Accès au cluster via l'interface de ligne de commandes (administrateurs de cluster uniquement)

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/system-admin/access-serial-port-task.html on September 12, 2024. Always check docs.netapp.com for the latest.

Sommaire

Accès au cluster via l'interface de ligne de commandes (administrateurs de cluster uniquement)

Accéder au cluster via le port série

Vous pouvez accéder directement au cluster depuis une console connectée au port série d'un nœud.

Étapes

1. Sur la console, appuyez sur entrée.

   Le système répond avec l'invite de connexion.

2. À l'invite de connexion, effectuez l'une des opérations suivantes :

Pour accéder au cluster avec…	Entrez le nom de compte suivant…
Compte de cluster par défaut	**`admin`**
Un autre compte d'utilisateur administratif	*`username`*

   Le système répond avec l'invite de mot de passe.

3. Entrez le mot de passe du compte administrateur ou administrateur, puis appuyez sur entrée.

Accédez au cluster via SSH

Vous pouvez envoyer des requêtes SSH à un cluster ONTAP pour effectuer des tâches d'administration. SSH est activé par défaut.

Avant de commencer

- Vous devez disposer d'un compte utilisateur configuré pour l'utilisation `ssh` comme méthode d'accès.

  Le `-application` paramètre du `security login` les commandes spécifie la méthode d'accès pour un compte utilisateur. Le `security login` "pages de manuel" contiennent des informations supplémentaires.

- Si vous utilisez un compte d'utilisateur de domaine Active Directory (AD) pour accéder au cluster, un tunnel d'authentification pour le cluster doit avoir été configuré via une VM de stockage compatible CIFS et votre compte d'utilisateur de domaine AD doit également avoir été ajouté au cluster avec `ssh` comme méthode d'accès et `domain` comme méthode d'authentification.

Description de la tâche

- Vous devez utiliser un client OpenSSH 5.7 ou version ultérieure.
- Seul le protocole SSH v2 est pris en charge ; SSH v1 n'est pas pris en charge.

- ONTAP prend en charge un maximum de 64 sessions SSH simultanées par nœud.

  Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

  Si le taux de connexions entrantes est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.

- ONTAP ne prend en charge que les algorithmes de cryptage AES et 3DES (également appelés *chiffrements*) pour SSH.

  AES est pris en charge avec des clés de 128, 192 et 256 bits. 3DES a une longueur clé de 56 bits comme dans les DES d'origine, mais elle est répétée trois fois.

- Lorsque le mode FIPS est activé, les clients SSH doivent négocier avec les algorithmes de clé publique ECDSA (Elliptic Curve Digital Signature Algorithm) pour que la connexion soit réussie.
- Pour accéder à l'interface de ligne de commandes de ONTAP à partir d'un hôte Windows, vous pouvez faire appel à un utilitaire tiers tel que PuTTY.
- Si vous utilisez un nom d'utilisateur Windows AD pour vous connecter à ONTAP, vous devez utiliser les mêmes lettres majuscules ou minuscules que celles qui ont été utilisées lorsque le nom d'utilisateur AD et le nom de domaine ont été créés dans ONTAP.

  Les noms d'utilisateur ET de domaine AD ne sont pas sensibles à la casse. Toutefois, les noms d'utilisateur ONTAP sont sensibles à la casse. La non-concordance de cas entre le nom d'utilisateur créé dans ONTAP et le nom d'utilisateur créé dans AD entraîne un échec de connexion.

Options d'authentification SSH

- À partir de ONTAP 9.3, vous pouvez "Activez l'authentification multifacteur SSH" pour les comptes d'administrateur local.

  Lorsque l'authentification multifacteur SSH est activée, les utilisateurs sont authentifiés à l'aide d'une clé publique et d'un mot de passe.

- À partir de ONTAP 9.4, vous pouvez "Activez l'authentification multifacteur SSH" Pour les utilisateurs distants LDAP et NIS.
- À partir de ONTAP 9.13.1, vous pouvez éventuellement ajouter la validation du certificat au processus d'authentification SSH afin d'améliorer la sécurité de la connexion. Pour ce faire, "Associer un certificat X.509 à la clé publique" qu'un compte utilise. Si vous vous connectez à l'aide de SSH avec une clé publique SSH et un certificat X.509, ONTAP vérifie la validité du certificat X.509 avant de vous authentifier à l'aide de la clé publique SSH. La connexion SSH est refusée si le certificat a expiré ou a été révoqué et si la clé publique SSH est automatiquement désactivée.
- À partir de ONTAP 9.14.1, les administrateurs ONTAP peuvent "Ajoutez l'authentification à deux facteurs Cisco Duo au processus d'authentification SSH" pour améliorer la sécurité de connexion. Lors de la première connexion après avoir activé l'authentification Cisco Duo, les utilisateurs doivent inscrire un périphérique pour qu'il serve d'authentificateur pour les sessions SSH.
- À partir de ONTAP 9.15.1, les administrateurs peuvent "Configurer l'autorisation dynamique" Fournir une authentification adaptative supplémentaire aux utilisateurs SSH en fonction du score de confiance de l'utilisateur.

Étapes

1. Depuis un hôte disposant d'un accès au réseau du cluster ONTAP, entrez dans le champ `ssh` commande dans l'un des formats suivants :

- **ssh *username@hostname_or_IP* [*command*]**
- **ssh -l *username hostname_or_IP* [*command*]**

Si vous utilisez un compte utilisateur de domaine AD, vous devez le préciser *username* au format de *domainname\\AD_accountname* (avec doubles barres obliques inverses après le nom de domaine) ou "*domainname\AD_accountname*" (entre guillemets doubles et avec une barre oblique inverse unique après le nom de domaine).

hostname_or_IP Est le nom d'hôte ou l'adresse IP de la LIF de cluster management ou une LIF de node management. Il est recommandé d'utiliser la LIF de cluster management. Vous pouvez utiliser une adresse IPv4 ou IPv6.

command N'est pas requis pour les sessions interactives SSH.

Exemples de requêtes SSH

Les exemples suivants montrent comment le compte utilisateur nommé « joe » peut émettre une demande SSH pour accéder à un cluster dont la LIF de gestion du cluster est 10.72.137.28 :

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

Les exemples suivants montrent comment le compte utilisateur nommé « john » du domaine nommé « `DOMAIN1' » peut émettre une requête SSH pour accéder à un cluster dont la LIF de gestion de cluster est 10.72.137.28 :

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

L'exemple suivant montre comment le compte utilisateur nommé « joe » peut émettre une demande SSH MFA pour accéder à un cluster dont la LIF de gestion du cluster est de 10.72.137.32 :

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

Informations associées

"Authentification de l'administrateur et RBAC"

Sécurité de connexion SSH

À partir de ONTAP 9.5, vous pouvez afficher des informations sur les connexions précédentes, les tentatives infructueuses de connexion et les modifications apportées à vos privilèges depuis votre dernière connexion réussie.

Les informations relatives à la sécurité s'affichent lorsque vous vous connectez en tant qu'utilisateur administrateur SSH. Vous êtes averti des conditions suivantes :

- La dernière fois que votre nom de compte a été connecté.

- Nombre de tentatives de connexion infructueuses depuis la dernière connexion réussie.
- Si le rôle a changé depuis la dernière connexion (par exemple, si le rôle du compte admin est passé de « admin » à « backup »).
- Les fonctionnalités d'ajout, de modification ou de suppression du rôle ont été modifiées depuis la dernière connexion.

> Si l'une des informations affichées est suspecte, contactez immédiatement votre service de sécurité.

Pour obtenir ces informations lors de votre connexion, les conditions préalables suivantes doivent être remplies :

- Votre compte utilisateur SSH doit être provisionné dans ONTAP.
- Votre identifiant de sécurité SSH doit être créé.
- Votre tentative de connexion doit réussir.

Restrictions et autres considérations relatives à la sécurité de la connexion SSH

Les restrictions et considérations suivantes s'appliquent aux informations de sécurité de connexion SSH :

- Les informations sont disponibles uniquement pour les connexions SSH.
- Pour les comptes admin basés sur un groupe, tels que LDAP/NIS et comptes AD, les utilisateurs peuvent afficher les informations de connexion SSH si le groupe dont ils sont membres est provisionné en tant que compte d'administrateur dans ONTAP.

  Cependant, les alertes relatives aux modifications du rôle du compte utilisateur ne peuvent pas être affichées pour ces utilisateurs. En outre, les utilisateurs appartenant à un groupe AD qui a été provisionné en tant que compte d'administrateur dans ONTAP ne peuvent pas afficher le nombre de tentatives de connexion ayant échoué qui se sont produites depuis la dernière connexion.

- Les informations conservées pour un utilisateur sont supprimées lorsque le compte utilisateur est supprimé de ONTAP.
- Les informations ne s'affichent pas pour les connexions à d'autres applications que SSH.

Exemples d'informations de sécurité de la connexion SSH

Les exemples suivants illustrent le type d'informations affichées après votre connexion.

- Ce message s'affiche après chaque connexion réussie :

```
Last Login : 7/19/2018 06:11:32
```

- Ces messages s'affichent si des tentatives de connexion ont échoué depuis la dernière connexion réussie :

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- Ces messages s'affichent si des tentatives de connexion ont échoué et que vos privilèges ont été modifiés depuis la dernière connexion réussie :

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

Activer l'accès Telnet ou RSH au cluster

En tant que pratique de sécurité, Telnet et RSH sont désactivés par défaut. Pour permettre au cluster d'accepter les demandes Telnet ou RSH, vous devez activer le service dans la stratégie de service de gestion par défaut.

Au fil du temps, la façon dont ONTAP gère le type de trafic pris en charge sur les LIF a changé.

- ONTAP 9.5 et les versions antérieures utilisent des rôles LIF et des services de pare-feu
- Les versions ONTAP 9.6 et ultérieures utilisent les stratégies de service LIF
  - La version ONTAP 9.5 a introduit les stratégies de service LIF
  - ONTAP 9.6 a remplacé les rôles LIF par des stratégies de service LIF
  - ONTAP 9.10.1 a remplacé les services de pare-feu par des politiques de service LIF

La méthode que vous configurez dépend de la version de ONTAP que vous utilisez.

Pour en savoir plus sur :

- Politiques de pare-feu, voir "Commande : firewall-policy-show"
- Rôles LIF, voir "Rôles LIF (ONTAP 9.5 et versions antérieures)"
- Politiques de service LIF, voir "LIF et règles de service (ONTAP 9.6 et versions ultérieures)"

Telnet et RSH ne sont pas des protocoles sécurisés, vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive. Pour plus d'informations, reportez-vous à la section "Accédez au cluster via SSH"

ONTAP 9.6 ou version ultérieure

Description de la tâche

- RSH n'est pas un protocole sécurisé.

  Vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive.

- ONTAP prend en charge un maximum de 50 sessions RSH simultanées par nœud.

  Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

  Si le taux de connexions entrantes est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.

- Les commandes RSH nécessitent des privilèges avancés.

Étapes

1. Vérifiez que le protocole de sécurité RSH ou Telnet est activé :

   ```
   security protocol show
   ```

   a. Si le protocole de sécurité RSH ou Telnet est activé, passez à l'étape suivante.
   b. Si le protocole de sécurité RSH ou Telnet n'est pas activé, utilisez la commande suivante pour l'activer :

      ```
      security protocol modify -application <rsh/telnet> -enabled true
      ```

2. Vérifier que le `management-rsh-server` service ou `management-telnet-server` existe sur les LIFs de management :

   ```
   network interface show -services management-rsh-server
   ```

   ou

   ```
   network interface show -services management-telnet-server
   ```

   a. Si le `management-rsh-server` service ou `management-telnet-server` existe, passez à l'étape suivante.
   b. Si le `management-rsh-server` service ou `management-telnet-server` n'existe pas, utilisez la commande suivante pour l'ajouter :

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

   ```
   network interface service-policy add-service -vserver cluster1 -policy
   default-management -service management-telnet-server
   ```

ONTAP 9.5 ou version antérieure

Description de la tâche

ONTAP vous empêche de modifier des règles de pare-feu prédéfinies, mais vous pouvez créer une

nouvelle règle en clonant la `mgmt` stratégie de pare-feu de gestion prédéfinie, puis en activant Telnet ou RSH dans le cadre de la nouvelle règle.

Étapes

1. Saisissez le mode de privilège avancé :

   ```
   set advanced
   ```

2. Activer un protocole de sécurité (RSH ou Telnet) :

   ```
   security protocol modify -application security_protocol -enabled true
   ```

3. Créez une nouvelle politique de pare-feu de gestion basée sur `mgmt` la politique de pare-feu de gestion :

   ```
   system services firewall policy clone -policy mgmt -destination-policy
   policy-name
   ```

4. Activer Telnet ou RSH dans la nouvelle politique de pare-feu de gestion :

   ```
   system services firewall policy create -policy policy-name -service
   security_protocol -action allow -ip-list ip_address/netmask
   ```

   Pour autoriser toutes les adresses IP, vous devez spécifier `-ip-list 0.0.0.0/0`

5. Associer la nouvelle politique au LIF de gestion du cluster :

   ```
   network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
   -firewall-policy policy-name
   ```

Accéder au cluster à l'aide de Telnet

Vous pouvez envoyer des requêtes Telnet au cluster pour effectuer des tâches administratives. Telnet est désactivé par défaut.

Au fil du temps, la façon dont ONTAP gère le type de trafic pris en charge sur les LIF a changé.

- ONTAP 9.5 et les versions antérieures utilisent des rôles LIF et des services de pare-feu
- Les versions ONTAP 9.6 et ultérieures utilisent les stratégies de service LIF
  - La version ONTAP 9.5 a introduit les stratégies de service LIF
  - ONTAP 9.6 a remplacé les rôles LIF par des stratégies de service LIF
  - ONTAP 9.10.1 a remplacé les services de pare-feu par des politiques de service LIF

La méthode que vous configurez dépend de la version de ONTAP que vous utilisez.

Pour en savoir plus sur :

- Politiques de pare-feu, voir "Commande : firewall-policy-show"
- Rôles LIF, voir "Rôles LIF (ONTAP 9.5 et versions antérieures)"

- Politiques de service LIF, voir "LIF et règles de service (ONTAP 9.6 et versions ultérieures)"

Telnet et RSH ne sont pas des protocoles sécurisés, vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive. Pour plus d'informations, reportez-vous à la section "Accédez au cluster via SSH"

ONTAP 9.6 ou version ultérieure

Avant de commencer

Les conditions suivantes doivent être remplies pour que vous puissiez utiliser Telnet pour accéder au cluster :

- Vous devez disposer d'un compte utilisateur local de cluster configuré pour utiliser Telnet.

  Le `-application` paramètre du `security login` les commandes spécifie la méthode d'accès pour un compte utilisateur. Pour plus d'informations, reportez-vous à la section `security login` pages de manuel.

Description de la tâche

- Telnet n'est pas un protocole sécurisé.

  Vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive.

- ONTAP prend en charge un maximum de 50 sessions Telnet simultanées par nœud.

  Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

  Si le taux de connexions en cours est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.

- Pour accéder à l'interface de ligne de commandes de ONTAP à partir d'un hôte Windows, vous pouvez faire appel à un utilitaire tiers tel que PuTTY.
- Les commandes RSH nécessitent des privilèges avancés.

Étapes

1. Vérifiez que le protocole de sécurité Telnet est activé :

   ```
   security protocol show
   ```

   a. Si le protocole de sécurité Telnet est activé, passez à l'étape suivante.
   b. Si le protocole de sécurité Telnet n'est pas activé, utilisez la commande suivante pour l'activer :

      ```
      security protocol modify -application telnet -enabled true
      ```

2. Vérifier que le `management-telnet-server` service existe sur les LIFs de management :

   ```
   network interface show -services management-telnet-server
   ```

   a. Si le `management-telnet-server` service existe, passez à l'étape suivante.
   b. Si le `management-telnet-server` service n'existe pas, utilisez la commande suivante pour l'ajouter :

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

Exemple de requête Telnet

L'exemple suivant montre comment l'utilisateur nommé « joe », qui a été configuré avec un accès Telnet, peut émettre une demande Telnet pour accéder à un cluster dont la LIF de gestion du cluster est 10.72.137.28 :

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

ONTAP 9.5 ou version antérieure

Avant de commencer

Les conditions suivantes doivent être remplies pour que vous puissiez utiliser Telnet pour accéder au cluster :

- Vous devez disposer d'un compte utilisateur local de cluster configuré pour utiliser Telnet.

  Le `-application` paramètre des commandes de connexion de sécurité spécifie la méthode d'accès pour un compte utilisateur. Pour plus d'informations, consultez les pages de manuel de connexion de sécurité.

- Telnet doit déjà être activé dans la politique de pare-feu de gestion utilisée par les LIF de cluster ou de node management afin que les requêtes Telnet puissent passer par le pare-feu.

  Par défaut, Telnet est désactivé. La commande de stratégie de pare-feu show des services système avec le paramètre `-service telnet `indique si Telnet a été activé dans une politique de pare-feu. Pour plus d'informations, consultez les pages de manuel de la politique de pare-feu des services système.

- Si vous utilisez des connexions IPv6, vous devez déjà configurer et activer IPv6 sur le cluster, et les politiques de pare-feu doivent déjà être configurées avec des adresses IPv6.

  La commande ipv6 show des options réseau indique si IPv6 est activé ou non. La commande system services firewall policy show affiche les politiques de pare-feu.

Description de la tâche

- Telnet n'est pas un protocole sécurisé.

  Vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive.

- ONTAP prend en charge un maximum de 50 sessions Telnet simultanées par nœud.

  Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

  Si le taux de connexions en cours est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.

- Pour accéder à l'interface de ligne de commandes de ONTAP à partir d'un hôte Windows, vous pouvez faire appel à un utilitaire tiers tel que PuTTY.

Étapes

1. Depuis un hôte d'administration, entrez la commande suivante :

   `telnet hostname_or_IP`

   `hostname_or_IP` Est le nom d'hôte ou l'adresse IP de la LIF de cluster management ou d'une LIF de node management. Il est recommandé d'utiliser la LIF de cluster management. Vous pouvez utiliser une adresse IPv4 ou IPv6.

Exemple de requête Telnet

L'exemple suivant montre comment l'utilisateur nommé « joe », qui a été configuré avec un accès Telnet, peut émettre une demande Telnet pour accéder à un cluster dont la LIF de cluster management est 10.72.137.28 :

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

Accéder au cluster à l'aide de RSH

Vous pouvez émettre des requêtes RSH au cluster pour effectuer des tâches administratives. RSH n'est pas un protocole sécurisé et est désactivé par défaut.

Au fil du temps, la façon dont ONTAP gère le type de trafic pris en charge sur les LIF a changé.

- ONTAP 9.5 et les versions antérieures utilisent des rôles LIF et des services de pare-feu
- Les versions ONTAP 9.6 et ultérieures utilisent les stratégies de service LIF
  - La version ONTAP 9.5 a introduit les stratégies de service LIF
  - ONTAP 9.6 a remplacé les rôles LIF par des stratégies de service LIF
  - ONTAP 9.10.1 a remplacé les services de pare-feu par des politiques de service LIF

La méthode que vous configurez dépend de la version de ONTAP que vous utilisez.

Pour en savoir plus sur :

- Politiques de pare-feu, voir "Commande : firewall-policy-show"
- Rôles LIF, voir "Rôles LIF (ONTAP 9.5 et versions antérieures)"
- Politiques de service LIF, voir "LIF et règles de service (ONTAP 9.6 et versions ultérieures)"

Telnet et RSH ne sont pas des protocoles sécurisés, vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive. Pour plus d'informations, reportez-vous à la section "Accédez au cluster via SSH"

ONTAP 9.6 ou version ultérieure

Avant de commencer

Les conditions suivantes doivent être remplies pour que vous puissiez utiliser RSH pour accéder au cluster :

- Vous devez disposer d'un compte utilisateur local de cluster configuré pour utiliser la fonction RSH comme méthode d'accès.

  Le `-application` paramètre du `security login` les commandes spécifie la méthode d'accès pour un compte utilisateur. Pour plus d'informations, reportez-vous à la section `security login` pages de manuel.

Description de la tâche

- RSH n'est pas un protocole sécurisé.

  Vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive.

- ONTAP prend en charge un maximum de 50 sessions RSH simultanées par nœud.

  Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

  Si le taux de connexions entrantes est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.

- Les commandes RSH nécessitent des privilèges avancés.

Étapes

1. Vérifiez que le protocole de sécurité RSH est activé :

   ```
   security protocol show
   ```

   a. Si le protocole de sécurité RSH est activé, passez à l'étape suivante.
   b. Si le protocole de sécurité RSH n'est pas activé, utilisez la commande suivante pour l'activer :

      ```
      security protocol modify -application rsh -enabled true
      ```

2. Vérifier que le `management-rsh-server` service existe sur les LIFs de management :

   ```
   network interface show -services management-rsh-server
   ```

   a. Si le `management-rsh-server` service existe, passez à l'étape suivante.
   b. Si le `management-rsh-server` service n'existe pas, utilisez la commande suivante pour l'ajouter :

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

Exemple de demande de RSH

L'exemple suivant montre comment l'utilisateur nommé « joe », qui a été configuré avec l'accès RSH, peut émettre une demande RSH pour exécuter l' `cluster show` commande :

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

ONTAP 9.5 ou version antérieure

Avant de commencer

Les conditions suivantes doivent être remplies pour que vous puissiez utiliser RSH pour accéder au cluster :

- Vous devez disposer d'un compte utilisateur local de cluster configuré pour utiliser la fonction RSH comme méthode d'accès.

  Le paramètre -application des commandes de connexion de sécurité spécifie la méthode d'accès pour un compte utilisateur. Pour plus d'informations, consultez les pages de manuel de connexion de sécurité.

- RSH doit déjà être activé dans la politique de pare-feu de gestion utilisée par les LIFs de cluster ou de node management afin que les requêtes RSH puissent passer par le pare-feu.

  Par défaut, RSH est désactivé. La commande system services firewall policy show avec le `-service rsh` paramètre indique si RSH a été activé dans une stratégie de pare-feu. Pour plus d'informations, consultez les `system services firewall policy` pages man.

- Si vous utilisez des connexions IPv6, vous devez déjà configurer et activer IPv6 sur le cluster, et les politiques de pare-feu doivent déjà être configurées avec des adresses IPv6.

  La `network options ipv6 show` commande indique si IPv6 est activé ou non. `system services firewall policy show`La commande affiche les politiques de pare-feu.

Description de la tâche

- RSH n'est pas un protocole sécurisé.

  Vous devez envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive.

- ONTAP prend en charge un maximum de 50 sessions RSH simultanées par nœud.

  Si la LIF de cluster management réside sur le nœud, il partage cette limite avec la LIF de node management.

  Si le taux de connexions en cours est supérieur à 10 par seconde, le service est temporairement désactivé pendant 60 secondes.

Étapes

1. Depuis un hôte d'administration, entrez la commande suivante :

   `rsh hostname_or_IP -l username:passwordcommand`

   `hostname_or_IP` Est le nom d'hôte ou l'adresse IP de la LIF de cluster management ou d'une LIF de node management. Il est recommandé d'utiliser la LIF de cluster management. Vous pouvez utiliser une adresse IPv4 ou IPv6.

   `command` Est la commande que vous souhaitez exécuter sur RSH.

Exemple de demande de RSH

L'exemple suivant montre comment l'utilisateur nommé « joe », qui a été configuré avec un accès RSH, peut émettre une requête RSH pour exécuter la commande cluster show :

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node  Health Eligibility
----  ------ -----------
node1 true   true
node2 true   true

2 entries were displayed.

admin_host
```

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 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.