



파일 보안 권한 ONTAP Automation

NetApp
April 21, 2024

목차

파일 보안 권한	1
파일 보안 및 감사 정책 관리 준비	1
파일에 대한 유효 사용 권한을 얻습니다	2
파일에 대한 감사 정보를 가져옵니다	3
파일에 새 사용 권한을 적용합니다	6
보안 설명자 정보를 업데이트합니다	7
액세스 제어 항목을 삭제합니다	8

파일 보안 권한

파일 보안 및 감사 정책 관리 준비

ONTAP 클러스터 내에서 SVM을 통해 사용할 수 있는 파일에 대한 권한 및 감사 정책을 관리할 수 있습니다.

개요

ONTAP에서는 SACL(시스템 액세스 제어 목록) 및 DACL(임의 액세스 제어 목록)을 사용하여 파일 개체에 사용 권한을 할당합니다. ONTAP 9.9.1부터 REST API는 SACL 및 DACL 권한 관리를 지원합니다. API를 사용하여 파일 보안 권한 관리를 자동화할 수 있습니다. 대부분의 경우 여러 CLI 명령 또는 ONTAPI(ZAPI) 호출 대신 단일 REST API 호출을 사용할 수 있습니다.



9.9.1 이전 버전의 ONTAP 릴리스에서는 CLI 통과 기능을 사용하여 SACL 및 DACL 권한 관리를 자동화할 수 있습니다. 을 참조하십시오 ["마이그레이션 고려 사항"](#) 및 ["전용 CLI를 사용하면 ONTAP REST API를 통해 패스루를 수행할 수 있습니다"](#) 를 참조하십시오.

REST API를 사용하여 ONTAP 파일 보안 서비스를 관리하는 방법을 보여주는 몇 가지 예제 워크플로우를 사용할 수 있습니다. 워크플로우를 사용하고 REST API 호출을 전송하기 전에 를 검토하십시오 ["워크플로우 사용을 준비하십시오"](#).

Python을 사용하는 경우 스크립트도 참조하십시오 ["file_security_permissions.py"](#) 일부 파일 보안 작업을 자동화하는 방법에 대한 예를 참조하십시오.

ONTAP REST API와 ONTAP CLI 명령 비교

대부분의 작업에서 ONTAP REST API를 사용할 경우 동일한 ONTAP CLI 명령 또는 ONTAPI(ZAPI) 호출보다 더 적은 수의 호출이 필요합니다. 아래 표에는 API 호출 목록과 각 작업에 필요한 CLI 명령 목록이 나와 있습니다.

ONTAP REST API를 참조하십시오	ONTAP CLI를 참조하십시오
'get/protocols/file-security/Effective-permissions/'	'vserver security file-directory show-Effective-permissions'를 선택합니다
'POST/PROTOCOLS/FILE-SECURITY/permissions/'	<ol style="list-style-type: none">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'를 참조하십시오5. 'vserver security file-directory policy task add'6. 'vserver security file-directory apply'
'패치/프로토콜/파일-보안/권한/'	'vserver security file-directory NTFS modify'를 참조하십시오

ONTAP REST API를 참조하십시오	ONTAP CLI를 참조하십시오
삭제/프로토콜/파일-보안/권한/	1. 'vserver security file-directory NTFS DACL remove' 2. 'vserver security file-directory NTFS SACL remove'

관련 정보

- ["파일 권한을 보여 주는 Python 스크립트"](#)
- ["ONTAP REST API를 통해 파일 보안 권한 관리 간소화"](#)
- ["전용 CLI를 사용하면 ONTAP REST API를 통해 패스스루를 수행할 수 있습니다"](#)

파일에 대한 유효 사용 권한을 얻습니다

특정 파일 또는 폴더에 대한 현재 유효 권한을 검색할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/protocols/file-security/effective-permissions/{svm.uuid}/{path}

처리 유형

동기식이다

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	파일이 포함된 SVM의 UUID입니다.
\$FILE_PATH입니다	경로	예	파일 또는 폴더의 경로입니다.

컬의 예

```
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"
```

JSON 출력 예

```
{
  "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"
  ]
}
```

파일에 대한 감사 정보를 가져옵니다

특정 파일 또는 폴더에 대한 감사 정보를 검색할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/protocols/file-security/permissions/{svm.uuid}/{path}

처리 유형

동기식이다

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니 다	설명
\$SVM_ID입니다	경로	예	파일이 포함된 SVM의 UUID입니다.
\$FILE_PATH입니다	경로	예	파일 또는 폴더의 경로입니다.

컬의 예

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

JSON 출력 예

```
{  
  "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"
}

```

파일에 새 사용 권한을 적용합니다

특정 파일이나 폴더에 새 보안 설명자를 적용할 수 있습니다.

1단계: 새 사용 권한을 적용합니다

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/api/protocols/file-security/permissions/{svm.uuid}/{path}

처리 유형

비동기식

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	파일이 포함된 SVM의 UUID입니다.
\$FILE_PATH입니다	경로	예	파일 또는 폴더의 경로입니다.

컬의 예

```
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\" }'
```

JSON 출력 예

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

2단계: 작업 상태를 검색합니다

워크플로우를 수행합니다 **"작업 인스턴스를 가져옵니다"**를 확인합니다 state 값은 입니다 success.

보안 설명자 정보를 업데이트합니다

기본 소유자, 그룹 또는 컨트롤 플래그를 포함하여 특정 파일 또는 폴더로 특정 보안 설명자를 업데이트할 수 있습니다.

1단계: 보안 설명자를 업데이트합니다

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
패치	/api/protocols/file-security/permissions/{svm.uuid}/{path}

처리 유형

비동기식

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	파일이 포함된 SVM의 UUID입니다.
\$FILE_PATH입니다	경로	예	파일 또는 폴더의 경로입니다.

컬의 예

```
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\"}'
```

JSON 출력 예

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

2단계: 작업 상태를 검색합니다

워크플로우를 수행합니다 **"작업 인스턴스를 가져옵니다"** 를 확인합니다 state 값은 입니다 success.

액세스 제어 항목을 삭제합니다

특정 파일 또는 폴더에서 기존 ACE(액세스 제어 항목)를 삭제할 수 있습니다. 변경 내용이 자식 개체에 전파됩니다.

1단계: ACE를 삭제합니다

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
삭제	/api/protocols/file-security/permissions/{svm.uuid}/{path}

처리 유형

비동기식

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	파일이 포함된 SVM의 UUID입니다.
\$FILE_PATH입니다	경로	예	파일 또는 폴더의 경로입니다.

컬의 예

```
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\"}'
```

JSON 출력 예

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

2단계: 작업 상태를 검색합니다

워크플로우를 수행합니다 **"작업 인스턴스를 가져옵니다"** 를 확인합니다 state 값은 입니다 success.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.