



Configurez les outils ONTAP

ONTAP tools for VMware vSphere 10

NetApp

September 30, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-tools-vmware-vsphere-100/configure/ip_whitelisting.html on September 30, 2025. Always check docs.netapp.com for the latest.

Sommaire

Configurez les outils ONTAP	1
Gérer l'accès au réseau	1
Configurez les rôles et privilèges utilisateur	1
Exigences de mappage des agrégats du SVM	2
Créez manuellement un utilisateur et un rôle ONTAP	3
Liste des privilèges minimaux requis pour les utilisateurs du cluster dont le périmètre global n'est pas défini sur admin	3
Interface utilisateur du gestionnaire d'outils ONTAP	4
Ajoutez vCenter	5
Ajout du système back-end de stockage	6
Associez le système back-end de stockage à vCenter	6
Systèmes back-end de stockage intégrés (SVM ou Cluster) avec vCenter	7
Enregistrez VASA Provider dans vCenter	7
Créer un datastore vVols	8
Vérifier le SVM enregistré	11

Configurez les outils ONTAP

Gérer l'accès au réseau

Cette fonction vous permet de spécifier une adresse hôte ESXi spécifique qui sera autorisée pour l'opération de montage du datastore.

Lorsque vous avez plusieurs adresses IP pour les hôtes ESXi, toutes les adresses IP découvertes de l'hôte sont ajoutées à une règle d'export. Si vous ne souhaitez pas ajouter toutes les adresses IP à la règle d'export, indiquez un paramètre pour les adresses IP blanches dans une liste ou une plage séparées par des virgules ou CIDR, ou une combinaison des trois pour chaque vCenter.

Si le paramètre n'est pas fourni, export policy ajoute toutes les adresses IP découvertes lors de l'étape de pré-montage. Si le paramètre est fourni, les outils ONTAP n'ajoutent que ceux qui se trouvent dans les adresses IP ou la plage blanches. Si aucune des adresses IP d'un hôte n'appartient aux adresses IP blanches, le montage sur cet hôte échoue.

Par défaut, toutes les adresses IP de l'hôte sont ajoutées à la export policy.

Utilisez l'API suivante pour ajouter des adresses IP pour la liste blanche :

```
patch /api/v1/vcenters/{vcguid}/settings/ip-whitelist

{
  value: string
}

GET /api/v1/vcenters/{vcguid}/settings/ip-whitelist

{
  value: string
}
```

Configurez les rôles et privilèges utilisateur

Vous pouvez configurer de nouveaux rôles et privilèges utilisateur pour la gestion des systèmes back-end de stockage à l'aide du fichier JSON fourni avec les outils ONTAP et ONTAP System Manager.

Ce dont vous aurez besoin

- Vous devez avoir téléchargé le fichier privilèges ONTAP à partir des outils ONTAP à l'aide de https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip.



La création d'utilisateurs s'effectue au niveau du cluster ou des serveurs virtuels de stockage directs (SVM). Vous pouvez également créer des utilisateurs sans utiliser le fichier `user_roles.json` et, si c'est le cas, vous devez disposer d'un ensemble minimal de privilèges au niveau du SVM.

- Vous devez vous être connecté avec des privilèges d'administrateur pour le back-end de stockage.

Étapes

1. Extrayez le téléchargé `https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip` fichier.
2. Accédez à ONTAP System Manager. Pour accéder à ONTAP System Manager, utilisez l'IP de gestion du cluster du cluster.
3. Se connecter en tant qu'utilisateur du cluster ou du SVM.
4. Sélectionnez **CLUSTER > Paramètres > volet utilisateurs et rôles**.
5. Sélectionnez **Ajouter** sous utilisateurs.
6. Dans la boîte de dialogue **Ajouter un utilisateur**, sélectionnez **produits de virtualisation**.
7. Sélectionnez **Parcourir** pour sélectionner et télécharger le fichier JSON de privilèges ONTAP.

Le champ **PRODUIT** est rempli automatiquement.

8. Sélectionnez la fonctionnalité requise dans le menu déroulant **FONCTIONNALITÉS DU PRODUIT**.

Le champ **ROLE** est renseigné automatiquement en fonction de la capacité du produit sélectionnée.

9. Saisissez le nom d'utilisateur et le mot de passe requis.
10. Sélectionnez les privilèges (découverte, création de stockage, modification de stockage, destruction de stockage, rôle NAS/SAN) requis pour l'utilisateur, puis cliquez sur **Ajouter**.

Le nouveau rôle et l'utilisateur sont ajoutés et vous pouvez voir les privilèges détaillés sous le rôle que vous avez configuré.



L'opération de désinstallation ne supprime pas les rôles d'outil ONTAP, mais supprime les noms localisés des privilèges spécifiques à l'outil ONTAP et ajoute le préfixe `xxx missing privilege` pour eux. Lorsque vous réinstallez les outils ONTAP ou que vous effectuez une mise à niveau vers une version plus récente des outils ONTAP, tous les rôles d'outils ONTAP standard et les privilèges spécifiques aux outils ONTAP sont restaurés.

Exigences de mappage des agrégats du SVM

Pour utiliser les identifiants de SVM directs pour le provisionnement des datastores, les outils ONTAP internes créent des volumes sur l'agrégat spécifié dans l'API POST DES datastores. La ONTAP ne permet pas la création de volumes sur des agrégats non mappés sur un SVM utilisant des informations d'identification SVM directes. Pour résoudre ce problème, vous devez mapper les SVM avec les agrégats à l'aide de l'API REST ou de l'interface de ligne de commandes comme décrit dans cette section.

API REST :

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

Interface de ligne de commande ONTAP :

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver      Aggregate      State      Size Type      SnapLock
Type-----
-----svm_test      sti115_vsim_ucs630f_aggr1
online      10.11GB vmdisk  non-snaplock
```

Créez manuellement un utilisateur et un rôle ONTAP

Suivez les instructions de cette section pour créer l'utilisateur et les rôles manuellement sans utiliser le fichier JSON.

1. Accédez à ONTAP System Manager. Pour accéder à ONTAP System Manager, utilisez l'IP de gestion du cluster du cluster.
2. Se connecter en tant qu'utilisateur du cluster ou du SVM.
3. Sélectionnez **CLUSTER > Paramètres > volet utilisateurs et rôles**.
4. Créer des rôles :
 - a. Sélectionnez **Ajouter** dans la table **rôles**.
 - b. Entrez les détails **NOM DE RÔLE** et **attributs de rôle**.

Ajoutez le **CHEMIN REST API PATH** et l'accès correspondant dans le menu déroulant.

- c. Ajoutez toutes les API nécessaires et enregistrez les modifications.
5. Créer des utilisateurs :
 - a. Sélectionnez **Ajouter** dans la table **utilisateurs**.
 - b. Dans la boîte de dialogue **Ajouter un utilisateur**, sélectionnez **System Manager**.
 - c. Entrez le **NOM D'UTILISATEUR**.
 - d. Sélectionnez **ROLE** parmi les options créées à l'étape **Create Roles** ci-dessus.
 - e. Entrez les applications à laquelle vous souhaitez accorder l'accès et la méthode d'authentification. ONTAPI et HTTP sont l'application requise et le type d'authentification est **Password**.
 - f. Définissez le **Mot de passe pour l'utilisateur** et le **Enregistrer** pour l'utilisateur.

Liste des privilèges minimaux requis pour les utilisateurs du cluster dont le périmètre global n'est pas défini sur admin

Les privilèges minimaux requis pour l'utilisateur de cluster avec périmètre global non-admin créé sans utiliser le fichier JSON d'utilisateurs sont répertoriés dans cette section. Si un cluster est ajouté au périmètre local, il est recommandé d'utiliser le fichier JSON pour créer les utilisateurs, car les outils ONTAP requièrent bien plus que les privilèges de lecture pour le provisionnement sur ONTAP.

À l'aide d'API :

API	NIVEAU D'ACCÈS	UTILISÉ POUR
/api/cluster	Lecture seule	Découverte de la configuration du cluster
/api/cluster/licences/licences	Lecture seule	Contrôle de licence pour les licences spécifiques au protocole
/api/cluster/nœuds	Lecture seule	Découverte du type de plate-forme
/api/stockage/agrégats	Lecture seule	Vérification de l'espace de l'agrégat lors du provisionnement des datastores/volumes
/api/stockage/cluster	Lecture seule	Pour obtenir les données d'espace et d'efficacité au niveau du cluster
/api/stockage/disques	Lecture seule	Pour obtenir les disques associés dans un agrégat
/api/stockage/qos/politiques	Lire/Créer/Modifier	Gestion de la QoS et de la stratégie des machines virtuelles
/api/svm/svm	Lecture seule	Pour obtenir la configuration du SVM en cas d'ajout local du Cluster.
/api/network/ip/interfaces	Lecture seule	Add Storage back-end : pour identifier le périmètre de la LIF de gestion, il s'agit de Cluster/SVM
/api	Lecture seule	L'utilisateur du cluster doit disposer de ce privilège pour obtenir l'état du back-end de stockage correct. Sinon, l'interface utilisateur du gestionnaire des outils ONTAP affiche l'état du back-end de stockage « inconnu ».

Interface utilisateur du gestionnaire d'outils ONTAP

Les outils ONTAP pour VMware vSphere 10.0 sont un système mutualisé qui gère plusieurs vCenter. Un administrateur a besoin de davantage de contrôle sur les vCenter gérés et les systèmes back-end de stockage intégrés.

ONTAP Tools Manager offre davantage de contrôle et d'alimentation à l'administrateur des outils ONTAP, ce qui facilite la gestion globale de l'appliance, des locataires et des systèmes back-end de stockage.

Les outils ONTAP effectuent les opérations suivantes :

- Gestion vCenter : enregistrez et désenregistrez des vCenters vers les outils ONTAP
- Gestion du stockage back-end : enregistrez et désenregistrez les clusters de stockage ONTAP dans les outils ONTAP et mappez-les vers des vCenters intégrés à l'échelle mondiale.

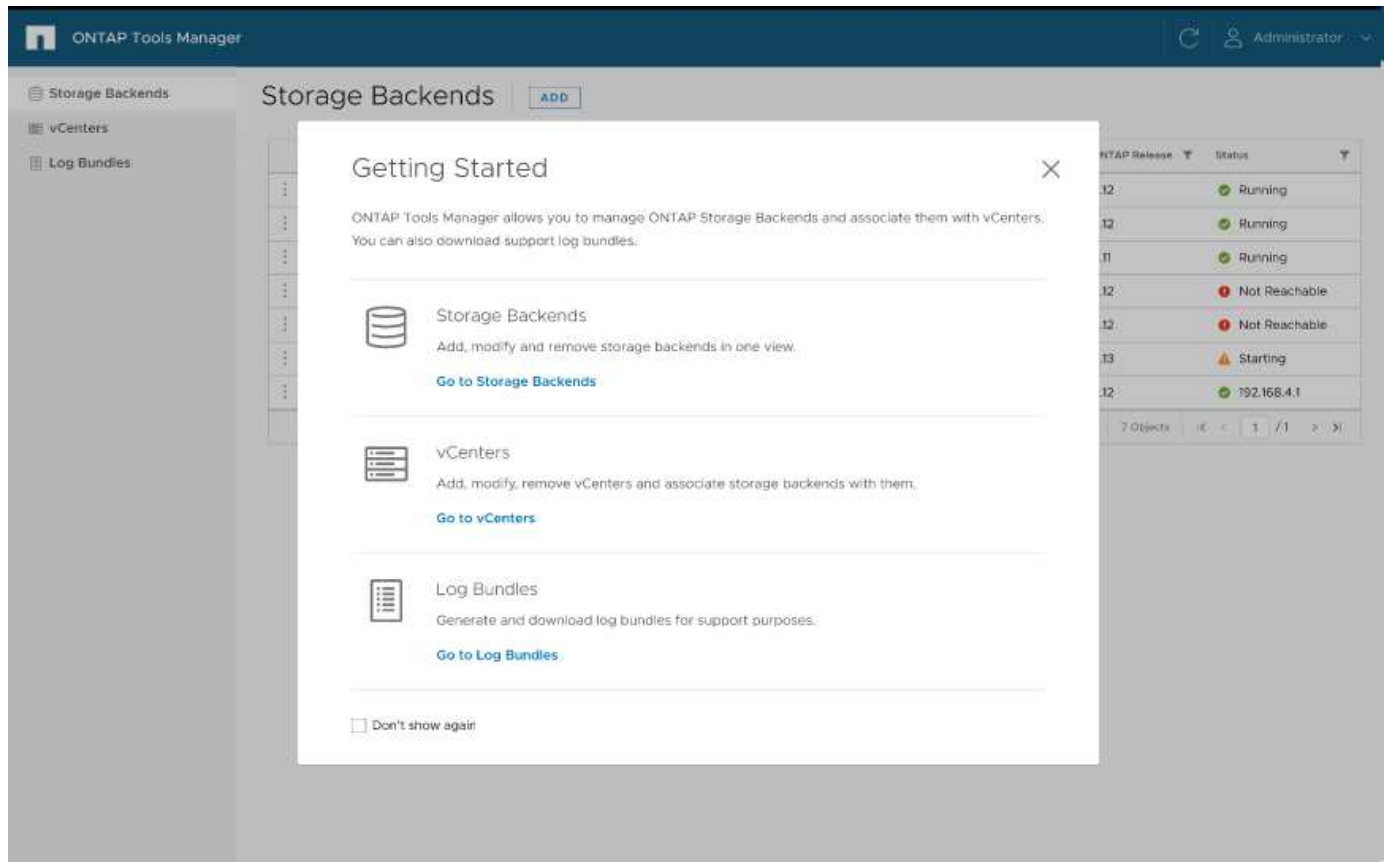
Le système back-end est global lorsqu'il est ajouté à partir du gestionnaire d'outils ONTAP ou des API

communes, et il est local lorsqu'il est ajouté à partir des API vCenter. Exemple : pour une configuration mutualisée, vous pouvez ajouter le système back-end de stockage (cluster) globalement et un SVM localement pour utiliser les identifiants directs du SVM.

- Téléchargements de lots de journaux

Pour accéder à l'interface utilisateur des outils ONTAP, lancez

<https://loadBalanceIP:8443/virtualization/ui/> Depuis le navigateur et connectez-vous avec les informations d'identification de l'administrateur des outils ONTAP fournies lors du déploiement.



Vous pouvez sélectionner l'option **ne plus afficher** pour ne pas voir cette fenêtre contextuelle lorsque vous vous connectez à nouveau à partir du même navigateur.

Ajoutez vCenter

Les vCenter sont des plateformes de gestion centrales qui vous permettent de contrôler les hôtes, les machines virtuelles (VM) et les systèmes back-end de stockage.

À propos de cette tâche

Vous pouvez ajouter et gérer plusieurs instances vCenter 10.0 à l'aide d'une seule instance d'outils ONTAP.

Étapes

1. Lancement <https://loadBalanceIP:8443/virtualization/ui/> À partir d'un navigateur avec les informations d'identification de l'administrateur des outils ONTAP fournies pendant le déploiement.
2. Sélectionnez vCenters dans la barre latérale

3. Sélectionnez **ADD** pour intégrer les vCenters avec l'adresse IP/le nom d'hôte vCenter, le nom d'utilisateur, le mot de passe et le port.

Voir "[Liste des privilèges minimaux requis pour les utilisateurs du cluster dont le périmètre global n'est pas défini sur admin](#)".

Ajout du système back-end de stockage

Les systèmes back-end de stockage sont des systèmes que les hôtes EXSi utilisent pour le stockage des données.

À propos de cette tâche

Cette tâche vous permet d'instruments d'instruments ONTAP.

Étapes

1. Lancement <https://loadBalanceIP:8443/virtualization/ui/> À partir d'un navigateur avec les informations d'identification de l'administrateur des outils ONTAP fournies pendant le déploiement.
2. Sélectionnez **systèmes back-end de stockage** dans la barre latérale.
3. Sélectionnez **Ajouter**.
4. Indiquez l'adresse IP du serveur ou le nom de domaine complet, le nom d'utilisateur et le mot de passe, puis sélectionnez **Ajouter**.



Seules les LIF de gestion IPV4 sont prises en charge.

Associez le système back-end de stockage à vCenter

La page de liste vCenter affiche le nombre de systèmes back-end de stockage associés. Chaque vCenter a la possibilité d'associer un système back-end de stockage

À propos de cette tâche

Cette tâche vous permet de créer un mappage entre le système back-end de stockage et vCenter intégré à l'échelle mondiale.

Étapes

1. Lancement <https://loadBalanceIP:8443/virtualization/ui/> À partir d'un navigateur avec les informations d'identification de l'administrateur des outils ONTAP fournies pendant le déploiement.
2. Sélectionnez vCenters dans la barre latérale.
3. Cliquez sur les points de suspension verticaux en regard du vCenter que vous souhaitez associer aux systèmes back-end de stockage.
4. Sélectionnez Storage backend dans la liste déroulante.
5. Sélectionnez l'option **associer le système back-end de stockage** pour associer vCenter au système back-end de stockage requis.

Voir "[Liste des privilèges minimaux requis pour les utilisateurs du cluster dont le périmètre global n'est pas](#)

défini sur admin".

Systèmes back-end de stockage intégrés (SVM ou Cluster) avec vCenter

Utilisez l'API suivante pour intégrer les systèmes back-end de stockage et mapper la SVM à vCenter localement. Voir "[Configurez les rôles et privilèges utilisateur](#)" Section concernant les privilèges utilisateur du SVM ONTAP.

```
POST /virtualization/api/v1/vcenters/<vcguid>/storage-backends

{
  "hostname_or_ip": "172.21.103.107",
  "username": "svm11",
  "password": "xxxxxx"
}
```



L'ID de la réponse de l'API ci-dessus est utilisé dans la découverte.

Vous devez transmettre x-auth pour l'API. Vous pouvez générer cette x-auth à partir de la nouvelle API ajoutée sous Auth dans swagger.

```
/virtualization/api/v1/auth/vcenter-login
```

Enregistrez VASA Provider dans vCenter

Vous pouvez enregistrer VASA Provide dans vCenter à l'aide d'un certificat auto-signé ou d'un certificat signé par une autorité de certification. Le certificat auto-signé est généré à l'aide de la poignée de main VMware CA.

À propos de cette tâche

Vous devez placer le certificat signé par l'autorité de certification dans vCenter lorsque vous utilisez la méthode de certificat signé par l'autorité de certification.

Étapes

1. Accédez au serveur vCenter.
2. Sélectionnez **configurer > fournisseurs de stockage**.
3. Cliquez sur l'icône **Ajouter**.
4. Entrez les informations de connexion du fournisseur de stockage :
 - a. Nom : tout nom convivial comme « ScaleoutVP »
 - b. URL : `https://<name>/virtualization/version.xml` - Le nom dans l'URL correspond à l'adresse IP virtuelle fournie lors du déploiement d'OVA pour le déploiement d'un seul vCenter (ou)

Nom de domaine pour les déploiements multi-vCenter. Ajoutez les certificats à l'URL. Les mêmes certificats sont publiés dans vCenter.

c. Informations d'identification : <nom d'utilisateur du fournisseur VASA>/< mot de passe du fournisseur VASA> fourni lors du déploiement d'OVA.

5. Une fois le fichier VASA enregistré, cliquez sur **OK**. Assurez-vous qu'il est répertorié sous fournisseur de stockage et que l'état est en ligne.

Si vous avez placé un certificat signé par l'autorité de certification dans vCenter, l'enregistrement VASA se poursuit avec le certificat signé par l'autorité de certification. Sinon, la liaison échoue et l'enregistrement est par défaut sur le certificat SSA.

6. Vous pouvez enregistrer plusieurs vCenters dans une seule instance vp scaleout. Répétez les étapes mentionnées ci-dessus pour enregistrer plusieurs vCenters.

Créer un datastore vVols

Vous pouvez créer un datastore vVols avec de nouveaux volumes ou avec des volumes existants. Vous pouvez également créer un datastore vVols en combinant des volumes existants et de nouveaux volumes.



Cette option permet de vérifier que les agrégats racine ne sont pas mappés sur un SVM.

Vous devez transmettre x-auth pour l'API. Vous pouvez générer cette x-auth à partir de la nouvelle API ajoutée sous Auth dans swagger.

```
/virtualization/api/v1/auth/vcenter-login
```

1. Créez un datastore vVols avec un nouveau volume. Get Aggregate ID, Storage_ID(SVM UUID) using ONTAP REST API.

```
POST /virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/datastores
```

Utilisez l'URI suivant pour vérifier l'état :

```
`\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?includeSubJobsAndTasks=true`
```

Corps de demande pour le datastore NFS

```
{
  "name":"nfsds1",
  "protocol":"nfs",
  "platform_type":"aff",
  "moref":"domain-c8",
  "volumes":[
    {
      "is_existing":false,
      "name":"vol_nfs_pvt",
      "size_in_mb":2048000,
      "space_efficiency":"thin",
      "aggregate":{
        "id":"d7078b3c-3827-4ac9-9273-0a32909455c2"
      },
      "qos":{
        "min_iops":200,
        "max_iops":5000
      }
    }
  ],
  "storage_backend":{
    "storage_id":"654c67bc-0f75-11ee-8a8c-00a09860a3ff"
  }
}
```

Corps de la demande pour le datastore iSCSI :

```
{
  "name" : "iscsi_custom",
  "protocol" : "iscsi",
  "platform_type": "aff",
  "moref" : "domain-c8",
  "volumes" : [
    {
      "is_existing" : false,
      "name" : "iscsi_custom",
      "size_in_mb" : 8034,
      "space_efficiency" : "thin",
      "aggregate" : {
        "id" : "54fe5dd4-e461-49c8-bb2d-6d62c5d75af2"
      }
    }
  ],
  "custom_igroup_name": "igroup1",
  "storage_backend": {
    "storage_id": "eb9d33ab-1960-11ee-9506-00a0985c6d9b"
  }
}
```

1. Créez un datastore vVols avec des volumes existants.

Obtenez Aggregate_ID et volume_ID à l'aide de l'API REST ONTAP.

```
POST /virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/datastores
```

Corps de la demande

```

{
  "name" : "nfsds2",
  "protocol" : "nfs",
  "platform_type": "aff",
  "moref" : "domain-c8",
  "volumes" : [
    {
      "is_existing": true,
      "id": "e632a632-1412-11ee-8a8c-00a09860a3ff"
    }
  ],
  "storage_backend": {
    "storage_id": "33a8b6b3-10cd-11ee-8a8c-
00a09860a3ff"
  }
}

```

Vérifier le SVM enregistré

Vérifier que le SVM intégré est répertorié sous VASA Provider dans l'interface utilisateur vCenter.

Étapes

1. Accédez à vCenter Server.
2. Connectez-vous avec les informations d'identification de l'administrateur.
3. Sélectionnez **fournisseurs de stockage**.
4. Sélectionnez **configurer**.
5. Sous fournisseur de stockage/systèmes back-end, vérifiez que le SVM intégré est correctement répertorié.

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.