



Visualizza informazioni sulla sicurezza dei file e sulle policy di audit

ONTAP 9

NetApp
April 24, 2024

Sommario

- Visualizza informazioni sulla sicurezza dei file e sulle policy di audit 1
 - Visualizza informazioni generali sulla sicurezza dei file e sui criteri di controllo 1
 - Visualizza le informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security. 2
 - Visualizza informazioni sulla sicurezza dei file su volumi misti di sicurezza 8
 - Visualizza informazioni sulla sicurezza dei file su volumi UNIX di tipo Security 11
 - Visualizza informazioni sui criteri di audit NTFS sui volumi FlexVol utilizzando l'interfaccia CLI. 14
 - Visualizza informazioni sui criteri di audit NFSv4 sui volumi FlexVol utilizzando la CLI 17
 - Modi per visualizzare informazioni sulla sicurezza dei file e sulle policy di audit. 18

Visualizza informazioni sulla sicurezza dei file e sulle policy di audit

Visualizza informazioni generali sulla sicurezza dei file e sui criteri di controllo

È possibile visualizzare informazioni sulla sicurezza dei file su file e directory contenuti nei volumi su macchine virtuali di storage (SVM). È possibile visualizzare informazioni sui criteri di controllo sui volumi FlexVol. Se configurato, è possibile visualizzare informazioni sulle impostazioni di protezione accesso a livello di storage e controllo dinamico degli accessi sui volumi FlexVol.

Visualizzazione delle informazioni sulla sicurezza dei file

È possibile visualizzare le informazioni sulla sicurezza dei file applicate ai dati contenuti nei volumi e nei qtree (per i volumi FlexVol) con i seguenti stili di sicurezza:

- NTFS
- UNIX
- Misto

Visualizzazione delle informazioni sui criteri di controllo

È possibile visualizzare informazioni sulle policy di audit per il controllo degli eventi di accesso sui volumi FlexVol sui seguenti protocolli NAS:

- SMB (tutte le versioni)
- NFSv4.x

Visualizzazione di informazioni sulla sicurezza di Storage-Level Access Guard (SLAG)

La protezione degli accessi a livello di storage può essere applicata a volumi FlexVol e oggetti qtree con i seguenti stili di sicurezza:

- NTFS
- Misto
- UNIX (se un server CIFS è configurato sulla SVM che contiene il volume)

Visualizzazione di informazioni sulla sicurezza del controllo dinamico degli accessi (DAC)

La protezione del controllo dinamico degli accessi può essere applicata a un oggetto all'interno di un volume FlexVol con i seguenti stili di protezione:

- NTFS

- Misto (se l'oggetto dispone di una protezione efficace NTFS)

Informazioni correlate

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

[Visualizzazione di informazioni su Storage-Level Access Guard](#)

Visualizza le informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security

È possibile visualizzare informazioni sulla sicurezza di file e directory sui volumi di sicurezza NTFS, inclusi lo stile di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli attributi DOS. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei dati di cui si desidera visualizzare le informazioni di sicurezza relative al file o alla cartella. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- Poiché i volumi e i qtree 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, i campi di output relativi a UNIX contengono informazioni sulle autorizzazioni per i file UNIX di sola visualizzazione.
- L'output ACL viene visualizzato per file e cartelle con protezione NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata sulla radice del volume o sul qtree, l'output di un volume o percorso del qtree in cui è configurato Storage-Level Access Guard potrebbe visualizzare sia gli ACL dei file normali che gli ACL di Storage-Level Access Guard.
- L'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se il controllo dinamico degli accessi è configurato per il percorso di file o directory specificato.

Fase

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Con dettagli più dettagliati	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso /vol4 in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4
```

```

        Vserver: vs1
        File Path: /vol4
    File Inode Number: 64
        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:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff
            ALLOW-Everyone-0x10000000-
```

OI|CI|IO

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza con maschere estese sul percorso /data/engineering In SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true
```

```

        Vserver: vs1
        File Path: /data/engineering
    File Inode Number: 5544
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
```

```

    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
    Control:0x8004

```

```

    1... .. = Self Relative
    .0.. .. = RM Control Valid
    ..0. .. = SACL Protected
    ...0 .. = DACL Protected
    .... 0... .. = SACL Inherited
    .... .0.. .. = DACL Inherited
    .... ..0. .. = SACL Inherit Required
    .... ...0 .. = DACL Inherit Required
    .... .... .0. .... = SACL Defaulted
    .... .... ...0 .... = SACL Present
    .... .... .... 0... = DACL Defaulted
    .... .... .... .1.. = DACL Present
    .... .... .... ..0. = Group Defaulted
    .... .... .... ...0 = Owner Defaulted

```

```

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs

```

```

    ALLOW-Everyone-0x1f01ff

```

	0... .. =
Generic Read	
	.0.. .. =
Generic Write	
	..0. =
Generic Execute	
	...0 =
Generic All	
0 =
System Security	
1 =
Synchronize	
 1... .. =
Write Owner	
1.. =
Write DAC	
1. =
Read Control	
1 =
Delete	

1..... =
Write Attributes	
1.... =
Read Attributes	
1... =
Delete Child	
1. =
Execute	
1 =
Write EA	
1... =
Read EA	
1... =
Append	
1. =
Write	
1 =
Read	
	ALLOW-Everyone-0x10000000-OI CI IO
	0.... =
Generic Read	
	.0... =
Generic Write	
	..0. =
Generic Execute	
	...1 =
Generic All	
0 =
System Security	
0 =
Synchronize	
0 =
Write Owner	
0... =
Write DAC	
0. =
Read Control	
0 =
Delete	
0 =
Write Attributes	
0... =
Read Attributes	
0... =
Delete Child	

Execute0..... =
Write EA0..... =
Read EA0..... =
Append0..... =
Write0..... =
Read0..... =

Nell'esempio riportato di seguito vengono visualizzate le informazioni di sicurezza, incluse le informazioni di protezione Storage-Level Access Guard, per il volume con il percorso /datavol1 In SVM vs1:


```
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:0x8004
          Owner: BUILTIN\Administrators
          Group: BUILTIN\Administrators
          DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

    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
```

Informazioni correlate

[Visualizzazione di informazioni sulla sicurezza dei file su volumi misti di tipo sicurezza](#)

[Visualizzazione delle informazioni sulla sicurezza dei file sui volumi UNIX di tipo Security](#)

Visualizza informazioni sulla sicurezza dei file su volumi misti di sicurezza

È possibile visualizzare informazioni sulla sicurezza di file e directory su volumi misti di sicurezza, inclusi lo stile di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sui proprietari e sui gruppi UNIX. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei dati di cui si desidera visualizzare le informazioni di sicurezza relative al file o alla cartella. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree misti di sicurezza possono contenere alcuni file e cartelle 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.
- L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

Questo campo è vuoto per i file e le directory che utilizzano la protezione UNIX e che hanno solo 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.
- 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 le autorizzazioni dei file UNIX che gli ACL Storage-Level Access Guard.
- Se il percorso immesso nel comando riguarda i dati con protezione effettiva NTFS, l'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se è configurato Dynamic Access Control per il percorso di file o directory specificato.

Fase

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Con dettagli più dettagliati	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/projects` in SVM `vs1` in forma di maschera espansa. Questo percorso misto in stile di sicurezza offre una sicurezza efficace per UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true
```

```

        Vserver: vs1
        File Path: /projects
        File Inode Number: 78
        Security Style: mixed
        Effective Style: unix
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: 0x10
        ....0 .... = Offline
        .... ..0. .... = Sparse
        .... .... 0... .... = Normal
        .... .... ..0. .... = Archive
        .... .... ...1 .... = Directory
        .... .... .... .0.. = System
        .... .... .... ..0. = Hidden
        .... .... .... ...0 = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
        Unix Mode Bits in Text: rwx-----
        ACLs: -
```

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso /data in SVM vs1. Questo percorso misto di sicurezza ha una protezione efficace NTFS.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data
```

```

        Vserver: vs1
        File Path: /data
    File Inode Number: 544
        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:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-
```

OI|CI|IO

Nell'esempio riportato di seguito vengono visualizzate le informazioni di sicurezza relative al volume nel percorso /datavol5 in SVM vs1. Il livello superiore di questo volume misto di sicurezza offre una protezione efficace per UNIX. Il volume dispone della protezione di Storage-Level Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
```

```
      Vserver: vs1
      File Path: /datavol5
File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
```

Informazioni correlate

[Visualizzazione delle informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security](#)

[Visualizzazione delle informazioni sulla sicurezza dei file sui volumi UNIX di tipo Security](#)

Visualizza informazioni sulla sicurezza dei file su volumi UNIX di tipo Security

È possibile visualizzare informazioni sulla sicurezza di file e directory sui volumi UNIX di

tipo Security, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sui proprietari e sui gruppi UNIX. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei dati di cui si desidera visualizzare le informazioni di sicurezza relative al file o alla directory. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree UNIX di sicurezza utilizzano solo le autorizzazioni dei file UNIX, ovvero i bit di modalità o gli ACL NFSv4 per determinare i diritti di accesso ai file.
- L'output ACL viene visualizzato solo per file e cartelle con protezione NFSv4.

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

- I campi di output del proprietario e del gruppo nell'output ACL non sono validi nel caso dei descrittori di protezione NFSv4.

Sono significativi solo per i descrittori di protezione NTFS.

- Poiché la protezione Storage-Level Access Guard è supportata su un volume o qtree UNIX se un server CIFS è configurato su SVM, l'output potrebbe contenere informazioni sulla protezione Storage-Level Access Guard applicata al volume o al qtree specificato in `-path` parametro.

Fase

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Con dettagli più dettagliati	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/home` in SVM `vs1`:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```

      Vserver: vs1
      File Path: /home
      File Inode Number: 9590
      Security Style: unix
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 1
      Unix Mode Bits: 700
      Unix Mode Bits in Text: rwx-----
      ACLs: -
```

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso /home in SVM vs1 sotto forma di maschera espansa:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true
```

```

      Vserver: vs1
      File Path: /home
      File Inode Number: 9590
      Security Style: unix
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: 0x10
      ...0 .... = Offline
      .... ..0. .... = Sparse
      .... .... 0... .... = Normal
      .... .... ..0. .... = Archive
      .... .... ...1 .... = Directory
      .... .... .... .0.. = System
      .... .... .... ..0. = Hidden
      .... .... .... ...0 = Read Only
      Unix User Id: 0
      Unix Group Id: 1
      Unix Mode Bits: 700
      Unix Mode Bits in Text: rwx-----
      ACLs: -
```

Informazioni correlate

[Visualizzazione delle informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security](#)

[Visualizzazione di informazioni sulla sicurezza dei file su volumi misti di tipo sicurezza](#)

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 i risultati per convalidare la configurazione della protezione o per risolvere i problemi di controllo.

A proposito di questa attività

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	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Come elenco dettagliato	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

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
```

Visualizza informazioni sui criteri di audit NFSv4 sui volumi FlexVol utilizzando la CLI

È possibile visualizzare informazioni sui criteri di controllo di NFSv4 sui volumi FlexVol utilizzando l'interfaccia CLI di ONTAP, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli elenchi di controllo dell'accesso al sistema (SACL). È possibile utilizzare i risultati per convalidare la configurazione della protezione o per risolvere i problemi di controllo.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei file o delle directory 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 UNIX di sicurezza utilizzano solo SACL NFSv4 per le policy di controllo.
- I file e le directory di un volume misto di sicurezza con stile UNIX possono applicare criteri di controllo NFSv4.
- 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 NFSv4.
- 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.
- 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 normali di file NFSv4, directory e SACL NTFS di Storage-Level Access Guard.
- Poiché la protezione Storage-Level Access Guard è supportata su un volume o qtree UNIX se un server CIFS è configurato su SVM, l'output potrebbe contenere informazioni sulla protezione Storage-Level Access Guard applicata al volume o al qtree specificato in `-path` parametro.

Fasi

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Con dettagli più dettagliati	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso /lab in SVM vs1. Questo percorso di sicurezza UNIX ha un SACL NFSv4.

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

      Vserver: vs1
      File Path: /lab
      File Inode Number: 288
      Security Style: unix
      Effective Style: unix
      DOS Attributes: 11
      DOS Attributes in Text: ----D--R
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 0
      Unix Mode Bits in Text: -----
      ACLs: NFSV4 Security Descriptor
            Control:0x8014
            SACL - ACEs
                  SUCCESSFUL-S-1-520-0-0xf01ff-SA
                  FAILED-S-1-520-0-0xf01ff-FA
            DACL - ACEs
                  ALLOW-S-1-520-1-0xf01ff
```

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 particolare 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 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.