Gérer les connexions de prise en charge

Element Software

NetApp
October 01, 2024

Sommaire

Gérer les connexions de prise en charge 1
Accès aux nœuds de stockage à l'aide de SSH pour le dépannage de base 1
Démarrer une session de support NetApp à distance 5
Gérez la fonctionnalité SSH sur le nœud de gestion 6

Gérer les connexions de prise en charge

Accès aux nœuds de stockage à l'aide de SSH pour le dépannage de base

Depuis l'Element 12.5, vous pouvez utiliser le compte système sfreadonly sur les nœuds de stockage pour un dépannage de base. Vous pouvez également activer et ouvrir l'accès au tunnel de support à distance pour le support NetApp afin de réaliser un dépannage avancé.

Le compte système sfreadonly permet d'accéder aux commandes de dépannage de base du système Linux et du réseau, y compris `ping`.

> Sauf avis du support NetApp, toute modification de ce système n'est pas prise en charge, annulation de votre contrat de support et risque d'entraîner une instabilité ou une inaccessibilité des données.

Avant de commencer

- **Autorisations d'écriture** : vérifiez que vous disposez des autorisations d'écriture sur le répertoire de travail actuel.
- **(Facultatif) générez votre propre paire de clés** : exécutez `ssh-keygen` à partir de Windows 10, MacOS ou Linux distribution. Il s'agit d'une action unique pour créer une paire de clés utilisateur et peut être réutilisée pour les sessions de dépannage futures. Vous pouvez utiliser des certificats associés aux comptes d'employés, qui fonctionneront également dans ce modèle.
- **Activer la fonctionnalité SSH sur le nœud de gestion** : pour activer la fonctionnalité d'accès à distance sur le mode de gestion, voir "cette rubrique". Pour les services de gestion version 2.18 ou ultérieure, la fonctionnalité d'accès à distance est désactivée par défaut sur le nœud de gestion.
- **Activer la fonctionnalité SSH sur le cluster de stockage** : pour activer la fonctionnalité d'accès à distance sur les nœuds du cluster de stockage, voir "cette rubrique".
- **Configuration du pare-feu** : si votre nœud de gestion est derrière un serveur proxy, les ports TCP suivants sont requis dans le fichier sshd.config :

Port TCP	Description	Direction de la connexion
443	Appels API/HTTPS pour le transfert du port inversé via le tunnel de support ouvert vers l'interface utilisateur Web	Nœud de gestion vers nœuds de stockage
22	Accès connexion SSH	Nœud de gestion, vers nœuds de stockage ou depuis les nœuds de stockage vers le nœud de gestion

Options de dépannage

- Dépanner un nœud de cluster
- Dépanner un nœud de cluster avec le support NetApp
- Dépannez un nœud qui ne fait pas partie du cluster

Dépanner un nœud de cluster

Vous pouvez effectuer un dépannage de base à l'aide du compte système sfreadonly :

Étapes

1. SSH vers le nœud de gestion à l'aide des informations d'identification de compte que vous avez sélectionnées lors de l'installation de la machine virtuelle du nœud de gestion.
2. Sur le nœud de gestion, accédez à `/sf/bin`.
3. Recherchez le script approprié pour votre système :
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

   > SignSshKeys.ps1 dépend de PowerShell 7 ou version ultérieure et SignSshKeys.py dépend de Python 3.6.0 ou version ultérieure et de "module requêtes".
   >
   > Le `SignSshKeys` script écrit `user`les fichiers , `user.pub` et `user-cert.pub` dans le répertoire de travail actuel, qui sont ensuite utilisés par la `ssh` commande. Cependant, lorsqu'un fichier de clé publique est fourni au script, seul un `<public_key>` fichier (`<public_key>`remplacé par le préfixe du fichier de clé publique transmis au script) est écrit dans le répertoire.

4. Exécutez le script sur le nœud de gestion pour générer le trousseau SSH. Le script active l'accès SSH à l'aide du compte système sfreadonly sur tous les nœuds du cluster.

   ```
   SignSshKeys --ip [ip address] --user [username] --duration [hours]
   --publickey [public key path]
   ```

   a. Remplacer la valeur entre crochets [ ] (y compris les crochets) pour chacun des paramètres suivants :

      > Vous pouvez utiliser le paramètre de forme abrégée ou complète.

      - **--ip | -i [adresse ip]** : adresse IP du nœud cible pour que l'API s'exécute.
      - **--user | -u [username]** : utilisateur de cluster utilisé pour exécuter l'appel d'API.
      - **(Facultatif) --duration | -d [heures]** : la durée pendant laquelle une clé signée doit rester valide comme un entier en heures. La valeur par défaut est de 24 heures.
      - **(Facultatif) --publickey | -k [chemin de clé publique]** : le chemin d'accès à une clé publique, si l'utilisateur choisit d'en fournir une.

   b. Comparez votre entrée à l'exemple de commande suivant. Dans cet exemple, `10.116.139.195` est l'adresse IP du nœud de stockage, `admin` est le nom d'utilisateur du cluster et la durée de validité de la clé est de deux heures :

      ```
      sh /sf/bin/SignSshKeys.sh --ip 10.116.139.195 --user admin --duration
      2
      ```

c. Lancer la commande.

5. SSH vers les adresses IP de nœud :

```
ssh -i user sfreadonly@[node_ip]
```

Vous pourrez exécuter des commandes de dépannage de base du système Linux et du réseau, telles que `ping`, et d'autres commandes en lecture seule.

6. (Facultatif) désactivez "fonctionnalité d'accès à distance" à nouveau une fois le dépannage terminé.

> Si vous ne désactivez pas SSH, l'option SSH reste activée sur le nœud de gestion. La configuration SSH activée persiste sur le nœud de gestion via des mises à jour et des mises à niveau jusqu'à ce qu'elle soit désactivée manuellement.

Dépanner un nœud de cluster avec le support NetApp

Le support NetApp peut effectuer un dépannage avancé après un compte système qui permet au technicien d'exécuter des diagnostics plus approfondis des éléments.

Étapes

1. SSH vers le nœud de gestion à l'aide des informations d'identification de compte que vous avez sélectionnées lors de l'installation de la machine virtuelle du nœud de gestion.
2. Exécutez la commande rst avec le numéro de port envoyé par le support NetApp pour ouvrir le tunnel de support :

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

Le support NetApp se connecte à votre nœud de gestion via le tunnel de support.

3. Sur le nœud de gestion, accédez à `/sf/bin`.
4. Recherchez le script approprié pour votre système :
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

> SignSshKeys.ps1 dépend de PowerShell 7 ou version ultérieure et SignSshKeys.py dépend de Python 3.6.0 ou version ultérieure et de "module requêtes".
>
> Le `SignSshKeys` script écrit `user`les fichiers , `user.pub` et `user-cert.pub` dans le répertoire de travail actuel, qui sont ensuite utilisés par la `ssh` commande. Cependant, lorsqu'un fichier de clé publique est fourni au script, seul un `<public_key>` fichier (`<public_key>`remplacé par le préfixe du fichier de clé publique transmis au script) est écrit dans le répertoire.

5. Exécutez le script pour générer le trousseau SSH avec l' `--sfadmin`indicateur. Le script active SSH sur tous les nœuds.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--sfadmin
```

Pour établir une connexion SSH en tant que `--sfadmin` nœud en cluster, vous devez générer le trousseau SSH en utilisant un `--user` avec `supportAdmin` accès sur le cluster.

Pour configurer l' `supportAdmin`accès aux comptes d'administrateur du cluster, vous pouvez utiliser l'interface utilisateur ou les API d'Element :

- "Configurez l'accès « supportAdmin » à l'aide de l'interface utilisateur Element"
- Configurer l' `supportAdmin`accès à l'aide d'API et en ajoutant `"supportAdmin" comme "access" type dans la requête d'API :
  - "Configurez l'accès « supportAdmin » pour un nouveau compte"
  - "Configurez l'accès « supportAdmin » pour un compte existant"

    Pour obtenir le `clusterAdminID`, vous pouvez utiliser l'"ListClusterAdmins"API.

Pour ajouter un `supportAdmin` accès, vous devez disposer d'un administrateur de cluster ou d'un Privileges administrateur.

a. Remplacer la valeur entre crochets [ ] (y compris les crochets) pour chacun des paramètres suivants :

   Vous pouvez utiliser le paramètre de forme abrégée ou complète.

   - **--ip | -i [adresse ip]** : adresse IP du nœud cible pour que l'API s'exécute.
   - **--user | -u [username]** : utilisateur de cluster utilisé pour exécuter l'appel d'API.
   - **(Facultatif) --duration | -d [heures]** : la durée pendant laquelle une clé signée doit rester valide comme un entier en heures. La valeur par défaut est de 24 heures.

b. Comparez votre entrée à l'exemple de commande suivant. Dans cet exemple `192.168.0.1`, est l'IP du nœud de stockage, `admin` est le nom d'utilisateur du cluster, la durée de validité de la clé est de deux heures et `--sfadmin` permet au nœud de support NetApp d'accéder à des fins de dépannage :

```
sh /sf/bin/SignSshKeys.sh --ip 192.168.0.1 --user admin --duration 2
--sfadmin
```

c. Lancer la commande.

6. SSH vers les adresses IP de nœud :

```
ssh -i user sfadmin@[node_ip]
```

7. Pour fermer le tunnel de support à distance, entrez ce qui suit :

```
rst --killall
```

8. (Facultatif) désactivez "fonctionnalité d'accès à distance" à nouveau une fois le dépannage terminé.

> Si vous ne désactivez pas SSH, l'option SSH reste activée sur le nœud de gestion. La configuration SSH activée persiste sur le nœud de gestion via des mises à jour et des mises à niveau jusqu'à ce qu'elle soit désactivée manuellement.

Dépannez un nœud qui ne fait pas partie du cluster

Vous pouvez effectuer le dépannage de base d'un nœud qui n'a pas encore été ajouté à un cluster. Vous pouvez utiliser le compte système sfreadonly pour utiliser ce compte avec ou sans l'aide du support NetApp. Si un nœud de gestion est configuré, vous pouvez l'utiliser pour SSH et exécuter le script fourni pour cette tâche.

1. Depuis un ordinateur Windows, Linux ou Mac sur lequel un client SSH est installé, exécutez le script approprié pour votre système fourni par le support NetApp.
2. SSH sur l'IP du nœud :

```
ssh -i user sfreadonly@[node_ip]
```

3. (Facultatif) désactivez "fonctionnalité d'accès à distance" à nouveau une fois le dépannage terminé.

> Si vous ne désactivez pas SSH, l'option SSH reste activée sur le nœud de gestion. La configuration SSH activée persiste sur le nœud de gestion via des mises à jour et des mises à niveau jusqu'à ce qu'elle soit désactivée manuellement.

Trouvez plus d'informations

- "Plug-in NetApp Element pour vCenter Server"
- "Page Ressources NetApp HCI"

Démarrer une session de support NetApp à distance

Si vous avez besoin d'un support technique pour votre système de stockage 100 % Flash SolidFire, le support NetApp peut se connecter à distance à votre système. Pour démarrer une session et obtenir un accès à distance, le support NetApp peut ouvrir une connexion SSH (reverse Secure Shell) à votre environnement.

Vous pouvez ouvrir un port TCP pour une connexion en tunnel SSH inversé avec le support NetApp. Cette connexion permet au support NetApp de se connecter à votre nœud de gestion.

Avant de commencer

- Pour les services de gestion version 2.18 ou ultérieure, la fonctionnalité d'accès à distance est désactivée par défaut sur le nœud de gestion. Pour activer la fonctionnalité d'accès à distance, reportez-vous àla section "Gérez la fonctionnalité SSH sur le nœud de gestion".
- Si votre nœud de gestion est derrière un serveur proxy, les ports TCP suivants sont requis dans le fichier sshd.config :

Port TCP	Description	Direction de la connexion
443	Appels API/HTTPS pour le transfert du port inversé via le tunnel de support ouvert vers l'interface utilisateur Web	Nœud de gestion vers nœuds de stockage
22	Accès connexion SSH	Nœud de gestion, vers nœuds de stockage ou depuis les nœuds de stockage vers le nœud de gestion

Étapes

- Connectez-vous à votre nœud de gestion et ouvrez une session de terminal.
- À l'invite, entrez les informations suivantes :

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

- Pour fermer le tunnel de support à distance, entrez ce qui suit :

```
rst --killall
```

- (Facultatif) Désactiver "fonctionnalité d'accès à distance" à nouveau.

> Si vous ne désactivez pas SSH, l'option SSH reste activée sur le nœud de gestion. La configuration SSH activée persiste sur le nœud de gestion via des mises à jour et des mises à niveau jusqu'à ce qu'elle soit désactivée manuellement.

Trouvez plus d'informations

- "Plug-in NetApp Element pour vCenter Server"
- "Documentation SolidFire et Element"

Gérez la fonctionnalité SSH sur le nœud de gestion

Vous pouvez désactiver, réactiver ou déterminer l'état de la fonctionnalité SSH sur le nœud de gestion (nœud M) à l'aide de l'API REST. La fonctionnalité SSH "Accès à la session de tunnel de support à distance (RST) de NetApp"de est désactivée par défaut sur les nœuds de gestion exécutant les services de gestion version 2.18 ou ultérieure.

Depuis les services de gestion 2.20.69, vous pouvez activer et désactiver la fonctionnalité SSH sur le nœud de gestion à l'aide de l'interface utilisateur NetApp Hybrid Cloud Control.

Ce dont vous avez besoin

- **Permissions de contrôle de cloud hybride NetApp** : vous disposez d'autorisations en tant qu'administrateur.
- **Autorisations d'administrateur de cluster** : vous disposez d'autorisations en tant qu'administrateur sur le cluster de stockage.
- **Logiciel Element** : votre cluster exécute le logiciel NetApp Element version 11.3 ou ultérieure.

- **Noeud de gestion** : vous avez déployé un noeud de gestion exécutant la version 11.3 ou ultérieure.
- **Mises à jour des services de gestion** :
  - Pour utiliser l'interface de contrôle du cloud hybride NetApp, vous avez mis à jour votre "pack de services de gestion" vers la version 2.20.69 ou ultérieure.
  - Pour utiliser l'interface utilisateur de l'API REST, vous avez mis à jour votre "pack de services de gestion" vers la version 2.17.

Options

- Désactivez ou activez la fonctionnalité SSH sur le nœud de gestion à l'aide de l'interface utilisateur NetApp Hybrid Cloud Control

Vous pouvez effectuer l'une des tâches suivantes après "authentifier":

- Désactivez ou activez la fonctionnalité SSH sur le nœud de gestion à l'aide d'API
- Détermination de l'état de la fonctionnalité SSH sur le nœud de gestion à l'aide d'API

Désactivez ou activez la fonctionnalité SSH sur le nœud de gestion à l'aide de l'interface utilisateur NetApp Hybrid Cloud Control

Vous pouvez désactiver ou réactiver la fonctionnalité SSH sur le nœud de gestion. La fonctionnalité SSH "Accès à la session de tunnel de support à distance (RST) de NetApp"de est désactivée par défaut sur les nœuds de gestion exécutant les services de gestion version 2.18 ou ultérieure. La désactivation de SSH ne met pas fin ou ne déconnecte pas les sessions client SSH existantes vers le nœud de gestion. Si vous désactivez SSH et choisissez de le réactiver ultérieurement, vous pouvez utiliser l'interface de contrôle du cloud hybride NetApp.

Pour activer ou désactiver l'accès de support à l'aide de SSH pour un cluster de stockage, vous devez utiliser "Page des paramètres de cluster de l'interface utilisateur Element".

Étapes

1. Dans le Tableau de bord, sélectionnez le menu d'options en haut à droite et sélectionnez **configurer**.
2. Dans l'écran **support Access for Management Node**, activez le commutateur pour activer SSH du noeud de gestion.
3. Une fois le dépannage terminé, dans l'écran **support Access for Management Node**, activez le commutateur pour désactiver le nœud de gestion SSH.

Désactivez ou activez la fonctionnalité SSH sur le nœud de gestion à l'aide d'API

Vous pouvez désactiver ou réactiver la fonctionnalité SSH sur le nœud de gestion. La fonctionnalité SSH "Accès à la session de tunnel de support à distance (RST) de NetApp"de est désactivée par défaut sur les nœuds de gestion exécutant les services de gestion version 2.18 ou ultérieure. La désactivation de SSH ne met pas fin ou ne déconnecte pas les sessions client SSH existantes vers le nœud de gestion. Si vous désactivez SSH et choisissez de le réactiver ultérieurement, vous pouvez le faire à l'aide de la même API.

Commande API

Pour les services de gestion version 2.18 ou ultérieure :

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Pour les services de gestion version 2.17 ou antérieure :

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Vous pouvez trouver le support `${TOKEN}` utilisé par la commande API lorsque vous "autoriser". Le support `${TOKEN}` est dans la réponse de boucle.

ÉTAPES DE L'INTERFACE UTILISATEUR DE L'API REST

1. Accédez à l'interface utilisateur de l'API REST pour le service d'API du nœud de gestion en saisissant l'adresse IP du nœud de gestion suivie de `/mnode/` :

   ```
   https://<ManagementNodeIP>/mnode/
   ```

2. Sélectionnez **Authorise** et procédez comme suit :
   a. Saisissez le nom d'utilisateur et le mot de passe du cluster.
   b. Entrez l'ID client comme `mnode-client`.
   c. Sélectionnez **Autoriser** pour démarrer une session.
   d. Fermez la fenêtre.
3. Dans l'interface utilisateur de l'API REST, sélectionnez **PUT /settings/ssh**.
   a. Sélectionnez **essayez-le**.
   b. Définissez le paramètre **enabled** sur `false` pour désactiver SSH ou `true` réactiver la capacité SSH précédemment désactivée.
   c. Sélectionnez **Exécuter**.

Détermination de l'état de la fonctionnalité SSH sur le nœud de gestion à l'aide d'API

Vous pouvez déterminer si la fonctionnalité SSH est activée ou non sur le nœud de gestion à l'aide d'une API de service de nœud de gestion. SSH est désactivé par défaut sur les nœuds de gestion exécutant les services de gestion 2.18 ou version ultérieure.

Commande API

Pour les services de gestion version 2.18 ou ultérieure :

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Pour les services de gestion version 2.17 ou antérieure :

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Vous pouvez trouver le support `${TOKEN}` utilisé par la commande API lorsque vous "autoriser". Le support `${TOKEN}` est dans la réponse de boucle.

ÉTAPES DE L'INTERFACE UTILISATEUR DE L'API REST

1. Accédez à l'interface utilisateur de l'API REST pour le service d'API du nœud de gestion en saisissant l'adresse IP du nœud de gestion suivie de `/mnode/` :

   ```
   https://<ManagementNodeIP>/mnode/
   ```

2. Sélectionnez **Authorise** et procédez comme suit :
   a. Saisissez le nom d'utilisateur et le mot de passe du cluster.
   b. Entrez l'ID client comme `mnode-client`.
   c. Sélectionnez **Autoriser** pour démarrer une session.
   d. Fermez la fenêtre.
3. Dans l'interface utilisateur de l'API REST, sélectionnez **GET /settings/ssh**.
   a. Sélectionnez **essayez-le**.
   b. Sélectionnez **Exécuter**.

Trouvez plus d'informations

- "Plug-in NetApp Element pour vCenter Server"
- "Documentation SolidFire et Element"

Informations sur le copyright

Informations sur les marques commerciales