Gestire l'autorizzazione dinamica

ONTAP 9

NetApp
June 19, 2024

Sommario

Gestire l’autorizzazione dinamica

Panoramica delle autorizzazioni dinamiche

A partire da ONTAP 9.15.1, gli amministratori possono configurare e abilitare l’autorizzazione dinamica per aumentare la sicurezza dell’accesso remoto a ONTAP, riducendo al contempo i potenziali danni che potrebbero essere causati da un soggetto malintenzionato. Con ONTAP 9.15.1, l’autorizzazione dinamica fornisce un framework iniziale per assegnare un punteggio di sicurezza agli utenti e, se la loro attività sembra sospetta, sfidarli con ulteriori controlli di autorizzazione o negare completamente un’operazione. Gli amministratori possono creare regole, assegnare punteggi di attendibilità e limitare comandi per determinare quando determinate attività sono consentite o negate per un utente. Gli amministratori possono abilitare l’autorizzazione dinamica per tutto il cluster o per singole macchine virtuali storage.

Come funziona l’autorizzazione dinamica

L’autorizzazione dinamica utilizza un sistema di punteggio di attendibilità per assegnare agli utenti un livello di attendibilità diverso a seconda dei criteri di autorizzazione. In base al livello di attendibilità dell’utente, è possibile consentire o negare un’attività da eseguire oppure richiedere un’ulteriore autenticazione.

Prendiamo ad esempio tre utenti che tentano di eliminare un volume. Nel momento in cui tentano di eseguire l’operazione, viene esaminato il livello di rischio per ciascun utente:

- Il primo utente accede da un dispositivo attendibile alle normali ore di lavoro, il che rende basso il livello di rischio; l’operazione è consentita senza autenticazione aggiuntiva.
- Il secondo utente effettua l’accesso da un dispositivo di fiducia nella propria abitazione al di fuori dell’orario di ufficio, il che rende moderato il livello di rischio; viene richiesta un’ulteriore autenticazione prima che l’operazione venga consentita.
- Il terzo utente effettua l’accesso da un dispositivo non attendibile in una nuova posizione al di fuori dell’orario di ufficio, il che rende il livello di rischio elevato; l’operazione non è consentita.

Cosa succederà

- "Personalizzare l’autorizzazione dinamica"
- "Attiva o disattiva l’autorizzazione dinamica"

Attiva o disattiva l’autorizzazione dinamica

A partire da ONTAP 9.15.1, gli amministratori possono configurare e abilitare l’autorizzazione dinamica in `visibility` per verificare la configurazione, o in `enforced` Modalità per attivare la configurazione per gli utenti CLI che si connettono tramite SSH. Se non è più necessaria l’autorizzazione dinamica, è possibile disattivarla. Quando si disattiva l’autorizzazione dinamica, le impostazioni di configurazione rimangono disponibili e possono essere utilizzate in un secondo momento se si decide di riattivarla.

Per ulteriori informazioni sui parametri di `security dynamic-authorization modify` Fare riferimento alle pagine del manuale di ONTAP.

Abilitare l'autorizzazione dinamica per il test

È possibile attivare l'autorizzazione dinamica in modalità visibilità, che consente di testare la funzione e garantire che gli utenti non vengano accidentalmente bloccati. In questa modalità, il punteggio di attendibilità viene controllato con ogni attività soggetta a restrizioni, ma non applicato. Tuttavia, viene registrata qualsiasi attività che sarebbe stata negata o soggetta a ulteriori problemi di autenticazione. Come Best practice, è necessario testare le impostazioni desiderate in questa modalità prima di applicarle.

> È possibile seguire questa procedura per attivare l'autorizzazione dinamica per la prima volta anche se non sono state ancora configurate altre impostazioni di autorizzazione dinamica. Fare riferimento a. "Personalizzare l'autorizzazione dinamica" procedura per configurare altre impostazioni di autorizzazione dinamiche per personalizzarle in base all'ambiente in uso.

Fasi

1. Abilitare l'autorizzazione dinamica in modalità visibilità configurando le impostazioni globali e modificando lo stato della funzione su `visibility`. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso. I parametri in grassetto sono obbligatori:

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Controllare il risultato utilizzando `show` comando per visualizzare la configurazione globale:

```
security dynamic-authorization show
```

Attivare l'autorizzazione dinamica in modalità forzata

È possibile attivare l'autorizzazione dinamica in modalità forzata. In genere, questa modalità viene utilizzata dopo aver completato il test con la modalità visibilità. In questa modalità, il punteggio di attendibilità viene controllato con ogni attività soggetta a restrizioni e le restrizioni di attività vengono applicate se vengono soddisfatte le condizioni di restrizione. Viene inoltre applicato l'intervallo di soppressione, evitando ulteriori sfide di autenticazione nell'intervallo specificato.

> Questa operazione presuppone che sia stata precedentemente configurata e attivata l'autorizzazione dinamica in `visibility` modalità, vivamente consigliata.

Fasi

1. Attiva autorizzazione dinamica in `enforced` modalita' cambiando il suo stato in `enforced`. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso. I parametri in grassetto sono obbligatori:

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. Controllare il risultato utilizzando `show` comando per visualizzare la configurazione globale:

```
security dynamic-authorization show
```

Disattiva autorizzazione dinamica

È possibile disattivare l'autorizzazione dinamica se non è più necessaria la protezione di autenticazione aggiuntiva.

Fasi

1. Disattivare l'autorizzazione dinamica impostandone lo stato su `disabled`. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso. I parametri in grassetto sono obbligatori:

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. Controllare il risultato utilizzando `show` comando per visualizzare la configurazione globale:

```
security dynamic-authorization show
```

Cosa succederà

(Opzionale) a seconda dell'ambiente, fare riferimento alla "Personalizzare l'autorizzazione dinamica" consente di configurare altre impostazioni di autorizzazione dinamica.

Personalizzare l'autorizzazione dinamica

In qualità di amministratore, è possibile personalizzare diversi aspetti della configurazione dinamica delle autorizzazioni per aumentare la sicurezza delle connessioni SSH dell'amministratore remoto al cluster ONTAP.

È possibile personalizzare le seguenti impostazioni di autorizzazione dinamica in base alle proprie esigenze di sicurezza:

- Configurare le impostazioni globali dell'autorizzazione dinamica
- Configurare i componenti del punteggio di attendibilità dell'autorizzazione dinamica

- Configurare un provider di punteggio di attendibilità personalizzato
- Configurare i comandi con restrizioni
- Configurare i gruppi di autorizzazione dinamici

Configurare le impostazioni globali dell'autorizzazione dinamica

È possibile configurare impostazioni globali per l'autorizzazione dinamica, inclusa la VM di storage da proteggere, l'intervallo di soppressione per le sfide di autenticazione e le impostazioni del punteggio di attendibilità.

Per ulteriori informazioni sui parametri e sui valori predefiniti per `security dynamic-authorization modify` Fare riferimento alle pagine del manuale di ONTAP.

Fasi

1. Configurare le impostazioni globali per l'autorizzazione dinamica. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso:

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Visualizzare la configurazione risultante:

```
security dynamic-authorization show
```

Configurare i comandi con restrizioni

Quando si attiva l'autorizzazione dinamica, la funzione include una serie predefinita di comandi con restrizioni. È possibile modificare questo elenco in base alle proprie esigenze. Fare riferimento a. "Documentazione di verifica multi-admin (MAV)" per informazioni sull'elenco predefinito di comandi con restrizioni.

Aggiungere un comando con restrizioni

È possibile aggiungere un comando all'elenco di comandi limitati con autorizzazione dinamica.

Per ulteriori informazioni sui parametri e sui valori predefiniti per `security dynamic-authorization rule create` Fare riferimento alle pagine del manuale di ONTAP.

Fasi

1. Aggiungere il comando. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. I parametri in grassetto sono obbligatori:

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. Visualizzare l'elenco risultante di comandi con restrizioni:

```
security dynamic-authorization rule show
```

Rimuovere un comando limitato

È possibile rimuovere un comando dall'elenco di comandi limitati con autorizzazione dinamica.

Per ulteriori informazioni sui parametri e sui valori predefiniti per `security dynamic-authorization rule delete` Fare riferimento alle pagine del manuale di ONTAP.

Fasi

1. Rimuovere il comando. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. I parametri in grassetto sono obbligatori:

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. Visualizzare l'elenco risultante di comandi con restrizioni:

```
security dynamic-authorization rule show
```

Configurare i gruppi di autorizzazione dinamici

Per impostazione predefinita, l'autorizzazione dinamica viene applicata a tutti gli utenti e gruppi non appena viene attivata. Tuttavia, è possibile creare gruppi utilizzando `security dynamic-authorization group create` in modo che l'autorizzazione dinamica si applichi solo a quegli utenti specifici.

Aggiungere un gruppo di autorizzazione dinamico

È possibile aggiungere un gruppo di autorizzazione dinamico.

Per ulteriori informazioni sui parametri e sui valori predefiniti per `security dynamic-authorization group create` Fare riferimento alle pagine del manuale di ONTAP.

Fasi

1. Creare il gruppo. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. I parametri in grassetto sono obbligatori:

```
security dynamic-authorization group create \
<strong>-group-name <group-name></strong> \
-vserver <storage_VM_name> \
-exclude-users <user1,user2,user3...>
```

2. Visualizzare i gruppi di autorizzazione dinamici risultanti:

```
security dynamic-authorization group show
```

Rimuovere un gruppo di autorizzazione dinamico

È possibile rimuovere un gruppo di autorizzazione dinamico.

Fasi

1. Eliminare il gruppo. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. I parametri in grassetto sono obbligatori:

```
security dynamic-authorization group delete \
<strong>-group-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. Visualizzare i gruppi di autorizzazione dinamici risultanti:

```
security dynamic-authorization group show
```

Configurare i componenti del punteggio di attendibilità dell'autorizzazione dinamica

È possibile configurare il peso massimo del punteggio per modificare la priorità dei criteri di valutazione o per rimuovere determinati criteri dal punteggio di rischio.

Come prassi migliore, è necessario lasciare i valori di peso del punteggio predefiniti e regolarli solo se necessario.

Per ulteriori informazioni sui parametri e sui valori predefiniti per `security dynamic-authorization trust-score-component modify` Fare riferimento alle pagine del manuale di ONTAP.

Di seguito sono riportati i componenti che è possibile modificare, insieme al punteggio predefinito e ai pesi percentuali:

Criteri	Nome del componente	Peso del punteggio grezzo predefinito	Peso percentuale predefinito
Dispositivo di fiducia	`trusted-device`	20	50
Cronologia autenticazione accesso utente	`authentication-history`	20	50

Fasi

1. Modificare i componenti del punteggio di attendibilità. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. I parametri in grassetto sono obbligatori:

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. Visualizzare le impostazioni del componente del punteggio di attendibilità risultante:

```
security dynamic-authorization trust-score-component show
```

Reimpostare il punteggio di attendibilità per un utente

Se a un utente viene negato l'accesso a causa dei criteri di sistema ed è in grado di dimostrare la propria identità, l'amministratore può reimpostare il punteggio di attendibilità dell'utente.

Per ulteriori informazioni sui parametri e sui valori predefiniti per `security dynamic-authorization user-trust-score reset` Fare riferimento alle pagine del manuale di ONTAP.

Fasi

1. Aggiungere il comando. Fare riferimento a. Configurare i componenti del punteggio di attendibilità dell'autorizzazione dinamica per un elenco dei componenti del punteggio di attendibilità che è possibile reimpostare. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. I parametri in grassetto sono obbligatori:

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

Visualizzare il punteggio di attendibilità

Un utente può visualizzare il proprio punteggio di attendibilità per una sessione di accesso.

Fasi

1. Visualizza il tuo punteggio di fiducia:

```
security login whoami
```

L'output dovrebbe essere simile a quanto segue:

```
User: admin
Role: admin
Trust Score: 50
```

Configurare un provider di punteggio di attendibilità personalizzato

Se si ricevono già metodi di punteggio da un provider di punteggio di attendibilità esterno, è possibile aggiungere il provider personalizzato alla configurazione di autorizzazione dinamica.

Prima di iniziare

- Il provider del punteggio di attendibilità personalizzato deve restituire una risposta JSON. Devono essere soddisfatti i seguenti requisiti di sintassi:
  - Il campo che restituisce il punteggio di attendibilità deve essere un campo scalare e non un elemento di una matrice.
  - Il campo che restituisce il punteggio di attendibilità può essere un campo nidificato, ad esempio `trust_score.value`.
  - Deve essere presente un campo all'interno della risposta JSON che restituisce un punteggio di attendibilità numerico. Se non è disponibile in modalità nativa, è possibile scrivere uno script wrapper per restituire questo valore.
- Il valore fornito può essere un punteggio di attendibilità o un punteggio di rischio. La differenza è che il punteggio di attendibilità è in ordine crescente con un punteggio più alto che indica un livello di attendibilità più elevato, mentre il punteggio di rischio è in ordine decrescente. Ad esempio, un punteggio di attendibilità di 90 per un intervallo di punteggio compreso tra 0 e 100 indica che il punteggio è molto affidabile e che potrebbe risultare in un "consenso" senza ulteriori sfide, mentre un punteggio di rischio pari a 90 per un intervallo di punteggio compreso tra 0 e 100 indica un rischio elevato e che potrebbe causare un "rifiuto" senza una sfida aggiuntiva.
- Il provider del punteggio di attendibilità personalizzato deve essere accessibile tramite l'API REST ONTAP.
- Il provider del punteggio di attendibilità personalizzato deve essere configurabile utilizzando uno dei parametri supportati. I provider di punteggi di attendibilità personalizzati che richiedono una configurazione non inclusa nell'elenco dei parametri supportati non sono supportati.

Per ulteriori informazioni sui parametri e sui valori predefiniti per `security dynamic-authorization trust-score-component create` Fare riferimento alle pagine del manuale di ONTAP.

Fasi

1. Aggiungere un provider di punteggio di attendibilità personalizzato. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. I parametri in grassetto sono obbligatori:

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. Visualizzare le impostazioni del provider del punteggio di attendibilità risultante:

```
security dynamic-authorization trust-score-component show
```

Configurare i tag del provider del punteggio di attendibilità personalizzato

È possibile comunicare con i provider di punteggi di attendibilità esterni utilizzando i tag. Ciò consente di inviare informazioni nell'URL al provider del punteggio di attendibilità senza esporre informazioni riservate.

Per ulteriori informazioni sui parametri e sui valori predefiniti per `security dynamic-authorization trust-score-component create` Fare riferimento alle pagine del manuale di ONTAP.

Fasi

1. Attiva tag provider punteggio di attendibilità. Aggiornare i valori tra parentesi <> in modo che corrispondano all'ambiente in uso. Se non si utilizza `-vserver` il comando viene eseguito a livello di cluster. I parametri in grassetto sono obbligatori:

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

   Ad esempio:

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

Informazioni sul copyright

Informazioni sul marchio commerciale