



# Dateisicherheitsberechtigungen

## ONTAP Automation

NetApp  
July 19, 2024

# Inhalt

- Dateisicherheitsberechtigungen ..... 1
  - Bereiten Sie sich auf das Management von Dateisicherheits- und Audit-Richtlinien vor ..... 1
  - Holen Sie sich die effektiven Berechtigungen für eine Datei ..... 2
  - Rufen Sie die Auditinformationen für eine Datei ab ..... 4
  - Neue Berechtigungen auf eine Datei anwenden ..... 7
  - Die Informationen zum Sicherheitsdeskriptor aktualisieren ..... 8
  - Löschen eines Zugriffskontrolleintrags ..... 9

# Dateisicherheitsberechtigungen

## Bereiten Sie sich auf das Management von Dateisicherheits- und Audit-Richtlinien vor

Sie können die Berechtigungen und Audit-Richtlinien für Dateien managen, die über die SVMs innerhalb eines ONTAP Clusters verfügbar sind.

### Überblick

ONTAP weist Dateiobjekten mithilfe von System Access Control Lists (SACLs) und Ermessensary Access Control Lists (DACLS) Berechtigungen zu. Ab ONTAP 9.9 unterstützt die REST-API das Management der SACL- und DACL-Berechtigungen. Sie können die API verwenden, um die Administration der Dateisicherheitsberechtigungen zu automatisieren. In vielen Fällen können Sie einen einzelnen REST API-Aufruf anstelle mehrerer CLI-Befehle oder ONTAPI (ZAPI)-Aufrufe verwenden.



Bei ONTAP-Versionen vor 9.9 können Sie die Verwaltung der SACL- und DACL-Berechtigungen mithilfe der CLI-Passthrough-Funktion automatisieren. Siehe ["Überlegungen zur Migration"](#) Und ["Verwenden des privaten CLI-Passthrough mit der ONTAP REST API"](#) Finden Sie weitere Informationen.

Es stehen verschiedene Beispiel-Workflows zur Verfügung, die veranschaulichen, wie Sie die ONTAP Dateisicherheitsdienste mithilfe der REST-API managen. Bevor Sie die Workflows verwenden und einen der REST-API-Aufrufe ausgeben, müssen Sie diese überprüfen ["Die Nutzung der Workflows wird vorbereitet"](#).

Wenn Sie Python verwenden, lesen Sie auch das Skript ["file\\_security\\_permissions.py"](#) Beispiele für die Automatisierung einiger Dateisicherheitsaktivitäten.

### ONTAP REST API im Vergleich zu ONTAP-CLI-Befehlen

Bei vielen Aufgaben erfordert die Verwendung der ONTAP REST-API weniger Aufrufe als die entsprechenden ONTAP CLI-Befehle oder ONTAPI (ZAPI)-Aufrufe. Die folgende Tabelle enthält eine Liste der API-Aufrufe und die entsprechenden CLI-Befehle, die für jede Aufgabe erforderlich sind.

ONTAP REST API	CLI VON 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"><li><code>vserver security file-directory ntfs create</code></li><li><code>vserver security file-directory ntfs dacl add</code></li><li><code>vserver security file-directory ntfs sacl add</code></li><li><code>vserver security file-directory policy create</code></li><li><code>vserver security file-directory policy task add</code></li><li><code>vserver security file-directory apply</code></li></ol>

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

#### Verwandte Informationen

- ["Python-Skript zur Darstellung von Dateiberechtigungen"](#)
- ["Vereinfachtes Management von Dateisicherheitsberechtigungen mit ONTAP REST-APIs"](#)
- ["Verwenden des privaten CLI-Passthrough mit der ONTAP REST API"](#)

## Holen Sie sich die effektiven Berechtigungen für eine Datei

Sie können die aktuellen effektiven Berechtigungen für eine bestimmte Datei oder einen bestimmten Ordner abrufen.

#### HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/protocols/file-Security/effective-permissions/{svm.uuid}/ path{

#### Verarbeitungsart

Synchron

#### Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Datei enthält.
Pfad FÜR DATEI	Pfad	Ja.	Dies ist der Pfad zur Datei oder zum Ordner.

## Beispiel für die Wellung

```
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"
```

## Beispiel für eine JSON-Ausgabe

```
{
  "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"
  ]
}
```

## Rufen Sie die Auditinformationen für eine Datei ab

Sie können die Überwachungsinformationen für eine bestimmte Datei oder einen bestimmten Ordner abrufen.

**HTTP-Methode und -Endpoint**

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
GET	/API/protocols/file-Security/permissions/{svm.uuid}/} path{

### Verarbeitungsart

Synchron

### Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Datei enthält.
PFAD FÜR DATEI	Pfad	Ja.	Dies ist der Pfad zur Datei oder zum Ordner.

### Beispiel für die Wellung

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

### Beispiel für eine JSON-Ausgabe

```
{  
  "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"
}

```

## Neue Berechtigungen auf eine Datei anwenden

Sie können eine neue Sicherheitsbeschreibung auf eine bestimmte Datei oder einen bestimmten Ordner anwenden.

### Schritt 1: Die neuen Berechtigungen anwenden

#### HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/protocols/file-Security/permissions/{svm.uuid}/ path{

#### Verarbeitungsart

Asynchron

#### Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Datei enthält.
PFAD FÜR DATEI	Pfad	Ja.	Dies ist der Pfad zur Datei oder zum Ordner.

## Beispiel für die Wellung

```
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\''
```

## Beispiel für eine JSON-Ausgabe

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

## Schritt 2: Rufen Sie den Status des Jobs ab

Führen Sie den Workflow aus ["Job-Instanz abrufen"](#) Und bestätigen Sie die state Wert ist success.

## Die Informationen zum Sicherheitsdeskriptor aktualisieren

Sie können eine bestimmte Sicherheitsbeschreibung auf eine bestimmte Datei oder einen bestimmten Ordner aktualisieren, einschließlich der primären Eigentümer-, Gruppen- oder Kontrollflags.

## Schritt 1: Aktualisieren Sie die Sicherheitsbeschreibung

### HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
PATCH	/API/protocols/file-Security/permissions/{svm.uuid}/ path{

### Verarbeitungsart

Asynchron

### Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Datei enthält.
PFAD FÜR DATEI	Pfad	Ja.	Dies ist der Pfad zur Datei oder zum Ordner.

### Beispiel für die Wellung

```
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\"}'
```

### Beispiel für eine JSON-Ausgabe

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

## Schritt 2: Rufen Sie den Status des Jobs ab

Führen Sie den Workflow aus ["Job-Instanz abrufen"](#) Und bestätigen Sie die state Wert ist success.

## Löschen eines Zugriffskontrolleintrags

Sie können einen vorhandenen ACE (Access Control Entry) aus einer bestimmten Datei oder einem bestimmten Ordner löschen. Die Änderung wird auf alle untergeordneten Objekte übertragen.

## Schritt 1: Löschen Sie ACE

### HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
Löschen	/API/protocols/file-Security/permissions/{svm.uuid}/} path{

### Verarbeitungsart

Asynchron

### Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

Parameter	Typ	Erforderlich	Beschreibung
SVM_ID USD	Pfad	Ja.	Dies ist die UUID der SVM, die die Datei enthält.
PFAD FÜR DATEI	Pfad	Ja.	Dies ist der Pfad zur Datei oder zum Ordner.

### Beispiel für die Wellung

```
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\"}'
```

### Beispiel für eine JSON-Ausgabe

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

## Schritt 2: Rufen Sie den Status des Jobs ab

Führen Sie den Workflow aus ["Job-Instanz abrufen"](#) Und bestätigen Sie die state Wert ist success.

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.