NAS

ONTAP Automation

NetApp
July 19, 2024

Sommaire

NAS

Autorisations de sécurité des fichiers

Préparez-vous à gérer la sécurité des fichiers et les stratégies d'audit

Vous pouvez gérer les autorisations et les règles d'audit pour les fichiers disponibles via les SVM au sein d'un cluster ONTAP.

Présentation

ONTAP utilise les listes de contrôle d'accès système (CLS) et les listes de contrôle d'accès discrétionnaire (listes ACL) pour attribuer des autorisations aux objets de fichier. Depuis ONTAP 9.9.1, l'API REST prend en charge la gestion des autorisations SACL et DACL. Vous pouvez utiliser l'API pour automatiser l'administration des autorisations de sécurité des fichiers. Dans la plupart des cas, vous pouvez utiliser un seul appel d'API REST au lieu de plusieurs commandes CLI ou appels ONTAPI (ZAPI).

> Pour les versions ONTAP antérieures à la version 9.9.1, vous pouvez automatiser l'administration des autorisations SACL et DACL à l'aide de la fonction de passerelle CLI. Voir "Considérations relatives à la migration" et "Utilisation de la passerelle CLI privée avec l'API REST de ONTAP" pour en savoir plus.

Plusieurs exemples de workflows sont disponibles pour illustrer la manière de gérer les services de sécurité des fichiers ONTAP à l'aide de l'API REST. Avant d'utiliser les flux de travail et d'émettre l'un des appels de l'API REST, assurez-vous de passer en revue "Préparez l'utilisation des workflows".

Si vous utilisez Python, consultez également le script "file_security_permissions.py" pour des exemples d'automatisation de certaines activités de sécurité des fichiers.

Comparaison des commandes de l'API REST ONTAP et de l'interface CLI ONTAP

Pour de nombreuses tâches, l'utilisation de l'API REST ONTAP requiert moins d'appels que les commandes CLI ONTAP ou les appels ONTAPI (ZAPI) équivalents. Le tableau ci-dessous présente une liste d'appels API et l'équivalent des commandes CLI nécessaires à chaque tâche.

L'API REST DE ONTAP	INTERFACE DE LIGNE DE COMMANDES DE 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`

L'API REST DE ONTAP	INTERFACE DE LIGNE DE COMMANDES DE 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`

Informations associées

- "Script Python illustrant les autorisations de fichier"
- "Gestion simplifiée des autorisations de sécurité de fichiers avec les API REST ONTAP"
- "Utilisation de la passerelle CLI privée avec l'API REST de ONTAP"

Obtenez les autorisations efficaces pour un fichier

Vous pouvez récupérer les autorisations effectives actuelles pour un fichier ou un dossier spécifique.

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
OBTENEZ	/api/protocoles/sécurité-fichier/autorisations-effectives/{svm.uuid}/{path}

Type de traitement

Synchrone

Paramètres d'entrée supplémentaires pour les exemples de boucles

Outre les paramètres communs à tous les appels API REST, les paramètres suivants sont également utilisés dans l'exemple curl de cette étape.

Paramètre	Type	Obligatoire	Description
$SVM_ID	Chemin	Oui.	Il s'agit de l'UUID du SVM contenant le fichier.
$FILE_PATH	Chemin	Oui.	Il s'agit du chemin d'accès au fichier ou au dossier.

Exemple de boucle

```
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"
```

Exemple de sortie JSON


```
{
  "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"
  ]
}
```


Obtenez les informations d’audit d’un fichier

Vous pouvez récupérer les informations d’audit d’un fichier ou d’un dossier spécifique.

Méthode HTTP et noeud final

Cet appel d’API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
OBTENEZ	/api/protocoles/sécurité-fichier/permissions/{svm.uuid}/{path}

Type de traitement

Synchrone

Paramètres d'entrée supplémentaires pour les exemples de boucles

Outre les paramètres communs à tous les appels API REST, les paramètres suivants sont également utilisés dans l'exemple curl de cette étape.

Paramètre	Type	Obligatoire	Description
$SVM_ID	Chemin	Oui.	Il s'agit de l'UUID du SVM contenant le fichier.
$FILE_PATH	Chemin	Oui.	Il s'agit du chemin d'accès au fichier ou au dossier.

Exemple de boucle

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

Exemple de sortie JSON

```
{
  "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"
}
```

Appliquer de nouvelles autorisations à un fichier

Vous pouvez appliquer un nouveau descripteur de sécurité à un fichier ou dossier spécifique.

Étape 1 : appliquez les nouvelles autorisations

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
POST	/api/protocoles/sécurité-fichier/permissions/{svm.uuid}/{path}

Type de traitement

Asynchrone

Paramètres d'entrée supplémentaires pour les exemples de boucles

Outre les paramètres communs à tous les appels API REST, les paramètres suivants sont également utilisés dans l'exemple curl de cette étape.

Paramètre	Type	Obligatoire	Description
$SVM_ID	Chemin	Oui.	Il s'agit de l'UUID du SVM contenant le fichier.
$FILE_PATH	Chemin	Oui.	Il s'agit du chemin d'accès au fichier ou au dossier.

Exemple de boucle

```
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\"}'
```

Exemple de sortie JSON

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

Étape 2 : récupération de l'état du travail

Exécutez le flux de travail "Obtenir l'instance de travail" et confirmez le `state` la valeur est `success`.

Mettez à jour les informations du descripteur de sécurité

Vous pouvez mettre à jour un descripteur de sécurité spécifique dans un fichier ou un dossier spécifique, y compris les indicateurs de propriétaire, de groupe ou de contrôle principal.

Étape 1 : mettez à jour le descripteur de sécurité

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
CORRECTIF	/api/protocoles/sécurité-fichier/permissions/{svm.uuid}/{path}

Type de traitement

Asynchrone

Paramètres d'entrée supplémentaires pour les exemples de boucles

Outre les paramètres communs à tous les appels API REST, les paramètres suivants sont également utilisés dans l'exemple curl de cette étape.

Paramètre	Type	Obligatoire	Description
$SVM_ID	Chemin	Oui.	Il s'agit de l'UUID du SVM contenant le fichier.
$FILE_PATH	Chemin	Oui.	Il s'agit du chemin d'accès au fichier ou au dossier.

Exemple de boucle

```
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\"}'
```

Exemple de sortie JSON

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

Étape 2 : récupération de l'état du travail

Exécutez le flux de travail "Obtenir l'instance de travail" et confirmez le `state` la valeur est `success`.

Supprimer une entrée de contrôle d'accès

Vous pouvez supprimer une entrée de contrôle d'accès (ACE) existante d'un fichier ou d'un dossier spécifique. La modification se propage à tous les objets enfants.

Étape 1 : supprimez l'ACE

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
SUPPRIMER	/api/protocoles/sécurité-fichier/permissions/{svm.uuid}/{path}

Type de traitement

Asynchrone

Paramètres d'entrée supplémentaires pour les exemples de boucles

Outre les paramètres communs à tous les appels API REST, les paramètres suivants sont également utilisés dans l'exemple curl de cette étape.

Paramètre	Type	Obligatoire	Description
$SVM_ID	Chemin	Oui.	Il s'agit de l'UUID du SVM contenant le fichier.
$FILE_PATH	Chemin	Oui.	Il s'agit du chemin d'accès au fichier ou au dossier.

Exemple de boucle

```
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\"}'
```

Exemple de sortie JSON

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

Étape 2 : récupération de l'état du travail

Exécutez le flux de travail "Obtenir l'instance de travail" et confirmez le `state` la valeur est `success`.

Informations sur le copyright

Informations sur les marques commerciales