . . 1
Modificare il ruolo assegnato a un amministratore . . . 1
Definire ruoli personalizzati . . . 1
Ruoli predefiniti per gli amministratori del cluster . . . 3
Ruoli predefiniti per gli amministratori SVM . . . 5
Controllare l’accesso dell’amministratore . . . 7

Gestire i ruoli di controllo degli accessi

Panoramica sui ruoli di controllo degli accessi

Il ruolo assegnato a un amministratore determina i comandi a cui l'amministratore ha accesso. Il ruolo viene assegnato quando si crea l'account per l'amministratore. È possibile assegnare un ruolo diverso o definire ruoli personalizzati in base alle esigenze.

Modificare il ruolo assegnato a un amministratore

È possibile utilizzare `security login modify` Comando per modificare il ruolo di un account di amministratore di cluster o SVM. È possibile assegnare un ruolo predefinito o personalizzato.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fase

1. Modificare il ruolo di un amministratore di cluster o SVM:

   `security login modify -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment`

   Per la sintassi completa dei comandi, vedere "foglio di lavoro".

   "Creazione o modifica degli account di accesso"

   Il seguente comando modifica il ruolo dell'account amministratore del cluster ad `DOMAIN1\guest1` al predefinito `readonly` ruolo.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   Il seguente comando modifica il ruolo degli account amministratore SVM nell'account di gruppo ad `DOMAIN1\adgroup` al personalizzato `vol_role` ruolo.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

Definire ruoli personalizzati

È possibile utilizzare `security login role create` per definire un ruolo personalizzato. È possibile eseguire il comando tutte le volte necessarie per ottenere la

combinazione esatta di funzionalità che si desidera associare al ruolo.

A proposito di questa attività

- Un ruolo, predefinito o personalizzato, concede o nega l'accesso ai comandi ONTAP o alle directory dei comandi.

  Una directory di comandi (`volume`, ad esempio) è un gruppo di sottodirectory di comandi e comandi correlati. Ad eccezione di quanto descritto in questa procedura, la concessione o il rifiuto dell'accesso a una directory di comandi concede o nega l'accesso a ciascun comando nella directory e nelle relative sottodirectory.

- L'accesso a comandi o sottodirectory specifici sovrascrive l'accesso alla directory principale.

  Se un ruolo viene definito con una directory di comandi e quindi viene definito nuovamente con un livello di accesso diverso per un comando specifico o per una sottodirectory della directory principale, il livello di accesso specificato per il comando o la sottodirectory sovrascrive quello della directory principale.

> Non è possibile assegnare a un amministratore SVM un ruolo che dia accesso a una directory di comandi o comandi disponibile solo per `admin` amministratore del cluster, ad esempio `security` directory dei comandi.

Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fase

1. Definire un ruolo personalizzato:

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

   Per la sintassi completa dei comandi, vedere "foglio di lavoro".

   I seguenti comandi assegnano a. `vol_role` accesso completo ai comandi in `volume` directory dei comandi e accesso in sola lettura ai comandi in `volume snapshot` sottodirectory.

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   I seguenti comandi assegnano a. `SVM_storage` accesso in sola lettura ai comandi in `storage` directory dei comandi, nessun accesso ai comandi in `storage encryption` sottodirectory e accesso completo a `storage aggregate plex offline` comando non intrinseco.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

Ruoli predefiniti per gli amministratori del cluster

I ruoli predefiniti per gli amministratori dei cluster devono soddisfare la maggior parte delle esigenze. È possibile creare ruoli personalizzati in base alle necessità. Per impostazione predefinita, a un amministratore del cluster viene assegnato il valore predefinito `admin` ruolo.

La seguente tabella elenca i ruoli predefiniti per gli amministratori del cluster:

Questo ruolo…	Dispone di questo livello di accesso…	Alle seguenti directory di comandi o comandi
amministratore	tutto	Tutte le directory dei comandi (`DEFAULT`)
admin-no-fsa (disponibile a partire da ONTAP 9.12.1)	Lettura/scrittura	• Tutte le directory dei comandi (`DEFAULT`) • `security login rest-role` • `security login role`

Di sola lettura	• security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics	Nessuno
volume file show-disk-usage	AutoSupport	tutto
• set • system node autosupport	nessuno	Tutte le altre directory di comando (DEFAULT)
backup	tutto	vserver services ndmp
readonly	volume	nessuno
Tutte le altre directory di comando (DEFAULT)	readonly	tutto

• security login password Solo per la gestione della password locale del proprio account utente e delle informazioni sulle chiavi • set	nessuno	security
readonly	Tutte le altre directory di comando (DEFAULT)	SnapLock
tutto	• set • volume create • volume modify • volume move • volume show	nessuno
• volume move governor • volume move recommend	nessuno	Tutte le altre directory di comando (DEFAULT)
nessuno	nessuno	Tutte le directory dei comandi (DEFAULT)

Il autosupport il ruolo viene assegnato al predefinito autosupport Account, utilizzato da AutoSupport OnDemand. ONTAP impedisce di modificare o eliminare autosupport account. ONTAP impedisce inoltre l'assegnazione di autosupport ruolo per altri account utente.

Ruoli predefiniti per gli amministratori SVM

I ruoli predefiniti per gli amministratori SVM devono soddisfare la maggior parte delle esigenze. È possibile creare ruoli personalizzati in base alle necessità. Per impostazione predefinita, a un amministratore SVM viene assegnato il valore predefinito vsadmin ruolo.

La seguente tabella elenca i ruoli predefiniti per gli amministratori SVM:

Nome del ruolo	Funzionalità

vsadmin	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione dei volumi, ad eccezione degli spostamenti dei volumi • Gestione di quote, qtree, copie Snapshot e file • Gestione delle LUN • Esecuzione delle operazioni SnapLock, ad eccezione dell'eliminazione con privilegi • Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurazione dei servizi: DNS, LDAP e NIS • Monitoraggio dei lavori • Monitoraggio delle connessioni di rete e dell'interfaccia di rete • Monitoraggio dello stato di salute di SVM
volume vsadmin	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione dei volumi, compresi gli spostamenti dei volumi • Gestione di quote, qtree, copie Snapshot e file • Gestione delle LUN • Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurazione dei servizi: DNS, LDAP e NIS • Interfaccia di rete di monitoraggio • Monitoraggio dello stato di salute di SVM
protocollo vsadmin	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurazione dei servizi: DNS, LDAP e NIS • Gestione delle LUN • Interfaccia di rete di monitoraggio • Monitoraggio dello stato di salute di SVM

vsadmin-backup	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione delle operazioni NDMP • Creazione di un volume ripristinato in lettura/scrittura • Gestione delle relazioni SnapMirror e delle copie Snapshot • Visualizzazione di volumi e informazioni di rete
vsadmin-snaplock	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione dei volumi, ad eccezione degli spostamenti dei volumi • Gestione di quote, qtree, copie Snapshot e file • Esecuzione di operazioni SnapLock, inclusa l'eliminazione con privilegi • Configurazione dei protocolli: NFS e SMB • Configurazione dei servizi: DNS, LDAP e NIS • Monitoraggio dei lavori • Monitoraggio delle connessioni di rete e dell'interfaccia di rete
vsadmin-readonly	• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Monitoraggio dello stato di salute di SVM • Interfaccia di rete di monitoraggio • Visualizzazione di volumi e LUN • Visualizzazione di servizi e protocolli

Controllare l'accesso dell'amministratore

Il ruolo assegnato a un amministratore determina le funzioni che l'amministratore può eseguire con System Manager. System Manager fornisce ruoli predefiniti per gli amministratori dei cluster e gli amministratori delle macchine virtuali dello storage. Il ruolo viene assegnato quando si crea l'account dell'amministratore oppure è possibile assegnarlo in un secondo momento.

A seconda di come è stato attivato l'accesso all'account, potrebbe essere necessario eseguire una delle seguenti operazioni:

- Associare una chiave pubblica a un account locale.
- Installare un certificato digitale del server firmato dalla CA.

- Configurare l’accesso ad, LDAP o NIS.

È possibile eseguire queste attività prima o dopo aver attivato l’accesso all’account.

Assegnazione di un ruolo a un amministratore

Assegnare un ruolo a un amministratore, come indicato di seguito:

Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Selezionare → accanto a **utenti e ruoli**.
3. Selezionare + Add in **utenti**.
4. Specificare un nome utente e selezionare un ruolo nel menu a discesa per **ruolo**.
5. Specificare un metodo di accesso e una password per l’utente.

Modifica del ruolo di amministratore

Modificare il ruolo di amministratore, come segue:

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Selezionare il nome dell’utente di cui si desidera modificare il ruolo, quindi fare clic sul ⋮ che viene visualizzato accanto al nome utente.
3. Fare clic su **Edit** (Modifica).
4. Selezionare un ruolo nel menu a discesa per **ruolo**.