Audit degli eventi NAS su SVM

ONTAP 9

NetApp
February 12, 2026

Sommario

Audit degli eventi NAS su SVM

Scopri come controllare l’accesso ai file utilizzando ONTAP sia per i protocolli SMB che NFS

È possibile utilizzare le funzionalità di controllo dell’accesso ai file disponibili per i protocolli SMB e NFS con ONTAP, come il controllo nativo e la gestione dei criteri dei file utilizzando FPolicy.

È necessario progettare e implementare il controllo degli eventi di accesso ai file SMB e NFS nei seguenti casi:

- È stato configurato l’accesso di base ai file dei protocolli SMB e NFS.
- Si desidera creare e gestire una configurazione di controllo utilizzando uno dei seguenti metodi:
  - Funzionalità ONTAP nativa
  - Server FPolicy esterni

Audit degli eventi NAS su SVM

Il controllo degli eventi NAS è una misura di sicurezza che consente di tenere traccia e registrare determinati eventi SMB e NFS sulle macchine virtuali di storage (SVM). In questo modo è possibile tenere traccia dei potenziali problemi di sicurezza e fornire prove di eventuali violazioni della sicurezza. È inoltre possibile organizzare e controllare le policy di accesso centrale di Active Directory per verificare il risultato dell’implementazione.

Eventi SMB

È possibile controllare i seguenti eventi:

- Eventi di accesso a file e cartelle SMB

  È possibile controllare gli eventi di accesso a file e cartelle SMB sugli oggetti memorizzati nei volumi FlexVol appartenenti alle SVM abilitate per l’auditing.

- Eventi di logon e logoff SMB

  È possibile controllare gli eventi di logon e logoff SMB per i server SMB sulle SVM.

- Eventi di staging dei criteri di accesso centrale

  È possibile controllare l’accesso effettivo degli oggetti sui server SMB utilizzando le autorizzazioni applicate attraverso le policy di accesso centrale proposte. Il controllo attraverso lo staging delle policy di accesso centrale consente di verificare gli effetti delle policy di accesso centrale prima che vengano implementate.

  Il controllo dello staging dei criteri di accesso centrale viene impostato utilizzando gli oggetti Criteri di gruppo di Active Directory; tuttavia, la configurazione di controllo SVM deve essere configurata per controllare gli eventi di staging dei criteri di accesso centrale.

  Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, gli eventi di staging dei criteri di accesso centrale vengono generati solo se è attivato il controllo dinamico degli accessi. Il controllo dinamico degli accessi viene attivato tramite un’opzione server SMB. Non è attivato per impostazione predefinita.

Eventi NFS

È possibile controllare gli eventi di file e directory utilizzando ACL NFSv4 sugli oggetti memorizzati sulle SVM.

Come funziona il controllo

Scoprite i concetti fondamentali di controllo di ONTAP

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.

Informazioni sul funzionamento del processo di auditing 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.

Prerequisiti per il controllo ONTAP

Prima di configurare e abilitare l'auditing sulla macchina virtuale di storage (SVM), è necessario essere a conoscenza di determinati requisiti e considerazioni.

- Il limite combinato per NFS e SVM abilitate all'audit S3 dipende dalla tua versione di ONTAP:

Versione di ONTAP	Massimo
9,8 e precedenti	50
9.9.1 e versioni successive	400

- Il controllo non è legato alle licenze SMB o NFS.

  È possibile configurare e abilitare il controllo anche se le licenze SMB e NFS non sono installate nel cluster.

- Il controllo NFS supporta ACE di sicurezza (tipo U).
- Per il controllo NFS, non esiste alcuna mappatura tra i bit di modalità e le ACE di controllo.

  Quando si convertono gli ACL in bit di modalità, gli ACE di controllo vengono ignorati. Quando si convertono i bit di modalità in ACL, non vengono generati ACE di controllo.

- La directory specificata nella configurazione di controllo deve esistere.

  Se non esiste, il comando per creare la configurazione di controllo non riesce.

- La directory specificata nella configurazione di controllo deve soddisfare i seguenti requisiti:
  - La directory non deve contenere collegamenti simbolici.

    Se la directory specificata nella configurazione di controllo contiene collegamenti simbolici, il comando per creare la configurazione di controllo non riesce.

  - Specificare la directory utilizzando un percorso assoluto.

    Non specificare un percorso relativo, ad esempio `/vs1/../`.

- Il controllo dipende dalla disponibilità di spazio nei volumi di staging.

  È necessario conoscere e disporre di un piano per garantire che vi sia spazio sufficiente per i volumi di staging negli aggregati che contengono volumi sottoposti a audit.

- Il controllo dipende dalla disponibilità di spazio nel volume contenente la directory in cui sono memorizzati i registri degli eventi convertiti.

  È necessario conoscere e disporre di un piano per garantire che vi sia spazio sufficiente nei volumi utilizzati per memorizzare i registri degli eventi. È possibile specificare il numero di registri eventi da conservare nella directory di controllo utilizzando `-rotate-limit` parametro durante la creazione di una configurazione di controllo, che può aiutare a garantire che vi sia spazio disponibile sufficiente per i registri degli eventi nel volume.

- Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, il controllo dinamico degli accessi deve essere abilitato per generare eventi di staging dei criteri di accesso centrale.

  Dynamic Access Control non è attivato per impostazione predefinita.

Aggregare le considerazioni sullo spazio quando si abilita il controllo

Quando viene creata una configurazione di audit e viene attivato il controllo su almeno una macchina virtuale di storage (SVM) nel cluster, il sottosistema di audit crea volumi di staging su tutti gli aggregati esistenti e su tutti i nuovi aggregati creati. Quando si abilita il controllo sul cluster, è necessario tenere conto di alcune considerazioni relative allo spazio aggregato.

La creazione del volume di staging potrebbe non riuscire a causa della non disponibilità di spazio in un aggregato. Questo potrebbe verificarsi se si crea una configurazione di controllo e gli aggregati esistenti non

dispongono di spazio sufficiente per contenere il volume di staging.

Prima di attivare il controllo su una SVM, è necessario assicurarsi che vi sia spazio sufficiente sugli aggregati esistenti per i volumi di staging.

Limitazioni sulle dimensioni dei file di staging per i record di controllo ONTAP

La dimensione di un record di audit in un file di staging non può essere superiore a 32 KB.

Quando possono verificarsi record di audit di grandi dimensioni

Durante il controllo della gestione potrebbero verificarsi record di audit di grandi dimensioni in uno dei seguenti scenari:

- Aggiunta o eliminazione di utenti a o da gruppi con un elevato numero di utenti.
- Aggiunta o eliminazione di un elenco di controllo di accesso (ACL) per la condivisione di file con un gran numero di utenti per la condivisione di file.
- Altri scenari.

Disattivare il controllo di gestione per evitare questo problema. A tale scopo, modificare la configurazione dell'audit e rimuovere quanto segue dall'elenco dei tipi di eventi di audit:

- condivisione file
- account utente
- security-group
- authorization-policy-change

  Dopo la rimozione, non verranno controllati dal sottosistema di controllo dei file Services.

Gli effetti di record di audit troppo grandi

- Se la dimensione di un record di audit è troppo grande (oltre 32 KB), il record di audit non viene creato e il sottosistema di audit genera un messaggio EMS (Event Management System) simile a quanto segue:

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  record because it was greater than max_audit_record_size value. Vserver
  UUID=%s, event_id=%u, size=%u
  ```

  Se il controllo è garantito, l'operazione del file non riesce perché non è possibile creare il relativo record di audit.

- Se la dimensione del record di audit è superiore a 9,999 byte, viene visualizzato lo stesso messaggio EMS riportato sopra. Viene creato un record di audit parziale con il valore chiave più grande mancante.
- Se il record di audit supera i 2,000 caratteri, viene visualizzato il seguente messaggio di errore anziché il valore effettivo:

  ```
  The value of this field was too long to display.
  ```

Informazioni sui formati supportati per i registri degli eventi di controllo ONTAP

I formati di file supportati per i registri degli eventi di audit convertiti sono `EVTX` e. `XML` formati di file.

È possibile specificare il tipo di formato del file quando si crea la configurazione di controllo. Per impostazione predefinita, ONTAP converte i registri binari in `EVTX` formato del file.

Visualizzare ed elaborare i registri degli eventi di controllo ONTAP

È possibile utilizzare i registri degli eventi di audit per determinare se si dispone di una protezione dei file adeguata e se si sono verificati tentativi di accesso a file e cartelle non corretti. È possibile visualizzare ed elaborare i registri degli eventi di audit salvati in `EVTX` oppure `XML` formati di file.

- `EVTX` formato del file

  È possibile aprire il file convertito `EVTX` Controllare i log degli eventi come file salvati utilizzando Microsoft Event Viewer.

  È possibile utilizzare due opzioni per la visualizzazione dei registri eventi mediante il Visualizzatore eventi:

  - Vista generale

    Le informazioni comuni a tutti gli eventi vengono visualizzate per il record dell'evento. In questa versione di ONTAP, i dati specifici dell'evento per il record dell'evento non vengono visualizzati. È possibile utilizzare la vista dettagliata per visualizzare i dati specifici dell'evento.

  - Vista dettagliata

    Sono disponibili una vista intuitiva e una vista XML. La visualizzazione semplice e la visualizzazione XML visualizzano sia le informazioni comuni a tutti gli eventi che i dati specifici dell'evento per il record dell'evento.

- `XML` formato del file

  È possibile visualizzare ed elaborare `XML` registri degli eventi di audit su applicazioni di terze parti che supportano `XML` formato del file. È possibile utilizzare gli strumenti di visualizzazione XML per visualizzare i registri di controllo, a condizione che si disponga dello schema XML e delle informazioni sulle definizioni dei campi XML. Per ulteriori informazioni sullo schema e sulle definizioni XML, vedere "Riferimento allo schema di controllo ONTAP".

Visualizzazione dei registri di controllo attivi mediante Event Viewer

Se il processo di consolidamento dell'audit è in esecuzione sul cluster, il processo di consolidamento aggiunge nuovi record al file di log dell'audit attivo per le macchine virtuali dello storage abilitate all'audit (SVM). È possibile accedere a questo registro di controllo attivo e aprirlo tramite una condivisione SMB in Microsoft Event Viewer.

Oltre a visualizzare i record di audit esistenti, Event Viewer offre un'opzione di refresh che consente di aggiornare il contenuto nella finestra della console. La possibilità di visualizzare i nuovi registri aggiunti nel Visualizzatore eventi dipende dall'attivazione o meno degli oplock nella condivisione utilizzata per accedere al registro di controllo attivo.

Impostazione degli oplock sulla condivisione	Comportamento
Attivato	Event Viewer apre il registro contenente gli eventi scritti fino a quel momento. L'operazione di refresh non aggiorna il log con nuovi eventi aggiunti dal processo di consolidamento.
Disattivato	Event Viewer apre il registro contenente gli eventi scritti fino a quel momento. L'operazione di refresh aggiorna il log con nuovi eventi aggiunti dal processo di consolidamento.

Queste informazioni sono valide solo per `EVTX` registri eventi. `XML` I registri degli eventi possono essere visualizzati tramite SMB in un browser o NFS utilizzando qualsiasi editor o visualizzatore XML.

Eventi SMB che possono essere verificati

Ulteriori informazioni sugli eventi SMB che ONTAP può controllare per interpretare i risultati

ONTAP può controllare alcuni eventi SMB, inclusi determinati eventi di accesso a file e cartelle, determinati eventi di accesso e disconnessione ed eventi di staging dei criteri di accesso centrale. Sapere quali eventi di accesso è possibile verificare è utile quando si interpretano i risultati dei registri eventi.

È possibile controllare i seguenti eventi SMB aggiuntivi:

ID EVENTO (EVT/EVTX)	Evento	Descrizione	Categoria
4670	Le autorizzazioni degli oggetti sono state modificate	OBJECT ACCESS (ACCESSO A OGGETTI): Autorizzazioni modificate.	Accesso al file
4907	Le impostazioni di controllo degli oggetti sono state modificate	OBJECT ACCESS (ACCESSO A OGGETTI): Impostazioni di controllo modificate.	Accesso al file
4913	La policy di accesso di Object Central è stata modificata	ACCESSO A OGGETTI: CAP MODIFICATO.	Accesso al file

I seguenti eventi SMB possono essere verificati in ONTAP 9.0 e versioni successive:

ID EVENTO (EVT/EVTX)	Evento	Descrizione	Categoria
540/4624	Un account è stato collegato correttamente	LOGON/LOGOFF: Accesso alla rete (SMB).	Accesso e disconnessione
529/4625	Impossibile accedere a un account	LOGON/LOGOFF: Nome utente sconosciuto o password errata.	Accesso e disconnessione
530/4625	Impossibile accedere a un account	LOGON/LOGOFF: Limite di tempo per l'accesso all'account.	Accesso e disconnessione
531/4625	Impossibile accedere a un account	LOGON/LOGOFF: Account attualmente disattivato.	Accesso e disconnessione
532/4625	Impossibile accedere a un account	LOGON/LOGOFF: L'account utente è scaduto.	Accesso e disconnessione
533/4625	Impossibile accedere a un account	LOGON/LOGOFF (ACCESSO/DISCONNESSIONE): L'utente non può accedere al computer.	Accesso e disconnessione
534/4625	Impossibile accedere a un account	LOGON/LOGOFF: L'utente non ha concesso il tipo di accesso qui.	Accesso e disconnessione
535/4625	Impossibile accedere a un account	LOGON/LOGOFF: La password dell'utente è scaduta.	Accesso e disconnessione
537/4625	Impossibile accedere a un account	LOGON/LOGOFF: Accesso non riuscito per motivi diversi da quelli sopra indicati.	Accesso e disconnessione
539/4625	Impossibile accedere a un account	LOGON/LOGOFF: Account bloccato.	Accesso e disconnessione
538/4634	Un account è stato disconnesso	LOGON/LOGOFF: Disconnessione dell'utente locale o di rete.	Accesso e disconnessione
560/4656	Apri oggetto/Crea oggetto	ACCESSO A OGGETTI: Oggetto (file o directory) aperto.	Accesso al file
563/4659	Aprire l'oggetto con l'intento di eliminare	ACCESSO A OGGETTI: È stato richiesto un handle a un oggetto (file o directory) con l'intento di eliminare.	Accesso al file

564/4660	Elimina oggetto	OBJECT ACCESS (ACCESSO A OGGETTI): Elimina oggetto (file o directory). ONTAP genera questo evento quando un client Windows tenta di eliminare l'oggetto (file o directory).	Accesso al file
567/4663	Read Object/Write Object/Get Object Attributes/Set Object Attributes	ACCESSO A OGGETTI: Tentativo di accesso a oggetti (lettura, scrittura, attributo get, attributo set). **Nota:** per questo evento, ONTAP controlla solo la prima operazione di lettura SMB e la prima operazione di scrittura SMB (successo o errore) su un oggetto. Ciò impedisce a ONTAP di creare voci di registro eccessive quando un singolo client apre un oggetto ed esegue molte operazioni di lettura o scrittura successive sullo stesso oggetto.	Accesso al file
NA/4664	Collegamento rigido	OBJECT ACCESS (ACCESSO A OGGETTI): Tentativo di creazione di un hard link.	Accesso al file
NA/4818	Il criterio di accesso centrale proposto non concede le stesse autorizzazioni di accesso del criterio di accesso centrale corrente	ACCESSO A OGGETTI: Gestione temporanea dei criteri di accesso centrale.	Accesso al file
ID evento Data ONTAP NA/NA 9999	Rinominare l'oggetto	ACCESSO AGLI OGGETTI: Oggetto rinominato. Si tratta di un evento ONTAP. Attualmente non è supportato da Windows come singolo evento.	Accesso al file
ID evento Data ONTAP NA/NA 9998	Scollegare l'oggetto	ACCESSO A OGGETTI: Oggetto non collegato. Si tratta di un evento ONTAP. Attualmente non è supportato da Windows come singolo evento.	Accesso al file

Ulteriori informazioni sull'evento 4656

Il `HandleID` tag nell'audit `XML` l'evento contiene l'handle dell'oggetto (file o directory) a cui si accede. Il `HandleID` Tag per L'evento EVTX 4656 contiene informazioni diverse a seconda che l'evento aperto sia per la creazione di un nuovo oggetto o per l'apertura di un oggetto esistente:

- Se l'evento open è una richiesta di apertura per creare un nuovo oggetto (file o directory), il `HandleID` Il tag nell'evento XML di audit mostra un valore vuoto `HandleID` (ad esempio: `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).

  Il `HandleID` È vuoto perché la richiesta DI APERTURA (per la creazione di un nuovo oggetto) viene controllata prima che avvenga la creazione effettiva dell'oggetto e prima che esista un handle. Gli eventi controllati successivi per lo stesso oggetto hanno il giusto handle di oggetto in `HandleID` tag.

- Se l'evento open è una richiesta aperta per aprire un oggetto esistente, l'evento di audit avrà l'handle assegnato di tale oggetto in `HandleID` tag (ad esempio: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

Determinare il percorso completo dell'oggetto controllato ONTAP

Il percorso dell'oggetto stampato in `<ObjectName>` il tag per un record di audit contiene il nome del volume (tra parentesi) e il percorso relativo dalla directory principale del volume contenente. Se si desidera determinare il percorso completo dell'oggetto sottoposto a audit, incluso il percorso di giunzione, è necessario eseguire alcuni passaggi.

Fasi

1. Determinare il nome del volume e il relativo percorso dell'oggetto sottoposto a controllo osservando il `<ObjectName>` tag nell'evento di audit.

   In questo esempio, il nome del volume è "data1" e il percorso relativo al file è `/dir1/file.txt`:

   ```
   <Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
   ```

2. Utilizzando il nome del volume determinato nella fase precedente, determinare il percorso di giunzione per il volume contenente l'oggetto verificato:

   In questo esempio, il nome del volume è "data1" e il percorso di giunzione per il volume contenente l'oggetto sottoposto a audit è `/data/data1`:

   ```
   volume show -junction -volume data1
   ```

   ```
                                Junction                       Junction
   Vserver   Volume       Language Active    Junction Path     Path Source
   --------- ------------ -------- --------  ----------------- -----------
   vs1       data1        en_US.UTF-8
                                   true      /data/data1       RW_volume
   ```

3. Determinare il percorso completo dell'oggetto verificato aggiungendo il percorso relativo trovato in `<ObjectName>` contrassegnare il percorso di giunzione per il volume.

   In questo esempio, il percorso di giunzione per il volume:

   ```
   /data/data1/dir1/file.text
   ```

Scopri di più sull'auditing ONTAP di collegamenti simbolici e hard link

Ci sono alcune considerazioni da tenere a mente quando si esegue il controllo dei collegamenti simbolici e dei collegamenti rigidi.

Un record di audit contiene informazioni sull'oggetto sottoposto a audit, incluso il percorso dell'oggetto sottoposto a audit, identificato in `ObjectName` tag. È necessario conoscere come vengono registrati i percorsi per i collegamenti simbolici e gli hard link in `ObjectName` tag.

Link simbolici

Un collegamento simbolico è un file con un inode separato che contiene un puntatore alla posizione di un oggetto di destinazione, noto come destinazione. Quando si accede a un oggetto tramite un collegamento simbolico, ONTAP interpreta automaticamente il collegamento simbolico e segue il percorso indipendente dal protocollo canonico effettivo verso l'oggetto di destinazione nel volume.

Nell'output dell'esempio seguente, sono presenti due collegamenti simbolici, entrambi rivolti a un file denominato `target.txt`. Uno dei link simbolici è un link simbolico relativo e uno è un link simbolico assoluto. Se uno dei collegamenti simbolici viene controllato, il `ObjectName` tag nell'evento di audit contiene il percorso del file `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

Collegamenti hardware

Un hard link è una voce di directory che associa un nome a un file esistente su un file system. L'hard link punta alla posizione inode del file originale. Analogamente a quanto ONTAP interpreta i collegamenti simbolici, ONTAP interpreta il collegamento rigido e segue il percorso canonico effettivo dell'oggetto di destinazione nel volume. Quando viene verificato l'accesso a un oggetto hard link, l'evento di audit registra questo percorso canonico assoluto in `ObjectName` piuttosto che il percorso hard link.

Ulteriori informazioni sul controllo ONTAP dei flussi di dati NTFS alternativi

È necessario tenere presente alcune considerazioni durante il controllo dei file con flussi di dati alternativi NTFS.

La posizione di un oggetto sottoposto a audit viene registrata in un record di evento utilizzando due tag, l' `ObjectName` tag (il percorso) e il `HandleID` tag (l'impugnatura). Per identificare correttamente le richieste di flusso registrate, è necessario conoscere i record ONTAP presenti in questi campi per i flussi di dati alternativi NTFS:

- ID EVTX: 4656 eventi (aprire e creare eventi di audit)
  - Il percorso del flusso di dati alternativo viene registrato in `ObjectName` tag.
  - L'handle del flusso di dati alternativo viene registrato in `HandleID` tag.

- ID EVTX: 4663 eventi (tutti gli altri eventi di audit, come lettura, scrittura, getattr e così via)
  - Il percorso del file di base, non del flusso di dati alternativo, viene registrato in `ObjectName` tag.
  - L'handle del flusso di dati alternativo viene registrato in `HandleID` tag.

Esempio

Nell'esempio seguente viene illustrato come identificare L'ID EVTX: 4663 eventi per flussi di dati alternativi che utilizzano `HandleID` tag. Anche se il `ObjectName` il tag (percorso) registrato nell'evento di controllo in lettura si trova nel percorso del file di base, il `HandleID` il tag può essere utilizzato per identificare l'evento come record di audit per il flusso di dati alternativo.

I nomi dei file di streaming hanno la forma `base_file_name:stream_name`. In questo esempio, il `dir1` la directory contiene un file di base con un flusso di dati alternativo con i seguenti percorsi:

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

L'output nel seguente esempio di evento viene troncato come indicato; l'output non visualizza tutti i tag di output disponibili per gli eventi.

Per un ID EVTX 4656 (evento di audit aperto), l'output del record di audit per il flusso di dati alternativo registra il nome del flusso di dati alternativo in `ObjectName` tag:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

Per un ID EVTX 4663 (evento di audit in lettura), l'output del record di audit per lo stesso flusso di dati alternativo registra il nome del file di base in `ObjectName` tag; tuttavia, l'handle in `HandleID` tag è l'handle alternativo del flusso di dati e può essere utilizzato per correlare questo evento con il flusso di dati alternativo:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

Ulteriori informazioni sul controllo ONTAP degli eventi di accesso a file e directory NFS

ONTAP può controllare alcuni eventi di accesso a file e directory NFS. Sapere quali eventi di accesso possono essere verificati è utile quando si interpretano i risultati dei registri degli eventi di audit convertiti.

È possibile controllare i seguenti eventi di accesso a file e directory NFS:

- LEGGI
- APRIRE
- CHIUDERE
- READDIR
- DI SCRITTURA
- SETATTR
- CREARE
- COLLEGAMENTO
- OPENATTR
- RIMUOVERE
- GETATTR
- VERIFICARE
- NVERIFICARE
- RINOMINARE

Per controllare in modo affidabile gli eventi DI RIDENOMINAZIONE NFS, è necessario impostare ACE di

controllo sulle directory invece che sui file, in quanto le autorizzazioni dei file non vengono controllate per un'operazione DI RIDENOMINAZIONE, se le autorizzazioni della directory sono sufficienti.

Pianificare la configurazione di audit sulle SVM di ONTAP

Prima di configurare il controllo sulle macchine virtuali di storage, è necessario comprendere quali opzioni di configurazione sono disponibili e pianificare i valori che si desidera impostare per ciascuna opzione. Queste informazioni possono aiutarti a configurare la configurazione di controllo che soddisfa le tue esigenze di business.

Alcuni parametri di configurazione sono comuni a tutte le configurazioni di controllo.

Inoltre, è possibile utilizzare alcuni parametri per specificare i metodi da utilizzare durante la rotazione dei registri di controllo consolidati e convertiti. Quando si configura il controllo, è possibile specificare uno dei tre metodi seguenti:

- Ruotare i registri in base alle dimensioni del registro

  Questo è il metodo predefinito utilizzato per ruotare i registri.

- Ruotare i registri in base a una pianificazione
- Rotazione dei registri in base alle dimensioni e alla pianificazione del registro (a seconda dell'evento che si verifica per primo)

È necessario impostare almeno uno dei metodi per la rotazione del log.

Parametri comuni a tutte le configurazioni di controllo

Sono necessari due parametri da specificare quando si crea la configurazione di controllo. Sono inoltre disponibili tre parametri opzionali che è possibile specificare:

Tipo di informazione	Opzione	Obbligatorio	Includi	I tuoi valori
Nome SVM Nome della SVM su cui creare la configurazione di controllo. La SVM deve già esistere.	`-vserver vserver_name`	Sì	Sì	

Percorso di destinazione del registro Specifica la directory in cui sono memorizzati i log di audit convertiti, in genere un volume dedicato o un qtree. Il percorso deve già esistere nello spazio dei nomi SVM. Il percorso può contenere fino a 864 caratteri e deve disporre di permessi di lettura/scrittura. Se il percorso non è valido, il comando di configurazione del controllo non riesce. Se SVM è un'origine di disaster recovery SVM, il percorso di destinazione del log non può trovarsi sul volume root. Questo perché il contenuto del volume root non viene replicato nella destinazione del disaster recovery. Non è possibile utilizzare un volume FlexCache come destinazione del registro (ONTAP 9.7 e versioni successive).	`-destination text`	Sì	Sì	

Categorie di eventi da controllare Specifica le categorie di eventi da controllare. È possibile verificare le seguenti categorie di eventi: • Eventi di accesso al file (SMB e NFSv4) • Eventi di logon e logoff SMB • Eventi di staging dei criteri di accesso centrale Gli eventi di staging dei criteri di accesso centrale sono disponibili a partire dai domini Active Directory di Windows 2012. • Replica-eliminazione • Eventi categoria condivisione file • Eventi di modifica delle policy di audit • Eventi di gestione dell'account utente locale • Eventi di gestione dei gruppi di sicurezza • Eventi di modifica del criterio di autorizzazione Per impostazione predefinita, viene eseguito il controllo dell'accesso al file e degli eventi di logon e logoff SMB. **Nota:** prima di poter specificare `cap-staging` Come categoria di evento, un server SMB deve esistere sulla SVM. Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, gli eventi di staging dei criteri di accesso centrale vengono generati solo se è attivato il controllo dinamico degli accessi. Il controllo dinamico degli accessi viene attivato tramite un'opzione server SMB. Non è attivato per impostazione predefinita.	`-events {file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`
`audit-policy-change`	`user-account`	`security-group`	`authorization-policy-change`	`async-delete}`

No			*Formato di output del file di log* Determina il formato di output dei registri di controllo. Il formato di output può essere specifico di ONTAP `XML` O Microsoft Windows `EVTX` formato del log. Per impostazione predefinita, il formato di output è `EVTX`.	`-format {xml`

`evtx}`	No			*Limite di rotazione dei file di log* Determina il numero di file di log di audit da conservare prima di estrarre il file di log più vecchio. Ad esempio, se si immette un valore di `5`, vengono conservati gli ultimi cinque file di log. Un valore di `0` indica che tutti i file di log vengono conservati. Il valore predefinito è 0.

Parametri utilizzati per determinare quando ruotare i registri degli eventi di audit

Ruota i registri in base alle dimensioni del registro

L'impostazione predefinita prevede la rotazione dei registri di controllo in base alle dimensioni.

- La dimensione predefinita del registro è 100 MB
- Se si desidera utilizzare il metodo di rotazione del log predefinito e la dimensione del log predefinita, non è necessario configurare alcun parametro specifico per la rotazione del log.
- Se si desidera ruotare i registri di controllo solo in base alle dimensioni del registro, utilizzare il comando seguente per annullare l'impostazione di `-rotate-schedule-minute` parametro: `vserver audit`

```
modify -vserver vs0 -destination / -rotate-schedule-minute -
```

Se non si desidera utilizzare la dimensione predefinita del registro, è possibile configurare `-rotate-size` parametro per specificare una dimensione di log personalizzata:

Tipo di informazione	Opzione	Obbligatorio	Includi	I tuoi valori
Limite dimensioni file di log Determina il limite delle dimensioni del file di log di audit.	`-rotate-size` {`integer`[KB	MB	GB	TB

Rotazione dei registri in base a una pianificazione

Se si sceglie di ruotare i registri di controllo in base a una pianificazione, è possibile pianificare la rotazione dei registri utilizzando i parametri di rotazione basati sul tempo in qualsiasi combinazione.

- Se si utilizza la rotazione basata sul tempo, il `-rotate-schedule-minute` il parametro è obbligatorio.
- Tutti gli altri parametri di rotazione basati sul tempo sono opzionali.
- Il programma di rotazione viene calcolato utilizzando tutti i valori relativi al tempo.

  Ad esempio, se si specifica solo il `-rotate-schedule-minute` i file di log di audit vengono ruotati in base ai minuti specificati in tutti i giorni della settimana, durante tutte le ore in tutti i mesi dell'anno.

- Se si specificano solo uno o due parametri di rotazione basati sul tempo (ad esempio, `-rotate -schedule-month` e. `-rotate-schedule-minutes`), i file di log vengono ruotati in base ai valori dei minuti specificati in tutti i giorni della settimana, durante tutte le ore, ma solo durante i mesi specificati.

  Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato durante i mesi di gennaio, marzo e agosto tutti i lunedì, mercoledì e sabato alle 10:30

- Se si specificano i valori per entrambi `-rotate-schedule-dayofweek` e. `-rotate-schedule-day`, sono considerati indipendenti.

  Ad esempio, se si specifica `-rotate-schedule-dayofweek` Come venerdì e. `-rotate-schedule -day` Come 13, i registri di audit verrebbero ruotati ogni venerdì e il 13° giorno del mese specificato, non solo ogni venerdì 13.

- Se si desidera ruotare i registri di controllo solo in base a una pianificazione, utilizzare il comando seguente per annullare l'impostazione di `-rotate-size` parametro: `vserver audit modify -vserver vs0 -destination / -rotate-size -`

È possibile utilizzare il seguente elenco di parametri di controllo disponibili per determinare i valori da utilizzare per la configurazione di una pianificazione per le rotazioni del registro eventi di controllo:

Tipo di informazione	Opzione	Obbligatorio	Includi	I tuoi valori

Programma di rotazione del log: Mese Determina la pianificazione mensile per la rotazione dei registri di audit. I valori validi sono `January` attraverso `December`, e. `all`. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato nei mesi di gennaio, marzo e agosto.	`-rotate-schedule-month chron_month`	No		
Programma di rotazione del log: Giorno della settimana Determina la pianificazione giornaliera (giorno della settimana) per la rotazione dei registri di audit. I valori validi sono `Sunday` attraverso `Saturday`, e. `all`. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato il martedì e il venerdì o durante tutti i giorni di una settimana.	`-rotate-schedule -dayofweek chron_dayofweek`	No		
Programma di rotazione del log: Giorno Determina il giorno della pianificazione del mese per la rotazione del registro di audit. I valori validi sono compresi tra `1` attraverso `31`. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato il 10° e il 20° giorno di un mese o tutti i giorni di un mese.	`-rotate-schedule-day chron_dayofmonth`	No		
Programma di rotazione del log: Ora Determina la pianificazione oraria per la rotazione del registro di audit. I valori validi sono compresi tra `0` (mezzanotte) a. `23` (11:00). Specificare `all` ruota i registri di controllo ogni ora. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato alle 6 (6:00) e alle 18 (18:00).	`-rotate-schedule-hour chron_hour`	No		

Log Rotation schedule: Minute Determina la pianificazione dei minuti per la rotazione del registro di controllo. I valori validi sono compresi tra `0` a. `59`. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato al 30° minuto.	`-rotate-schedule-minute chron_minute`	Sì, se si configura la rotazione del log in base alla pianificazione; in caso contrario, no		

Rotazione dei registri in base alle dimensioni e alla pianificazione dei registri

È possibile scegliere di ruotare i file di log in base alle dimensioni e alla pianificazione del log impostando entrambi i campi `-rotate-size` e i parametri di rotazione basati sul tempo in qualsiasi combinazione. Ad esempio: Se `-rotate-size` È impostato su 10 MB e. `-rotate-schedule-minute` È impostato su 15, i file di log ruotano quando le dimensioni del file di log raggiungono i 10 MB o al 15° minuto di ogni ora (a seconda dell'evento che si verifica per primo).

Creare una configurazione di controllo di file e directory sulle SVM

Creare una configurazione di audit di file e directory su SVM ONTAP

La creazione di una configurazione per il controllo di file e directory sulla macchina virtuale di storage (SVM) include la comprensione delle opzioni di configurazione disponibili, la pianificazione della configurazione, quindi la configurazione e l'abilitazione della configurazione. È quindi possibile visualizzare le informazioni sulla configurazione di controllo per confermare che la configurazione risultante è quella desiderata.

Prima di iniziare il controllo degli eventi di file e directory, è necessario creare una configurazione di controllo sulla macchina virtuale di storage (SVM).

Prima di iniziare

Se si prevede di creare una configurazione di controllo per lo staging dei criteri di accesso centrale, è necessario che un server SMB esista sulla SVM.

- Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, gli eventi di staging dei criteri di accesso centrale vengono generati solo se è attivato il controllo dinamico degli accessi.

  Il controllo dinamico degli accessi viene attivato tramite un'opzione server SMB. Non è attivato per impostazione predefinita.

- Se gli argomenti di un campo in un comando non sono validi, ad esempio voci non valide per campi, voci duplicate e voci non esistenti, il comando non riesce prima della fase di audit.

  Tali errori non generano un record di audit.

A proposito di questa attività

Se SVM è un'origine di disaster recovery SVM, il percorso di destinazione non può trovarsi sul volume root.

Fase

1. Utilizzando le informazioni contenute nel foglio di lavoro di pianificazione, creare la configurazione di controllo per ruotare i registri di controllo in base alle dimensioni del log o a una pianificazione:

Se si desidera ruotare i registri di audit di…	Inserisci…
Dimensione del log	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
Un calendario	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

Esempi

Nell'esempio seguente viene creata una configurazione di controllo che controlla le operazioni dei file e gli eventi di logon e logoff SMB (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. Il formato del log è `EVTX` (impostazione predefinita). I registri vengono memorizzati in `/audit_log` directory. Il limite delle dimensioni del file di registro è `200 MB`. I log vengono ruotati quando raggiungono le dimensioni di 200 MB:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

Nell'esempio seguente viene creata una configurazione di controllo che controlla le operazioni dei file e gli eventi di logon e logoff SMB (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. Il formato del log è `EVTX` (impostazione predefinita). I registri vengono memorizzati in `/cifs_event_logs` directory. Il limite delle dimensioni del file di registro è `100 MB` (l'impostazione predefinita) e il limite di rotazione del registro è `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

Nell'esempio seguente viene creata una configurazione di controllo che controlla le operazioni dei file, gli eventi di logon e logoff di CIFS e gli eventi di staging dei criteri di accesso centrale utilizzando la rotazione basata sul tempo. Il formato del log è `EVTX` (impostazione predefinita). I registri di audit vengono ruotati mensilmente alle 12:30 tutti i giorni della settimana. Il limite di rotazione del log è `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

Informazioni correlate

- "Abilitare il controllo su SVM"
- "Verificare la configurazione di controllo"

Attivare l'audit sulle SVM di ONTAP dopo aver configurato l'audit della configurazione

Una volta completata l'impostazione della configurazione di controllo, è necessario attivare il controllo sulla macchina virtuale di storage (SVM).

Prima di iniziare

La configurazione dell'audit SVM deve già esistere.

A proposito di questa attività

Quando una configurazione di eliminazione dell'ID di disaster recovery SVM viene avviata per la prima volta (dopo il completamento dell'inizializzazione di SnapMirror) e la SVM dispone di una configurazione di controllo, ONTAP disattiva automaticamente la configurazione di controllo. Il controllo viene disattivato sulla SVM di sola lettura per impedire il riempimento dei volumi di staging. È possibile attivare il controllo solo dopo che la relazione SnapMirror è stata interrotta e la SVM è in lettura/scrittura.

Fasi

1. Abilitare il controllo su SVM:

```
vserver audit enable -vserver vserver_name

vserver audit enable -vserver vs1
```

Informazioni correlate

- "Creare la configurazione di controllo"
- "Verificare la configurazione di controllo"

Verificare la configurazione di controllo ONTAP

Dopo aver completato la configurazione di controllo, verificare che il controllo sia configurato correttamente e che sia attivato.

Fasi

1. Verificare la configurazione di controllo:

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

   Il seguente comando visualizza sotto forma di elenco tutte le informazioni di controllo della configurazione per la macchina virtuale di storage (SVM) vs1:

   ```
   vserver audit show -instance -vserver vs1
   ```

   ```
                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
        Categories of Events to Audit: file-ops
                          Log Format: evtx
                  Log File Size Limit: 200MB
         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
   ```

Informazioni correlate

- "Creare la configurazione di controllo"
- "Abilitare il controllo su SVM"

Configurare i criteri di controllo di file e cartelle

Abilitare la configurazione di audit sulle SVM di ONTAP e configurare le policy di audit di file e cartelle

L'implementazione del controllo sugli eventi di accesso a file e cartelle è un processo in due fasi. Innanzitutto, è necessario creare e abilitare una configurazione di controllo sulle macchine virtuali di storage (SVM). In secondo luogo, è necessario configurare i criteri di controllo nei file e nelle cartelle che si desidera monitorare. È possibile configurare criteri di controllo per monitorare i tentativi di accesso riusciti e non riusciti.

È possibile configurare policy di audit SMB e NFS. Le policy di audit SMB e NFS hanno requisiti di configurazione e funzionalità di audit differenti.

Se sono configurati i criteri di audit appropriati, ONTAP monitora gli eventi di accesso SMB e NFS come specificato nelle policy di audit solo se i server SMB o NFS sono in esecuzione.

Configurare i criteri di controllo ONTAP su file e directory con stile di protezione NTFS

Prima di poter controllare le operazioni di file e directory, è necessario configurare i criteri di audit sui file e sulle directory per cui si desidera raccogliere le informazioni di audit. Oltre all'impostazione e all'abilitazione della configurazione di audit. È possibile configurare i criteri di controllo NTFS utilizzando la scheda protezione di Windows o l'interfaccia utente di ONTAP.

Configurazione dei criteri di controllo NTFS mediante la scheda protezione di Windows

È possibile configurare i criteri di controllo NTFS su file e directory utilizzando la scheda **Windows Security** nella finestra Proprietà di Windows. Si tratta dello stesso metodo utilizzato per la configurazione dei criteri di controllo sui dati che risiedono su un client Windows, che consente di utilizzare la stessa interfaccia GUI utilizzata.

Prima di iniziare

Il controllo deve essere configurato sulla macchina virtuale di storage (SVM) che contiene i dati a cui si applicano gli elenchi di controllo di accesso al sistema (SACL).

A proposito di questa attività

La configurazione dei criteri di audit NTFS viene eseguita aggiungendo voci ai SACL NTFS associate a un descrittore di protezione NTFS. Il descrittore di protezione viene quindi applicato ai file e alle directory NTFS. Queste attività vengono gestite automaticamente dalla GUI di Windows. Il descrittore di protezione può contenere elenchi di controllo degli accessi discrezionali (DACL) per l'applicazione delle autorizzazioni di accesso a file e cartelle, SACL per il controllo di file e cartelle o SACL e DACL.

Per impostare i criteri di controllo NTFS utilizzando la scheda protezione di Windows, completare la seguente procedura su un host Windows:

Fasi

1. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
2. Completare la casella **Map Network Drive** (Connetti unità di rete):

    a. Selezionare una lettera **Drive**.

b. Nella casella **Folder** (cartella), digitare il nome del server SMB che contiene la condivisione, contenente i dati che si desidera controllare e il nome della condivisione.

   È possibile specificare l'indirizzo IP dell'interfaccia dati per il server SMB invece del nome del server SMB.

   Se il nome del server SMB è "SMB_SERVER" e la condivisione è denominata "share1", immettere `\\SMB_SERVER\share1`.

c. Fare clic su **fine**.

Il disco selezionato viene montato e pronto con la finestra Esplora risorse che visualizza i file e le cartelle contenuti nella condivisione.

3. Selezionare il file o la directory per cui si desidera abilitare l'accesso di controllo.
4. Fare clic con il pulsante destro del mouse sul file o sulla directory, quindi selezionare **Proprietà**.
5. Selezionare la scheda **sicurezza**.
6. Fare clic su **Avanzate**.
7. Selezionare la scheda **Auditing**.
8. Eseguire le azioni desiderate:

Se si desidera	Effettuare le seguenti operazioni
Impostare il controllo per un nuovo utente o gruppo	a. Fare clic su **Aggiungi**. b. Nella casella immettere il nome dell'oggetto da selezionare, digitare il nome dell'utente o del gruppo che si desidera aggiungere. c. Fare clic su **OK**.
Rimuovere il controllo da un utente o gruppo	a. Nella casella immettere il nome dell'oggetto da selezionare, selezionare l'utente o il gruppo che si desidera rimuovere. b. Fare clic su **Rimuovi**. c. Fare clic su **OK**. d. Ignorare il resto di questa procedura.
Controllo delle modifiche per un utente o un gruppo	a. Nella casella immettere il nome dell'oggetto da selezionare, selezionare l'utente o il gruppo che si desidera modificare. b. Fare clic su **Edit** (Modifica). c. Fare clic su **OK**.

Se si imposta il controllo su un utente o un gruppo o si modifica il controllo su un utente o un gruppo esistente, viene visualizzata la casella voce di controllo per <object>.

9. Nella casella **Applica a**, selezionare la modalità di applicazione della voce di controllo.

   È possibile selezionare una delle seguenti opzioni:

   - **Questa cartella, sottocartelle e file**

- **Questa cartella e sottocartelle**
- **Solo questa cartella**
- **Questa cartella e file**
- **Solo sottocartelle e file**
- **Solo sottocartelle**
- **Solo file** se si imposta il controllo su un singolo file, la casella **Applica a** non è attiva. L'impostazione predefinita della casella **Applica a** è **solo questo oggetto**.

> Poiché il controllo richiede risorse SVM, selezionare solo il livello minimo che fornisce gli eventi di controllo che soddisfano i requisiti di sicurezza.

10. Nella casella **Access**, selezionare i dati da sottoporre a verifica e se si desidera controllare gli eventi di successo, gli eventi di errore o entrambi.
    - Per controllare gli eventi riusciti, selezionare la casella Success (successo).
    - Per controllare gli eventi di errore, selezionare la casella Failure (errore).

      Selezionare solo le azioni da monitorare per soddisfare i requisiti di sicurezza. Per ulteriori informazioni su questi eventi verificabili, consultare la documentazione di Windows. È possibile controllare i seguenti eventi:

    - **Controllo completo**
    - **Cartella Traverse / file di esecuzione**
    - **Elenca cartella / leggi dati**
    - **Attributi di lettura**
    - **Leggi attributi estesi**
    - **Creare file / scrivere dati**
    - **Crea cartelle/Aggiungi dati**
    - **Attributi di scrittura**
    - **Scrivi attributi estesi**
    - **Elimina sottocartelle e file**
    - **Elimina**
    - **Permessi di lettura**
    - **Modifica delle autorizzazioni**
    - **Assumere la proprietà**
11. Se non si desidera che l'impostazione di controllo si propaghi ai file e alle cartelle successivi del contenitore originale, selezionare la casella **Applica queste voci di controllo solo agli oggetti e/o ai contenitori all'interno di questo contenitore**.
12. Fare clic su **Apply** (Applica).
13. Dopo aver aggiunto, rimosso o modificato le voci di controllo, fare clic su **OK**.

    La casella voce di controllo per <object> viene chiusa.

14. Nella casella **Auditing**, selezionare le impostazioni di ereditarietà per questa cartella.

Selezionare solo il livello minimo che fornisce gli eventi di controllo che soddisfano i requisiti di sicurezza. È possibile scegliere una delle seguenti opzioni:

- Selezionare la casella Includi voci di controllo ereditabili dall'oggetto principale.
- Selezionare la casella Sostituisci tutte le voci di controllo ereditabili esistenti su tutti i discendenti con voci di controllo ereditabili da questo oggetto.
- Selezionare entrambe le caselle.
- Selezionare nessuna delle due caselle. Se si impostano SACL su un singolo file, la casella di controllo Sostituisci tutte le voci di controllo ereditabili esistenti su tutti i discendenti con voci di controllo ereditabili da questo oggetto non è presente nella casella di controllo.

15. Fare clic su **OK**.

    La finestra Auditing si chiude.

Configurare i criteri di audit NTFS utilizzando l'interfaccia CLI di ONTAP

È possibile configurare i criteri di controllo su file e cartelle utilizzando l'interfaccia utente di ONTAP. Ciò consente di configurare le policy di audit NTFS senza la necessità di connettersi ai dati utilizzando una condivisione SMB su un client Windows.

È possibile configurare i criteri di audit NTFS utilizzando `vserver security file-directory` famiglia di comandi.

È possibile configurare SACL NTFS solo utilizzando la CLI. La configurazione dei SACL NFSv4 non è supportata con questa famiglia di comandi ONTAP. Ulteriori informazioni sull'utilizzo di questi comandi per configurare e aggiungere SACL NTFS ai file e alle cartelle in "Riferimento al comando ONTAP".

Configurare il controllo ONTAP per file e directory di stile di protezione UNIX

È possibile configurare il controllo per i file e le directory di sicurezza UNIX aggiungendo ACE di controllo agli ACL NFSv4.x. Ciò consente di monitorare determinati eventi di accesso a file e directory NFS per motivi di sicurezza.

A proposito di questa attività

Per NFSv4.x, le ACE discrezionali e di sistema sono memorizzate nello stesso ACL. Non sono memorizzati in DACL e SACL separati. Pertanto, è necessario prestare attenzione quando si aggiungono ACE di audit a un ACL esistente per evitare di sovrascrivere e perdere un ACL esistente. L'ordine in cui si aggiungono le ACE di audit a un ACL esistente non ha importanza.

Fasi

1. Recuperare l'ACL esistente per il file o la directory utilizzando `nfs4_getfacl` o comando equivalente.

   Per ulteriori informazioni sulla manipolazione degli ACL, vedere "Riferimento al comando ONTAP".

2. Aggiungere gli ACE di audit desiderati.
3. Applicare l'ACL aggiornato al file o alla directory utilizzando `nfs4_setfacl` o comando equivalente.

Visualizza informazioni sui criteri di controllo applicati a file e directory

Visualizzare le informazioni sui criteri di controllo ONTAP accedendo alla scheda protezione di Windows

È possibile visualizzare informazioni sui criteri di controllo applicati a file e directory utilizzando la scheda Security (protezione) della finestra Windows Properties (Proprietà di Windows). Si tratta dello stesso metodo utilizzato per i dati residenti su un server Windows, che consente ai clienti di utilizzare la stessa interfaccia GUI a cui sono abituati.

A proposito di questa attività

La visualizzazione delle informazioni sui criteri di controllo applicati a file e directory consente di verificare che siano impostati gli elenchi di controllo di accesso di sistema (SACL) appropriati su file e cartelle specificati.

Per visualizzare informazioni sui SACL applicati a file e cartelle NTFS, completare la seguente procedura su un host Windows.

Fasi

1. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
2. Completare la finestra di dialogo **Map Network Drive** (Connetti unità di rete):

   a. Selezionare una lettera **Drive**.

   b. Nella casella **Folder** (cartella), digitare l'indirizzo IP o il nome del server SMB della macchina virtuale di storage (SVM) contenente la condivisione che contiene sia i dati che si desidera controllare che il nome della condivisione.

      Se il nome del server SMB è "SMB_SERVER" e la condivisione è denominata "share1", immettere `\\SMB_SERVER\share1`.

      > È possibile specificare l'indirizzo IP dell'interfaccia dati per il server SMB invece del nome del server SMB.

   c. Fare clic su **fine**.

   Il disco selezionato viene montato e pronto con la finestra Esplora risorse che visualizza i file e le cartelle contenuti nella condivisione.

3. Selezionare il file o la directory per cui vengono visualizzate le informazioni di controllo.
4. Fare clic con il pulsante destro del mouse sul file o sulla directory e selezionare **Proprietà**.
5. Selezionare la scheda **sicurezza**.
6. Fare clic su **Avanzate**.
7. Selezionare la scheda **Auditing**.
8. Fare clic su **continua**.

   Viene visualizzata la finestra Auditing. Nella casella **voci di controllo** viene visualizzato un riepilogo degli utenti e dei gruppi a cui sono stati applicati SACL.

9. Nella casella **voci di controllo** selezionare l'utente o il gruppo di cui si desidera visualizzare le voci SACL.

10. Fare clic su **Edit** (Modifica).

    Viene visualizzata la finestra voce di controllo per <object>.

11. Nella casella **Access**, visualizzare i SACL correnti applicati all'oggetto selezionato.
12. Fare clic su **Annulla** per chiudere la casella **voce di controllo per <object>**.
13. Fare clic su **Annulla** per chiudere la casella **controllo**.

Visualizza informazioni sui criteri di controllo NTFS sui volumi ONTAP FlexVol

È possibile visualizzare informazioni sui criteri di controllo NTFS sui volumi FlexVol, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli elenchi di controllo degli accessi al sistema. È possibile utilizzare le informazioni per convalidare la configurazione della protezione o per risolvere i problemi di controllo.

A proposito di questa attività

La visualizzazione delle informazioni sui criteri di controllo applicati a file e directory consente di verificare che siano impostati gli elenchi di controllo di accesso di sistema (SACL) appropriati su file e cartelle specificati.

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei file o delle cartelle di cui si desidera visualizzare le informazioni di audit. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree di sicurezza NTFS utilizzano solo SACL (System Access Control List) NTFS per i criteri di controllo.
- I file e le cartelle in un volume misto di sicurezza con protezione efficace NTFS possono applicare criteri di controllo NTFS.

  I volumi misti di sicurezza e le qtree possono contenere alcuni file e directory che utilizzano permessi di file UNIX, i bit di modalità o gli ACL NFSv4 e alcuni file e directory che utilizzano permessi di file NTFS.

- Il livello superiore di un volume misto di sicurezza può avere una protezione efficace UNIX o NTFS e potrebbe contenere o meno SACL NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata su un volume misto di sicurezza o qtree anche se lo stile di sicurezza effettivo della root del volume o del qtree è UNIX, L'output di un volume o percorso qtree in cui Storage-Level Access Guard è configurato potrebbe visualizzare sia SACL NFSv4 di file e cartelle standard che SACL NTFS di Storage-Level Access Guard.
- Se il percorso immesso nel comando è relativo ai dati con protezione effettiva NTFS, l'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se Dynamic Access Control è configurato per il percorso di file o directory specificato.
- Quando si visualizzano informazioni di sicurezza su file e cartelle con protezione efficace NTFS, i campi di output relativi a UNIX contengono informazioni di autorizzazione file UNIX di sola visualizzazione.

  I file e le cartelle di sicurezza NTFS utilizzano solo le autorizzazioni per i file NTFS e gli utenti e i gruppi Windows per determinare i diritti di accesso ai file.

- L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

  Questo campo è vuoto per i file e le cartelle che utilizzano la protezione UNIX e che dispongono solo delle autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi owner e group output nell'output ACL sono validi solo nel caso di descrittori di protezione NTFS.

Fase

1. Visualizzare le impostazioni dei criteri di controllo di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni…	Immettere il seguente comando…
In forma riassuntiva	`vserver security file-directory show -vserver vserver_name -path path`
Come elenco dettagliato	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il percorso `/corp` In SVM vs1. Il percorso offre una protezione efficace con NTFS. Il descrittore di protezione NTFS contiene sia una voce SACL RIUSCITA che UNA SACL RIUSCITA/NON RIUSCITA.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il

percorso `/datavol1` In SVM vs1. Il percorso contiene SACL di file e cartelle e SACL Storage-Level Access Guard.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Utilizzare i caratteri jolly per visualizzare le informazioni sulla protezione dei file ONTAP e sui criteri di controllo

È possibile utilizzare il carattere jolly (*) per visualizzare informazioni sulla sicurezza dei file e sulle policy di controllo di tutti i file e le directory in un determinato percorso o volume root.

Il carattere jolly (*) può essere utilizzato come ultimo sottocomponente di un determinato percorso di directory al di sotto del quale si desidera visualizzare le informazioni di tutti i file e le directory.

Se si desidera visualizzare le informazioni di un determinato file o directory denominata "*", è necessario fornire il percorso completo tra virgolette doppie (" ").

Esempio

Il seguente comando con il carattere jolly visualizza le informazioni su tutti i file e le directory sotto il percorso `/1/` Di SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

Il seguente comando visualizza le informazioni di un file denominato "*" sotto il percorso `/vol1/a` Di SVM vs1. Il percorso è racchiuso tra virgolette doppie (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: NFSV4 Security Descriptor
                        Control:0x8014
                        SACL - ACEs
                          AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                        DACL - ACEs
                          ALLOW-EVERYONE@-0x1f00a9-FI|DI
                          ALLOW-OWNER@-0x1f01ff-FI|DI
                          ALLOW-GROUP@-0x1200a9-IG
```

CLI modifica gli eventi che possono essere verificati

Ulteriori informazioni sugli eventi di modifica della CLI di ONTAP che possono essere verificati

ONTAP è in grado di controllare alcuni eventi di modifica dell'interfaccia CLI, tra cui determinati eventi di condivisione SMB, determinati eventi dei criteri di controllo, determinati eventi dei gruppi di protezione locali, eventi dei gruppi di utenti locali ed eventi dei criteri di autorizzazione. La comprensione degli eventi di modifica che è possibile verificare è utile quando si interpretano i risultati dei registri degli eventi.

È possibile gestire la macchina virtuale dello storage (SVM) per il controllo degli eventi di modifica della CLI ruotando manualmente i registri di controllo, attivando o disattivando il controllo, visualizzando le informazioni relative al controllo degli eventi di modifica, modificando gli eventi di modifica del controllo ed eliminando gli eventi di modifica del controllo.

In qualità di amministratore, se si esegue un comando per modificare la configurazione relativa agli eventi SMB-share, User-group locale, Security-group locale, Authorization-policy e audit-policy, viene generato un record e viene verificato l'evento corrispondente:

Categoria di controllo	Eventi	ID evento	Eseguire questo comando…

Mhost Auditing	cambiamento di policy	[4719] Configurazione dell'audit modificata	`vserver audit disable
enable	modify`	condivisione file	[5142] è stata aggiunta la condivisione di rete
`vserver cifs share create`	[5143] la condivisione di rete è stata modificata	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] condivisione di rete eliminata	`vserver cifs share delete`
Controllo	account utente	[4720] utente locale creato	`vserver cifs users-and-groups local-user create vserver services name-service unix-user create`
[4722] utente locale abilitato	`vserver cifs users-and-groups local-user create	modify`	[4724] reimpostazione della password utente locale
`vserver cifs users-and-groups local-user set-password`	[4725] utente locale disattivato	`vserver cifs users-and-groups local-user create	modify`
[4726] utente locale cancellato	`vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete`	[4738] Modifica utente locale	`vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify`
[4781] Rinomina utente locale	`vserver cifs users-and-groups local-user rename`	security-group	[4731] Gruppo di sicurezza locale creato
`vserver cifs users-and-groups local-group create vserver services name-service unix-group create`	[4734] Gruppo di sicurezza locale cancellato	`vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete`	[4735] Gruppo di sicurezza locale modificato

`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] utente aggiunto al gruppo locale	`vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser`
[4733] utente rimosso dal gruppo locale	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	authorization-policy-change	[4704] diritti utente assegnati
`vserver cifs users-and-groups privilege add-privilege`	[4705] diritti utente rimossi	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

Informazioni correlate

- "server virtuale"

Gestire gli eventi ONTAP di condivisione file

Quando viene configurato un evento di condivisione file per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit. Gli eventi di condivisione file vengono generati quando la condivisione di rete SMB viene modificata utilizzando `vserver cifs share` comandi correlati.

Gli eventi di file-share con gli id evento 5142, 5143 e 5144 vengono generati quando una condivisione di rete SMB viene aggiunta, modificata o eliminata per la SVM. La configurazione della condivisione di rete SMB viene modificata utilizzando `cifs share access control create|modify|delete` comandi.

Nell'esempio seguente viene visualizzato un evento di condivisione file con ID 5143, quando viene creato un oggetto di condivisione denominato 'audit_dest':

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

Gestire eventi ONTAP di modifica della policy di audit

Quando viene configurato un evento audit-policy-change per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit. Gli eventi audit-policy-change vengono generati quando un criterio di audit viene modificato utilizzando `vserver audit` comandi correlati.

L'evento audit-policy-change con l'id evento 4719 viene generato ogni volta che un criterio di audit viene disattivato, attivato o modificato e aiuta a identificare quando un utente tenta di disattivare il controllo per coprire le tracce. È configurato per impostazione predefinita e richiede il privilegio di diagnostica per la disattivazione.

Nell'esempio riportato di seguito viene visualizzato un evento di modifica della policy di audit con l'ID 4719 generato, quando un audit viene disattivato:

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

Consente di gestire gli eventi ONTAP degli account utente

Quando viene configurato un evento account utente per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi dell'account utente con id evento 4720, 4722, 4724, 4725, 4726, 4738 e 4781 vengono generati quando un utente SMB o NFS locale viene creato o cancellato dal sistema, l'account utente locale viene attivato, disattivato o modificato e la password utente SMB locale viene reimpostata o modificata. Gli eventi dell'account utente vengono generati quando un account utente viene modificato utilizzando `vserver cifs users-and-groups <local user>` e. `vserver services name-service <unix user>` comandi.

Nell'esempio seguente viene visualizzato un evento dell'account utente con l'ID 4720 generato, quando viene creato un utente SMB locale:

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

Nell'esempio seguente viene visualizzato un evento dell'account utente con l'ID 4781 generato, quando l'utente SMB locale creato nell'esempio precedente viene rinominato:

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

Gestire gli eventi ONTAP dei gruppi di sicurezza

Quando viene configurato un evento di gruppo di sicurezza per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi del gruppo di sicurezza con id evento 4731, 4732, 4733, 4734 e 4735 vengono generati quando un gruppo SMB o NFS locale viene creato o cancellato dal sistema e l'utente locale viene aggiunto o rimosso dal gruppo. Gli eventi-gruppo-sicurezza vengono generati quando un account utente viene modificato utilizzando `vserver cifs users-and-groups <local-group>` e. `vserver services name-service <unix-group>` comandi.

Nell'esempio seguente viene visualizzato un evento del gruppo di protezione con l'ID 4731 generato quando viene creato un gruppo di protezione UNIX locale:

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

Gestire gli eventi ONTAP di modifica dei criteri di autorizzazione

Quando l'evento Authorization-policy-change viene configurato per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi Authorization-policy-change con ID evento 4704 e 4705 vengono generati ogni volta che vengono concessi o revocati i diritti di autorizzazione per un utente SMB e un gruppo SMB. Gli eventi Authorization-policy-change vengono generati quando i diritti di autorizzazione vengono assegnati o revocati utilizzando `vserver cifs users-and-groups privilege` comandi correlati.

Nell'esempio seguente viene visualizzato un evento del criterio di autorizzazione con l'ID 4704 generato, quando vengono assegnati i diritti di autorizzazione per un gruppo di utenti SMB:

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

Gestire le configurazioni di controllo

Ruotare manualmente i registri degli eventi di audit per visualizzare log degli eventi SVM di ONTAP specifici

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.

Attiva o disattiva l'auditing in ONTAP 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).

Prima di iniziare

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	`vserver audit enable -vserver vserver_name`
Disattivato	`vserver audit disable -vserver vserver_name`

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
```

Visualizza le informazioni sulle configurazioni di controllo ONTAP

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.

   Ulteriori informazioni su `vserver audit show` nella "Riferimento al comando ONTAP".

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 ONTAP 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	`vserver audit modify` con `-destination` parametro

Modificare la categoria di eventi da controllare	`vserver audit modify` con `-events` parametro 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).
Modificare il formato del registro	`vserver audit modify` con `-format` parametro
Attivazione dei salvataggi automatici in base alle dimensioni interne del file di log	`vserver audit modify` con `-rotate-size` parametro
Attivazione dei salvataggi automatici in base a un intervallo di tempo	`vserver audit modify` con `-rotate-schedule -month`, `-rotate-schedule-dayofweek`, `-rotate-schedule-day`, `-rotate-schedule -hour`, e. `-rotate-schedule-minute` parametri
Specifica del numero massimo di file di log salvati	`vserver audit modify` con `-rotate-limit` parametro

Eliminazione di una configurazione di audit su una SVM ONTAP

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 di un cluster ONTAP sottoposto a revisione

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.

Risolvere i problemi di auditing e staging dello spazio dei volumi di ONTAP

Possono verificarsi problemi quando lo spazio disponibile sui volumi di staging o sul volume contenente i registri degli eventi di audit è insufficiente. Se lo spazio è insufficiente, non è possibile creare nuovi record di audit, impedendo ai client di accedere ai dati e impedendo l'esecuzione delle richieste di accesso. Dovresti sapere come risolvere questi problemi di spazio del volume.

Risolvere i problemi di spazio relativi ai volumi del registro eventi

Se i volumi contenenti file di log degli eventi esauriranno lo spazio, il controllo non potrà convertire i record di log in file di log. Ciò comporta errori di accesso al client. È necessario sapere come risolvere i problemi di spazio relativi ai volumi del registro eventi.

- Gli amministratori di Storage Virtual Machine (SVM) e del cluster possono determinare se lo spazio dei volumi è insufficiente visualizzando informazioni sull'utilizzo e sulla configurazione di volumi e aggregati.
- Se lo spazio disponibile nei volumi contenenti registri eventi è insufficiente, gli amministratori di SVM e cluster possono risolvere i problemi di spazio rimuovendo alcuni file di registro eventi o aumentando le dimensioni del volume.

> Se l'aggregato che contiene il volume del registro eventi è pieno, è necessario aumentare le dimensioni dell'aggregato prima di poter aumentare le dimensioni del volume. Solo un amministratore del cluster può aumentare le dimensioni di un aggregato.

- Il percorso di destinazione dei file di registro eventi può essere modificato in una directory di un altro volume modificando la configurazione di controllo.

> L'accesso ai dati viene negato nei seguenti casi:
>
> - La directory di destinazione viene eliminata.
> - Il limite di file su un volume, che ospita la directory di destinazione, raggiunge il livello massimo.

Scopri di più su:

- "Come visualizzare informazioni sui volumi e aumentare le dimensioni del volume".
- "Come visualizzare informazioni sugli aggregati e sulla gestione degli aggregati".

Risolvere i problemi di spazio relativi ai volumi di staging

Se uno dei volumi contenenti file di staging per la macchina virtuale di storage (SVM) esaurisce lo spazio, il controllo non può scrivere record di log nei file di staging. Ciò comporta errori di accesso al client. Per risolvere questo problema, è necessario determinare se uno dei volumi di staging utilizzati nella SVM è pieno visualizzando le informazioni sull'utilizzo del volume.

Se il volume contenente i file di registro eventi consolidati dispone di spazio sufficiente ma si verificano ancora errori di accesso del client a causa di spazio insufficiente, i volumi di staging potrebbero essere fuori spazio. L'amministratore di SVM deve contattare l'utente per determinare se i volumi di staging che contengono file di staging per SVM hanno spazio insufficiente. Il sottosistema di controllo genera un evento EMS se non è possibile generare eventi di controllo a causa dello spazio insufficiente in un volume di staging. Viene visualizzato il seguente messaggio: `No space left on device`. Solo gli amministratori SVM possono visualizzare informazioni sui volumi di staging.

Tutti i nomi dei volumi di staging iniziano con `MDV_aud_` Seguito dall'UUID dell'aggregato contenente il volume di staging. L'esempio seguente mostra quattro volumi di sistema sulla SVM amministrativa, creati automaticamente quando è stata creata una configurazione di controllo dei file service per una SVM di dati nel cluster:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
5%
4 entries were displayed.
```

Se lo spazio disponibile nei volumi di staging è insufficiente, è possibile risolvere i problemi di spazio aumentando le dimensioni del volume.

> Se l'aggregato che contiene il volume di staging è pieno, è necessario aumentare le dimensioni dell'aggregato prima di poter aumentare le dimensioni del volume. Solo gli amministratori di SVM possono aumentare le dimensioni di un aggregato.

Se uno o più aggregati hanno uno spazio disponibile inferiore a 2GB GB (in ONTAP 9.14.1 e versioni precedenti) o 5GB GB (a partire da ONTAP 9.15.1), la creazione del controllo SVM non riesce. Quando la creazione dell'audit SVM non riesce, i volumi di staging creati vengono cancellati.

Informazioni sul copyright

Informazioni sul marchio commerciale