



Permessi di sicurezza del file

ONTAP Automation

NetApp
July 11, 2024

Sommario

- Permessi di sicurezza del file 1
 - Prepararsi a gestire la sicurezza dei file e le policy di controllo 1
 - Ottenere le autorizzazioni effettive per un file 2
 - Ottenere le informazioni di controllo per un file 4
 - Applicare nuove autorizzazioni a un file 7
 - Aggiornare le informazioni del descrittore di protezione 8
 - Eliminare una voce di controllo degli accessi 9

Permessi di sicurezza del file

Prepararsi a gestire la sicurezza dei file e le policy di controllo

È possibile gestire le autorizzazioni e le policy di audit per i file disponibili nelle SVM all'interno di un cluster ONTAP.

Panoramica

ONTAP utilizza gli elenchi di controllo di accesso di sistema (SACL) e gli elenchi di controllo di accesso discrezionali (DACL) per assegnare le autorizzazioni agli oggetti file. A partire da ONTAP 9.9.1, l'API REST include il supporto per la gestione delle autorizzazioni SACL e DACL. È possibile utilizzare l'API per automatizzare l'amministrazione delle autorizzazioni di protezione dei file. In molti casi è possibile utilizzare una singola chiamata API REST invece di più comandi CLI o chiamate ONTAPI (ZAPI).



Per le versioni ONTAP precedenti alla 9.9.1, è possibile automatizzare l'amministrazione delle autorizzazioni SACL e DACL utilizzando la funzione Passthrough CLI. Vedere ["Considerazioni sulla migrazione"](#) e ["Utilizzo del pass-through CLI privato con l'API REST di ONTAP"](#) per ulteriori informazioni.

Sono disponibili diversi flussi di lavoro di esempio per illustrare come gestire i servizi di sicurezza dei file ONTAP utilizzando l'API REST. Prima di utilizzare i flussi di lavoro e di inviare una qualsiasi delle chiamate API REST, assicurarsi di riesaminarla ["Preparati a utilizzare i flussi di lavoro"](#).

Se si utilizza Python, vedere anche lo script ["file_security_permissions.py"](#) per esempi su come automatizzare alcune attività di protezione dei file.

API REST ONTAP e comandi CLI ONTAP

Per molte attività, l'utilizzo dell'API REST ONTAP richiede un numero inferiore di chiamate rispetto ai comandi CLI o alle chiamate ONTAPI (ZAPI) di ONTAP equivalenti. La tabella seguente include un elenco di chiamate API e l'equivalente dei comandi CLI necessari per ciascuna attività.

API REST di ONTAP	CLI ONTAP
GET /protocols/file-security/effective-permissions/	<code>vserver security file-directory show-effective-permissions</code>
POST /protocols/file-security/permissions/	<ol style="list-style-type: none"><code>vserver security file-directory ntfs create</code><code>vserver security file-directory ntfs dacl add</code><code>vserver security file-directory ntfs sacl add</code><code>vserver security file-directory policy create</code><code>vserver security file-directory policy task add</code><code>vserver security file-directory apply</code>

API REST di ONTAP	CLI ONTAP
PATCH /protocols/file-security/permissions/	vserver security file-directory ntfs modify
DELETE /protocols/file-security/permissions/	<ol style="list-style-type: none"> 1. vserver security file-directory ntfs dacl remove 2. vserver security file-directory ntfs sacl remove

Informazioni correlate

- ["Script Python che illustra le autorizzazioni dei file"](#)
- ["Gestione semplificata delle autorizzazioni di sicurezza dei file con le API REST di ONTAP"](#)
- ["Utilizzo del pass-through CLI privato con l'API REST di ONTAP"](#)

Ottenere le autorizzazioni effettive per un file

È possibile recuperare le autorizzazioni effettive correnti per un file o una cartella specifici.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/protocolli/file-security/effective-permissions/{svm.uuid}/{path}

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
\$SVM_ID	Percorso	Sì	UUUID della SVM che contiene il file.
\$PERCORSO_FILE	Percorso	Sì	Questo è il percorso del file o della cartella.

Esempio di arricciamento

```
curl --request GET \  
--location "https://$FQDN_IP/api/protocols/file-security/effective-  
permissions/$SVM_ID/$FILE_PATH" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

Esempio di output JSON

```
{
  "svm": {
    "uuid": "cf5f271a-1beb-11ea-8fad-005056bb645e",
    "name": "vs1"
  },
  "user": "administrator",
  "type": "windows",
  "path": "/",
  "share": {
    "path": "/"
  },
  "file_permission": [
    "read",
    "write",
    "append",
    "read_ea",
    "write_ea",
    "execute",
    "delete_child",
    "read_attributes",
    "write_attributes",
    "delete",
    "read_control",
    "write_dac",
    "write_owner",
    "synchronize",
    "system_security"
  ],
  "share_permission": [
    "read",
    "read_ea",
    "execute",
    "read_attributes",
    "read_control",
    "synchronize"
  ]
}
```

Ottenere le informazioni di controllo per un file

È possibile recuperare le informazioni di controllo per un file o una cartella specifici.

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
OTTIENI	/api/protocolli/file-security/permissions/{svm.uuid}/{path}

Tipo di elaborazione

Sincrono

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligat orio	Descrizione
\$SVM_ID	Percorso	Sì	UUUID della SVM che contiene il file.
\$PERCORSO_FILE	Percorso	Sì	Questo è il percorso del file o della cartella.

Esempio di arricciamento

```
curl --request GET \
--location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Esempio di output JSON

```
{
  "svm": {
    "uuid": "9479099d-5b9f-11eb-9c4e-0050568e8682",
    "name": "vs1"
  },
  "path": "/parent",
  "owner": "BUILTIN\\Administrators",
  "group": "BUILTIN\\Administrators",
  "control_flags": "0x8014",
  "acls": [
    {
      "user": "BUILTIN\\Administrators",
      "access": "access_allow",
      "apply_to": {
        "files": true,
        "sub_folders": true,
        "this_folder": true
      },
      "advanced_rights": {
        "append_data": true,
```

```

        "delete": true,
        "delete_child": true,
        "execute_file": true,
        "full_control": true,
        "read_attr": true,
        "read_data": true,
        "read_ea": true,
        "read_perm": true,
        "write_attr": true,
        "write_data": true,
        "write_ea": true,
        "write_owner": true,
        "synchronize": true,
        "write_perm": true
    },
    "access_control": "file_directory"
},
{
    "user": "BUILTIN\\Users",
    "access": "access_allow",
    "apply_to": {
        "files": true,
        "sub_folders": true,
        "this_folder": true
    },
    "advanced_rights": {
        "append_data": true,
        "delete": true,
        "delete_child": true,
        "execute_file": true,
        "full_control": true,
        "read_attr": true,
        "read_data": true,
        "read_ea": true,
        "read_perm": true,
        "write_attr": true,
        "write_data": true,
        "write_ea": true,
        "write_owner": true,
        "synchronize": true,
        "write_perm": true
    },
    "access_control": "file_directory"
}
],
"inode": 64,

```



```
"security_style": "mixed",
"effective_style": "ntfs",
"dos_attributes": "10",
"text_dos_attr": "----D---",
"user_id": "0",
"group_id": "0",
"mode_bits": 777,
"text_mode_bits": "rwxrwxrwx"
}
```

Applicare nuove autorizzazioni a un file

È possibile applicare un nuovo descrittore di protezione a un file o una cartella specifici.

Passaggio 1: Applicare le nuove autorizzazioni

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/protocolli/file-security/permissions/{svm.uuid}/{path}

Tipo di elaborazione

Asincrono

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
\$SVM_ID	Percorso	Sì	UUUID della SVM che contiene il file.
\$PERCORSO_FILE	Percorso	Sì	Questo è il percorso del file o della cartella.

Esempio di arricciamento

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{ \acl\": [ { \access\": \access_allow\", \advanced_rights\": { \append_data\": true, \delete\": true, \delete_child\": true, \execute_file\": true, \full_control\": true, \read_attr\": true, \read_data\": true, \read_ea\": true, \read_perm\": true, \write_attr\": true, \write_data\": true, \write_ea\": true, \write_owner\": true, \write_perm\": true }, \apply_to\": { \files\": true, \sub_folders\": true, \this_folder\": true }, \user\": \administrator\" } ], \control_flags\": \32788\", \group\": \S-1-5-21-2233347455-2266964949-1780268902-69700\", \ignore_paths\": [ \parent/child2\" ], \owner\": \S-1-5-21-2233347455-2266964949-1780268902-69304\", \propagation_mode\": \propagate\''
```

Esempio di output JSON

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Passo 2: Recupero dello stato del lavoro

Eeguire il flusso di lavoro ["Recupera istanza lavoro"](#) e confermare state il valore è success.

Aggiornare le informazioni del descrittore di protezione

È possibile aggiornare un descrittore di protezione specifico a un file o una cartella specifici, inclusi i flag del proprietario, del gruppo o del controllo principale.

Passaggio 1: Aggiornare il descrittore di protezione

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
PATCH	/api/protocolli/file-security/permissions/{svm.uuid}/{path}

Tipo di elaborazione

Asincrono

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
\$SVM_ID	Percorso	Sì	UUUID della SVM che contiene il file.
\$PERCORSO_FILE	Percorso	Sì	Questo è il percorso del file o della cartella.

Esempio di arricciamento

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{ \"control_flags\": \"32788\", \"group\": \"everyone\", \"owner\": \"user1\"}'
```

Esempio di output JSON

```
{
  "job": {
    "uuid": "6f89e612-5bbd-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/6f89e612-5bbd-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Passo 2: Recupero dello stato del lavoro

Eseguire il flusso di lavoro ["Recupera istanza lavoro"](#) e confermare state il valore è success.

Eliminare una voce di controllo degli accessi

È possibile eliminare una voce ACE (Access Control Entry) esistente da un file o una cartella specifici. La modifica si propaga a qualsiasi oggetto figlio.

Passaggio 1: Eliminare l'ACE

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
ELIMINARE	/api/protocolli/file-security/permissions/{svm.uuid}/{path}

Tipo di elaborazione

Asincrono

Parametri di input aggiuntivi per esempi di arricciatura

Oltre ai parametri comuni a tutte le chiamate REST API, nell'esempio curl in questo passo vengono utilizzati anche i seguenti parametri.

Parametro	Tipo	Obbligatorio	Descrizione
\$SVM_ID	Percorso	Sì	UUUID della SVM che contiene il file.
\$PERCORSO_FILE	Percorso	Sì	Questo è il percorso del file o della cartella.

Esempio di arricciamento

```
curl --request DELETE --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{ "access": "access_allow", "apply_to": { "files": true, "sub_folders": true, "this_folder": true }, "ignore_paths": [ "/parent/child2" ], "propagation_mode": "propagate" }'
```

Esempio di output JSON

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

Passo 2: Recupero dello stato del lavoro

Eseguire il flusso di lavoro ["Recupera istanza lavoro"](#) e confermare state il valore è success.

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.