Gestion du protocole SNMP sur le cluster (administrateurs du cluster uniquement)

ONTAP 9

NetApp
March 24, 2023

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/networking/manage_snmp_on_the_cluster_@cluster_administrators_only@_overview.html on March 24, 2023. Always check docs.netapp.com for the latest.

Table des matières

Gestion du protocole SNMP sur le cluster (administrateurs du cluster uniquement)

Présentation

Vous pouvez configurer le protocole SNMP pour surveiller les SVM au sein de votre cluster afin d'éviter les problèmes avant qu'ils ne se produisent et de répondre aux problèmes en cas de survenue. La gestion de SNMP implique la configuration des utilisateurs SNMP et la configuration des destinations de Traphost SNMP (stations de travail de gestion) pour tous les événements SNMP. SNMP est désactivé par défaut sur les LIFs de données.

Vous pouvez créer et gérer des utilisateurs SNMP en lecture seule dans la SVM de données. Les LIFs data doivent être configurées de sorte à recevoir des requêtes SNMP sur le SVM.

Les postes de travail SNMP de gestion de réseau, ou gestionnaires, peuvent interroger l'agent SNMP du SVM pour obtenir des informations. L'agent SNMP recueille des informations et les transmet aux gestionnaires SNMP. L'agent SNMP génère également des notifications d'interruption lorsque des événements spécifiques se produisent. L'agent SNMP du SVM possède des privilèges en lecture seule ; il ne peut pas être utilisé pour des opérations définies ou pour effectuer une action corrective en réponse à un trap. ONTAP fournit un agent SNMP compatible avec les versions SNMP v1, v2c et v3. SNMPv3 offre une sécurité avancée en utilisant des phrases de passe et le cryptage.

Pour plus d'informations sur la prise en charge SNMP dans les systèmes ONTAP, voir "Tr-4220 : prise en charge SNMP dans Data ONTAP".

Que sont les MIB

Une base MIB (Management information base) est un fichier texte qui décrit les objets SNMP et les traps.

Les MIB décrivent la structure des données de gestion du système de stockage et utilisent un espace de noms hiérarchique contenant des identifiants d'objets (OID). Chaque OID identifie une variable qui peut être lue à l'aide de SNMP.

Étant donné que les MIB ne sont pas des fichiers de configuration et que ONTAP ne lit pas ces fichiers, la fonctionnalité SNMP n'est pas affectée par les MIB. ONTAP fournit le fichier MIB suivant :

- Une MIB personnalisées NetApp (`netapp.mib`)

ONTAP prend en charge les MIB IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) et ICMP (RFC 2466), qui affichent à la fois des données IPv4 et IPv6.

ONTAP fournit également une référence croisée courte entre les identificateurs d'objet (OID) et les noms courts d'objet dans le `traps.dat` fichier.

Les dernières versions des fichiers MIB ONTAP et `traps.dat `sont disponibles sur le site de support NetApp. Cependant, les versions de ces fichiers sur le site de support ne correspondent pas nécessairement aux capacités SNMP de votre version ONTAP. Ces fichiers sont fournis pour vous aider à évaluer les fonctions SNMP dans la dernière version de ONTAP.

Interruptions SNMP

Les interruptions SNMP capturent les informations de surveillance du système envoyées en tant que notification asynchrone de l'agent SNMP au gestionnaire SNMP.

Il existe trois types d'interruptions SNMP : standard, intégré et défini par l'utilisateur. Les interruptions définies par l'utilisateur ne sont pas prises en charge dans ONTAP.

Un trap peut être utilisé pour vérifier périodiquement les seuils opérationnels ou les échecs définis dans la MIB. Si un seuil est atteint ou qu'une panne est détectée, l'agent SNMP envoie un message (interruption) aux Traphosts les alertant de l'événement.

ONTAP prend en charge les déroutements SNMPv1 et, staring dans ONTAP 9.1, SNMPv3 déroutements. ONTAP ne prend pas en charge les déroutements SNMPv2c et n'informe pas.

Interruptions SNMP standard

Ces interruptions sont définies dans RFC 1215. Il existe cinq interruptions SNMP standard prises en charge par ONTAP : coldstart, warmstart, Linkdown, linkup et authenticationFailure.

Le trap authenticationFailure est désactivé par défaut. Vous devez utiliser le `system snmp authtrap` commande pour activer le trap. Pour plus d'informations, consultez les pages man : "Commandes ONTAP 9"

Interruptions SNMP intégrées

Les interruptions intégrées sont prédéfinies dans ONTAP et sont automatiquement envoyées aux stations de gestion du réseau de la liste des Traphost si un événement se produit. Ces interruptions, telles que diskFailedShutdown, cpuTooBusy et volume NearlyFull, sont définies dans la MIB personnalisées.

Chaque trappe intégrée est identifiée par un code d'interruption unique.

Créer une communauté SNMP et l'attribuer à une LIF

Vous pouvez créer une communauté SNMP qui agit comme un mécanisme d'authentification entre le poste de gestion et le SVM (Storage Virtual machine) en cas d'utilisation des protocoles SNMPv1 et SNMPv2c.

En créant des communautés SNMP dans un SVM de données, vous pouvez exécuter des commandes telles que `snmpwalk` et `snmpget` Sur les LIF de données.

Description de la tâche

- Dans les nouvelles installations de ONTAP, SNMPv1 et SNMPv2c sont désactivés par défaut.

  Les protocoles SNMPv1 et SNMPv2c sont activés après la création d'une communauté SNMP.

- ONTAP prend en charge les communautés en lecture seule.
- Par défaut la politique de pare-feu « données » qui est attribuée aux LIFs de données a le service SNMP défini sur `deny`.

  Vous devez créer une nouvelle politique de pare-feu avec le service SNMP défini sur `allow` Lors de la création d'un utilisateur SNMP pour un SVM de données.

  > Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "Configuration des politiques de pare-feu pour les LIF".

- Vous pouvez créer des communautés SNMP pour les utilisateurs SNMPv1 et SNMPv2c pour la SVM d'administration et la SVM de données.
- Comme un SVM ne fait pas partie de la norme SNMP, les requêtes relatives aux LIF de données doivent inclure l'OID racine NetApp (1.3.6.1.4.1.789), par exemple `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Étapes

1. Créez une communauté SNMP en utilisant le `system snmp community add` commande. La commande suivante montre comment créer une communauté SNMP dans le SVM admin cluster-1 :

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   La commande suivante montre comment créer une communauté SNMP dans le SVM de données vs1 :

   ```
   system snmp community add -type ro -community-name comty2 -vserver vs1
   ```

2. Vérifiez que les communautés ont été créées à l'aide de la commande system snmp community show.

   La commande suivante présente les deux communautés créées pour SNMPv1 et SNMPv2c :

   ```
   system snmp community show
   cluster-1
   rocomty1
   vs1
   rocomty2
   ```

3. Vérifier si SNMP est autorisé en tant que service dans la politique de pare-feu « data » en utilisant le `system services firewall policy show` commande.

   La commande suivante indique que le service snmp n'est pas autorisé dans la politique de pare-feu « data » par défaut (le service snmp est autorisé dans la politique de pare-feu « mgmt » uniquement) :

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. Créez une nouvelle politique de pare-feu qui autorise l'accès à l'aide du système `snmp` service à l'aide du `system services firewall policy create` commande.

   Les commandes suivantes créent une nouvelle politique de pare-feu de données nommée « data1 » qui autorise le `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. Appliquer la politique de pare-feu à une LIF de données à l'aide de la commande `network interface modify `avec le paramètre -firewall-policy.

La commande suivante attribue la nouvelle politique de pare-feu « data1 » à LIF « datalif1 » :

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

Configurez les utilisateurs SNMPv3 dans un cluster

SNMPv3 est un protocole sécurisé lorsqu'il est comparé au protocole SNMPv1 et SNMPv2c. Pour utiliser SNMPv3, vous devez configurer un utilisateur SNMPv3 pour exécuter les utilitaires SNMP à partir du gestionnaire SNMP.

Étape

Utilisez la commande « Security login create » pour créer un utilisateur SNMPv3.

Vous êtes invité à fournir les informations suivantes :

- ID moteur : la valeur par défaut et la valeur recommandée sont l'ID moteur local
- Protocole d'authentification
- Mot de passe d'authentification
- Protocole de confidentialité
- Mot de passe du protocole de confidentialité

Résultat

L'utilisateur SNMPv3 peut se connecter à partir du gestionnaire SNMP en utilisant le nom d'utilisateur et le mot de passe et en exécutant les commandes de l'utilitaire SNMP.

Paramètres de sécurité SNMPv3

SNMPv3 inclut une fonctionnalité d'authentification qui, lorsqu'elle est sélectionnée, demande aux utilisateurs de saisir leurs noms, un protocole d'authentification, une clé d'authentification et le niveau de sécurité souhaité lors de l'appel d'une commande.

Le tableau suivant répertorie les paramètres de sécurité SNMPv3 :

Paramètre	Option de ligne de commandes	Description
ID d'ingénierie	-E EngineID	ID moteur de l'agent SNMP. La valeur par défaut est local EngineID (recommandé).
Nom de sécurité	-U Nom	Le nom d'utilisateur ne doit pas dépasser 32 caractères.
Protocole d'authentification	-A {none	MD5

SHA	SHA-256}	Le type d'authentification peut être aucun, MD5, SHA ou SHA-256.
AuthKey	-UNE PHRASE DE PASSE	Phrase de passe avec un minimum de huit caractères.
Niveau de sécurité	-L {authNoPriv	AuthPriv
noAuthNoPriv}	Le niveau de sécurité peut être authentification, aucune confidentialité, authentification, confidentialité ou aucune authentification, Aucune confidentialité.	Protocole privé
-x { none	des	aes128}
Le protocole de confidentialité peut être aucun, des ou aes128	Mot de passe privé	-X mot de passe

Exemples de niveaux de sécurité différents

Cet exemple montre comment un utilisateur SNMPv3 créé avec différents niveaux de sécurité peut utiliser les commandes SNMP côté client, telles que `snmpwalk`, pour interroger les objets de cluster.

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.

Vous devez utiliser `snmpwalk` 5.3.1 ou version ultérieure lorsque le protocole d'authentification est SHA.

Niveau de sécurité : AuthPriv

Le résultat suivant montre la création d'un utilisateur SNMPv3 avec le niveau de sécurité d'authPriv.

```
security login create -username snmpv3user -application snmp -authmethod
usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose  (none, md5, sha)
[none]:sha
```

Mode FIPS

```
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose  (none, des) [none]: des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Test snmpwalk

La sortie suivante montre l'utilisateur SNMPv3 exécutant la commande snmpwalk :

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Niveau de sécurité : AuthNoPriv

Le résultat suivant montre la création d'un utilisateur SNMPv3 avec le niveau de sécurité authNoPriv.

```
security login create -username snmpv3user1 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

Mode FIPS

```
Which privacy protocol do you want to choose (aes128) [aes128]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (none, des) [none]: none
```

Test snmpwalk

La sortie suivante montre l'utilisateur SNMPv3 exécutant la commande snmpwalk :

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Niveau de sécurité : NoAuthNoPriv

La sortie suivante montre la création d'un utilisateur SNMPv3 avec le niveau de sécurité noAuthNoPriv.

```
security login create -username snmpv3user2 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

Mode FIPS

FIPS ne vous permettra pas de choisir aucun

Test snmpwalk

La sortie suivante montre l'utilisateur SNMPv3 exécutant la commande snmpwalk :

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Configurez les Traphosts pour recevoir des notifications SNMP

Vous pouvez configurer le Traphost (gestionnaire SNMP) pour recevoir des notifications (PDU d'interruption SNMP) lorsque des interruptions SNMP sont générées dans le cluster. Vous pouvez spécifier le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) du Traphost SNMP.

Avant de commencer

- Les traps SNMP doivent être activés sur le cluster.

> Les interruptions SNMP et SNMP sont activées par défaut.

- Le DNS doit être configuré sur le cluster pour la résolution des noms de Traphost.
- IPv6 doit être activé sur le cluster pour configurer les Traphosts SNMP à l'aide des adresses IPv6.
- Pour ONTAP 9.1 et versions ultérieures, vous devez avoir spécifié l'authentification d'un modèle de sécurité utilisateur prédéfini (USM) et des informations d'identification de confidentialité lors de la création de Traphosts.

Étape

Ajouter un Traphost SNMP :

```
system snmp traphost add
```

> Les interruptions ne peuvent être envoyées que lorsqu'au moins une station de gestion SNMP est spécifiée comme un traphost.

La commande suivante ajoute un nouvel hôte SNMPv3 nommé yyy.example.com avec un utilisateur USM connu :

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

La commande suivante ajoute un Traphost à l'aide de l'adresse IPv6 de l'hôte :

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

Commandes pour la gestion de SNMP

Vous pouvez utiliser le `system snmp` Commandes permettant de gérer SNMP, les traps et les Traphosts. Vous pouvez utiliser le `security` Commandes permettant de gérer les utilisateurs SNMP par SVM. Vous pouvez utiliser le `event` Commandes pour gérer les événements liés aux traps SNMP.

Commandes permettant de configurer SNMP

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez SNMP sur le cluster	`options -option-name snmp.enable -option-value on` Le service SNMP doit être autorisé conformément à la politique de pare-feu de gestion. Vous pouvez vérifier si le protocole SNMP est autorisé via la commande system services firewall policy show.
Désactiver le protocole SNMP sur le cluster	`options -option-name snmp.enable -option-value off`

Commandes pour la gestion des utilisateurs SNMP v1, v2c et v3

Les fonctions que vous recherchez…	Utilisez cette commande…
Configurez les utilisateurs SNMP	`security login create`
Afficher les utilisateurs SNMP	`security snmpusers and security login show -application snmp`
Supprimer les utilisateurs SNMP	`security login delete`
Modifier le nom du rôle de contrôle d'accès d'une méthode de connexion pour les utilisateurs SNMP	`security login modify`

Commandes permettant de fournir des informations de contact et d'emplacement

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher ou modifier les détails du contact du cluster	`system snmp contact`
Afficher ou modifier les détails d'emplacement du cluster	`system snmp location`

Commandes pour la gestion des communautés SNMP

Les fonctions que vous recherchez…	Utilisez cette commande…
Ajoutez une communauté en lecture seule (ro) pour un SVM ou pour tous les SVM du cluster	`system snmp community add`

Supprimer une communauté ou toutes les communautés	`system snmp community delete`
Afficher la liste de toutes les communautés	`system snmp community show`

Les SVM ne faisant pas partie de la norme SNMP, les requêtes relatives aux LIF de données doivent inclure l'OID racine NetApp (1.3.6.1.4.1.789), par exemple. `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Commande pour l'affichage des valeurs d'option SNMP

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher les valeurs actuelles de toutes les options SNMP, y compris le contact de cluster, l'emplacement de contact, si le cluster est configuré pour envoyer des traps, la liste des Traphosts, la liste des communautés et le type de contrôle d'accès	`system snmp show`

Commandes pour la gestion des interruptions SNMP et des Traphosts

Les fonctions que vous recherchez…	Utilisez cette commande…
Activer les traps SNMP envoyés depuis le cluster	`system snmp init -init 1`
Désactiver les traps SNMP envoyés depuis le cluster	`system snmp init -init 0`
Ajoutez un Traphost qui reçoit des notifications SNMP pour des événements spécifiques dans le cluster	`system snmp traphost add`
Supprimer un Traphost	`system snmp traphost delete`
Affiche la liste des Traphosts	`system snmp traphost show`

Commandes pour la gestion des événements liés aux traps SNMP

Les fonctions que vous recherchez…	Utilisez cette commande…

Afficher les événements pour lesquels des interruptions SNMP (intégrées) sont générées	`event route show` Utilisez le `-snmp-support true` Paramètre pour afficher uniquement les événements SNMP. Utilisez le `instance -messagename <message>` paramètre permettant d'afficher une description détaillée de la raison d'un événement et de toute action corrective. Le routage des événements de déroutement SNMP individuels vers des destinations de traphost spécifiques n'est pas pris en charge. Tous les événements de déroutement SNMP sont envoyés à toutes les destinations de Traphost.
Affiche la liste des enregistrements de l'historique des interruptions SNMP, qui sont des notifications d'événements envoyées à des interruptions SNMP	`event snmphistory show`
Supprimer un enregistrement de l'historique des interruptions SNMP	`event snmphistory delete`

Pour plus d'informations sur le `system snmp`, `security`, et `event` commandes, voir les pages de manuels : "Commandes ONTAP 9"

Informations sur le copyright

Copyright © 2023 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 DÉLICTUELLE (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.