NAS

ONTAP automation

NetApp
January 12, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/ontap-automation/workflows/wf_nas_fs_prepare.html on January 12, 2026. Always check docs.netapp.com for the latest.

目录

NAS . . . 1
文件安全权限 . . . 1
准备使用ONTAP REST API管理文件安全和审核策略 . . . 1
使用ONTAP REST API获取文件的有效权限 . . . 2
使用ONTAP REST API获取文件的审核信息 . . . 3
使用ONTAP REST API将新权限应用于文件 . . . 6
使用ONTAP REST API更新安全描述符信息 . . . 7
使用ONTAP REST API删除访问控制条目 . . . 8

NAS

文件安全权限

准备使用ONTAP REST API管理文件安全和审核策略

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` 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`
`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` 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"

使用ONTAP REST API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"
  ]
}
```


使用ONTAP REST API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"
}
```

使用ONTAP REST API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`。

使用ONTAP REST API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`。

使用**ONTAP REST API**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`。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。