Configurare i criteri di controllo di file e cartelle

ONTAP 9

NetApp
September 12, 2024

Sommario

Configurare i criteri di controllo di file e cartelle

Configurare i criteri di controllo 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 le policy di audit su file e directory di sicurezza 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. Consultare le pagine man per ulteriori informazioni sull'utilizzo di questi comandi per configurare e aggiungere SACL NTFS a file e cartelle.

Configurare il controllo per i file e le directory di sicurezza 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, consulta le pagine man del tuo client NFS.

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