Configurer les notifications

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-918/config/task_configure_unified_manager_to_send_alert_notifications.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Configurer les notifications . . . 1
- Configurez Active IQ Unified Manager pour envoyer des notifications d'alerte . . . 1
- Configurez les paramètres de notification d'événements dans Active IQ Unified Manager . . . 1
- Activer l'authentification à distance dans Active IQ Unified Manager . . . 2
- Désactivez les groupes imbriqués de l'authentification à distance dans Active IQ Unified Manager . . . 4
- Configurez les services d'authentification dans Active IQ Unified Manager . . . 4
- Ajouter des serveurs d'authentification à Active IQ Unified Manager . . . 5
- Testez la configuration des serveurs d'authentification dans Active IQ Unified Manager . . . 7
- Ajouter des alertes dans Active IQ Unified Manager . . . 7
  - Exemple d'ajout d'une alerte . . . 9

Configurer les notifications

Configurez Active IQ Unified Manager pour envoyer des notifications d'alerte

Vous pouvez configurer Unified Manager pour envoyer des notifications qui vous alertent sur les événements survenant dans votre environnement. Avant que ces notifications puissent être envoyées, vous devez configurer plusieurs autres options d'Unified Manager.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Après avoir déployé Unified Manager et effectué la configuration initiale, vous devriez envisager de configurer votre environnement pour déclencher des alertes et générer des e-mails de notification ou des traps SNMP à la réception d'événements.

Étapes

1. "Configurer les paramètres de notification d'événements".

   Si vous souhaitez que des notifications d'alerte soient envoyées lorsque certains événements se produisent dans votre environnement, vous devez configurer un serveur SMTP et fournir une adresse e-mail à partir de laquelle la notification d'alerte sera envoyée. Si vous souhaitez utiliser des traps SNMP, vous pouvez sélectionner cette option et fournir les informations nécessaires.

2. "Activer l'authentification à distance".

   Si vous souhaitez que les utilisateurs LDAP ou Active Directory distants puissent accéder à l'instance Unified Manager et recevoir des notifications d'alerte, vous devez activer l'authentification à distance.

3. "Ajouter des serveurs d'authentification".

   Vous pouvez ajouter des serveurs d'authentification afin que les utilisateurs distants du serveur d'authentification puissent accéder à Unified Manager.

4. "Ajouter des utilisateurs".

   Vous pouvez ajouter différents types d'utilisateurs locaux ou distants et leur attribuer des rôles spécifiques. Lorsque vous créez une alerte, vous désignez un utilisateur pour recevoir les notifications d'alerte.

5. "Ajouter des alertes".

   Une fois que vous avez ajouté l'adresse e-mail pour l'envoi des notifications, ajouté les utilisateurs qui recevront les notifications, configuré vos paramètres réseau et configuré les options SMTP et SNMP nécessaires à votre environnement, vous pouvez alors attribuer des alertes.

Configurez les paramètres de notification d'événements dans Active IQ Unified Manager

Vous pouvez configurer Unified Manager pour qu'il envoie des notifications d'alerte

lorsqu'un événement est généré ou attribué à un utilisateur. Vous pouvez configurer le serveur SMTP utilisé pour l'envoi des alertes et définir différents mécanismes de notification : par exemple, les notifications d'alerte peuvent être envoyées par e-mail ou par traps SNMP.

Avant de commencer

Vous devez disposer des informations suivantes :

- Adresse électronique à partir de laquelle la notification d'alerte est envoyée

  L'adresse électronique apparaît dans le champ "From" des notifications d'alerte envoyées. Si l'e-mail ne peut pas être distribué pour une raison quelconque, cette adresse électronique est également utilisée comme destinataire des messages non distribuables.

- nom de l'hôte du serveur SMTP, ainsi que le nom d'utilisateur et le mot de passe permettant d'accéder au serveur
- Nom d'hôte ou adresse IP de l'hôte de destination du trap qui recevra le trap SNMP, ainsi que la version SNMP, le port de trap sortant, la communauté et les autres valeurs de configuration SNMP requises

  Pour spécifier plusieurs destinations de trap, séparez chaque hôte par une virgule. Dans ce cas, tous les autres paramètres SNMP, tels que la version et le port de trap sortant, doivent être identiques pour tous les hôtes de la liste.

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Notifications**.
2. Sur la page Notifications, configurez les paramètres appropriés.

   Remarques :

   - Si l'adresse d'expéditeur est préremplie avec l'adresse « ActiveIQUnifiedManager@localhost.com », vous devez la modifier par une adresse électronique valide afin de garantir la bonne réception de toutes les notifications par e-mail.
   - Si le nom de l'hôte du serveur SMTP ne peut pas être résolu, vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) du serveur SMTP au lieu du nom de l'hôte.
3. Cliquez sur **Enregistrer**.
4. Si vous avez sélectionné l'option **Utiliser STARTTLS** ou **Utiliser SSL**, une page de certificat s'affiche après avoir cliqué sur le bouton **Enregistrer**. Vérifiez les détails du certificat et acceptez-le pour enregistrer les paramètres de notification.

   Vous pouvez cliquer sur le bouton **Afficher les détails du certificat** pour afficher les détails du certificat. Si le certificat actuel a expiré, décochez la case **Utiliser STARTTLS** ou **Utiliser SSL**, enregistrez les paramètres de notification, puis cochez à nouveau la case **Utiliser STARTTLS** ou **Utiliser SSL** pour afficher un nouveau certificat.

Activer l'authentification à distance dans Active IQ Unified Manager

Vous pouvez activer l'authentification à distance pour que le serveur Unified Manager

puisse communiquer avec vos serveurs d'authentification. Les utilisateurs du serveur d'authentification pourront alors accéder à l'interface graphique d'Unified Manager pour gérer les objets de stockage et les données.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

> Le serveur Unified Manager doit être connecté directement au serveur d'authentification. Vous devez désactiver tous les clients LDAP locaux tels que SSSD (System Security Services Daemon) ou NSLCD (Name Service LDAP Caching Daemon).

Vous pouvez activer l'authentification à distance via Open LDAP ou Active Directory. Si l'authentification à distance est désactivée, les utilisateurs distants ne pourront pas accéder à Unified Manager.

L'authentification à distance est prise en charge via LDAP et LDAPS (LDAP sécurisé). Unified Manager utilise le port 389 par défaut pour les communications non sécurisées et le port 636 par défaut pour les communications sécurisées.

> Le certificat utilisé pour authentifier les utilisateurs doit être conforme au format X.509.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Cochez la case **Activer l'authentification à distance…**.
3. Dans le champ Service d'authentification, sélectionnez le type de service et configurez le service d'authentification.

Pour le type d'authentification…	Veuillez saisir les informations suivantes…
Active Directory	• Nom de l'administrateur du serveur d'authentification dans l'un des formats suivants : ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (en utilisant la notation LDAP appropriée) • Mot de passe administrateur • Nom unique de base (en utilisant la notation LDAP appropriée)
Open LDAP	• Nom unique de liaison (dans la notation LDAP appropriée) • Mot de passe de liaison • nom unique de base

Si l'authentification d'un utilisateur Active Directory prend beaucoup de temps ou expire, il est probable que le serveur d'authentification mette du temps à répondre. La désactivation de la prise en charge des groupes imbriqués dans Unified Manager peut réduire le temps d'authentification.

Si vous sélectionnez l'option Utiliser une connexion sécurisée pour le serveur d'authentification, Unified Manager communique avec le serveur d'authentification à l'aide du protocole SSL (Secure Sockets Layer).

4. **Facultatif:** Ajoutez des serveurs d'authentification et testez l'authentification.
5. Cliquez sur **Enregistrer**.

Désactivez les groupes imbriqués de l'authentification à distance dans Active IQ Unified Manager

Si l'authentification à distance est activée, vous pouvez désactiver l'authentification par groupes imbriqués afin que seuls les utilisateurs individuels, et non les membres d'un groupe, puissent s'authentifier à distance auprès d'Unified Manager. Vous pouvez désactiver les groupes imbriqués pour améliorer le temps de réponse de l'authentification Active Directory.

Avant de commencer

- Vous devez posséder le rôle d'administrateur d'application.
- La désactivation des groupes imbriqués n'est applicable que lors de l'utilisation d'Active Directory.

La désactivation de la prise en charge des groupes imbriqués dans Unified Manager peut réduire le temps d'authentification. Si cette prise en charge est désactivée et qu'un groupe distant est ajouté à Unified Manager, chaque utilisateur doit être membre du groupe distant pour s'authentifier auprès d'Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Cochez la case **Désactiver la recherche de groupes imbriqués**.
3. Cliquez sur **Enregistrer**.

Configurez les services d'authentification dans Active IQ Unified Manager

Les services d'authentification permettent d'authentifier les utilisateurs ou les groupes distants sur un serveur d'authentification avant de leur donner accès à Unified Manager. Vous pouvez authentifier les utilisateurs à l'aide de services d'authentification prédéfinis (tels qu'Active Directory ou OpenLDAP) ou en configurant votre propre mécanisme d'authentification.

Avant de commencer

- Vous devez avoir activé l'authentification à distance.
- Vous devez posséder le rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Sélectionnez l'un des services d'authentification suivants :

Si vous sélectionnez…	Ensuite, faites ceci…
Active Directory	a. Saisissez le nom d'administrateur et le mot de passe. b. Spécifiez le nom unique de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom unique est **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Saisissez le nom unique et le mot de passe de liaison. b. Spécifiez le nom unique de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom unique est **cn=ou,dc=domain,dc=com**.
Autres	a. Saisissez le nom unique et le mot de passe de liaison. b. Spécifiez le nom unique de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom unique est **cn=ou,dc=domain,dc=com**. c. Spécifiez la version du protocole LDAP prise en charge par le serveur d'authentification. d. Saisissez le nom d'utilisateur, l'appartenance au groupe, le groupe d'utilisateurs et les attributs du membre.

Si vous souhaitez modifier le service d'authentification, vous devez supprimer tous les serveurs d'authentification existants, puis ajouter de nouveaux serveurs d'authentification.

3. Cliquez sur **Enregistrer**.

Ajouter des serveurs d'authentification à Active IQ Unified Manager

Vous pouvez ajouter des serveurs d'authentification et activer l'authentification à distance sur le serveur de gestion afin que les utilisateurs distants au sein du serveur d'authentification puissent accéder à Unified Manager.

Avant de commencer

- Les informations suivantes doivent être disponibles :
  - Nom de l'hôte ou adresse IP du serveur d'authentification

    - Numéro de port du serveur d'authentification
- Vous devez avoir activé l'authentification à distance et configuré votre service d'authentification afin que le serveur de gestion puisse authentifier les utilisateurs ou les groupes distants sur le serveur d'authentification.
- Vous devez posséder le rôle d'administrateur d'application.

Si le serveur d'authentification que vous ajoutez fait partie d'une paire haute disponibilité (utilisant la même base de données), vous pouvez également ajouter le serveur d'authentification partenaire. Cela permet au serveur de gestion de communiquer avec le partenaire lorsqu'un des serveurs d'authentification est injoignable.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Activez ou désactivez l'option **Utiliser une connexion sécurisée** :

Si vous voulez…	Ensuite, faites ceci…
Activez-le	a. Sélectionnez l'option **Utiliser une connexion sécurisée**. b. Dans la section Serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue Ajouter un serveur d'authentification, entrez le nom d'authentification ou l'adresse IP (IPv4 ou IPv6) du serveur. d. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Afficher le certificat. e. Dans la boîte de dialogue Afficher le certificat, vérifiez les informations du certificat, puis cliquez sur **Fermer**. f. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Oui**. Lorsque vous activez l'option **Utiliser l'authentification par connexion sécurisée**, Unified Manager communique avec le serveur d'authentification et affiche le certificat. Unified Manager utilise le port 636 par défaut pour les communications sécurisées et le port 389 pour les communications non sécurisées.

Si vous voulez…	Ensuite, faites ceci…
Désactivez-le	a. Décochez l'option **Utiliser une connexion sécurisée**. b. Dans la section Serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue Ajouter un serveur d'authentification, spécifiez soit le nom de l'hôte, soit l'adresse IP (IPv4 ou IPv6) du serveur, ainsi que les informations sur le port. d. Cliquez sur **Add**.

Le serveur d'authentification que vous avez ajouté s'affiche dans la zone Serveurs.

3. Effectuez un test d'authentification pour confirmer que vous pouvez authentifier les utilisateurs dans le serveur d'authentification que vous avez ajouté.

Testez la configuration des serveurs d'authentification dans Active IQ Unified Manager

Vous pouvez valider la configuration de vos serveurs d'authentification pour vous assurer que le serveur de gestion peut communiquer avec eux. Pour ce faire, recherchez un utilisateur ou un groupe distant sur vos serveurs d'authentification et authentifiez-le à l'aide des paramètres configurés.

Avant de commencer

- Vous devez avoir activé l'authentification à distance et configuré votre service d'authentification afin que le serveur Unified Manager puisse authentifier l'utilisateur ou le groupe distant.
- Vous devez avoir ajouté vos serveurs d'authentification afin que le serveur de gestion puisse rechercher l'utilisateur distant ou le groupe distant sur ces serveurs et les authentifier.
- Vous devez posséder le rôle d'administrateur d'application.

Si le service d'authentification est configuré sur Active Directory et que vous validez l'authentification d'utilisateurs distants appartenant au groupe principal du serveur d'authentification, les informations relatives au groupe principal ne sont pas affichées dans les résultats d'authentification.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Cliquez sur **Test Authentication**.
3. Dans la boîte de dialogue Test User, spécifiez le nom d'utilisateur et le mot de passe de l'utilisateur distant ou le nom du groupe distant, puis cliquez sur **Test**.

   Si vous authentifiez un groupe distant, vous ne devez pas saisir le mot de passe.

Ajouter des alertes dans Active IQ Unified Manager

Vous pouvez configurer des alertes pour être notifié lorsqu'un événement particulier est généré. Vous pouvez configurer des alertes pour une ressource unique, pour un groupe

de ressources ou pour des événements d'un type de gravité particulier. Vous pouvez définir la fréquence à laquelle vous souhaitez être notifié et associer un script à l'alerte.

Avant de commencer

- Vous devez avoir configuré les paramètres de notification, tels que l'adresse e-mail de l'utilisateur, le serveur SMTP et l'hôte de trap SNMP, pour permettre au serveur Active IQ Unified Manager d'utiliser ces paramètres afin d'envoyer des notifications aux utilisateurs lorsqu'un événement est généré.
- Vous devez connaître les ressources et les événements pour lesquels vous souhaitez déclencher l'alerte, ainsi que les noms d'utilisateur ou les adresses électroniques des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez qu'un script s'exécute en fonction de l'événement, vous devez l'avoir ajouté à Unified Manager via la page Scripts.
- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous pouvez créer une alerte directement depuis la page de détails de l'événement après avoir reçu un événement, en plus de la possibilité de créer une alerte depuis la page de configuration des alertes, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
2. Sur la page Configuration des alertes, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter une alerte, cliquez sur **Nom**, puis saisissez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources**, et sélectionnez les ressources à inclure dans l'alerte ou à exclure de l'alerte.

   Vous pouvez définir un filtre en saisissant une chaîne de caractères dans le champ « Le nom contient » afin de sélectionner un groupe de ressources. En fonction de la chaîne de caractères que vous spécifiez, la liste des ressources disponibles n'affiche que les ressources qui correspondent à la règle de filtrage. La chaîne de caractères que vous spécifiez est sensible à la casse.

   Si une ressource correspond à la fois aux règles d'inclusion et d'exclusion que vous avez spécifiées, la règle d'exclusion prévaut sur la règle d'inclusion, et aucune alerte n'est générée pour les événements liés à la ressource exclue.

5. Cliquez sur **Events**, puis sélectionnez les événements en fonction du nom de l'événement ou du type de gravité de l'événement pour lesquels vous souhaitez déclencher une alerte.

   

   Pour sélectionner plusieurs événements, maintenez la touche Ctrl enfoncée pendant que vous effectuez vos sélections.

6. Cliquez sur **Actions**, puis sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence des notifications, indiquez si un trap SNMP doit être envoyé au récepteur de traps, et attribuez un script à exécuter lorsqu'une alerte est générée.

   

   Si vous modifiez l'adresse e-mail spécifiée pour l'utilisateur et rouvrez l'alerte pour la modifier, le champ Nom apparaît vide, car l'adresse e-mail modifiée n'est plus associée à l'utilisateur précédemment sélectionné. De même, si vous modifiez l'adresse e-mail de l'utilisateur sélectionné depuis la page Users, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

   Vous pouvez également choisir d'informer les utilisateurs via des traps SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

Cet exemple montre comment créer une alte qui répond aux exigences suivantes :

- Nom de l'alerte : HealthTest
- Ressources : inclut tous les volumes dont le nom contient « `abc` » et exclut tous les volumes dont le nom contient « `xyz` »
- Événements : inclut tous les événements de santé critiques
- Actions : comprennent « sample@domain.com », un script « `Test` » et l'utilisateur doit être notifié toutes les 15 minutes

Dans la boîte de dialogue Ajouter une alerte, procédez comme suit :

Étapes

1. Cliquez sur **Nom** et saisissez **HealthTest** dans le champ **Nom de l'alerte**.
2. Cliquez sur **Ressources**, puis dans l'onglet Inclure, sélectionnez **Volumes** dans la liste déroulante.
   a. Saisissez **abc** dans le champ **Le nom contient** pour afficher les volumes dont le nom contient « `abc` ».
   b. Sélectionnez **<<All Volumes whose name contains 'abc'>>** dans la zone Ressources disponibles et déplacez-le vers la zone Ressources sélectionnées.
   c. Cliquez sur **Exclure**, puis saisissez **xyz** dans le champ **Le nom contient**, puis cliquez sur **Ajouter**.
3. Cliquez sur **Événements**, puis sélectionnez **Critique** dans le champ Gravité de l'événement.
4. Sélectionnez **Tous les événements critiques** dans la zone Événements correspondants, et déplacez-les vers la zone Événements sélectionnés.
5. Cliquez sur **Actions**, puis saisissez **sample@domain.com** dans le champ **Alert these users**.
6. Sélectionnez **Rappeler toutes les 15 minutes** pour notifier l'utilisateur toutes les 15 minutes.

   Vous pouvez configurer une alerte pour envoyer des notifications répétées aux destinataires pendant une période déterminée. Vous devez définir l'heure à partir de laquelle la notification d'événement est active pour cette alerte.

7. Dans le menu Sélectionner le script à exécuter, sélectionnez le script **Test**.
8. Cliquez sur **Enregistrer**.

Informations sur le copyright

Copyright © 2026 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.