Come funziona il controllo

ONTAP 9

NetApp
April 24, 2024

Sommario

Come funziona il controllo

Concetti di controllo di base

Per comprendere il controllo in ONTAP, è necessario conoscere alcuni concetti di base relativi al controllo.

- **File di staging**

  I file binari intermedi sui singoli nodi in cui vengono memorizzati i record di audit prima del consolidamento e della conversione. I file di staging sono contenuti nei volumi di staging.

- **Volume di staging**

  Un volume dedicato creato da ONTAP per memorizzare i file di staging. Esiste un volume di staging per aggregato. I volumi di staging sono condivisi da tutte le SVM (Storage Virtual Machine) abilitate all'audit per memorizzare i record di audit dell'accesso ai dati per i volumi di dati in quel particolare aggregato. I record di audit di ogni SVM sono memorizzati in una directory separata all'interno del volume di staging.

  Gli amministratori dei cluster possono visualizzare informazioni sui volumi di staging, ma la maggior parte delle altre operazioni sui volumi non è consentita. Solo ONTAP può creare volumi di staging. ONTAP assegna automaticamente un nome ai volumi di staging. Tutti i nomi dei volumi di staging iniziano con `MDV_aud_` Seguito dall'UUID dell'aggregato contenente il volume di staging (ad esempio: `MDV_aud_1d0131843d4811e296fc123478563412`.)

- **Volumi di sistema**

  Volume FlexVol contenente metadati speciali, ad esempio metadati per i log di audit dei servizi file. La SVM amministrativa possiede i volumi di sistema, visibili all'interno del cluster. I volumi di staging sono un tipo di volume di sistema.

- **Attività di consolidamento**

  Un'attività che viene creata quando viene attivato il controllo. Questa attività a esecuzione prolungata su ogni SVM prende i record di audit dai file di staging attraverso i nodi membri della SVM. Questa attività unisce i record di audit in ordine cronologico ordinato, quindi li converte in un formato di registro eventi leggibile dall'utente specificato nella configurazione di controllo, ovvero IL formato DI file EVTX o XML. I registri eventi convertiti vengono memorizzati nella directory del registro eventi di controllo specificata nella configurazione di controllo SVM.

Come funziona il processo di audit di ONTAP

Il processo di controllo di ONTAP è diverso dal processo di controllo di Microsoft. Prima di configurare il controllo, è necessario comprendere il funzionamento del processo di controllo di ONTAP.

I record di audit vengono inizialmente memorizzati in file di staging binari su singoli nodi. Se il controllo è attivato su una SVM, ogni nodo membro mantiene i file di staging per tale SVM. Periodicamente, vengono consolidati e convertiti in registri eventi leggibili dall'utente, memorizzati nella directory del registro eventi di controllo per SVM.

Processo quando il controllo è attivato su una SVM

Il controllo può essere attivato solo sulle SVM. Quando l'amministratore dello storage abilita il controllo sulla SVM, il sottosistema di controllo verifica se sono presenti volumi di staging. Per ogni aggregato che contiene volumi di dati di proprietà di SVM deve esistere un volume di staging. Il sottosistema di auditing crea tutti i volumi di staging necessari, se non esistono.

Il sottosistema di auditing completa anche altre attività prerequisite prima che sia attivato il controllo:

- Il sottosistema di controllo verifica che il percorso della directory di log sia disponibile e non contenga symlink.

  La directory di log deve già esistere come percorso all'interno dello spazio dei nomi SVM. Si consiglia di creare un nuovo volume o qtree per contenere i file di log dell'audit. Il sottosistema di controllo non assegna una posizione predefinita per il file di log. Se il percorso della directory di log specificato nella configurazione di controllo non è un percorso valido, il controllo della creazione della configurazione non riesce con `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` errore.

  La creazione della configurazione non riesce se la directory esiste ma contiene collegamenti simbolici.

- Il controllo pianifica l'attività di consolidamento.

  Una volta pianificata questa attività, viene attivato il controllo. La configurazione di controllo SVM e i file di log rimangono durante un riavvio o se i server NFS o SMB vengono arrestati o riavviati.

Consolidamento del registro eventi

Il consolidamento dei log è un'attività pianificata che viene eseguita di routine fino alla disattivazione del controllo. Quando il controllo è disattivato, l'attività di consolidamento verifica che tutti i log rimanenti siano consolidati.

Auditing garantito

Per impostazione predefinita, il controllo è garantito. ONTAP garantisce la registrazione di tutti gli eventi di accesso ai file verificabili (come specificato dagli ACL dei criteri di controllo configurati), anche se un nodo non è disponibile. Un'operazione di file richiesta non può essere completata fino a quando il record di audit per tale operazione non viene salvato nel volume di staging sullo storage persistente. Se non è possibile eseguire il commit dei record di audit sul disco nei file di staging, a causa di spazio insufficiente o a causa di altri problemi, le operazioni del client vengono negate.

> Un amministratore, o un utente di account con accesso a livello di privilegio, può ignorare l'operazione di registrazione dell'audit del file utilizzando NetApp Manageability SDK o API REST. È possibile determinare se sono state eseguite azioni sui file utilizzando NetApp Manageability SDK o API REST esaminando i log della cronologia dei comandi memorizzati in `audit.log` file.
>
> Per ulteriori informazioni sui registri di audit della cronologia dei comandi, vedere la sezione "Gestione della registrazione dell'audit per le attività di gestione" in "Amministrazione del sistema".

Processo di consolidamento quando un nodo non è disponibile

Se un nodo contenente volumi appartenenti a una SVM con il controllo attivato non è disponibile, il comportamento dell'attività di consolidamento del controllo dipende dalla disponibilità del partner di storage failover (SFO) del nodo (o del partner ha nel caso di un cluster a due nodi):

- Se il volume di staging è disponibile tramite il partner SFO, l'ultima scansione dei volumi di staging segnalati dal nodo viene eseguita e il consolidamento procede normalmente.
- Se il partner SFO non è disponibile, l'attività crea un file di log parziale.

  Quando un nodo non è raggiungibile, l'attività di consolidamento consolida i record di audit degli altri nodi disponibili di tale SVM. Per identificare che non è completo, l'attività aggiunge il suffisso `.partial` al nome del file consolidato.

- Una volta disponibile il nodo non disponibile, i record di audit in quel nodo vengono consolidati con i record di audit degli altri nodi in quel momento.
- Tutti i record di audit vengono conservati.

Rotazione del registro eventi

I file di log degli eventi di audit vengono ruotati quando raggiungono una dimensione di log di soglia configurata o in base a una pianificazione configurata. Quando un file di registro eventi viene ruotato, l'attività di consolidamento pianificata rinomina prima il file convertito attivo in un file di archivio con data e ora, quindi crea un nuovo file di registro eventi convertito attivo.

Processo quando il controllo è disattivato su SVM

Quando il controllo viene disattivato sulla SVM, l'attività di consolidamento viene attivata una volta finale. Tutti i record di audit registrati in sospeso vengono registrati in un formato leggibile dall'utente. I registri eventi esistenti memorizzati nella directory del registro eventi non vengono cancellati quando il controllo viene disattivato sulla SVM e sono disponibili per la visualizzazione.

Una volta consolidati tutti i file di staging esistenti per la SVM, l'attività di consolidamento viene rimossa dalla pianificazione. La disattivazione della configurazione di controllo per SVM non rimuove la configurazione di controllo. Un amministratore dello storage può riabilitare il controllo in qualsiasi momento.

Il processo di consolidamento di controllo, creato quando viene attivato il controllo, monitora l'attività di consolidamento e la ricrea se l'attività di consolidamento viene chiusa a causa di un errore. Gli utenti non possono eliminare il processo di consolidamento del controllo.