



Configurare e applicare i criteri di controllo ai file e alle cartelle NTFS utilizzando la CLI

ONTAP 9

NetApp
April 24, 2024

Sommario

- Configurare e applicare i criteri di controllo ai file e alle cartelle NTFS utilizzando la panoramica CLI 1
 - Creare un descrittore di protezione NTFS 1
 - Aggiungere le voci di controllo dell'accesso NTFS SACL al descrittore di protezione NTFS 3
 - Creare policy di sicurezza 4
 - Aggiungere un'attività alla policy di sicurezza 4
 - Applicare le policy di sicurezza 6
 - Monitorare il processo di policy di sicurezza 7
 - Verificare la policy di audit applicata 7

Configurare e applicare i criteri di controllo ai file e alle cartelle NTFS utilizzando la panoramica CLI

È necessario eseguire diversi passaggi per applicare i criteri di controllo a file e cartelle NTFS quando si utilizza l'interfaccia utente di ONTAP. Innanzitutto, si crea un descrittore di protezione NTFS e si aggiungono SACL al descrittore di protezione. Quindi, creare una policy di sicurezza e aggiungere attività di policy. Quindi, applicare il criterio di protezione a una macchina virtuale di storage (SVM).

A proposito di questa attività

Dopo aver applicato il criterio di protezione, è possibile monitorare il processo di criteri di protezione e verificare le impostazioni per il criterio di controllo applicato.



Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

Informazioni correlate

[Protezione dell'accesso ai file mediante Storage-Level Access Guard](#)

[Limiti di utilizzo della CLI per impostare la sicurezza di file e cartelle](#)

[Come vengono utilizzati i descrittori di protezione per applicare la sicurezza di file e cartelle](#)

["Controllo SMB e NFS e tracciamento della sicurezza"](#)

[Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI](#)

Creare un descrittore di protezione NTFS

La creazione di un criterio di audit del descrittore di protezione NTFS è il primo passo nella configurazione e nell'applicazione degli elenchi di controllo di accesso (ACL) NTFS a file e cartelle che risiedono all'interno delle SVM. Il descrittore di protezione verrà associato al percorso del file o della cartella in un'attività di policy.

A proposito di questa attività

È possibile creare descrittori di protezione NTFS per file e cartelle che risiedono all'interno di volumi di sicurezza NTFS o per file e cartelle che risiedono su volumi misti di tipo sicurezza.

Per impostazione predefinita, quando viene creato un descrittore di protezione, vengono aggiunte quattro voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) a tale descrittore di protezione. Le quattro ACE predefinite sono le seguenti:

| Oggetto | Tipo di accesso | Diritti di accesso | Dove applicare le autorizzazioni |
|--------------------------|-----------------|--------------------|--------------------------------------|
| BUILTIN/amministratori | Consentire | Controllo completo | questa-cartella, sottocartelle, file |
| BUILTIN/utenti | Consentire | Controllo completo | questa-cartella, sottocartelle, file |
| PROPRIETARIO DEL CREATOR | Consentire | Controllo completo | questa-cartella, sottocartelle, file |
| AUTORITÀ/SISTEMA NT | Consentire | Controllo completo | questa-cartella, sottocartelle, file |

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Proprietario del descrittore di protezione
- Gruppo primario del proprietario
- Flag di controllo raw

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Se si desidera utilizzare i parametri avanzati, impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Creare un descrittore di sicurezza: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

`vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`
3. Verificare che la configurazione del descrittore di protezione sia corretta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. Se si è nel livello di privilegio avanzato, tornare al livello di privilegio admin: `set -privilege admin`

Aggiungere le voci di controllo dell'accesso NTFS SACL al descrittore di protezione NTFS

L'aggiunta di voci di controllo di accesso (ACE) SACL (elenco di controllo di accesso al sistema) al descrittore di protezione NTFS è la seconda fase della creazione di criteri di controllo NTFS per file o cartelle in SVM. Ogni voce identifica l'utente o il gruppo che si desidera controllare. La voce SACL definisce se si desidera controllare i tentativi di accesso riusciti o non riusciti.

A proposito di questa attività

È possibile aggiungere uno o più ACE al SACL del descrittore di protezione.

Se il descrittore di protezione contiene un SACL con ACE esistenti, il comando aggiunge il nuovo ACE al SACL. Se il descrittore di protezione non contiene un SACL, il comando crea il SACL e aggiunge il nuovo ACE.

È possibile configurare le voci SACL specificando i diritti da controllare per gli eventi di successo o di errore per l'account specificato in `-account` parametro. Esistono tre metodi di esclusione reciproca per specificare i diritti:

- Diritti
- Diritti avanzati
- Diritti raw (privilegio avanzato)



Se non si specificano i diritti per la voce SACL, l'impostazione predefinita è `Full Control`.

È possibile personalizzare le voci SACL specificando come applicare l'ereditarietà con `apply to` parametro. Se non si specifica questo parametro, l'impostazione predefinita prevede l'applicazione di questa voce SACL a questa cartella, sottocartelle e file.

Fasi

1. Aggiungere una voce SACL a un descrittore di protezione: `vserver security file-directory ntfs sac1 add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDOptional_parameters`

```
vserver security file-directory ntfs sac1 add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Verificare che la voce SACL sia corretta: `vserver security file-directory ntfs sac1 show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

```
vserver security file-directory ntfs sac1 show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

Creare policy di sicurezza

La creazione di un criterio di audit per le macchine virtuali di storage (SVM) è la terza fase della configurazione e dell'applicazione degli ACL a un file o a una cartella. Un criterio agisce come un contenitore per varie attività, in cui ogni attività è una singola voce che può essere applicata a file o cartelle. È possibile aggiungere attività al criterio di protezione in un secondo momento.

A proposito di questa attività

Le attività aggiunte a un criterio di protezione contengono associazioni tra il descrittore di protezione NTFS e i percorsi di file o cartelle. Pertanto, è necessario associare la policy di sicurezza a ciascuna macchina virtuale di storage (SVM) (contenente volumi di sicurezza NTFS o volumi misti di sicurezza).

Fasi

1. Creare una policy di sicurezza: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. Verificare la policy di sicurezza: `vserver security file-directory policy show`

```
vserver security file-directory policy show
Vserver      Policy Name
-----
vs1          policy1
```

Aggiungere un'attività alla policy di sicurezza

La creazione e l'aggiunta di un'attività di policy a un criterio di sicurezza è la quarta fase della configurazione e dell'applicazione degli ACL a file o cartelle in SVM. Quando si crea l'attività relativa ai criteri, l'attività viene associata a un criterio di protezione. È possibile aggiungere una o più voci di attività a un criterio di protezione.

A proposito di questa attività

La policy di sicurezza è un container per un'attività. Un'attività si riferisce a una singola operazione che può essere eseguita da un criterio di protezione a file o cartelle con NTFS o protezione mista (o a un oggetto volume se si configura Storage-Level Access Guard).

Esistono due tipi di attività:

- Attività di file e directory

Consente di specificare le attività che applicano i descrittori di protezione a file e cartelle specifici. Gli ACL applicati attraverso le attività di file e directory possono essere gestiti con client SMB o CLI ONTAP.

- Attività di Access Guard a livello di storage

Consente di specificare le attività che applicano i descrittori di protezione di Storage-Level Access Guard a un volume specificato. Gli ACL applicati tramite le attività di Access Guard a livello di storage possono essere gestiti solo tramite l'interfaccia utente di ONTAP.

Un'attività contiene le definizioni per la configurazione di sicurezza di un file (o di una cartella) o di un set di file (o di cartelle). Ogni attività di una policy è identificata in modo univoco dal percorso. Un'unica attività per percorso può essere presente all'interno di un singolo criterio. Un criterio non può avere voci di attività duplicate.

Linee guida per l'aggiunta di un'attività a un criterio:

- È possibile includere un massimo di 10,000 voci di attività per policy.
- Un criterio può contenere una o più attività.

Anche se un criterio può contenere più attività, non è possibile configurare un criterio in modo che contenga sia le attività file-directory che Storage-Level Access Guard. Un criterio deve contenere tutte le attività Storage-Level Access Guard o tutte le attività di file-directory.

- Storage-Level Access Guard viene utilizzato per limitare le autorizzazioni.

Non assegnerà mai autorizzazioni di accesso aggiuntive.

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Tipo di sicurezza
- Modalità di propagazione
- Posizione dell'indice
- Tipo di controllo dell'accesso

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` è il valore predefinito di `-access-control` parametro. La specifica del tipo di

controllo dell'accesso durante la configurazione delle attività di accesso a file e directory è facoltativa.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. Verificare la configurazione dell'attività del criterio: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1
```

| Index | File/Folder | Access | Security | NTFS | NTFS |
|-----------------|-------------|----------------|----------|-----------|------|
| Security | Path | Control | Type | Mode | |
| Descriptor Name | | | | | |
| ----- | ----- | ----- | ----- | ----- | |
| ----- | | | | | |
| 1 | /home/dir1 | file-directory | ntfs | propagate | sd2 |

Applicare le policy di sicurezza

L'applicazione di un criterio di audit alle SVM è l'ultimo passo nella creazione e nell'applicazione di ACL NTFS a file o cartelle.

A proposito di questa attività

È possibile applicare le impostazioni di protezione definite nel criterio di protezione ai file e alle cartelle NTFS che risiedono nei volumi FlexVol (NTFS o stile di protezione misto).



Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Quando vengono applicati un criterio di protezione e i DACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

Fase

1. Applicare una policy di sicurezza: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

Il processo di applicazione della policy viene pianificato e viene restituito l'ID lavoro.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```


Monitorare il processo di policy di sicurezza

Quando si applica la policy di sicurezza alle macchine virtuali di storage (SVM), è possibile monitorare l'avanzamento dell'attività monitorando il processo di policy di sicurezza. Ciò è utile se si desidera verificare che l'applicazione del criterio di protezione sia riuscita. Questo è utile anche se si dispone di un processo a esecuzione prolungata in cui si applica la protezione in blocco a un gran numero di file e cartelle.

A proposito di questa attività

Per visualizzare informazioni dettagliate su un processo di policy di sicurezza, utilizzare `-instance` parametro.

Fase

1. Monitorare il processo di policy di sicurezza: `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

| Job ID | Name | Vserver | Node | State |
|--|-----------------|---------|-------|---------|
| 53322 | Fsecurity Apply | vs1 | node1 | Success |
| Description: File Directory Security Apply Job | | | | |

Verificare la policy di audit applicata

È possibile verificare il criterio di controllo per confermare che i file o le cartelle sulla macchina virtuale di storage (SVM) a cui è stato applicato il criterio di protezione dispongano delle impostazioni di sicurezza di controllo desiderate.

A proposito di questa attività

Si utilizza `vserver security file-directory show` comando per visualizzare le informazioni sui criteri di controllo. Specificare il nome della SVM che contiene i dati e il percorso dei dati di cui si desidera visualizzare le informazioni sui criteri di controllo del file o della cartella.

Fase

1. Visualizzare le impostazioni dei criteri di controllo: `vserver security file-directory show -vserver vserver_name -path path`

Esempio

Il seguente comando visualizza le informazioni di policy di audit applicate al percorso `/corp` in SVM vs1. Il percorso ha applicato 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
      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
```

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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.