Visualizza informazioni sui criteri di controllo applicati a file e directory

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/it-it/ontap/nas-audit/display-audit-policies-windows-security-tab-task.html on September 12, 2024. Always check docs.netapp.com for the latest.

Sommario

Visualizza informazioni sui criteri di controllo applicati a file e directory 1
Visualizzare le informazioni sui criteri di controllo utilizzando la scheda protezione di Windows 1
Visualizza informazioni sui criteri di audit NTFS sui volumi FlexVol utilizzando l'interfaccia CLI 2
Modi per visualizzare informazioni sulla sicurezza dei file e sulle policy di audit 6

Visualizza informazioni sui criteri di controllo applicati a file e directory

Visualizzare le informazioni sui criteri di controllo utilizzando la 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 audit NTFS sui volumi FlexVol utilizzando l'interfaccia CLI

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
```

Modi per visualizzare informazioni sulla sicurezza dei file e sulle policy di audit

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
```

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.