NAS

ONTAP automation

NetApp
January 12, 2026

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

目次

NAS . . . 1
ファイルセキュリティ権限 . . . 1
ONTAP REST APIを使用してファイルセキュリティと監査ポリシーを管理するための準備 . . . 1
ONTAP REST APIを使用して、ファイルに対して有効な権限を取得する . . . 2
ONTAP REST APIを使用したファイルの監査情報の取得 . . . 3
ONTAP REST APIを使用してファイルに新しい権限を適用する . . . 6
ONTAP REST APIを使用したセキュリティ記述子情報の更新 . . . 7
ONTAP REST APIを使用してアクセス制御エントリを削除する . . . 8

NAS

ファイルセキュリティ権限

ONTAP REST APIを使用してファイルセキュリティと監査ポリシーを管理するための準備

ONTAPクラスタ内のSVMから使用可能なファイルの権限と監査ポリシーを管理できます。

概要

ONTAP では、システムアクセス制御リスト（ SACL ）と随意アクセス制御リスト（ DACL ）を使用してファイルオブジェクトに権限を割り当てます。ONTAP 9.9.1以降では、REST APIでSACLとDACLの権限の管理がサポートされます。APIを使用すると、ファイルセキュリティ権限の管理を自動化できます。多くの場合、複数のCLIコマンドやONTAPI（ZAPI）呼び出しではなく、1つのREST API呼び出しを使用できます。

> 9.9.1より前のONTAPリリースでは、CLIパススルー機能を使用して、SACLおよびDACL権限の管理を自動化できます。を参照してください "移行に関する考慮事項" および "ONTAP REST API でプライベート CLI パススルーを使用する" を参照してください。

REST APIを使用してONTAPファイルセキュリティサービスを管理する方法を示すワークフローの例をいくつか紹介します。ワークフローを使用してREST API呼び出しを実行する前に、 "ワークフローを使用する準備をします"。

Pythonを使用する場合は、スクリプトも参照してください。 "file_security_permissions.py" ファイルセキュリティアクティビティの一部を自動化する方法の例を参照してください。

ONTAP REST API コマンドと ONTAP CLI コマンドの比較

多くのタスクで、ONTAP REST APIを使用する場合、同等のONTAP CLIコマンドやONTAPI（ZAPI）呼び出しよりも少ない呼び出しで済みます。次の表に、API呼び出しと、各タスクに必要なCLIコマンドを示します。

ONTAP REST API	ONTAP CLI
「 get/protocols/file-security/effected-permissions/ 」	vserver security file-directory show-effected-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 CLI
'delete/protocols/file-security/permissions/	1. 「 vserver security file-directory ntfs dacl remove 」 2. 「 vserver security file-directory ntfs sacl remove 」

関連情報

- "ファイル権限を示すPythonスクリプト"
- "ONTAP REST API を使用してファイルセキュリティ権限を簡単に管理できます"
- "ONTAP REST API でプライベート CLI パススルーを使用する"

ONTAP REST APIを使用して、ファイルに対して有効な権限を取得する

特定のファイルまたはフォルダに対して現在有効な権限を取得できます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/protocols/file-security/effective-permissions/｛svm.uuid｝/｛path｝

処理のタイプ

同期

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
$SVM_ID	パス	はい。	これは、ファイルが含まれているSVMのUUIDです。
$file_path	パス	はい。	ファイルまたはフォルダへのパスです。

カールの例

```
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 出力例


```
{
  "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"
  ]
}
```


ONTAP REST APIを使用したファイルの監査情報の取得

特定のファイルまたはフォルダの監査情報を取得できます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/protocols/file-security/permissions/｛svm.uuid｝/｛path｝

処理のタイプ

同期

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
$SVM_ID	パス	はい。	これは、ファイルが含まれているSVMのUUIDです。
$file_path	パス	はい。	ファイルまたはフォルダへのパスです。

カールの例

```
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 出力例

```
{
  "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"
}
```

ONTAP REST APIを使用してファイルに新しい権限を適用する

新しいセキュリティ記述子を特定のファイルまたはフォルダに適用できます。

手順1：新しい権限を適用する

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿（ Post ）	/api/protocols/file-security/permissions/｛svm.uuid｝/｛path｝

処理のタイプ

非同期

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
$SVM_ID	パス	はい。	これは、ファイルが含まれているSVMのUUIDです。
$file_path	パス	はい。	ファイルまたはフォルダへのパスです。

カールの例

```
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 出力例

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

手順**2**：ジョブのステータスを取得する

ワークフローを実行 "ジョブインスタンスの取得" をクリックし、 `state` 値は `success`。

ONTAP REST APIを使用したセキュリティ記述子情報の更新

特定のセキュリティ記述子を、プライマリ所有者、グループ、制御フラグなど、特定のファイルまたはフォルダに対して更新できます。

手順**1**：セキュリティ記述子を更新する

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
パッチ	/api/protocols/file-security/permissions/｛svm.uuid｝/｛path｝

処理のタイプ

非同期

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
$SVM_ID	パス	はい。	これは、ファイルが含まれているSVMのUUIDです。
$file_path	パス	はい。	ファイルまたはフォルダへのパスです。

カールの例

```
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 出力例

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

手順2：ジョブのステータスを取得する

ワークフローを実行 "ジョブインスタンスの取得" をクリックし、 `state` 値は `success`。

ONTAP REST APIを使用してアクセス制御エントリを削除する

特定のファイルまたはフォルダから既存のAccess Control Entry（ACE；アクセス制御エントリ）を削除できます。変更はすべての子オブジェクトに伝播されます。

手順1：ACEの削除

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
削除	/api/protocols/file-security/permissions/｛svm.uuid｝/｛path｝

処理のタイプ

非同期

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
$SVM_ID	パス	はい。	これは、ファイルが含まれているSVMのUUIDです。
$file_path	パス	はい。	ファイルまたはフォルダへのパスです。

カールの例

```
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 出力例

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

手順2：ジョブのステータスを取得する

ワークフローを実行 "ジョブインスタンスの取得" をクリックし、 `state` 値は `success`。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。