



Gestire le configurazioni di controllo

ONTAP 9

NetApp
April 24, 2024

Sommario

- Gestire le configurazioni di controllo 1
 - Ruotare manualmente i registri degli eventi di audit 1
 - Abilitare e disabilitare il controllo sulle SVM. 1
 - Visualizzare le informazioni relative al controllo delle configurazioni 2
 - Comandi per la modifica delle configurazioni di controllo 4
 - Eliminare una configurazione di controllo 5
 - Comprendere le implicazioni del ripristino del cluster 5

Gestire le configurazioni di controllo

Ruotare manualmente i registri degli eventi di audit

Prima di poter visualizzare i registri degli eventi di audit, è necessario convertirli in formati leggibili dall'utente. Se si desidera visualizzare i registri degli eventi per una specifica macchina virtuale di storage prima che ONTAP ruoti automaticamente il registro, è possibile ruotare manualmente i registri degli eventi di audit su una SVM.

Fase

1. Ruotare i registri degli eventi di audit utilizzando `vserver audit rotate-log` comando.

```
vserver audit rotate-log -vserver vs1
```

Il registro eventi di audit viene salvato nella directory del registro eventi di audit SVM con il formato specificato dalla configurazione di audit (XML oppure EVTX), e possono essere visualizzati utilizzando l'applicazione appropriata.

Abilitare e disabilitare il controllo sulle SVM

È possibile attivare o disattivare il controllo sulle macchine virtuali di storage (SVM). È possibile interrompere temporaneamente il controllo di file e directory disattivando il controllo. È possibile attivare il controllo in qualsiasi momento (se esiste una configurazione di controllo).

Di cosa hai bisogno

Prima di poter attivare il controllo su SVM, la configurazione di controllo di SVM deve già esistere.

["Creare la configurazione di controllo"](#)

A proposito di questa attività

La disattivazione del controllo non elimina la configurazione del controllo.

Fasi

1. Eseguire il comando appropriato:

Se si desidera che il controllo sia...	Immettere il comando...
Attivato	<code>vserver audit enable -vserver vserver_name</code>
Disattivato	<code>vserver audit disable -vserver vserver_name</code>

2. Verificare che il controllo si trovi nello stato desiderato:

```
vserver audit show -vserver vserver_name
```

Esempi

Nell'esempio seguente viene attivato il controllo per SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

          Vserver: vs1
      Auditing state: true
    Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
          Log Format: evtX
      Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
      Log Rotation Schedule: Day: -
      Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
          Rotation Schedules: -
      Log Files Rotation Limit: 10
```

Nell'esempio seguente viene disattivato il controllo per SVM vs1:

```
cluster1::> vserver audit disable -vserver vs1

          Vserver: vs1
      Auditing state: false
    Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
          Log Format: evtX
      Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
      Log Rotation Schedule: Day: -
      Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
          Rotation Schedules: -
      Log Files Rotation Limit: 10
```

Visualizzare le informazioni relative al controllo delle configurazioni

È possibile visualizzare le informazioni relative al controllo delle configurazioni. Le informazioni consentono di determinare se la configurazione è quella desiderata per ogni SVM. Le informazioni visualizzate consentono inoltre di verificare se è attivata una

configurazione di controllo.

A proposito di questa attività

È possibile visualizzare informazioni dettagliate sulle configurazioni di controllo su tutte le SVM oppure personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali. Se non si specifica alcun parametro opzionale, viene visualizzato quanto segue:

- Nome SVM a cui si applica la configurazione di controllo
- Lo stato di audit, che può essere `true` oppure `false`

Se lo stato di audit è `true`, il controllo è attivato. Se lo stato di audit è `false`, il controllo è disattivato.

- Le categorie di eventi da controllare
- Il formato del registro di controllo
- La directory di destinazione in cui il sottosistema di controllo memorizza i registri di controllo consolidati e convertiti

Fase

1. Visualizzare le informazioni sulla configurazione di controllo utilizzando `vserver audit show` comando.

Per ulteriori informazioni sull'utilizzo del comando, vedere le pagine `man`.

Esempi

Nell'esempio seguente viene visualizzato un riepilogo della configurazione di controllo per tutte le SVM:

```
cluster1::> vserver audit show
```

Vserver	State	Event Types	Log Format	Target Directory
vs1	false	file-ops	evtx	/audit_log

Nell'esempio seguente vengono visualizzate, sotto forma di elenco, tutte le informazioni di configurazione per il controllo di tutte le SVM:

```
cluster1::> vserver audit show -instance

Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
Log Format: evtX
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
```

Comandi per la modifica delle configurazioni di controllo

Se si desidera modificare un'impostazione di controllo, è possibile modificare la configurazione corrente in qualsiasi momento, tra cui la modifica della destinazione del percorso di log e del formato di log, la modifica delle categorie di eventi da controllare, la modalità di salvataggio automatico dei file di log e il numero massimo di file di log da salvare.

Se si desidera...	Utilizzare questo comando...
Modificare il percorso di destinazione del log	<code>vserver audit modify con -destination parametro</code>
Modificare la categoria di eventi da controllare	<div> <div></div> <div>Per controllare gli eventi di staging dei criteri di accesso centrale, è necessario attivare l'opzione del server SMB DAC (Dynamic Access Control) sulla macchina virtuale di storage (SVM).</div> </div> <div><code>vserver audit modify con -events parametro</code></div>
Modificare il formato del registro	<code>vserver audit modify con -format parametro</code>
Attivazione dei salvataggi automatici in base alle dimensioni interne del file di log	<code>vserver audit modify con -rotate-size parametro</code>

Attivazione dei salvataggi automatici in base a un intervallo di tempo	<code>vserver audit modify</code> con <code>-rotate-schedule-month</code> , <code>-rotate-schedule-dayofweek</code> , <code>-rotate-schedule-day</code> , <code>-rotate-schedule-hour</code> , e. <code>-rotate-schedule-minute</code> parametri
Specifica del numero massimo di file di log salvati	<code>vserver audit modify</code> con <code>-rotate-limit</code> parametro

Eliminare una configurazione di controllo

Se non si desidera più controllare gli eventi di file e directory sulla macchina virtuale di storage (SVM) e non si desidera mantenere una configurazione di controllo sulla SVM, è possibile eliminare la configurazione di controllo.

Fasi

1. Disattivare la configurazione di controllo:

```
vserver audit disable -vserver vserver_name
```

```
vserver audit disable -vserver vs1
```

2. Eliminare la configurazione di controllo:

```
vserver audit delete -vserver vserver_name
```

```
vserver audit delete -vserver vs1
```

Comprendere le implicazioni del ripristino del cluster

Se si prevede di ripristinare il cluster, è necessario conoscere il processo di revert che ONTAP segue quando nel cluster sono presenti macchine virtuali di storage abilitate per l'auditing. È necessario eseguire determinate azioni prima di eseguire il ripristino.

Ripristino di una versione di ONTAP che non supporta il controllo degli eventi di logon e logoff SMB e degli eventi di staging dei criteri di accesso centrale

Il supporto per il controllo degli eventi di logon e logoff SMB e per gli eventi di staging dei criteri di accesso centrale inizia con Clustered Data ONTAP 8.3. Se si ripristina una versione di ONTAP che non supporta questi tipi di eventi e si dispone di configurazioni di controllo che monitorano questi tipi di eventi, è necessario modificare la configurazione di controllo per tali SVM abilitate all'audit prima di eseguire il ripristino. È necessario modificare la configurazione in modo che vengano controllati solo gli eventi del file-op.

Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.