



Autorisation du client

ONTAP 9

NetApp
January 10, 2025

Sommaire

- Autorisation du client 1
 - Présentation et options de l'autorisation client ONTAP 1
 - Oscilloscopes OAuth 2.0 autonomes 2
 - Utilisation des groupes 4
 - Mappage de rôles externes 7
 - Comment ONTAP détermine l'accès client 9

Autorisation du client

Présentation et options de l'autorisation client ONTAP

L'implémentation ONTAP OAuth 2.0 est conçue pour être flexible et robuste, et vous offre les fonctionnalités dont vous avez besoin pour sécuriser votre environnement ONTAP. Plusieurs options de configuration mutuellement exclusives sont disponibles. Les décisions d'autorisation sont finalement basées sur les rôles REST ONTAP contenus dans ou dérivés des jetons d'accès OAuth 2.0.



Vous pouvez uniquement utiliser "[Rôles REST ONTAP](#)" Lors de la configuration de l'autorisation pour OAuth 2.0. Les anciens rôles ONTAP traditionnels ne sont pas pris en charge.

ONTAP applique l'option d'autorisation la plus appropriée en fonction de votre configuration. Pour plus d'informations sur la manière dont ONTAP prend les décisions d'accès client, reportez-vous à la section "[Comment ONTAP détermine l'accès](#)".

Oscilloscopes autonomes OAuth 2.0

Ces étendues contiennent un ou plusieurs rôles REST personnalisés, chacun encapsulé dans une seule chaîne dans le jeton d'accès. Ils sont indépendants des définitions de rôles ONTAP. Vous devez configurer les chaînes de portée sur votre serveur d'autorisation. Voir "[Oscilloscopes OAuth 2.0 autonomes](#)" pour plus d'informations.

Rôles REST ONTAP locaux

Un seul rôle REST nommé, intégré ou personnalisé, peut être utilisé. La syntaxe de portée d'un rôle nommé est `ontap-role-<URL-encoded-ONTAP-role-name>`. Par exemple, si le rôle ONTAP est `admin` la chaîne de portée sera `ontap-role-admin`.

Utilisateurs

Le nom d'utilisateur dans le jeton d'accès défini avec l'accès à l'application « http » peut être utilisé. Un utilisateur est testé dans l'ordre suivant en fonction de la méthode d'authentification définie : mot de passe, domaine (Active Directory), nsswitch (LDAP).

Groupes

Les serveurs d'autorisation peuvent être configurés pour utiliser des groupes ONTAP pour l'autorisation. Si les définitions ONTAP locales sont examinées mais qu'aucune décision d'accès ne peut être prise, les groupes Active Directory (« domaine ») ou LDAP (« nsswitch ») sont utilisés. Les informations de groupe peuvent être spécifiées de deux manières :

- Chaîne de portée OAuth 2.0

Prend en charge les applications confidentielles en utilisant le flux d'informations d'identification du client lorsqu'aucun utilisateur n'est membre d'un groupe. Le périmètre doit être nommé `ontap-group-<URL-encoded-ONTAP-group-name>`. Par exemple, si le groupe est « développement », la chaîne de portée sera « `ontap-groupe-développement` ».

- Dans la réclamation « Groupe »

Ceci est destiné aux jetons d'accès émis par ADFS à l'aide du flux propriétaire de la ressource (mot de passe Grant).

Voir "[Utilisation des groupes](#)" pour plus d'informations.

Oscilloscopes OAuth 2.0 autonomes

Les étendues autonomes sont des chaînes portées dans le jeton d'accès. Chacune d'entre elles constitue une définition de rôle personnalisée complète et comprend tout ce dont ONTAP a besoin pour prendre une décision d'accès. Le périmètre est distinct et celui de tous les rôles REST définis au sein de ONTAP lui-même.

Format de la chaîne de portée

Au niveau de la base, la portée est représentée sous la forme d'une chaîne contiguë et composée de six valeurs séparées par deux points. Les paramètres utilisés dans la chaîne de portée sont décrits ci-dessous.

Littéral ONTAP

La portée doit commencer par la valeur littérale `ontap` en minuscules. Cette opération identifie la portée en tant que spécifique à ONTAP.

Cluster

Il définit le cluster ONTAP auquel la portée s'applique. Les valeurs peuvent inclure :

- UUID de cluster

Identifie un seul cluster.

- Astérisque (*)

Indique que la portée s'applique à tous les clusters.

Vous pouvez utiliser la commande CLI de ONTAP `cluster identity show` Pour afficher l'UUID de votre cluster. Si elle n'est pas spécifiée, la portée s'applique à tous les clusters.

Rôle

Nom du rôle REST contenu dans le périmètre autonome. Cette valeur n'est pas examinée par ONTAP ou associée à tout rôle REST existant défini sur ONTAP. Le nom est utilisé pour la journalisation.

Niveau d'accès

Cette valeur indique le niveau d'accès appliqué à l'application client lors de l'utilisation du noeud final de l'API dans le périmètre. Il existe six valeurs possibles, comme décrit dans le tableau ci-dessous.

Niveau d'accès	Description
Aucune	Refuse tout accès au noeud final spécifié.
lecture seule	Autorise uniquement l'accès en lecture à l'aide de GET.
read_create	Permet l'accès en lecture ainsi que la création de nouvelles instances de ressources à l'aide de POST.

Niveau d'accès	Description
lire_modifier	Permet l'accès en lecture ainsi que la mise à jour des ressources existantes à l'aide d'un CORRECTIF.
read_create_modify	Permet tous les accès sauf supprimer. Les opérations autorisées comprennent OBTENIR (lire), POST (créer) et PATCH (mettre à jour).
tous	Permet un accès complet.

SVM

Nom du SVM au sein du cluster auquel la portée s'applique. Utilisez la valeur * (astérisque) pour indiquer tous les SVM.



Cette fonctionnalité n'est pas entièrement prise en charge par ONTAP 9.14.1. Vous pouvez ignorer le paramètre du SVM et utiliser un astérisque comme emplacement réservé. Vérifiez le ["Notes de version de ONTAP"](#) Pour vérifier la prise en charge future des SVM.

URI DE L'API REST

Chemin complet ou partiel d'une ressource ou d'un ensemble de ressources associées. La chaîne doit commencer par `/api`. Si vous ne spécifiez pas de valeur, la portée s'applique à tous les terminaux d'API du cluster ONTAP.

Exemples de portée

Quelques exemples de portées autonomes sont présentés ci-dessous.

ontap:*:joes-role:read_create_modify:*/api/cluster

Permet à l'utilisateur affecté à ce rôle d'accéder en lecture, création et modification à `/cluster` point final.

Outil d'administration CLI

Pour faciliter l'administration des étendues autonomes et réduire le risque d'erreur, ONTAP fournit la commande CLI `security oauth2 scope` pour générer des chaînes de portée basées sur vos paramètres d'entrée.

La commande `security oauth2 scope` propose deux cas d'utilisation basés sur vos commentaires :

- Paramètres de l'interface de ligne de commande pour la chaîne de périmètre

Vous pouvez utiliser cette version de la commande pour générer une chaîne de portée basée sur les paramètres d'entrée.

- Chaîne d'étendue aux paramètres CLI

Vous pouvez utiliser cette version de la commande pour générer les paramètres de la commande en fonction de la chaîne de périmètre d'entrée.

Exemple

L'exemple suivant génère une chaîne de périmètre avec le résultat inclus après l'exemple de commande ci-dessous. La définition s'applique à tous les clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Utilisation des groupes

ONTAP propose plusieurs options de configuration de groupes en fonction de votre serveur d'autorisation. Les groupes peuvent ensuite être mappés à des rôles qui sont utilisés par ONTAP pour déterminer l'accès.

Comment les groupes sont identifiés

Lorsque vous configurez un groupe sur un serveur d'autorisation, il est identifié et transporté par un jeton d'accès OAuth 2.0 à l'aide d'un nom ou d'un UUID. Vous devez savoir comment votre serveur d'autorisation gère les groupes avant de configurer ONTAP.



Si plusieurs groupes sont inclus dans un jeton d'accès, ONTAP tente d'utiliser chacun d'eux jusqu'à ce qu'il y ait correspondance.

Noms de groupe

De nombreux serveurs d'autorisation identifient et représentent des groupes à l'aide d'un nom. Voici un fragment d'un jeton d'accès JSON généré par ADFS (Active Directory Federation Service) contenant plusieurs groupes. Voir [Gérer les groupes avec des noms](#) pour plus d'informations.

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

UUID de groupe

Certains serveurs d'autorisation identifient et représentent des groupes à l'aide d'un UUID. Voici un fragment d'un jeton d'accès JSON généré par Microsoft Entra ID contenant plusieurs groupes. Voir [Gestion des groupes avec des UUID](#) pour plus d'informations.

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

Gérer les groupes avec des noms

Si votre serveur d'autorisation utilise des noms pour identifier des groupes, vous devez vous assurer que chaque groupe est défini sur ONTAP. Selon votre environnement de sécurité, il se peut que le groupe soit déjà défini.

Voici un exemple de commande CLI définissant un groupe pour ONTAP. Notez qu'il utilise un groupe nommé à partir de l'exemple de jeton d'accès. Vous devez être au niveau de privilège ONTAP **admin** pour exécuter la commande.

Exemple

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```



Vous pouvez également configurer cette fonctionnalité à l'aide de l'API REST ONTAP. Pour en savoir plus, consultez le ["Documentation sur l'automatisation ONTAP"](#).

Gestion des groupes avec des UUID

Si votre serveur d'autorisation représente des groupes utilisant des valeurs UUID, vous devez effectuer une configuration en deux étapes avant d'utiliser un groupe. À partir de ONTAP 9.16.1, deux fonctionnalités de mappage sont disponibles et ont été testées avec Microsoft Entra ID. Vous devez être au niveau de privilège ONTAP **admin** pour exécuter les commandes CLI.



Vous pouvez également configurer ces fonctionnalités à l'aide de l'API REST ONTAP. Pour en savoir plus, consultez le ["Documentation sur l'automatisation ONTAP"](#).

Informations associées

- ["Commandes ONTAP CLI"](#)

Mapper un UUID de groupe sur un nom de groupe

Si vous utilisez un serveur d'autorisation qui représente des groupes à l'aide de valeurs UUID, vous devez mapper les UUID du groupe aux noms des groupes. Les principales opérations de l'interface de ligne de commandes ONTAP sont décrites ci-dessous.

Création

Vous pouvez définir une nouvelle configuration de mappage de groupe à l'aide de la `security login group create` commande. L'UUID et le nom du groupe doivent correspondre à la configuration du serveur d'autorisation.

Paramètres

Les paramètres utilisés pour créer un mappage de groupe sont décrits ci-dessous.

Paramètre	Description
<code>vserver</code>	Spécifier éventuellement le nom du SVM (<code>vserver</code>) auquel le groupe est associé. Si vous omettez le paramètre, le groupe est associé au cluster ONTAP.
<code>name</code>	Nom unique du groupe que ONTAP utilisera.
<code>type</code>	Cette valeur indique le fournisseur d'identité dont provient le groupe.
<code>uuid</code>	Spécifie l'identificateur unique universel du groupe tel que fourni par le serveur d'autorisation.

Voici un exemple de commande CLI définissant un groupe pour ONTAP. Notez qu'il utilise un groupe UUID à partir de l'exemple de jeton d'accès.

Exemple

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra  
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

Une fois le groupe créé, un identifiant d'entier unique en lecture seule est généré pour le groupe.

Autres opérations de l'interface de ligne de commande

La commande prend en charge plusieurs opérations supplémentaires, notamment :

- Afficher
- Modifier
- Supprimer

Vous pouvez utiliser `show` l'option pour récupérer l'ID de groupe unique généré pour un groupe. Pour plus d'informations, reportez-vous à la documentation de référence des commandes ONTAP.

Mapper un UUID de groupe à un rôle

Si vous utilisez un serveur d'autorisation qui représente des groupes à l'aide de valeurs UUID, vous pouvez mapper le groupe à un rôle. Les principales opérations de l'interface de ligne de commandes ONTAP sont décrites ci-dessous. Vous devez également être au niveau de privilège ONTAP **admin** pour exécuter les commandes.



Vous devez d'abord [Mapper un UUID de groupe sur un nom de groupe](#) récupérer l'ID d'entier unique généré pour le groupe. Vous aurez besoin de l'ID pour mapper le groupe à un rôle.

Création

Vous pouvez définir un nouveau mappage de rôles à l'aide de la `security login group role-mapping create` commande.

Paramètres

Les paramètres utilisés pour mapper un groupe à un rôle sont décrits ci-dessous.

Paramètre	Description
group-id	Spécifie l'ID unique généré pour le groupe à l'aide de la commande <code>security login group create</code> .
role	Nom du rôle ONTAP auquel le groupe est mappé.

Exemple

```
security login group role-mapping create -group-id 1 -role admin
```

Autres opérations de l'interface de ligne de commande

La commande prend en charge plusieurs opérations supplémentaires, notamment :

- Afficher
- Modifier
- Supprimer

Pour plus d'informations, reportez-vous à la documentation de référence des commandes ONTAP.

Mappage de rôles externes

Un rôle externe est défini dans un fournisseur d'identification configuré pour une utilisation par ONTAP. Vous pouvez créer et gérer des relations de mappage entre ces rôles externes et les rôles ONTAP à l'aide de l'interface de ligne de commandes ONTAP.



Vous pouvez également configurer la fonction de mappage de rôles externes à l'aide de l'API REST ONTAP. Pour en savoir plus, consultez le "[Documentation sur l'automatisation ONTAP](#)".

Informations associées

- "[Commandes ONTAP CLI](#)".

Rôles externes dans un jeton d'accès

Voici un fragment d'un jeton d'accès JSON contenant deux rôles externes.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Configuration

Vous pouvez utiliser l'interface de ligne de commande ONTAP pour administrer la fonction de mappage de rôle externe.

Création

Vous pouvez définir une configuration de mappage de rôles à l'aide de la `security login external-role-mapping create` commande. Vous devez être au niveau de privilège ONTAP **admin** pour exécuter cette commande ainsi que les options associées.

Paramètres

Les paramètres utilisés pour créer un mappage de groupe sont décrits ci-dessous.

Paramètre	Description
<code>external-role</code>	Nom du rôle défini au niveau du fournisseur d'identité externe.
<code>provider</code>	Nom du fournisseur d'identité. Il doit s'agir de l'identifiant du système.
<code>ontap-role</code>	Indique le rôle ONTAP existant vers lequel le rôle externe est mappé.

Exemple

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Autres opérations de l'interface de ligne de commande

La commande prend en charge plusieurs opérations supplémentaires, notamment :

- Afficher
- Modifier
- Supprimer

Pour plus d'informations, reportez-vous à la documentation de référence sur les commandes ONTAP ou aux pages man sur l'interface de ligne de commande ONTAP.

Comment ONTAP détermine l'accès client

Pour bien concevoir et mettre en œuvre OAuth 2.0, vous devez comprendre comment ONTAP utilise votre configuration d'autorisation pour prendre des décisions d'accès pour les clients. Les principales étapes permettant de déterminer l'accès sont présentées ci-dessous en fonction de la version de ONTAP.



Il n'y a pas eu de mises à jour OAuth 2.0 significatives avec ONTAP 9.15.1. Si vous utilisez la version 9.15.1, reportez-vous à la description de ONTAP 9.14.1.

Informations associées

- ["Fonctionnalités OAuth 2.0 prises en charge dans ONTAP"](#)

ONTAP 9.16.1

ONTAP 9.16.1 étend la prise en charge standard d'OAuth 2.0 pour inclure des extensions spécifiques d'Entra ID Microsoft pour les groupes d'ID Entra natifs ainsi que le mappage de rôles externes.

Déterminez l'accès client pour ONTAP 9.16.1

Étape 1 : oscilloscopes autonomes

Si le jeton d'accès contient des étendues autonomes, ONTAP examine d'abord ces étendues. S'il n'y a pas de portées autonomes, passez à l'étape 2.

Avec une ou plusieurs portées autonomes présentes, ONTAP applique chaque portée jusqu'à ce qu'une décision explicite **ALLOW** ou **DENY** puisse être prise. Si une décision explicite est prise, le traitement prend fin.

Si ONTAP ne peut pas prendre de décision explicite en matière d'accès, passez à l'étape 2.

Étape 2 : vérifiez l'indicateur de rôles locaux

ONTAP examine le paramètre booléen `use-local-roles-if-present`. La valeur de cet indicateur est définie séparément pour chaque serveur d'autorisation défini sur ONTAP.

- Si la valeur est de `true` passez à l'étape 3.
- Si la valeur est de `false` le traitement se termine et l'accès est refusé.

Étape 3 : rôle REST ONTAP nommé

Si le jeton d'accès contient un rôle REST nommé dans le `scope` champ ou `scp`, ou en tant que sinistre, ONTAP utilise le rôle pour prendre la décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S'il n'y a pas de rôle REST nommé ou si le rôle est introuvable, passez à l'étape 4.

Étape 4 : utilisateurs

Extrayez le nom d'utilisateur du jeton d'accès et essayez de le faire correspondre aux utilisateurs ayant accès à l'application « http ». Les utilisateurs sont examinés en fonction de la méthode d'authentification dans l'ordre suivant :

- mot de passe
- Domaine (Active Directory)
- Nsswitch (LDAP)

Si un utilisateur correspondant est trouvé, ONTAP utilise le rôle défini pour l'utilisateur afin de prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

Si un utilisateur ne correspond pas ou s'il n'y a pas de nom d'utilisateur dans le jeton d'accès, passez à l'étape 5.

Étape 5 : groupes

Si un ou plusieurs groupes sont inclus, le format est examiné. Si les groupes sont représentés en tant qu'UUID, une table de mappage de groupe interne est recherchée. S'il existe une correspondance de groupe et un rôle associé, ONTAP utilise le rôle défini pour le groupe pour prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement. Pour plus d'informations, voir "[Utilisation des groupes](#)".

Si les groupes sont représentés par des noms et configurés avec l'autorisation domaine ou nsswitch, ONTAP tente de les faire correspondre à un groupe Active Directory ou LDAP, respectivement. S'il existe une correspondance de groupe, ONTAP utilise le rôle défini pour le groupe pour prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S'il n'y a pas de correspondance de groupe ou s'il n'y a pas de groupe dans le jeton d'accès, l'accès est refusé et le traitement se termine.

ONTAP 9.14.1

La version initiale de OAuth 2.0 prise en charge est introduite avec ONTAP 9.14.1 en fonction des fonctionnalités standard de OAuth 2.0.

Déterminez l'accès client pour ONTAP 9.14.1

Étape 1 : oscilloscopes autonomes

Si le jeton d'accès contient des étendues autonomes, ONTAP examine d'abord ces étendues. S'il n'y a pas de portées autonomes, passez à l'étape 2.

Avec une ou plusieurs portées autonomes présentes, ONTAP applique chaque portée jusqu'à ce qu'une décision explicite **ALLOW** ou **DENY** puisse être prise. Si une décision explicite est prise, le traitement prend fin.

Si ONTAP ne peut pas prendre de décision explicite en matière d'accès, passez à l'étape 2.

Étape 2 : vérifiez l'indicateur de rôles locaux

ONTAP examine le paramètre booléen `use-local-roles-if-present`. La valeur de cet indicateur est définie séparément pour chaque serveur d'autorisation défini sur ONTAP.

- Si la valeur est de `true` passez à l'étape 3.
- Si la valeur est de `false` le traitement se termine et l'accès est refusé.

Étape 3 : rôle REST ONTAP nommé

Si le jeton d'accès contient un rôle REST nommé dans le `scope` champ ou `scp`, ONTAP utilise le rôle pour prendre la décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S'il n'y a pas de rôle REST nommé ou si le rôle est introuvable, passez à l'étape 4.

Étape 4 : utilisateurs

Extrayez le nom d'utilisateur du jeton d'accès et essayez de le faire correspondre aux utilisateurs ayant accès à l'application « http ». Les utilisateurs sont examinés en fonction de la méthode d'authentification dans l'ordre suivant :

- mot de passe
- Domaine (Active Directory)
- Nsswitch (LDAP)

Si un utilisateur correspondant est trouvé, ONTAP utilise le rôle défini pour l'utilisateur afin de prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

Si un utilisateur ne correspond pas ou s'il n'y a pas de nom d'utilisateur dans le jeton d'accès, passez à l'étape 5.

Étape 5 : groupes

Si un ou plusieurs groupes sont inclus et configurés avec l'autorisation `domain` ou `nsswitch`, ONTAP tente de les associer à un groupe Active Directory ou LDAP, respectivement.

S'il existe une correspondance de groupe, ONTAP utilise le rôle défini pour le groupe pour prendre une décision d'accès. Cela entraîne toujours une décision **ALLOW** ou **DENY** et la fin du traitement.

S'il n'y a pas de correspondance de groupe ou s'il n'y a pas de groupe dans le jeton d'accès, l'accès est refusé et le traitement se termine.

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.