Registrazione dell'audit

ONTAP 9

NetApp
September 12, 2024

Sommario

Registrazione dell'audit

Come ONTAP implementa la registrazione dell'audit

Le attività di gestione registrate nel registro di audit sono incluse nei report standard di AutoSupport e alcune attività di registrazione sono incluse nei messaggi EMS. È inoltre possibile inoltrare il registro di controllo alle destinazioni specificate e visualizzare i file di registro di controllo utilizzando la CLI o un browser Web.

A partire da ONTAP 9.11.1, è possibile visualizzare il contenuto del registro di controllo utilizzando Gestione di sistema.

A partire da ONTAP 9.12.1, ONTAP fornisce avvisi di manomissione per i registri di controllo. ONTAP esegue un lavoro giornaliero in background per verificare la presenza di manomissioni di file audit.log e invia un avviso EMS se trova file di registro modificati o manomessi.

ONTAP registra le attività di gestione eseguite sul cluster, ad esempio la richiesta emessa, l'utente che ha attivato la richiesta, il metodo di accesso dell'utente e l'ora della richiesta.

Le attività di gestione possono essere di uno dei seguenti tipi:

- Richieste SET, che in genere si applicano a comandi o operazioni non di visualizzazione:
  - Queste richieste vengono emesse quando si esegue un `create`, `modify`, o. `delete` ad esempio.
  - Le richieste di set vengono registrate per impostazione predefinita.
- Richieste GET, che recuperano le informazioni e le visualizzano nell'interfaccia di gestione:
  - Queste richieste vengono emesse quando si esegue un `show` ad esempio.
  - LE richieste GET non vengono registrate per impostazione predefinita, ma è possibile controllare se LE richieste GET inviate dall'interfaccia CLI ONTAP (`-cliget`), dall'API ONTAP (`-ontapiget`) O dall'API REST (`-httpget`) sono registrati nel file.

ONTAP registra le attività di gestione in `/mroot/etc/log/mlog/audit.log` file di un nodo. I comandi delle tre shell per i comandi CLI—la clustershell, il nodeshell e la shell di sistema non interattiva (i comandi interattivi della shell di sistema non sono registrati)--così come i comandi API sono registrati qui. I registri di audit includono timestamp per mostrare se tutti i nodi di un cluster sono sincronizzati in base all'ora.

Il `audit.log` Il file viene inviato dallo strumento AutoSupport ai destinatari specificati. È inoltre possibile inoltrare il contenuto in modo sicuro alle destinazioni esterne specificate, ad esempio un server Splunk o syslog.

Il `audit.log` il file viene ruotato ogni giorno. La rotazione si verifica anche quando raggiunge 100 MB di dimensione e le precedenti 48 copie vengono conservate (con un totale massimo di 49 file). Quando il file di audit esegue la rotazione giornaliera, non viene generato alcun messaggio EMS. Se il file di audit ruota a causa del superamento del limite di dimensione del file, viene generato un messaggio EMS.

Modifiche alla registrazione dell'audit in ONTAP 9

A partire da ONTAP 9 `command-history.log` il file viene sostituito da `audit.log`e il `mgwd.log` il file non contiene più informazioni di audit. Se si esegue

l'aggiornamento a ONTAP 9, è necessario esaminare gli script o gli strumenti che fanno riferimento ai file legacy e al loro contenuto.

Dopo l'aggiornamento a ONTAP 9, esistente `command-history.log` i file vengono conservati. Vengono ruotati verso l'esterno (cancellati) come nuovi `audit.log` i file vengono ruotati in (creati).

Strumenti e script che controllano `command-history.log` il file potrebbe continuare a funzionare, perché un collegamento soft da `command-history.log` a. `audit.log` viene creato al momento dell'aggiornamento. Tuttavia, strumenti e script che controllano `mgwd.log` il file non riesce, perché non contiene più informazioni di audit.

Inoltre, i registri di controllo di ONTAP 9 e versioni successive non includono più le seguenti voci, in quanto non sono considerate utili e causano attività di registrazione non necessarie:

- Comandi interni eseguiti da ONTAP (ovvero, dove username=root)
- Alias dei comandi (separatamente dal comando a cui puntano)

A partire da ONTAP 9, è possibile trasmettere i registri di controllo in modo sicuro a destinazioni esterne utilizzando i protocolli TCP e TLS.

Visualizzare il contenuto del registro di controllo

È possibile visualizzare il contenuto dei cluster `/mroot/etc/log/mlog/audit.log` Utilizzando l'interfaccia utente di ONTAP, Gestore di sistema o un browser Web.

Le voci del file di log del cluster includono quanto segue:

Ora
: Data e ora della voce di registro.

Applicazione
: L'applicazione utilizzata per connettersi al cluster. Esempi di valori possibili sono `internal, console, ssh, http, ontapi, snmp, rsh, telnet,` e. `service-processor`.

Utente
: Il nome utente dell'utente remoto.

Stato
: Lo stato corrente della richiesta di audit, che potrebbe essere `success, pending,` oppure `error`.

Messaggio
: Campo facoltativo che potrebbe contenere informazioni aggiuntive o errori sullo stato di un comando.

ID sessione
: L'ID della sessione in cui viene ricevuta la richiesta. A ogni *sessione* SSH viene assegnato un ID sessione, mentre a ogni *richiesta* HTTP, ONTAPI o SNMP viene assegnato un ID sessione univoco.

VM di storage
: SVM attraverso cui l'utente si è connesso.

Scopo

Viene visualizzato `svm` Quando la richiesta si trova su una macchina virtuale per lo storage dei dati, altrimenti viene visualizzato `cluster`.

ID comando

L'ID di ciascun comando ricevuto in una sessione CLI. In questo modo è possibile correlare una richiesta e una risposta. Le richieste ZAPI, HTTP e SNMP non dispongono di ID comando.

È possibile visualizzare le voci di registro del cluster dall'interfaccia utente di ONTAP, da un browser Web e a partire da ONTAP 9.11.1, da Gestore di sistema.

System Manager

- Per visualizzare l'inventario, selezionare **Eventi e processi > registri di controllo**. + ogni colonna dispone di controlli per filtrare, ordinare, cercare, mostrare e inventariare le categorie. I dettagli dell'inventario possono essere scaricati come guida Excel.
- Per impostare i filtri, fare clic sul pulsante **Filter** (filtro) in alto a destra, quindi selezionare i campi desiderati. + è inoltre possibile visualizzare tutti i comandi eseguiti nella sessione in cui si è verificato un errore facendo clic sul collegamento Session ID (ID sessione).

CLI

Per visualizzare le voci di audit unite da più nodi nel cluster, immettere:
`security audit log show` *`[parameters]`*

È possibile utilizzare `security audit log show` comando per visualizzare le voci di audit per i singoli nodi o unite da più nodi nel cluster. È inoltre possibile visualizzare il contenuto di `/mroot/etc/log/mlog` directory su un singolo nodo utilizzando un browser web. Per ulteriori informazioni, consulta la pagina man.

Browser Web

È possibile visualizzare il contenuto di `/mroot/etc/log/mlog` directory su un singolo nodo utilizzando un browser web. "Scopri come accedere ai file di log, core dump e MIB di un nodo utilizzando un browser Web".

Gestire le impostazioni di richiesta DI VERIFICA GET

Sebbene LE richieste SET siano registrate per impostazione predefinita, le richieste GET non lo sono. Tuttavia, è possibile controllare se LE richieste GET inviate dall'HTML di ONTAP (`-httpget`), l'interfaccia utente di ONTAP (`-cliget`), o dalle API ONTAP (`-ontapiget`) sono registrati nel file.

È possibile modificare le impostazioni di registrazione dell'audit dalla CLI di ONTAP e, a partire da ONTAP 9.11.1, da Gestore di sistema.

System Manager

1. Selezionare **Eventi e processi > registri di controllo**.
2. Fare clic su ⚙ nell'angolo superiore destro, quindi scegliere le richieste da aggiungere o rimuovere.

CLI

- Per specificare che le richieste GET dall'interfaccia utente o dalle API ONTAP devono essere registrate nel registro di controllo (il file audit.log), oltre alle richieste set predefinite, immettere:
  `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Per visualizzare le impostazioni correnti, immettere:
  `security audit show`

Per ulteriori informazioni, consulta le pagine man.

Gestire le destinazioni del registro di controllo

È possibile inoltrare il registro di controllo a un massimo di 10 destinazioni. Ad esempio, è possibile inoltrare il log a un server Splunk o syslog per scopi di monitoraggio, analisi o backup.

A proposito di questa attività

Per configurare l'inoltro, è necessario fornire l'indirizzo IP dell'host syslog o Splunk, il relativo numero di porta, un protocollo di trasmissione e la funzione syslog da utilizzare per i registri inoltrati. "Scopri le funzionalità di syslog".

È possibile selezionare uno dei seguenti valori di trasmissione:

UDP non crittografato
: User Datagram Protocol senza sicurezza (impostazione predefinita)

TCP non crittografato
: Transmission Control Protocol senza sicurezza

Crittografia TCP
: Transmission Control Protocol with Transport Layer Security (TLS) + Un'opzione **verify server** è disponibile quando si seleziona il protocollo crittografato TCP.

È possibile inoltrare i registri di controllo dall'interfaccia utente di ONTAP e, a partire da ONTAP 9.11.1, da Gestore di sistema.

System Manager

- Per visualizzare le destinazioni del registro di controllo, selezionare **Cluster > Impostazioni**. + Un numero di destinazioni del registro viene visualizzato nel riquadro **Gestione notifiche**. Fare clic ⋮ per visualizzare i dettagli.
- Per aggiungere, modificare o eliminare le destinazioni del registro di controllo, selezionare **Eventi e processi > registri di controllo**, quindi fare clic su **Gestisci destinazioni di controllo** nella parte superiore destra della schermata. + fare clic su + Add o fare clic ⋮ nella colonna **Indirizzo host** per modificare o eliminare le voci.

CLI

1. Per ciascuna destinazione a cui si desidera inoltrare il registro di controllo, specificare l'indirizzo IP o il nome host di destinazione e le opzioni di sicurezza.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - Se il `cluster log-forwarding create` impossibile eseguire il ping dell'host di destinazione per verificare la connettività, il comando non riesce e viene visualizzato un errore. Anche se non consigliato, utilizzare `-force` il parametro con il comando ignora la verifica della connettività.
   - Quando si imposta `-verify-server` parametro a. `true`, l'identità della destinazione di inoltro del log viene verificata convalidando il relativo certificato. È possibile impostare il valore su `true` solo quando si seleziona `tcp-encrypted` valore in `-protocol` campo.

2. Verificare che i record di destinazione siano corretti utilizzando `cluster log-forwarding show` comando.

```
cluster1::> cluster log-forwarding show

                                                  Verify Syslog
Destination Host          Port   Protocol         Server Facility
------------------------- ------ --------         ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            514    tcp-encrypted   true   user
2 entries were displayed.
```

Per ulteriori informazioni, consulta le pagine man.