Contrôle d'accès basé sur les attributs

ONTAP Technical Reports

NetApp
February 23, 2026

Sommaire

Contrôle d’accès basé sur les attributs

Contrôle d’accès basé sur les attributs avec ONTAP

À partir de la version 9.12.1, vous pouvez configurer ONTAP avec les étiquettes de sécurité NFSv4.2 et les attributs étendus (xattrs) pour prendre en charge le contrôle d’accès basé sur les rôles (RBAC) avec des attributs et le contrôle d’accès basé sur les attributs (ABAC).

ABAC est une stratégie d’autorisation qui définit les autorisations en fonction des attributs utilisateur, des attributs de ressource et des conditions environnementales. L’intégration de ONTAP avec les étiquettes de sécurité NFS v4.2 et les xattrs est conforme aux normes NIST pour les solutions ABAC, comme indiqué dans la publication spéciale NIST 800-162.

Vous pouvez utiliser les étiquettes de sécurité NFS v4.2 et les xattrs pour attribuer des attributs et des étiquettes définis par l’utilisateur de fichiers. ONTAP peut s’intégrer au logiciel de gestion des accès et des identités orienté ABAC pour appliquer des règles de contrôle d’accès granulaires aux fichiers et dossiers en fonction de ces attributs et étiquettes.

Informations associées

- "Approches de l’ABAC avec ONTAP"
- "NFS dans NetApp ONTAP : guide des bonnes pratiques et d’implémentation"

Approches du contrôle d’accès basé sur les attributs (ABAC) dans ONTAP

ONTAP propose plusieurs approches pour assurer le contrôle d’accès basé sur des attributs (ABAC) au niveau des fichiers, notamment les étiquettes de sécurité NFS v4.2 et les attributs étendus (xattrs) à l’aide de NFS.

Étiquettes de sécurité NFS v4.2

À partir de ONTAP 9.9.1, la fonctionnalité NFS v4.2 appelée NFS est prise en charge.

Les étiquettes de sécurité NFS v4.2 permettent de gérer l’accès granulaire aux fichiers et dossiers à l’aide d’étiquettes SELinux et de MAC (obligatoire Access Control). Ces étiquettes MAC sont stockées avec des fichiers et des dossiers et fonctionnent en conjonction avec les autorisations UNIX et les listes de contrôle d’accès NFS v4.x.

La prise en charge des étiquettes de sécurité NFS v4.2 signifie que ONTAP reconnaît et comprend désormais les paramètres d’étiquette SELinux du client NFS. Les étiquettes de sécurité NFS v4.2 sont couvertes par la norme RFC-7204.

Voici quelques cas d’utilisation des étiquettes de sécurité NFS v4.2 :

- Étiquetage MAC des images de machines virtuelles (VM)
- Classification de sécurité des données pour le secteur public (secret, secret et autres classifications)
- Conformité en matière de sécurité

- Linux sans disque

Activez les étiquettes de sécurité NFS v4.2

Vous pouvez activer ou désactiver les étiquettes de sécurité NFS v4.2 à l'aide de la commande suivante (privilège avancé requis) :

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

Pour en savoir plus, `vserver nfs modify` consultez le "Référence des commandes ONTAP".

Modes d'application pour les étiquettes de sécurité NFS v4.2

À partir de ONTAP 9.9.1, ONTAP prend en charge les modes d'application suivants :

- **Mode serveur limité** : ONTAP ne peut pas appliquer les étiquettes mais peut les stocker et les transmettre.

  La possibilité de modifier les étiquettes MAC revient au client de les appliquer.

- **Mode invité** : si le client n'est pas étiqueté NFS-Aware (v4.1 ou inférieur), les étiquettes MAC ne sont pas transmises.

  ONTAP ne prend actuellement pas en charge le mode complet (stockage et application des étiquettes MAC).

Exemples d'étiquettes de sécurité NFS v4.2

L'exemple de configuration suivant illustre les concepts d'utilisation de Red Hat Enterprise Linux version 9.3 (Plough).

L'utilisateur `jrsmith`, créé à partir des informations d'identification de John R. Smith, possède le compte Privileges suivant :

- Nom d'utilisateur = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

Il existe deux rôles : le compte admin qui est un utilisateur privilégié et un utilisateur `jrsmith` comme décrit dans le tableau Privileges MLS suivant :

Utilisateurs	Rôle	Type	Niveaux
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

Dans cet exemple d'environnement, l'utilisateur `jrsmith` a accès aux fichiers aux niveaux de `s0 s3` . Nous pouvons améliorer les classifications de sécurité existantes, comme décrit ci-dessous, afin de nous assurer

que les administrateurs n'ont pas accès aux données spécifiques aux utilisateurs.

- s0 = données utilisateur admin des privilèges
- s0 = données non classées
- s1 = confidentiel
- s2 = données secrètes
- s3 = données les plus secrètes

Exemple d'étiquettes de sécurité NFS v4.2 avec MCS

Outre la sécurité multi-niveaux (MLS), une autre fonctionnalité appelée sécurité multi-catégories (MCS) vous permet de définir des catégories telles que des projets.

Étiquette de sécurité NFS	Valeur
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

Attributs étendus (xattrs)

À partir de ONTAP 9.12.1, ONTAP prend en charge xattrs. Xattrs permet d'associer des métadonnées à des fichiers et des répertoires au-delà de ce qui est fourni par le système, tels que les listes de contrôle d'accès (ACL) ou les attributs définis par l'utilisateur.

Pour implémenter xattrs, vous pouvez utiliser `setfattr` et `getfattr` les utilitaires de ligne de commande sous Linux. Ces outils fournissent un moyen puissant de gérer des métadonnées supplémentaires pour les fichiers et les répertoires. Elles doivent être utilisées avec précaution, car une utilisation inappropriée peut entraîner des comportements inattendus ou des problèmes de sécurité. Reportez-vous toujours aux `setfattr` pages de manuel et `getfattr` ou à toute autre documentation fiable pour obtenir des instructions d'utilisation détaillées.

Lorsque xattrs est activé sur un système de fichiers ONTAP, les utilisateurs peuvent définir, modifier et récupérer des attributs arbitraires sur les fichiers. Ces attributs peuvent être utilisés pour stocker des informations supplémentaires sur le fichier qui ne sont pas capturées par l'ensemble standard d'attributs de fichier, telles que les informations de contrôle d'accès.

Il existe plusieurs exigences et limites pour l'utilisation de xattrs dans ONTAP :

- Red Hat Enterprise Linux 8.4 ou version ultérieure
- Ubuntu 22.04 ou version ultérieure
- Chaque fichier peut avoir jusqu'à 128 xattrs
- Les clés xattr sont limitées à 255 octets
- La taille de la clé ou de la valeur combinée est de 1,729 octets par xattr
- Les répertoires et les fichiers peuvent avoir des xattrs
- Pour définir et récupérer les xattrs, `w` ou les bits de mode d'écriture doivent être activés pour l'utilisateur et le groupe

Les Xattrs sont utilisés dans l'espace de nom de l'utilisateur et n'ont aucune signification intrinsèque à ONTAP lui-même. Au lieu de cela, leurs applications pratiques sont déterminées et gérées exclusivement par

l'application côté client qui interagit avec le système de fichiers.

Exemples de cas d'utilisation de xattr :

- Enregistrement du nom de l'application responsable de la création d'un fichier
- Conservation d'une référence à l'e-mail à partir duquel un fichier a été obtenu
- Établissement d'un cadre de catégorisation pour l'organisation des objets de fichier
- Étiquetage des fichiers avec l'URL de leur source de téléchargement d'origine

Commandes de gestion des xattrs

- `setfattr` définit un attribut étendu d'un fichier ou d'un répertoire :

  `setfattr -n <attribute_name> -v <attribute_value> <file or directory name>`

  Exemple de commande :

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr` récupère la valeur d'un attribut étendu spécifique ou répertorie tous les attributs étendus d'un fichier ou d'un répertoire :

  Attribut spécifique : `getfattr -n <attribute_name> <file or directory name>`

  Tous les attributs : `getfattr <file or directory name>`

  Exemple de commande :

  ```
  getfattr -n user.comment example.txt
  ```

Exemples de paires de valeurs de clé xattr

Le tableau suivant présente deux exemples de paire de valeurs de clé xattr :

xattr	Valeur
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

Autorisations utilisateur avec ACE pour xattrs

Une entrée de contrôle d'accès (ACE) est un composant d'une liste de contrôle d'accès qui définit les droits ou autorisations d'accès accordés à un utilisateur individuel ou à un groupe d'utilisateurs pour une ressource spécifique, comme un fichier ou un répertoire. Chaque ACE spécifie le type d'accès autorisé ou refusé et est

associé à une entité de sécurité particulière (identité d'utilisateur ou de groupe).

Entrée de contrôle d'accès (ACE) requise pour les xattrs

- Retrieve xattr : autorisations requises pour qu'un utilisateur puisse lire les attributs étendus d'un fichier ou d'un répertoire. Le « R » signifie que l'autorisation de lecture est nécessaire.
- Set xattrs : les autorisations nécessaires pour modifier ou définir les attributs étendus. « A », « W » et « T » représentent différents exemples d'autorisations, telles que l'ajout, l'écriture et une autorisation spécifique liée aux xattrs.
- Fichiers : les utilisateurs doivent ajouter, écrire et éventuellement accorder une autorisation spéciale liée aux xattrs pour définir des attributs étendus.
- Répertoires : une autorisation spécifique « T » est requise pour définir des attributs étendus.

Type de fichier	Récupérer xattr	Définissez xattrs
Fichier	R	A,W,T
Répertoire	R	T

Intégration au logiciel ABAC Identity and Access Control

Pour exploiter pleinement les capacités d'ABAC, ONTAP peut s'intégrer à un logiciel de gestion des identités et des accès orienté ABAC.

Dans un système ABAC, le point d'application de la politique (PEP) et le point de décision de la politique (PDP) jouent des rôles cruciaux. Le PPE est responsable de l'application des politiques de contrôle d'accès, tandis que le PDP prend la décision d'accorder ou de refuser l'accès en fonction des politiques.

Dans la pratique, une entreprise utiliserait un mélange d'étiquettes de sécurité NFS et de xattrs. Ils sont utilisés pour représenter une variété de métadonnées, y compris la classification, la sécurité, l'application et le contenu, qui sont tous des éléments essentiels dans la prise de décisions ABAC. Xattrs, par exemple, peut être utilisé pour stocker les attributs de ressource que le PDP utilise pour son processus de prise de décision. Un attribut peut être défini pour représenter le niveau de classification d'un fichier (par exemple, « non classé », « confidentiel », « secret » ou « secret supérieur »). Le PDP pourrait alors utiliser cet attribut pour appliquer une stratégie qui limite les utilisateurs à accéder uniquement aux fichiers dont le niveau de classification est égal ou inférieur à leur niveau d'autorisation.

Ce contenu suppose que l'identité, l'authentification et les services d'accès du client incluent au moins une PPE et un PDP qui servent d'intermédiaires pour l'accès au système de fichiers.

Exemple de flux de processus pour ABAC

1. L'utilisateur présente les informations d'identification (par exemple, PKI, OAuth, SAML) pour accéder au système à PEP et obtient les résultats du PDP.

   Le rôle du PPE est d'intercepter la demande d'accès de l'utilisateur et de la transférer au PDP.

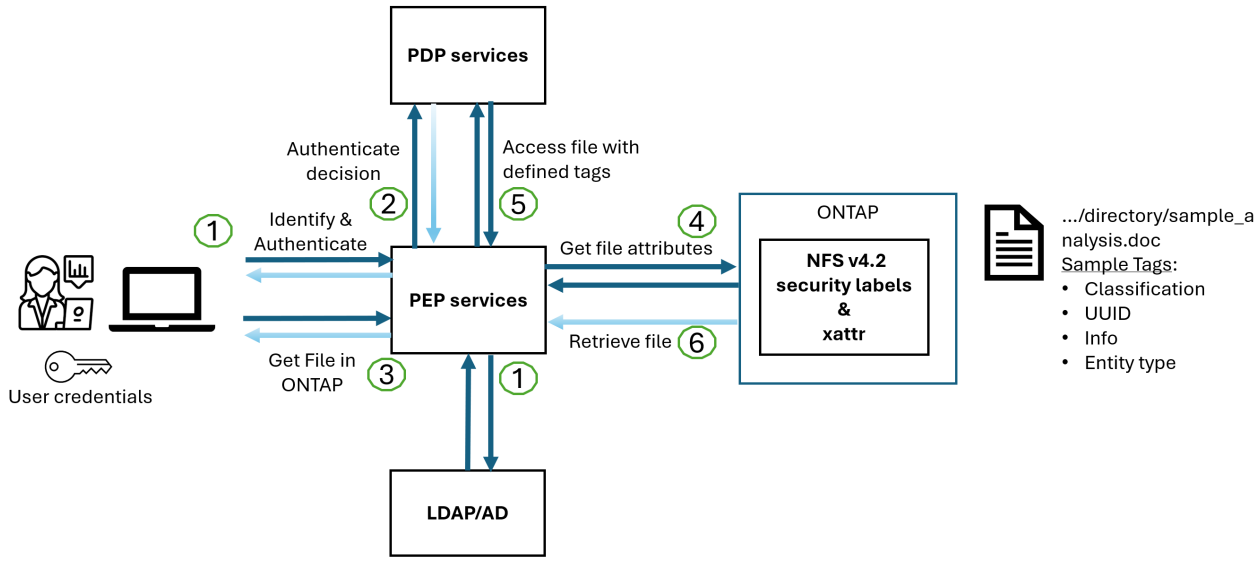
2. Le PDP évalue ensuite cette demande par rapport aux politiques établies de l'ABAC.

   Ces stratégies tiennent compte de divers attributs liés à l'utilisateur, à la ressource en question et à l'environnement environnant. En fonction de ces politiques, le PDP prend une décision d'accès d'autoriser ou de refuser, puis communique cette décision à la PPE.

   PDP fournit une politique à PEP pour qu'elle l'applique. Le PPE applique ensuite cette décision, en accordant ou en refusant la demande d'accès de l'utilisateur conformément à la décision du PDP.

3. Après une demande réussie, l'utilisateur demande un fichier stocké dans ONTAP (AFF, AFF-C, par exemple).
4. Si la demande réussit, PEP obtient des étiquettes de contrôle d'accès à grain fin à partir du document.
5. PEP demande la politique de l'utilisateur en fonction des certificats de cet utilisateur.
6. PEP prend une décision en fonction de la politique et des balises si l'utilisateur a accès au fichier et permet à l'utilisateur de le récupérer.

L'accès réel peut être effectué à l'aide de jetons.



Clonage ONTAP et SnapMirror

Les technologies de clonage et de SnapMirror de ONTAP sont conçues pour offrir des fonctionnalités de réplication et de clonage des données efficaces et fiables, garantissant que tous les aspects des données de fichiers, y compris les xattrs, sont conservés et transférés avec le fichier. Les xattrs sont essentiels car ils stockent des métadonnées supplémentaires associées à un fichier, telles que des étiquettes de sécurité, des informations de contrôle d'accès et des données définies par l'utilisateur, qui sont essentielles pour maintenir le contexte et l'intégrité du fichier.

Lorsqu'un volume est cloné à l'aide de la technologie FlexClone de ONTAP, une réplique inscriptible exacte du volume est créée. Ce processus de clonage est instantané et compact. Il inclut toutes les données de fichiers et métadonnées, garantissant ainsi la réplication complète des fichiers xattrs. De même, SnapMirror garantit la mise en miroir parfaite des données vers un système secondaire. Cela inclut les xattrs, qui sont essentiels pour que les applications qui s'appuient sur ces métadonnées fonctionnent correctement.

En incluant les xattrs dans les opérations de clonage et de réplication, NetApp ONTAP s'assure que l'ensemble du dataset, avec toutes ses caractéristiques, est disponible et cohérent sur l'ensemble des systèmes de stockage primaire et secondaire. Cette approche globale de la gestion des données est cruciale pour les entreprises qui ont besoin d'une protection cohérente des données, d'une restauration rapide et du respect des normes de conformité et réglementaires. Elle simplifie également la gestion des données entre différents environnements, sur site ou dans le cloud, garantissant ainsi aux utilisateurs que leurs données sont complètes et non modifiées au cours de ces processus.

Les étiquettes de sécurité NFS v4.2 présentent les restrictions définies dans le Étiquettes de sécurité NFS v4.2.

Audit des modifications apportées aux étiquettes

L'audit des modifications apportées aux étiquettes de sécurité xattrs ou NFS constitue un aspect essentiel de la gestion et de la sécurité du système de fichiers. Les outils d'audit standard du système de fichiers permettent de surveiller et de consigner toutes les modifications apportées à un système de fichiers, y compris les modifications apportées aux xattrs et aux étiquettes de sécurité.

Dans les environnements Linux, le `auditd` démon est généralement utilisé pour établir un audit pour les événements du système de fichiers. Il permet aux administrateurs de configurer des règles pour surveiller des appels système spécifiques liés aux modifications xattr, telles que `setxattr`, `lsetxattr` et pour définir des attributs et, `lremovexattr` et `fsetxattr` `fremovexattr` pour supprimer des attributs `removexattr`.

ONTAP FPolicy étend ces fonctionnalités en fournissant une structure robuste pour la surveillance et le contrôle en temps réel des opérations de fichiers. FPolicy peut être configuré pour prendre en charge divers événements xattr, offrant un contrôle granulaire des opérations sur fichiers et la possibilité d'appliquer des règles complètes de gestion des données.

Pour les utilisateurs utilisant xattrs, en particulier dans les environnements NFS v3 et NFS v4, seules certaines combinaisons d'opérations et de filtres de fichiers sont prises en charge pour la surveillance. La liste des combinaisons de filtres et d'opérations de fichiers prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFS v3 et NFS v4 est détaillée ci-dessous :

Opérations de fichiers prises en charge	Filtres pris en charge
`setattr`	`offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory`

Exemple de fragment de journal auditd pour une opération setattr :

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

L'activation "ONTAP FPolicy" pour les utilisateurs travaillant avec xattrs fournit une couche de visibilité et de contrôle qui est essentielle au maintien de l'intégrité et de la sécurité du système de fichiers. Grâce aux fonctionnalités avancées de surveillance de FPolicy, les entreprises peuvent s'assurer que toutes les modifications apportées aux xattrs font l'objet d'un suivi, d'un audit et d'une mise en adéquation avec leurs

normes de sécurité et de conformité. Cette approche proactive de la gestion du système de fichiers explique pourquoi l'activation de ONTAP FPolicy est fortement recommandée pour toute entreprise qui souhaite améliorer ses stratégies de gouvernance et de protection des données.

Exemples de contrôle de l'accès aux données

L'exemple d'entrée ci-dessous pour les données stockées dans le certificat PKI de John R. Smith montre comment l'approche de NetApp peut être appliquée à un fichier et fournit un contrôle d'accès précis.

> Ces exemples sont fournis à titre d'exemple et il incombe au client de déterminer les métadonnées associées aux étiquettes de sécurité et aux fichiers xattrs NFS v4.2. Les détails sur la mise à jour et la conservation des étiquettes sont omis pour plus de simplicité.

Exemple de valeurs de certificat PKI

Clé	Valeur
EntitySecurityMark	t:s01 = non confidentiel

Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

spécifications	« DOD »

Clé	Valeur
uuid	b4111349-7875-4115-ad30-0928565f2e15

AdminOrganisation	{
	"value": "DoD"
	}

réunions d'information	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

État de la citoyenneté	{
	"value": "US"
	}

jeux	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

Clé	Valeur

PaysOfaffiliations	[
	{
	"value": "USA"
	}
	]

Identificateur numérique	{
	"classification": "UNCLASSIFIED",
	"value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us"
	}

Démontez	{
	"value": "DoD"
	}

DutyOrganisation	{
	"value": "DoD"
	}

EntityType	{
	"value": "GOV"
	}

Clé	Valeur

FineAccessControls	[
	{
	"value": "SI"
	},
	{
	"value": "TK"
	},
	{
	"value": "NSYS"
	}
	]

Ces droits ICP montrent les détails d'accès de John R. Smith, y compris l'accès par type de données et l'attribution.

Dans les cas où les métadonnées IC-TDF sont stockées séparément du fichier, NetApp préconise une couche supplémentaire de contrôle d'accès granulaire. Cela implique le stockage des informations de contrôle d'accès au niveau du répertoire et en association avec chaque fichier. Prenons l'exemple des balises suivantes liées à un fichier :

- Étiquettes de sécurité NFS v4.2 : utilisées pour prendre les décisions relatives à la sécurité
- Xattrs : fournir des renseignements supplémentaires pertinents au dossier et aux exigences du programme organisationnel

Les paires clé-valeur suivantes sont des exemples de métadonnées qui peuvent être stockées sous forme de xattrs et fournissent des informations détaillées sur le créateur du fichier et les classifications de sécurité associées. Ces métadonnées peuvent être exploitées par les applications client pour prendre des décisions éclairées en matière d'accès et organiser les fichiers en fonction des normes et des exigences de l'entreprise.

Exemple de paires clé-valeur xattr

Clé	Valeur
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

Clé	Valeur

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

Clé	Valeur
`user.geo_point`	`[-78.7941, 35.7956]`

```
    }
}
```

Informations associées

- "NFS dans NetApp ONTAP : guide des bonnes pratiques et d'implémentation"
- "Référence des commandes ONTAP"
- Demande de commentaires (RFC)
  - "RFC 7204 : exigences pour le protocole NFS étiqueté"
  - "RFC 2203 : spécification du protocole RPCSEC_GSS"
  - "RFC 3530 : protocole NFS (Network File System) version 4"

Informations sur le copyright

Informations sur les marques commerciales