# NAS

## ONTAP Automation

NetApp
July 11, 2024

# 目录

# NAS

## 文件安全权限

### 准备管理文件安全性和审核策略

您可以管理ONTAP集群中通过SVM提供的文件的权限和审核策略。

#### 概述

ONTAP 使用系统访问控制列表（ SACL ）和随机访问控制列表（ DACL ）为文件对象分配权限。从ONTAP 9.9.1开始、REST API支持管理SACL和DACL权限。您可以使用API自动管理文件安全权限。在许多情况下、您可以使用单个REST API调用、而不是多个命令行界面命令或ONTAP PI (ZAPI)调用。

> 对于9.9.1之前的ONTAP版本、您可以使用命令行界面直通功能自动管理SACL和DACL权限。请参见 "迁移注意事项" 和 "将专用命令行界面直通与 ONTAP REST API 结合使用" 有关详细信息 …

我们提供了几个示例工作流来说明如何使用REST API管理ONTAP文件安全服务。在使用工作流并发出任何REST API调用之前、请务必查看 "准备使用这些工作流"。

如果您使用Python、另请参见脚本 "file_security_permissions.py" 有关如何自动执行某些文件安全活动的示例。

#### ONTAP REST API 与 ONTAP 命令行界面命令

对于许多任务、使用ONTAP REST API所需的调用比等效的ONTAP命令行界面命令或ONTAP API (ZAPI)调用更少。下表列出了API调用以及每项任务所需的等效命令行界面命令。

| ONTAP REST API | ONTAP 命令行界面 |
| --- | --- |
| `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`<br>2. `vserver security file-directory ntfs dacl add`<br>3. `vserver security file-directory ntfs sacl add`<br>4. `vserver security file-directory policy create`<br>5. `vserver security file-directory policy task add`<br>6. `Vserver security file-directory apply` |
| `patch /protocols/file-security/permissions/` | `vserver security file-directory ntfs modify` |

| ONTAP REST API | ONTAP 命令行界面 |
| --- | --- |
| `delete /protocols/file-security/permissions/` | 1. `vserver security file-directory ntfs dacl remove`<br>2. `vserver security file-directory ntfs sacl remove` |

相关信息

- "展示文件权限的Python脚本"
- "使用 ONTAP REST API 简化文件安全权限的管理"
- "将专用命令行界面直通与 ONTAP REST API 结合使用"

## 获取文件的有效权限

您可以检索特定文件或文件夹的当前有效权限。

**HTTP**方法和端点

此REST API调用使用以下方法和端点。

| HTTP 方法 | 路径 |
| --- | --- |
| 获取 | /api/protocols文件安全性/有效权限/｛svm.unid｝/｛path｝ |

处理类型

同步

**CURL**示例的其他输入参数

除了所有REST API调用通用的参数之外、此步骤中的cURL示例还会使用以下参数。

| 参数 | Type | Required | Description |
| --- | --- | --- | --- |
| $SVM_ID | 路径 | 是的。 | 这是包含该文件的SVM的UUID。 |
| $file_path | 路径 | 是的。 | 这是文件或文件夹的路径。 |

**curl** 示例

```
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 输出示例**


```
{
  "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"
  ]
}
```


## 获取文件的审核信息

您可以检索特定文件或文件夹的审核信息。

**HTTP方法和端点**

此REST API调用使用以下方法和端点。

| HTTP 方法 | 路径 |
| --- | --- |
| 获取 | /api/protocols /文件安全性/权限/｛svm.unid｝/｛path｝ |

处理类型

同步

**CURL**示例的其他输入参数

除了所有REST API调用通用的参数之外、此步骤中的cURL示例还会使用以下参数。

| 参数 | Type | Required | Description |
| --- | --- | --- | --- |
| $SVM_ID | 路径 | 是的。 | 这是包含该文件的SVM的UUID。 |
| $file_path | 路径 | 是的。 | 这是文件或文件夹的路径。 |

**curl** 示例

```
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** 输出示例

```
{
  "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"
}
```

## 将新权限应用于文件

您可以将新的安全描述符应用于特定文件或文件夹。

### 第1步：应用新权限

**HTTP**方法和端点

此REST API调用使用以下方法和端点。

| HTTP 方法 | 路径 |
| --- | --- |
| 发布 | /api/protocols /文件安全性/权限/｛svm.unid｝/｛path｝ |

处理类型

异步

**CURL**示例的其他输入参数

除了所有REST API调用通用的参数之外、此步骤中的cURL示例还会使用以下参数。

| 参数 | Type | Required | Description |
| --- | --- | --- | --- |
| $SVM_ID | 路径 | 是的。 | 这是包含该文件的SVM的UUID。 |
| $file_path | 路径 | 是的。 | 这是文件或文件夹的路径。 |

**curl 示例**

```
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 输出示例**

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

第**2**步：检索作业状态

执行工作流 "获取作业实例" 并确认 `state` 值为 `success`。

## 更新安全描述符信息

您可以将特定安全描述符更新到特定文件或文件夹、包括主所有者、组或控制标志。

第**1**步：更新安全描述符

**HTTP**方法和端点

此REST API调用使用以下方法和端点。

| **HTTP** 方法 | 路径 |
| --- | --- |
| patch | /api/protocols /文件安全性/权限/ {svm.unid} / {path} |

处理类型

异步

**CURL**示例的其他输入参数

除了所有REST API调用通用的参数之外、此步骤中的cURL示例还会使用以下参数。

| 参数 | Type | Required | Description |
| --- | --- | --- | --- |
| $SVM_ID | 路径 | 是的。 | 这是包含该文件的SVM的UUID。 |
| $file_path | 路径 | 是的。 | 这是文件或文件夹的路径。 |

**curl** 示例

```
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** 输出示例

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

第**2**步：检索作业状态

执行工作流 "获取作业实例" 并确认 `state` 值为 `success`。

## 删除访问控制条目

您可以从特定文件或文件夹中删除现有访问控制条目(ACE)。更改会传播到任何子对象。

第**1**步：删除**ACE**

**HTTP**方法和端点

此REST API调用使用以下方法和端点。

| HTTP 方法 | 路径 |
| --- | --- |
| 删除 | /api/protocols /文件安全性/权限/｛svm.unid｝/｛path｝ |

处理类型

异步

**CURL**示例的其他输入参数

除了所有REST API调用通用的参数之外、此步骤中的cURL示例还会使用以下参数。

| 参数 | Type | Required | Description |
| --- | --- | --- | --- |
| $SVM_ID | 路径 | 是的。 | 这是包含该文件的SVM的UUID。 |
| $file_path | 路径 | 是的。 | 这是文件或文件夹的路径。 |

**curl** 示例

```
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** 输出示例

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

第**2**步：检索作业状态

执行工作流 "获取作业实例" 并确认 `state` 值为 `success`。