



# Surveiller les ports réseau

## ONTAP 9

NetApp  
April 24, 2024

This PDF was generated from [https://docs.netapp.com/fr-fr/ontap/networking/monitor\\_the\\_health\\_of\\_network\\_ports.html](https://docs.netapp.com/fr-fr/ontap/networking/monitor_the_health_of_network_ports.html) on April 24, 2024. Always check docs.netapp.com for the latest.

# Sommaire

- Surveiller les ports réseau ..... 1
  - Contrôle de l'état de santé des ports réseau ..... 1
  - Surveiller l'accessibilité des ports réseau (ONTAP 9.8 et versions ultérieures)..... 2
  - Présentation des ports ONTAP ..... 5
  - Ports internes ONTAP ..... 6

# Surveiller les ports réseau

## Contrôle de l'état de santé des ports réseau

La gestion ONTAP des ports réseau inclut un contrôle automatique de l'état de santé et un ensemble de moniteurs pour vous aider à identifier les ports réseau qui ne conviennent pas à l'hébergement des LIF.

### Description de la tâche

Si un contrôle de l'état détermine qu'un port réseau est défectueux, il avertit les administrateurs via un message EMS ou indique que le port est dégradé. ONTAP évite d'héberger les LIF sur des ports réseau dégradés si d'autres cibles de basculement sont présentes pour cette LIF. Un port peut se dégrader en raison d'un événement de panne logicielle, tel que le fait de sauter des liaisons (rebondissement rapide des liaisons entre le haut et le bas) ou le partitionnement réseau :

- Les ports réseaux du cluster IPspace sont marqués comme détériorées lorsqu'ils connaissent une liaison flipant ou une perte de la capacité de couche 2 (L2) à d'autres ports réseau du domaine de diffusion.
- Les ports réseau des IPspaces sans cluster sont marqués comme dégradés lorsqu'ils réalisent des liaisons téléphoniques.

Vous devez connaître les comportements suivants d'un port dégradé :

- Un port dégradé ne peut pas être inclus dans un VLAN ou dans un groupe d'interfaces.

Si un port membre d'un groupe d'interface est marqué comme dégradé, mais que le groupe d'interfaces est toujours marqué comme défectueux, les LIF peuvent être hébergées sur ce groupe d'interface.

- Les LIF sont automatiquement migrées depuis les ports dégradés vers les ports sains.
- Lors d'un événement de basculement, un port dégradé n'est pas considéré comme la cible de basculement. Si aucun port défectueux n'est disponible, les ports LIF hôtes sont dégradés conformément à la politique de basculement normale.
- Vous ne pouvez ni créer, ni migrer, ni restaurer une LIF vers un port dégradé.

Vous pouvez modifier le `ignore-health-status` définition du port réseau sur `true`. Vous pouvez ensuite héberger une LIF sur les ports sains.

### Étapes

1. Connectez-vous au mode de privilège avancé :

```
set -privilege advanced
```

2. Vérifiez les moniteurs d'intégrité qui sont activés pour surveiller l'intégrité des ports du réseau :

```
network options port-health-monitor show
```

L'état de santé d'un port est déterminé par la valeur des moniteurs d'intégrité.

Les contrôles d'état suivants sont disponibles et activés par défaut dans ONTAP :

- Surveillance de l'état du cerclage : surveille le cerclage de liaison

Si la liaison d'un port est plus d'une fois dans cinq minutes, ce port est marqué comme dégradé.

- Moniteur d'intégrité de la capacité d'accessibilité L2 : surveille si tous les ports configurés dans le même domaine de diffusion ont une capacité d'accessibilité L2 entre eux

Ce contrôle de l'état signale les problèmes de réabilité L2 dans tous les IPspaces, mais il marque uniquement les ports du cluster IPspace comme étant dégradés.

- Contrôle CRC : surveille les statistiques CRC sur les ports

Ce contrôle de l'état ne marque pas un port comme dégradé mais génère un message EMS lorsqu'un taux de défaillance CRC très élevé est observé.

3. Activez ou désactivez tous les moniteurs de santé pour un IPspace comme vous le souhaitez en utilisant le `network options port-health-monitor modify` commande.

4. Pour afficher l'état de santé détaillé d'un port :

```
network port show -health
```

Le résultat de la commande affiche le statut d'état de santé du port, ignore `health status` paramètre et liste des raisons pour lesquelles le port est marqué comme dégradé.

Un état de santé du port peut être `healthy` ou `degraded`.

Si le `ignore health status` le paramètre est `true`, il indique que le statut de l'état de santé du port a été modifié de `degraded` à `healthy` par l'administrateur.

Si le `ignore health status` le paramètre est `false`, l'état d'intégrité du port est déterminé automatiquement par le système.

## Surveiller l'accessibilité des ports réseau (ONTAP 9.8 et versions ultérieures)

La surveillance de l'accessibilité est intégrée à ONTAP 9.8 et versions ultérieures. Utilisez cette surveillance pour identifier si la topologie de réseau physique ne correspond pas à la configuration ONTAP. Dans certains cas, ONTAP peut réparer l'accessibilité des ports. Dans d'autres cas, des étapes supplémentaires sont nécessaires.

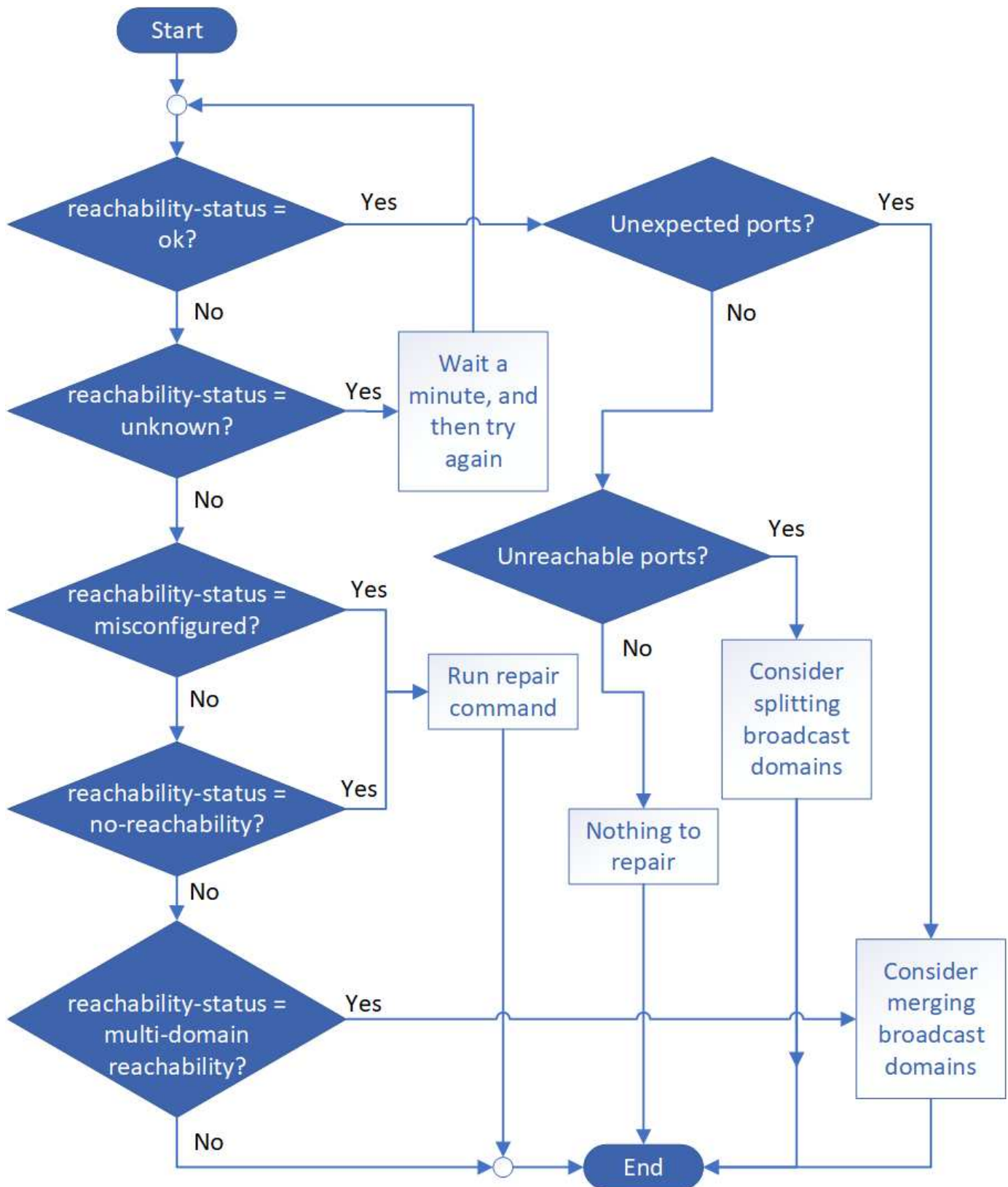
### Description de la tâche

Utilisez ces commandes pour vérifier, diagnostiquer et réparer les erreurs de configuration du réseau qui ne correspondent pas au câblage physique ou à la configuration du commutateur réseau.

### Étape

1. Afficher la capacité de port :

2. Utilisez l'arbre de décision et le tableau suivants pour déterminer l'étape suivante, le cas échéant.



État-accessibilité	Description
ok	<p>Le port a une capacité de réachbilité de couche 2 à son domaine de diffusion attribué. Si l'état de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inattendus », envisagez de fusionner un ou plusieurs domaines de diffusion. Pour plus d'informations, reportez-vous à la <i>Unexpected ports row</i> suivante.</p> <p>Si le statut de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inaccessibles », envisagez de diviser un ou plusieurs domaines de diffusion. Pour plus d'informations, reportez-vous à la ligne <i>ports inaccessibles</i> suivante.</p> <p>Si l'état de la capacité de reprise est « ok » et qu'il n'y a pas de ports inattendus ou inaccessibles, votre configuration est correcte.</p>
Ports inattendus	<p>Le port a une capacité de réachbilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast.</p> <p>Examinez la connectivité physique et la configuration du commutateur pour déterminer si elle est incorrecte ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion.</p> <p>Pour plus d'informations, voir <a href="#">"Fusionner les domaines de diffusion"</a>.</p>
Ports inaccessibles	<p>Si un seul domaine de diffusion a été partitionné en deux ensembles de capacité d'accès différents, vous pouvez fractionner un domaine de diffusion pour synchroniser la configuration ONTAP avec la topologie de réseau physique.</p> <p>En général, la liste des ports inaccessibles définit l'ensemble des ports qui doivent être divisés en un autre domaine de diffusion après avoir vérifié que la configuration physique et du commutateur est exacte.</p> <p>Pour plus d'informations, voir <a href="#">"Séparer les domaines de diffusion"</a>.</p>
mauvaise configuration de la capacité de réachbilité	<p>Le port n'a pas la capacité de reachcapacité de couche 2 à son domaine de diffusion affecté ; cependant, le port a une capacité de réachcapacité de couche 2 à un domaine de diffusion différent.</p> <p>Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port au broadcast domain auquel il a la capacité de reachcapacité :</p> <pre>network port reachability repair -node -port</pre> <p>Pour plus d'informations, voir <a href="#">"Réparation de l'accessibilité de l'orifice"</a>.</p>

sans trabilité	<p>Le port n'a pas la possibilité de reachcapacité de couche 2 à un domaine de diffusion existant.</p> <p>Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port à un nouveau domaine de diffusion créé automatiquement dans l'IPspace par défaut :</p> <pre>network port reachability repair -node -port</pre> <p>Pour plus d'informations, voir "<a href="#">Réparation de l'accessibilité de l'orifice</a>".</p>
accessibilité multi-domaines	<p>Le port a une capacité de réachabilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast.</p> <p>Examinez la connectivité physique et la configuration du commutateur pour déterminer si elle est incorrecte ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion.</p> <p>Pour plus d'informations, voir "<a href="#">Fusionner les domaines de diffusion</a>" ou "<a href="#">Réparation de l'accessibilité de l'orifice</a>".</p>
inconnu	<p>Si l'état de la capacité d'accessibilité est « inconnu », attendez quelques minutes et essayez à nouveau la commande.</p>

Une fois que vous avez réparé un port, vous devez vérifier et résoudre les LIFs et les VLAN déplacés. Si le port faisait partie d'un groupe d'interfaces, vous devez également connaître ce qui s'est passé pour ce groupe. Pour plus d'informations, voir "[Réparation de l'accessibilité de l'orifice](#)".

## Présentation des ports ONTAP

Un certain nombre de ports connus sont réservés pour les communications ONTAP avec des services spécifiques. Des conflits de ports se produisent si une valeur de port dans votre environnement de réseau de stockage est identique à celle du port ONTAP.

Le tableau suivant répertorie les ports TCP et UDP utilisés par ONTAP.

Service	Port/Protocole	Description
ssh	22/TCP	Connexion au shell sécurisée
telnet	23/TCP	Connexion à distance
DNS	53/TCP	DNS avec équilibrage de charge
http	80/TCP	Protocole de transfert de texte
rpcbind	111/TCP	Appel de procédure à distance
rpcbind	111/UDP	Appel de procédure à distance
ntp	123/UDP	Protocole de temps réseau
msrpc	135/UDP	MSRPC

netbios-ssn	139/TCP	Session de service NetBIOS
snmp	161/UDP	Protocole de gestion de réseau simple
https	443/TCP	HTTP sur TLS
microsoft- ds	445/TCP	Microsoft- ds
montage	635/TCP	Montage NFS
montage	635/UDP	Montage NFS
nommé	953/UDP	Nom démon
nfs	2049/UDP	Démon du serveur NFS
nfs	2049/TCP	Démon du serveur NFS
nrv	2050/TCP	Protocole NetApp Remote Volume
iscsi	3260/TCP	Port cible iSCSI
verrouillage	4045/TCP	Démon de verrouillage NFS
verrouillage	4045/UDP	Démon de verrouillage NFS
NSM	4046/TCP	Moniteur d'état du réseau
NSM	4046/UDP	Moniteur d'état du réseau
rquotad	4049/UDP	Protocole NFS rquotad
krb524	4444/UDP	Kerberos 524
mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Port HTTPS : protocole binaire d'écoute
https	8443/TCP	Interface graphique 7MTT via https
ndmp	10000/TCP	Protocole de gestion des données réseau
Peering de clusters	11104/TCP	Peering de cluster, bidirectionnel
Peering de cluster, bidirectionnel	11105/TCP	Peering de clusters
NDMP	18600 - 18699/TCP	NDMP
NDMP	30000/TCP	accepte les connexions de contrôle sur les prises femelles sécurisées
port témoin cifs	40001/TCP	port témoin cifs
tls	50000/TCP	Sécurité de la couche de transport
iscsi	65200/TCP	Port iSCSI

## Ports internes ONTAP

Le tableau suivant répertorie les ports TCP et UDP utilisés en interne par ONTAP. Ces ports permettent d'établir une communication LIF intracluster :



Port/Protocole	Description
514	Syslog
900	RPC NetApp Cluster
902	RPC NetApp Cluster
904	RPC NetApp Cluster
905	RPC NetApp Cluster
910	RPC NetApp Cluster
911	RPC NetApp Cluster
913	RPC NetApp Cluster
914	RPC NetApp Cluster
915	RPC NetApp Cluster
918	RPC NetApp Cluster
920	RPC NetApp Cluster
921	RPC NetApp Cluster
924	RPC NetApp Cluster
925	RPC NetApp Cluster
927	RPC NetApp Cluster
928	RPC NetApp Cluster
929	RPC NetApp Cluster
931	RPC NetApp Cluster
932	RPC NetApp Cluster
933	RPC NetApp Cluster
934	RPC NetApp Cluster
935	RPC NetApp Cluster
936	RPC NetApp Cluster
937	RPC NetApp Cluster
939	RPC NetApp Cluster
940	RPC NetApp Cluster
951	RPC NetApp Cluster
954	RPC NetApp Cluster
955	RPC NetApp Cluster
956	RPC NetApp Cluster
958	RPC NetApp Cluster
961	RPC NetApp Cluster

963	RPC NetApp Cluster
964	RPC NetApp Cluster
966	RPC NetApp Cluster
967	RPC NetApp Cluster
982	RPC NetApp Cluster
983	RPC NetApp Cluster
5125	Port de contrôle secondaire pour le disque
5133	Port de contrôle secondaire pour le disque
5144	Port de contrôle secondaire pour le disque
65502	Étendue des nœuds SSH
65503	Partage de LIF
7810	RPC NetApp Cluster
7811	RPC NetApp Cluster
7812	RPC NetApp Cluster
7813	RPC NetApp Cluster
7814	RPC NetApp Cluster
7815	RPC NetApp Cluster
7816	RPC NetApp Cluster
7817	RPC NetApp Cluster
7818	RPC NetApp Cluster
7819	RPC NetApp Cluster
7820	RPC NetApp Cluster
7821	RPC NetApp Cluster
7822	RPC NetApp Cluster
7823	RPC NetApp Cluster
7824	RPC NetApp Cluster
8023	Périmètre de nœud TELNET
8514	Étendue du nœud RSH
9877	Port client KMIP (hôte local interne uniquement)

## Informations sur le copyright

Copyright © 2024 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.