Dateisicherheitsberechtigungen

ONTAP Automation

NetApp
July 19, 2024

Inhalt

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/`	`vserver security file-directory show-effective-permissions`
`POST /protocols/file-security/permissions/`	1. `vserver security file-directory ntfs create` 2. `vserver security file-directory ntfs dacl add` 3. `vserver security file-directory ntfs sacl add` 4. `vserver security file-directory policy create` 5. `vserver security file-directory policy task add` 6. `vserver security file-directory apply`

ONTAP REST API	CLI VON ONTAP
`PATCH /protocols/file-security/permissions/`	`vserver security file-directory ntfs modify`
`DELETE /protocols/file-security/permissions/`	1. `vserver security file-directory ntfs dacl remove` 2. `vserver security file-directory ntfs sacl remove`

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 -Endpunkt

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
'{ \"acls\": [ { \"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`.