



Agents de la console de maintenance

NetApp Console setup and administration

NetApp
January 23, 2026

Sommaire

Agents de la console de maintenance	1
Maintenir un hôte VCenter ou ESXi pour l'agent de console	1
Accéder à la console de maintenance de la machine virtuelle	1
Installer un certificat signé par une autorité de certification pour l'accès à la console Web	4
Installer un certificat HTTPS	4
Renouveler le certificat HTTPS de la console	6
Configurer un agent de console pour utiliser un serveur proxy	6
Configurations prises en charge	7
Activer un proxy explicite sur un agent de console	7
Activer un proxy transparent pour un agent de console	8
Mettre à jour le proxy de l'agent de console s'il perd l'accès à Internet	9
Activer le trafic API direct	9
Dépanner l'agent de la console	9
Messages d'erreur courants et résolutions	10
Vérifiez l'état de l'agent de la console	10
Afficher la version de l'agent de la console	11
Vérifier l'accès au réseau	11
Problèmes d'installation de l'agent de console	12
Travailler avec le support NetApp	13
Corriger les échecs de téléchargement lors de l'utilisation d'une passerelle Google Cloud NAT	14
Obtenez de l'aide auprès de la base de connaissances NetApp	14
Désinstaller et supprimer un agent de console	14
Désinstaller l'agent lors de l'utilisation du mode standard ou restreint	14
Supprimer les agents de la console	15

Agents de la console de maintenance

Maintenir un hôte VCenter ou ESXi pour l'agent de console

Vous pouvez apporter des modifications à votre hôte VCenter ou ESXi existant après avoir déployé l'agent de console. Par exemple, vous pouvez augmenter la CPU ou la RAM de l'instance de machine virtuelle qui héberge l'agent de console.

Effectuez ces tâches de maintenance à l'aide de la console Web de la machine virtuelle :

- Augmenter la taille du disque
- Redémarrer l'agent
- Mettre à jour les routes statiques
- Mettre à jour les domaines de recherche

Limites

La mise à niveau de l'agent via la console n'est pas encore prise en charge. De plus, vous ne pouvez afficher que les informations sur l'adresse IP, le DNS et les passerelles.

Accéder à la console de maintenance de la machine virtuelle

Vous pouvez accéder à la console de maintenance à partir du client VSphere.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.

Changer le mot de passe de l'utilisateur principal

Vous pouvez modifier le mot de passe pour le `maint` utilisateur.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer 1 pour voir le `System Configuration` menu.
6. Entrer 1 pour modifier le mot de passe de l'utilisateur de maintenance et suivre les instructions à l'écran.

Augmenter le CPU ou la RAM de l'instance VM

Vous pouvez augmenter la CPU ou la RAM de l'instance de machine virtuelle qui héberge l'agent de console.

Modifiez les paramètres de l'instance de machine virtuelle dans votre hôte VCenter ou ESXi, puis utilisez la console de maintenance pour appliquer les modifications.

Étapes du client VSphere

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Cliquez avec le bouton droit sur l'instance de VM et sélectionnez **Modifier les paramètres**.
4. Augmentez l'espace disque dur utilisé pour la partition /opt ou /var.
 - a. Sélectionnez **Disque dur 2** pour augmenter l'espace disque dur utilisé pour /opt.
 - b. Sélectionnez **Disque dur 3** pour augmenter l'espace disque dur utilisé pour /var.
5. Enregistrez vos modifications.

Étapes de la console de maintenance

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer 1 to view the `System Configuration menu.
6. Entrer 2 et suivez les instructions à l'écran. La console recherche de nouveaux paramètres et augmente la taille des partitions.

Afficher les paramètres réseau de la machine virtuelle de l'agent

Affichez les paramètres réseau de la machine virtuelle de l'agent dans le client VSphere pour confirmer ou résoudre les problèmes de réseau. Vous ne pouvez afficher (et non mettre à jour) que les paramètres réseau suivants : adresse IP et détails DNS.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer 2 pour voir le Network Configuration menu.
6. Saisissez un nombre compris entre 1 et 6 pour afficher les paramètres réseau correspondants.

Mettre à jour les routes statiques pour la machine virtuelle de l'agent

Ajoutez, mettez à jour ou supprimez des itinéraires statiques pour la machine virtuelle de l'agent selon les

besoins.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer 2 pour voir le Network Configuration menu.
6. Entrer 7 pour mettre à jour les itinéraires statiques et suivre les invites à l'écran.
7. Appuyez sur Entrée.
8. Vous pouvez également apporter des modifications supplémentaires.
9. Entrer 9 pour valider vos modifications.

Mettre à jour les paramètres de recherche de domaine pour la machine virtuelle de l'agent

Vous pouvez mettre à jour les paramètres du domaine de recherche pour la machine virtuelle de l'agent.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer 2 ` pour voir le Network Configuration menu.
6. Entrer 8 pour mettre à jour les paramètres de recherche de domaine et suivre les invites à l'écran.
7. Appuyez sur Entrée.
8. Vous pouvez également apporter des modifications supplémentaires.
9. Entrer 9 pour valider vos modifications.

Accéder aux outils de diagnostic de l'agent

Accédez aux outils de diagnostic pour résoudre les problèmes avec l'agent de la console. Le support NetApp peut vous demander de le faire lors du dépannage.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.

5. Entrer 3 pour afficher le menu Support et Diagnostics.
6. Entrer 1 pour accéder aux outils de diagnostic et suivre les instructions à l'écran. + Par exemple, vous pouvez vérifier que tous les services d'agent sont en cours d'exécution. "[Vérifiez l'état de l'agent de la console](#)" .

Accéder aux outils de diagnostic de l'agent à distance

Vous pouvez accéder aux outils de diagnostic à distance avec un outil tel que Putty. Activez l'accès SSH à la machine virtuelle de l'agent en attribuant un mot de passe à usage unique.

L'accès SSH permet des fonctionnalités de terminal avancées telles que le copier-coller.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer 3 pour voir le Support and Diagnostics menu.
6. Entrer 2 pour accéder aux outils de diagnostic et suivre les invites à l'écran pour configurer un mot de passe à usage unique qui expire dans 24 heures.
7. Utilisez un outil SSH tel que Putty pour vous connecter à la machine virtuelle de l'agent à l'aide du nom d'utilisateur `diag` et le mot de passe à usage unique que vous avez configuré.

Installer un certificat signé par une autorité de certification pour l'accès à la console Web

Lorsque vous utilisez la NetApp Console en mode restreint, l'interface utilisateur est accessible à partir de la machine virtuelle de l'agent de console déployée dans votre région cloud ou sur site. Par défaut, la console utilise un certificat SSL auto-signé pour fournir un accès HTTPS sécurisé à la console Web exécutée sur l'agent de console.

Si votre entreprise l'exige, vous pouvez installer un certificat signé par une autorité de certification (CA), qui offre une meilleure protection de sécurité qu'un certificat auto-signé. Une fois le certificat installé, la console utilise le certificat signé par une autorité de certification lorsque les utilisateurs accèdent à la console Web.

Installer un certificat HTTPS

Installez un certificat signé par une autorité de certification pour un accès sécurisé à la console Web exécutée sur l'agent de console.

À propos de cette tâche

Vous pouvez installer le certificat en utilisant l'une des options suivantes :

- Générez une demande de signature de certificat (CSR) à partir de la console, soumettez la demande de certificat à une autorité de certification, puis installez le certificat signé par l'autorité de certification sur l'agent de la console.

La paire de clés utilisée par la console pour générer le CSR est stockée en interne sur l'agent de la console. La console récupère automatiquement la même paire de clés (clé privée) lorsque vous installez le certificat sur l'agent de la console.

- Installez un certificat signé par une autorité de certification que vous possédez déjà.

Avec cette option, le CSR n'est pas généré via la console. Vous générez le CSR séparément et stockez la clé privée en externe. Vous fournissez la clé privée à la console lorsque vous installez le certificat.

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'action pour un agent de console et sélectionnez **Configuration HTTPS**.

L'agent Console doit être connecté pour pouvoir le modifier.

3. Dans la page de configuration HTTPS, installez un certificat en générant une demande de signature de certificat (CSR) ou en installant votre propre certificat signé par une autorité de certification :

Option	Description
Générer un CSR	<ol style="list-style-type: none">Saisissez le nom d'hôte ou le DNS de l'hôte de l'agent de console (son nom commun), puis sélectionnez Générer la CSR. La console affiche une demande de signature de certificat.Utilisez le CSR pour soumettre une demande de certificat SSL à une autorité de certification. Le certificat doit utiliser le format X.509 codé en base 64 (Privacy Enhanced Mail) PEM.Téléchargez le fichier de certificat, puis sélectionnez Installer.
Installez votre propre certificat signé par une autorité de certification	<ol style="list-style-type: none">Sélectionnez Installer le certificat signé par une autorité de certification.Chargez à la fois le fichier de certificat et la clé privée, puis sélectionnez Installer. Le certificat doit utiliser le format X.509 codé en base 64 (Privacy Enhanced Mail) PEM.

Résultat

L'agent de console utilise désormais le certificat signé par une autorité de certification pour fournir un accès HTTPS sécurisé. L'image suivante montre un agent configuré pour un accès sécurisé :

HTTPS Certificate

✓ HTTPS Setup is active

Expiration: Aug 15, 2029 10:09:01 am

Issuer: C=IL, ST=Israel, L=Tel Aviv, O=NetApp, OU=Dev, CN= Localhost, E=Admin@netapp.com

Subject: C=IL, ST=Israel, L=Tel Aviv, O=NetApp, OU=Dev, CN= Localhost, E=Admin@netapp.com

Certificate: [View CSR](#)

Renouveler le certificat HTTPS de la console

Vous devez renouveler le certificat HTTPS de l'agent avant son expiration pour garantir un accès sécurisé. Si vous ne renouvez pas le certificat avant son expiration, un avertissement apparaît lorsque les utilisateurs accèdent à la console Web via HTTPS.

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'action pour un agent de console et sélectionnez **Configuration HTTPS**.
Les détails sur le certificat s'affichent, y compris la date d'expiration.
3. Sélectionnez **Modifier le certificat** et suivez les étapes pour générer un CSR ou installer votre propre certificat signé par une autorité de certification.

Configurer un agent de console pour utiliser un serveur proxy

Si vos politiques d'entreprise exigent que vous utilisez un serveur proxy pour toutes les communications vers Internet, vous devez configurer vos agents pour qu'ils utilisent ce serveur proxy. Si vous n'avez pas configuré un agent de console pour utiliser un serveur proxy lors de l'installation, vous pouvez configurer l'agent de console pour utiliser ce serveur proxy à tout moment.

Le serveur proxy de l'agent permet l'accès Internet sortant sans IP publique ni passerelle NAT. Le serveur proxy fournit une connectivité sortante uniquement pour l'agent de console, et non pour les systèmes Cloud Volumes ONTAP .

Si les systèmes Cloud Volumes ONTAP ne disposent pas d'un accès Internet sortant, la console les configure pour utiliser le serveur proxy de l'agent de la console. Vous devez vous assurer que le groupe de sécurité de l'agent de console autorise les connexions entrantes sur le port 3128. Ouvrez ce port après avoir déployé l'agent de console.

Si l'agent de console lui-même ne dispose pas d'une connexion Internet sortante, les systèmes Cloud Volumes ONTAP ne peuvent pas utiliser le serveur proxy configuré.

Configurations prises en charge

- Les serveurs proxy transparents sont pris en charge pour les agents qui servent les systèmes Cloud Volumes ONTAP . Si vous utilisez les services de données NetApp avec Cloud Volumes ONTAP, créez un agent dédié pour Cloud Volumes ONTAP où vous pouvez utiliser un serveur proxy transparent.
- Les serveurs proxy explicites sont pris en charge avec tous les agents, y compris ceux qui gèrent les systèmes Cloud Volumes ONTAP et ceux qui gèrent les services de données NetApp .
- HTTP et HTTPS.
- Le serveur proxy peut résider dans le cloud ou dans votre réseau.



Une fois que vous avez configuré un proxy, vous ne pouvez pas modifier le type de proxy. Si vous devez modifier le type de proxy, supprimez l'agent de console et ajoutez un nouvel agent avec le nouveau type de proxy.

Activer un proxy explicite sur un agent de console

Lorsque vous configurez un agent de console pour utiliser un serveur proxy, cet agent et les systèmes Cloud Volumes ONTAP qu'il gère (y compris les médiateurs HA) utilisent tous le serveur proxy.

Cette opération redémarre l'agent de la console. Vérifiez que l'agent de la console est inactif avant de continuer.

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'action pour un agent de console et sélectionnez **Modifier l'agent**.

L'agent de la console doit être actif pour pouvoir le modifier.

3. Sélectionnez **Configuration du proxy HTTP**.
4. Sélectionnez **Proxy explicite** dans le champ **Type de configuration**.
5. Sélectionnez **Activer le proxy**.
6. Spécifiez le serveur en utilisant la syntaxe `http://address:port` ou `https://address:port`
7. Spécifiez un nom d'utilisateur et un mot de passe si une authentification de base est requise pour le serveur.

Notez ce qui suit :

- L'utilisateur peut être un utilisateur local ou un utilisateur de domaine.

- Pour un utilisateur de domaine, vous devez saisir le code ASCII du \ comme suit : nom-de-domaine%92nom-d'utilisateur

Par exemple : netapp%92proxy

- La console ne prend pas en charge les mots de passe qui incluent le caractère @.

8. Sélectionnez **Enregistrer**.

Activer un proxy transparent pour un agent de console

Seul Cloud Volumes ONTAP prend en charge l'utilisation d'un proxy transparent sur l'agent de la console. Si vous utilisez des services de données NetApp en plus de Cloud Volumes ONTAP, vous devez créer un agent distinct à utiliser pour les services de données ou pour Cloud Volumes ONTAP.

Avant d'activer un proxy transparent, assurez-vous que les exigences suivantes sont remplies :

- L'agent est installé sur le même réseau que le serveur proxy transparent.
- L'inspection TLS est activée sur le serveur proxy.
- Vous disposez d'un certificat au format PEM qui correspond à celui utilisé sur le serveur proxy transparent.
- Vous n'utilisez pas l'agent de console pour d'autres services de données NetApp que Cloud Volumes ONTAP.

Pour configurer un agent existant afin d'utiliser un serveur proxy transparent, utilisez l'outil de maintenance de l'agent de console disponible via la ligne de commande sur l'hôte de l'agent de console.

Lorsque vous configurez un serveur proxy, l'agent de la console redémarre. Vérifiez que l'agent de la console est inactif avant de continuer.

Étapes

Assurez-vous que vous disposez d'un fichier de certificat au format PEM pour le serveur proxy. Si vous ne disposez pas de certificat, contactez votre administrateur réseau pour en obtenir un.

1. Ouvrez une interface de ligne de commande sur l'hôte de l'agent de console.
2. Accédez au répertoire de l'outil de maintenance de l'agent de console :
`/opt/application/netapp/service-manager-2/agent-maint-console`
3. Exécutez la commande suivante pour activer le proxy transparent, où `/home/ubuntu/<certificate-file>.pem` est le répertoire et le fichier de certificat de nom que vous avez pour le serveur proxy :

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Assurez-vous que le fichier de certificat est au format PEM et réside dans le même répertoire que la commande ou spécifiez le chemin d'accès complet au fichier de certificat.

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Modifier le proxy transparent pour l'agent de la console

Vous pouvez mettre à jour le serveur proxy transparent existant d'un agent Console en utilisant la `proxy update` commande ou supprimer le serveur proxy transparent en utilisant la `proxy remove` commande. Pour plus d'informations, consultez la documentation relative à "[Console de maintenance des agents](#)" .



Une fois que vous avez configuré un proxy, vous ne pouvez pas modifier le type de proxy. Si vous devez modifier le type de proxy, supprimez l'agent de console et ajoutez un nouvel agent avec le nouveau type de proxy.

Mettre à jour le proxy de l'agent de console s'il perd l'accès à Internet

Si la configuration proxy de votre réseau change, votre agent risque de perdre l'accès à Internet. Par exemple, si quelqu'un modifie le mot de passe du serveur proxy ou met à jour le certificat. Dans ce cas, vous devrez accéder directement à l'interface utilisateur depuis l'hôte de l'agent de la console et mettre à jour les paramètres. Assurez-vous que vous disposez d'un accès réseau à l'hôte de l'agent de la console et que vous pouvez vous connecter à la console.

Activer le trafic API direct

Si vous avez configuré un agent Console pour utiliser un serveur proxy, vous pouvez activer le trafic API direct sur l'agent Console afin d'envoyer des appels API directement aux services du fournisseur cloud sans passer par le proxy. Les agents exécutés sur AWS, Azure ou Google Cloud prennent en charge cette option.

Si vous désactivez Azure Private Links avec Cloud Volumes ONTAP et utilisez des points de terminaison de service, activez le trafic API direct. Sinon, le trafic ne sera pas acheminé correctement.

["En savoir plus sur l'utilisation d'un lien privé Azure ou de points de terminaison de service avec Cloud Volumes ONTAP"](#)

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'action pour un agent de console et sélectionnez **Modifier l'agent**.
L'agent de la console doit être actif pour pouvoir le modifier.
3. Sélectionnez **Prendre en charge le trafic API direct**.
4. Cochez la case pour activer l'option, puis sélectionnez **Enregistrer**.

Dépanner l'agent de la console

Pour résoudre les problèmes avec un agent de console, vous pouvez vérifier les problèmes vous-même ou travailler avec le support NetApp qui peut vous demander votre ID système, la version de l'agent ou les derniers messages AutoSupport .

Si vous disposez d'un compte sur le site de support NetApp , vous pouvez également consulter le "[Base de connaissances NetApp](#) ."

Messages d'erreur courants et résolutions

Ce tableau répertorie les messages d'erreur courants et indique comment les corriger :

Message d'erreur	Explication	Ce qu'il faut faire
Impossible de charger l'interface utilisateur de l'agent de la console	L'installation de l'agent a échoué	<ul style="list-style-type: none">Vérifiez que le service Service Manager est actif.Vérifiez que tous les conteneurs sont en cours d'exécution.Assurez-vous que votre pare-feu autorise l'accès au service sur le port 8888.Si vous rencontrez toujours des problèmes, contactez l'assistance.
Impossible d'accéder à l'interface utilisateur de l'agent NetApp	Ce message apparaît lorsque vous essayez d'accéder à l'adresse IP d'un agent. L'agent peut ne pas s'initialiser s'il ne dispose pas de l'accès réseau correct ou s'il est instable.	<ul style="list-style-type: none">Connectez-vous à l'agent de la console.Vérifiez que le service Service ManagerVérifiez que l'agent dispose de l'accès réseau dont il a besoin."En savoir plus sur les points de terminaison d'accès réseau requis."
Impossible de charger les paramètres de l'agent	La console affiche ce message lorsque vous essayez d'accéder à la page des paramètres de l'agent.	<ul style="list-style-type: none">Vérifiez si le conteneur OCCM est en cours d'exécution et fonctionne.Si le problème persiste, contactez le support.
Impossible de charger les informations d'assistance pour l'agent.	Ce message s'affiche si l'agent ne peut pas accéder à votre compte d'assistance.	<ul style="list-style-type: none">Vérifiez que l'agent dispose d'un accès sortant aux points de terminaison requis."En savoir plus sur les points de terminaison d'accès réseau requis."

Vérifiez l'état de l'agent de la console

Utilisez l'une des commandes suivantes pour vérifier votre agent de console. Tous les services doivent avoir le statut *En cours d'exécution*. Si ce n'est pas le cas, contactez le support NetApp .

 Pour plus d'informations sur l'accès aux diagnostics de l'agent de la console, consultez les rubriques suivantes :

- ["Vérifier l'état de l'agent de la console \(pour les déploiements d'hôtes Linux\)"](#)
- ["Vérifier l'état de l'agent de la console \(pour les déploiements VCenter\)"](#)

Docker (pour les déploiements Ubuntu et VCenter)

```
docker ps -a
```

Podman (pour les déploiements RedHat Enterprise Linux)

```
podman ps -a
```

Afficher la version de l'agent de la console

Affichez la version de l'agent de la console pour confirmer la mise à niveau ou partagez-la avec votre représentant NetApp .

Étapes

1. Sélectionnez **Administration > Support > Agents**.

La console affiche la version en haut de la page.

Vérifier l'accès au réseau

Assurez-vous que l'agent de console dispose de l'accès réseau dont il a besoin.["En savoir plus sur les points d'accès réseau requis."](#)

Effectuez des vérifications de configuration sur l'agent de la console.

Effectuez des vérifications de configuration sur les agents de la console depuis la console ou la console de maintenance des agents pour vous assurer qu'ils sont connectés.

Vous pouvez également effectuer des vérifications de configuration à l'aide de la console de maintenance de l'agent.["Apprenez-en davantage sur l'utilisation de la commande de validation de config-checker."](#)



Vous ne pouvez valider que les agents dont le statut est **Connecté**.

Étapes depuis la console

1. Sélectionnez **Administration > Agents**.
2. Sélectionnez le menu d'actions de l'agent Console que vous souhaitez vérifier et choisissez **Valider**.

Name	Location	Status	Region
BXP9161ga		Connected	N/A
BXP9181		Connected	N/A
nikhilm	aws	Failed	US
nikhilm	aws	Failed	IIS

La validation peut prendre jusqu'à 15 minutes. Les résultats s'affichent une fois terminé.

Problèmes d'installation de l'agent de console

Si l'installation échoue, consultez le rapport et les journaux pour résoudre les problèmes.

Vous pouvez également accéder au rapport de validation au format JSON et aux journaux de configuration directement depuis l'hôte de l'agent de la console dans les répertoires suivants :

```
/tmp/netapp-console-agents/logs  
/tmp/netapp-console-agents/results.json
```

-  • Pour les nouveaux déploiements d'agents, NetApp vérifie les points de terminaison suivants : "répertorié ici". Cette vérification de configuration échoue avec une erreur si vous utilisez les points de terminaison précédents utilisés pour les mises à niveau, "répertorié ici". NetApp recommande de mettre à jour vos règles de pare-feu pour autoriser l'accès aux points de terminaison actuels et bloquer l'accès aux points de terminaison précédents dès que possible. ["Apprenez à mettre à jour votre réseau"](#).
- Si vous mettez à jour les points de terminaison de votre pare-feu, vos agents existants continueront de fonctionner.

Désactiver les vérifications de configuration pour les installations manuelles

Il peut arriver que vous ayez besoin de désactiver les contrôles de configuration qui vérifient la connectivité sortante lors de l'installation. Par exemple, lors de l'installation manuelle d'un agent dans votre environnement Government Cloud, vous devez désactiver les vérifications de configuration, sinon l'installation échouera.

Étapes

Vous désactivez la vérification de configuration en définissant l'indicateur `skipConfigCheck` dans le fichier `/com/opt/application/netapp/service-manager-2/config.json`. Par défaut, cet indicateur est défini sur faux et la vérification de configuration vérifie l'accès sortant pour l'agent. Définissez cet indicateur sur vrai pour désactiver la vérification. Familiarisez-vous avec la syntaxe JSON avant de passer à l'étape suivante.

Pour réactiver la vérification de configuration, procédez comme suit et définissez l'indicateur `skipConfigCheck` sur false.

Étapes

1. Accédez à l'hôte de l'agent de la console en tant que root ou avec les privilèges sudo.
2. Créez une copie de sauvegarde du fichier `/opt/application/netapp/service-manager-2/config.json` pour vous assurer de pouvoir annuler vos modifications.
3. Arrêtez le service Service Manager 2 en exécutant la commande suivante :

```
systemctl stop netapp-service-manager.service
```

1. Modifiez le fichier `/opt/application/netapp/service-manager-2/config.json` et remplacez la valeur de l'indicateur `skipConfigCheck` par true.

```
"skipConfigCheck": true
```

2. Enregistrez votre fichier.
3. Redémarrez le service Service Manager 2 en exécutant la commande suivante :

```
systemctl restart netapp-service-manager.service
```

Travailler avec le support NetApp

Si vous n'avez pas pu résoudre les problèmes avec votre agent de console, vous pouvez contacter le support NetApp . Le support NetApp peut vous demander l'ID de l'agent de console ou de lui envoyer les journaux de l'agent de console s'il ne les possède pas déjà.

Rechercher l'ID de l'agent de la console

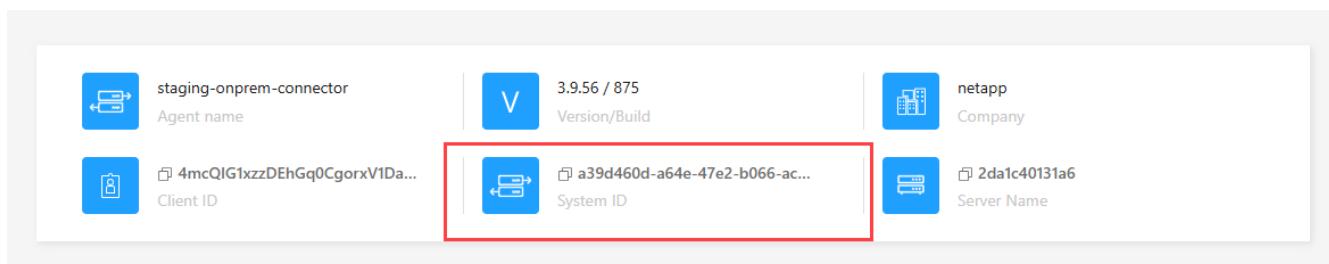
Pour vous aider à démarrer, vous aurez peut-être besoin de l'ID système de votre agent de console. L'ID est généralement utilisé à des fins de licence et de dépannage.

Étapes

1. Sélectionnez **Administration > Support > Agents**.

Vous pouvez trouver l'ID système en haut de la page.

Exemple



2. Survolez et cliquez sur l'ID pour le copier.

Téléchargez ou envoyez un message AutoSupport

Si vous rencontrez des problèmes, NetApp peut vous demander d'envoyer un message AutoSupport au support NetApp à des fins de dépannage.



La NetApp Console prend jusqu'à cinq heures pour envoyer des messages AutoSupport en raison de l'équilibrage de charge. Pour une communication urgente, téléchargez le fichier et envoyez-le manuellement.

Étapes

1. Sélectionnez **Administration > Support > Agents**.
2. Selon la manière dont vous devez envoyer les informations au support NetApp , choisissez l'une des options suivantes :

- a. Sélectionnez l'option permettant de télécharger le message AutoSupport sur votre ordinateur local. Vous pouvez ensuite l'envoyer au support NetApp en utilisant la méthode de votre choix.
- b. Sélectionnez **Envoyer AutoSupport** pour envoyer directement le message au support NetApp .

Corriger les échecs de téléchargement lors de l'utilisation d'une passerelle Google Cloud NAT

L'agent de console télécharge automatiquement les mises à jour logicielles pour Cloud Volumes ONTAP. Votre configuration peut entraîner l'échec du téléchargement si elle utilise une passerelle NAT Google Cloud. Vous pouvez corriger ce problème en limitant le nombre de parties dans lesquelles l'image du logiciel est divisée. Cette étape doit être complétée en utilisant l'API.

Étape

1. Soumettez une requête PUT à /occm/config avec le JSON suivant comme corps :

```
{  
    "maxDownloadSessions": 32  
}
```

La valeur de *maxDownloadSessions* peut être 1 ou tout entier supérieur à 1. Si la valeur est 1, l'image téléchargée ne sera pas divisée.

Notez que 32 est une valeur d'exemple. La valeur dépend de votre configuration NAT et du nombre de sessions simultanées.

["En savoir plus sur l'appel API /occm/config"](#)

Obtenez de l'aide auprès de la base de connaissances NetApp

["Consultez les informations de dépannage créées par l'équipe de support NetApp"](#) .

Désinstaller et supprimer un agent de console

Désinstallez un agent de console pour résoudre les problèmes ou pour le supprimer définitivement de l'hôte. Les étapes à suivre dépendent du mode de déploiement que vous utilisez. Une fois que vous avez supprimé un agent de console de votre environnement, vous pouvez le supprimer de la console.

["En savoir plus sur les modes de déploiement de la NetApp Console"](#) .

Désinstaller l'agent lors de l'utilisation du mode standard ou restreint

Si vous utilisez le mode standard ou le mode restreint (en d'autres termes, l'hôte de l'agent dispose d'une connectivité sortante), vous devez suivre les étapes ci-dessous pour désinstaller l'agent.

Étapes

1. Connectez-vous à la machine virtuelle Linux pour l'agent.
2. Depuis l'hôte Linux, exécutez le script de désinstallation :

```
/opt/application/netapp/service-manager-2/uninstall.sh [silent]
```

silent exécute le script sans vous demander de confirmation.

Supprimer les agents de la console

Si vous avez supprimé une machine virtuelle d'agent ou désinstallé l'agent, vous devez la retirer de la liste des agents dans la console. Après la suppression d'une machine virtuelle d'agent ou la désinstallation du logiciel d'agent, l'agent affiche l'état **Déconnecté** dans la console.

Notez les points suivants concernant la suppression d'un agent de console :

- Cette action ne supprime pas la machine virtuelle.
- Cette action ne peut pas être annulée : une fois que vous avez supprimé un agent de console, vous ne pouvez pas le rajouter.

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'actions d'un agent déconnecté et sélectionnez **Supprimer l'agent**.
3. Saisissez le nom de l'agent pour confirmer, puis sélectionnez **Supprimer**.

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 JOUSSANCE, 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.