



Collaborer avec le nœud de gestion

Element Software

NetApp
November 12, 2025

Sommaire

Collaborer avec le nœud de gestion	1
Vue d'ensemble du nœud de gestion	1
Installer ou récupérer un nœud de gestion	2
Installer un nœud de gestion	2
Créez un rôle NetApp HCC dans vCenter.	8
Configurer un contrôleur d'interface réseau (NIC) de stockage	14
Récupérer un nœud de gestion	16
Accédez au nœud de gestion	21
Accéder à l'interface utilisateur du nœud de gestion	21
Accédez à l'interface utilisateur de l'API REST du nœud de gestion	22
Modifier le certificat SSL par défaut du nœud de gestion	23
Trouver plus d'informations	24
Utiliser l'interface utilisateur du nœud de gestion	24
Aperçu de l'interface utilisateur du nœud de gestion	24
Configurer la surveillance des alertes	25
Modifier et tester les paramètres du réseau, du cluster et du système du nœud de gestion	25
Exécutez les utilitaires système à partir du nœud de gestion	27
Utilisez l'API REST du nœud de gestion	28
Présentation de l'interface utilisateur de l'API REST du nœud de gestion	28
Obtenir l'autorisation d'utiliser les API REST	29
Activer la surveillance Active IQ et NetApp	30
Configurer NetApp Hybrid Cloud Control pour plusieurs vCenters	33
Ajouter une ressource de contrôleur au nœud de gestion	34
Créer et gérer des ressources de cluster de stockage	35
Afficher ou modifier les ressources de contrôleur existantes	41
Configurer un serveur proxy	42
Vérifier les versions du système d'exploitation et des services du nœud de gestion	44
Récupération des journaux des services de gestion	45
Gérer les connexions d'assistance	46
Accès aux nœuds de stockage via SSH pour le dépannage de base	46
Démarrer une session d'assistance NetApp à distance	51
Gérer la fonctionnalité SSH sur le nœud de gestion	52

Collaborer avec le nœud de gestion

Vue d'ensemble du nœud de gestion

Vous pouvez utiliser le nœud de gestion (mNode) pour utiliser les services système, gérer les ressources et les paramètres du cluster, exécuter des tests et des utilitaires système, configurer Active IQ pour la surveillance du système et activer l'accès au support NetApp pour le dépannage.



Il est recommandé, par mesure de précaution, d'associer un seul nœud de gestion à une seule instance VMware vCenter et d'éviter de définir les mêmes ressources de stockage et de calcul ou les mêmes instances vCenter sur plusieurs nœuds de gestion.

Pour les clusters exécutant la version 11.3 ou ultérieure du logiciel Element, vous pouvez interagir avec le nœud de gestion en utilisant l'une des deux interfaces suivantes :

- Avec l'interface utilisateur du nœud de gestion([https://\[mNode IP\]:442](https://[mNode IP]:442)), vous pouvez modifier les paramètres réseau et de cluster, exécuter des tests système ou utiliser les utilitaires système.
- Avec l'interface utilisateur de l'API REST intégrée([https://\[mNode IP\]/mnode](https://[mNode IP]/mnode)), vous pouvez exécuter ou comprendre les API relatives aux services du nœud de gestion, notamment la configuration du serveur proxy, les mises à jour du niveau de service ou la gestion des actifs.

Installer ou récupérer un nœud de gestion :

- "["Installer un nœud de gestion"](#)
- "["Configurer un contrôleur d'interface réseau \(NIC\) de stockage"](#)
- "["Récupérer un nœud de gestion"](#)

Accédez au nœud de gestion :

- "["Accéder au nœud de gestion \(interface utilisateur ou API REST\)"](#)

Modifier le certificat SSL par défaut :

- "["Modifier le certificat SSL par défaut du nœud de gestion"](#)

Effectuez des tâches avec l'interface utilisateur du nœud de gestion :

- "["Aperçu de l'interface utilisateur du nœud de gestion"](#)

Effectuez des tâches avec les API REST du nœud de gestion :

- "["Présentation de l'interface utilisateur de l'API REST du nœud de gestion"](#)

Activez ou désactivez la fonctionnalité SSH à distance ou démarrez une session de tunnel d'assistance à distance avec le support NetApp pour vous aider à résoudre le problème :

- "["Accès aux nœuds de stockage via SSH pour le dépannage de base"](#)
 - "["Activer les connexions d'assistance NetApp à distance"](#)
 - "["Gérer la fonctionnalité SSH sur le nœud de gestion"](#)

Trouver plus d'informations

- ["Module d'extension NetApp Element pour vCenter Server"](#)
- ["Documentation logicielle SolidFire et Element"](#)

Installer ou récupérer un nœud de gestion

Installer un nœud de gestion

Vous pouvez installer manuellement le nœud de gestion de votre cluster exécutant le logiciel NetApp Element en utilisant l'image appropriée à votre configuration.

Cette procédure manuelle est destinée aux administrateurs de stockage 100 % flash SolidFire qui n'utilisent pas le moteur de déploiement NetApp pour l'installation du nœud de gestion.

Avant de commencer

- Votre version de cluster exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
- Votre installation utilise IPv4. Le nœud de gestion 11.3 ne prend pas en charge IPv6.



Si vous avez besoin de la prise en charge IPv6, vous pouvez utiliser le nœud de gestion 11.1.

- Vous êtes autorisé à télécharger des logiciels depuis le site d'assistance NetApp .
- Vous avez identifié le type d'image de nœud de gestion qui convient à votre plateforme :

Plate-forme	type d'image d'installation
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

- (Nœud de gestion 12.0 et versions ultérieures avec serveur proxy) Vous avez mis à jour NetApp Hybrid Cloud Control vers la version 2.16 des services de gestion avant de configurer un serveur proxy.

À propos de cette tâche

Le nœud de gestion Element 12.2 est une mise à niveau optionnelle. Cela n'est pas nécessaire pour les déploiements existants.

Avant de suivre cette procédure, vous devez comprendre "[Volumes persistants](#)" et que vous souhaitez ou non les utiliser. Les volumes persistants sont optionnels mais recommandés pour la récupération des données de configuration du nœud de gestion en cas de perte d'une machine virtuelle (VM).

Étape 1 : Téléchargez l'ISO ou l'OVA et déployez la machine virtuelle.

Téléchargez le fichier ISO ou OVA approprié depuis le site de support NetApp et installez la machine virtuelle.

Étapes

1. Téléchargez le fichier OVA ou ISO pour votre installation depuis le site web "[Element Software](#)" page sur le site d'assistance NetApp .
 - a. Sélectionnez **Télécharger la dernière version** et acceptez le CLUF.
 - b. Sélectionnez l'image du nœud de gestion que vous souhaitez télécharger.
2. Si vous avez téléchargé le fichier OVA, suivez ces étapes :
 - a. Déployez l'OVA.
 - b. Si votre cluster de stockage se trouve sur un sous-réseau distinct de votre nœud de gestion (eth0) et que vous souhaitez utiliser des volumes persistants, ajoutez un deuxième contrôleur d'interface réseau (NIC) à la VM sur le sous-réseau de stockage (par exemple, eth1) ou assurez-vous que le réseau de gestion peut router vers le réseau de stockage.
3. Si vous avez téléchargé l'ISO, suivez ces étapes :
 - a. Créez une nouvelle machine virtuelle 64 bits à partir de votre hyperviseur avec la configuration suivante :
 - Six processeurs virtuels
 - 24 Go de RAM
 - Type d'adaptateur de stockage défini sur LSI Logic Parallel



Le système de gestion par défaut de votre nœud peut être LSI Logic SAS. Dans la fenêtre **Nouvelle machine virtuelle**, vérifiez la configuration de l'adaptateur de stockage en sélectionnant **Personnaliser le matériel > Matériel virtuel**. Si nécessaire, remplacez LSI Logic SAS par **LSI Logic Parallel**.

- Disque virtuel de 400 Go, provisionnement dynamique
- Une interface réseau virtuelle avec accès internet et accès au stockage MVIP.
- (Optionnel) Une interface réseau virtuelle avec accès au réseau de gestion du cluster de stockage. Si votre cluster de stockage se trouve sur un sous-réseau distinct de votre nœud de gestion (eth0) et que vous souhaitez utiliser des volumes persistants, ajoutez un deuxième contrôleur d'interface réseau (NIC) à la VM sur le sous-réseau de stockage (eth1) ou assurez-vous que le réseau de gestion peut router vers le réseau de stockage.



N'allumez pas la machine virtuelle avant l'étape qui vous invitera à le faire plus loin dans cette procédure.

- b. Attachez l'ISO à la VM et démarrez sur l'image d'installation .iso.



L'installation d'un nœud de gestion à l'aide de cette image peut entraîner un délai de 30 secondes avant l'affichage de l'écran de démarrage.

4. Mettez sous tension la machine virtuelle du nœud de gestion une fois l'installation terminée.

Étape 2 : Créer le nœud d'administration et configurer le réseau

Une fois l'installation de la machine virtuelle terminée, créez l'utilisateur administrateur du nœud de gestion et configuez le réseau du nœud de gestion.

Étapes

1. À l'aide de l'interface utilisateur du terminal (TUI), créez un utilisateur administrateur de nœud de gestion.



Pour naviguer dans les options du menu, appuyez sur les touches fléchées Haut ou Bas. Pour naviguer entre les boutons, appuyez sur Tab. Pour passer des boutons aux champs, appuyez sur la touche Tab. Pour naviguer entre les champs, appuyez sur les touches fléchées Haut ou Bas.

2. S'il existe un serveur DHCP (Dynamic Host Configuration Protocol) sur le réseau qui attribue des adresses IP avec une unité de transmission maximale (MTU) inférieure à 1500 octets, vous devez effectuer les étapes suivantes :

- Placez temporairement le nœud de gestion sur un réseau vSphere sans DHCP, tel que iSCSI.
- Redémarrez la machine virtuelle ou redémarrez le réseau de la machine virtuelle.
- À l'aide de l'interface utilisateur technique (TUI), configurez l'adresse IP correcte sur le réseau de gestion avec une MTU supérieure ou égale à 1500 octets.
- Réattribuez le réseau VM correct à la VM.



Un serveur DHCP attribuant des adresses IP avec une MTU inférieure à 1500 octets peut vous empêcher de configurer le réseau du nœud de gestion ou d'utiliser l'interface utilisateur du nœud de gestion.

3. Configurez le réseau du nœud de gestion (eth0).



Si vous avez besoin d'une carte réseau supplémentaire pour isoler le trafic de stockage, consultez les instructions relatives à la configuration d'une autre carte réseau : ["Configurer un contrôleur d'interface réseau \(NIC\) de stockage"](#).

Étape 3 : Configurer la synchronisation de l'heure

Avant de configurer le nœud de gestion, synchronisez l'heure entre le nœud de gestion et le cluster de stockage.

Étapes

1. Vérifiez que l'heure est synchronisée entre le nœud de gestion et le cluster de stockage à l'aide de NTP :



À partir de l'élément 12.3.1, les sous-étapes (a) à (e) sont exécutées automatiquement. Pour le nœud de gestion 12.3.1, passez à [sous-étape \(f\)](#) pour terminer la configuration de la synchronisation horaire.

1. Connectez-vous au nœud de gestion en utilisant SSH ou la console fournie par votre hyperviseur.

2. Stop NTPD :

```
sudo service ntpd stop
```

3. Modifier le fichier de configuration NTP /etc/ntp.conf :

- Commentez les serveurs par défaut(`server 0.gentoo.pool.ntp.org`) en ajoutant un # devant chacun.
- Ajoutez une nouvelle ligne pour chaque serveur de temps par défaut que vous souhaitez ajouter. Les serveurs de temps par défaut doivent être les mêmes serveurs NTP que ceux utilisés sur le cluster de

stockage que vous utiliserez dans un [étape ultérieure](#).

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

c. Enregistrez le fichier de configuration une fois terminé.

4. Forcez une synchronisation NTP avec le serveur nouvellement ajouté.

```
sudo ntpd -gq
```

5. Redémarrez NTPD.

```
sudo service ntpd start
```

6. Désactiver la synchronisation de l'heure avec l'hôte via l'hyperviseur (voici un exemple VMware) :



Si vous déployez le mNode dans un environnement d'hyperviseur autre que VMware, par exemple à partir de l'image .iso dans un environnement Openstack, reportez-vous à la documentation de l'hyperviseur pour connaître les commandes équivalentes.

a. Désactiver la synchronisation horaire périodique :

```
vmware-toolbox-cmd timesync disable
```

b. Afficher et confirmer l'état actuel du service :

```
vmware-toolbox-cmd timesync status
```

c. Dans vSphere, vérifiez que la **Synchronize guest time with host** La case correspondante est décochée dans les options de la machine virtuelle.



Ne pas activer cette option si vous apportez des modifications ultérieures à la machine virtuelle.



Ne modifiez pas le protocole NTP après avoir terminé la configuration de la synchronisation horaire, car cela affectera le protocole NTP lors de son exécution. [commande de configuration](#) sur le nœud de gestion.

Étape 4 : Configurer le nœud de gestion

Configurez le nœud de gestion à l'aide de `setup-mnode` commande.

Étapes

1. Configurez et exécutez la commande d'installation du nœud de gestion :

 Vous serez invité à saisir vos mots de passe dans une fenêtre sécurisée. Si votre cluster se trouve derrière un serveur proxy, vous devez configurer les paramètres du proxy pour pouvoir accéder à un réseau public.

```
sudo /sf/packages/mnode/setup-mnode --mnode_admin_user [username]
--storage_mvip [mvip] --storage_username [username] --telemetry_active
[true]
```

- a. Remplacez la valeur entre crochets [] (crochets compris) pour chacun des paramètres obligatoires suivants :



La forme abrégée du nom de la commande est entre parenthèses () et peut être substituée au nom complet.

- **--mnode_admin_user (-mu) [nom_utilisateur]**: Le nom d'utilisateur du compte administrateur du nœud de gestion. Il s'agit probablement du nom d'utilisateur du compte utilisateur que vous avez utilisé pour vous connecter au nœud de gestion.
- **--storage_mvip (-sm) [Adresse MVIP]**: L'adresse IP virtuelle de gestion (MVIP) du cluster de stockage exécutant le logiciel Element. Configurez le nœud de gestion avec le même cluster de stockage que celui que vous avez utilisé lors de [configuration des serveurs NTP](#).
- **--storage_username (-su) [nom_utilisateur]** : Nom d'utilisateur de l'administrateur du cluster de stockage pour le cluster spécifié par le `--storage_mvip` paramètre.
- **--telemetry_active (-t) [true]**: Conserver la valeur true qui active la collecte de données pour l'analyse par Active IQ.

- b. (Facultatif) : Ajoutez les paramètres de point de terminaison Active IQ à la commande :

- **--remote_host (-rh) [AIQ_endpoint]**: Le point de terminaison où les données de télémétrie Active IQ sont envoyées pour être traitées. Si le paramètre n'est pas inclus, le point de terminaison par défaut est utilisé.

- c. (Recommandé) : Ajoutez les paramètres de volume persistants suivants. Ne modifiez ni ne supprimez le compte et les volumes créés pour la fonctionnalité de volumes persistants, sous peine de perdre vos capacités de gestion.

- **--use_persistent_volumes (-pv) [true/false, default: false]**: Activer ou désactiver les volumes persistants. Saisissez la valeur « true » pour activer la fonctionnalité des volumes persistants.
- **--persistent_volumes_account (-pva) [nom_du_compte]**: Si `--use_persistent_volumes` est activée, utilisez ce paramètre et saisissez le nom du compte de stockage qui sera utilisé pour les volumes persistants.



Utilisez un nom de compte unique pour les volumes persistants, différent de tout nom de compte existant sur le cluster. Il est absolument essentiel de séparer le compte des volumes persistants du reste de votre environnement.

- **--persistent_volumes_mvip (-pvm) [mvip]**: Entrez l'adresse IP virtuelle de gestion (MVIP) du cluster de stockage exécutant le logiciel Element qui sera utilisée avec les volumes persistants. Cela n'est nécessaire que si plusieurs clusters de stockage sont gérés par le nœud de gestion. Si plusieurs clusters ne sont pas gérés, le cluster par défaut MVIP sera utilisé.

d. Configurer un serveur proxy :

- **--use_proxy (-up) [true/false, default: false]**: Activer ou désactiver l'utilisation du proxy. Ce paramètre est nécessaire pour configurer un serveur proxy.
- **--proxy_hostname_or_ip (-pi) [hôte]**: Le nom d'hôte ou l'adresse IP du proxy. Ceci est nécessaire si vous souhaitez utiliser un proxy. Si vous spécifiez cela, vous serez invité à saisir des informations. **--proxy_port** .
- **--proxy_username (-pu) [nom_utilisateur]**: Le nom d'utilisateur du proxy. Ce paramètre est facultatif.
- **--proxy_password (-pp) [mot_de_passe]**: Le mot de passe du proxy. Ce paramètre est facultatif.
- **--proxy_port (-pq) [port, par défaut : 0]**: Le port proxy. Si vous spécifiez cette option, vous serez invité à saisir le nom d'hôte ou l'adresse IP du proxy. (**--proxy_hostname_or_ip**).
- **--proxy_ssh_port (-ps) [port, par défaut : 443]** : Le port du proxy SSH. Par défaut, le port utilisé est le 443.

e. (Facultatif) Utilisez l'aide relative aux paramètres si vous avez besoin d'informations supplémentaires sur chaque paramètre :

- **--help (-h)**: Renvoie des informations sur chaque paramètre. Les paramètres sont définis comme obligatoires ou facultatifs en fonction du déploiement initial. Les exigences relatives aux paramètres de mise à niveau et de redéploiement peuvent varier.

f. Exécutez la `setup-mnode` commande.

Étape 5 : Configurer les ressources du contrôleur

Localisez l'ID d'installation et ajoutez une ressource de contrôleur vCenter.

Étapes

1. Localisez l'identifiant d'installation :

- Depuis un navigateur, connectez-vous à l'interface utilisateur de l'API REST du nœud de gestion :
- Accédez au serveur MVIP de stockage et connectez-vous. Cette action permettra d'accepter le certificat pour l'étape suivante.
- Ouvrez l'interface utilisateur de l'API REST du service d'inventaire sur le nœud de gestion :

```
https://<ManagementNodeIP>/inventory/1/
```

d. Sélectionnez **Autoriser** et complétez les informations suivantes :

- Saisissez le nom d'utilisateur et le mot de passe du cluster.
- Saisissez l'identifiant du client comme `mnode-client` .
- Sélectionnez **Autoriser** pour démarrer une session.

e. Dans l'interface utilisateur de l'API REST, sélectionnez **GET /installations**.

f. Sélectionnez **Essayer**.

- g. Sélectionnez **Exécuter**.
- h. À partir du corps de la réponse du code 200, copiez et enregistrez le `id` pour l'installation en vue d'une utilisation ultérieure.
- Votre installation possède une configuration de ressources de base qui a été créée lors de l'installation ou de la mise à niveau.
2. Ajoutez un contrôleur vCenter pour NetApp Hybrid Cloud Control aux ressources connues du nœud de gestion :
- Accédez à l'interface utilisateur de l'API du service `mnode` sur le nœud de gestion en saisissant l'adresse IP du nœud de gestion suivie de `/mnode` :

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

- Sélectionnez **Autoriser** ou toute icône de verrouillage et procédez comme suit :
 - Saisissez le nom d'utilisateur et le mot de passe du cluster.
 - Saisissez l'identifiant du client comme `mnode-client`.
 - Sélectionnez **Autoriser** pour démarrer une session.
 - Ferme la fenêtre.
- Sélectionnez **POST /assets/{asset_id}/controllers** pour ajouter un sous-élément de contrôleur.



Vous devez créer un nouveau rôle NetApp HCC dans vCenter pour ajouter un sous-actif de contrôleur. Ce nouveau rôle NetApp HCC limitera la vue des services du nœud de gestion aux seuls actifs NetApp. Voir "[Créez un rôle NetApp HCC dans vCenter](#)." .

- Sélectionnez **Essayer**.
- Saisissez l'identifiant de l'actif de base parent que vous avez copié dans votre presse-papiers dans le champ **asset_id**.
- Saisissez les valeurs de charge utile requises avec le type `vCenter` et les identifiants vCenter.
- Sélectionnez **Exécuter**.

Pour en savoir plus, consultez les informations disponibles.

- ["Volumes persistants"](#)
- ["Ajouter une ressource de contrôleur au nœud de gestion"](#)
- ["Configurer une carte réseau de stockage"](#)
- ["Module d'extension NetApp Element pour vCenter Server"](#)
- ["Documentation logicielle SolidFire et Element"](#)

Créez un rôle NetApp HCC dans vCenter.

Vous devez créer un rôle NetApp HCC dans vCenter pour ajouter manuellement des ressources vCenter (contrôleurs) au nœud de gestion après l'installation ou pour modifier les contrôleurs existants.

Ce rôle NetApp HCC limite la vue des services de votre nœud de gestion aux seules ressources NetApp.

À propos de cette tâche

- Cette procédure décrit les étapes disponibles dans la version 6.7 de vSphere. L'interface utilisateur de votre vSphere peut différer légèrement de celle décrite, selon la version de vSphere installée. Pour obtenir de l'aide supplémentaire, consultez la documentation de VMware vCenter.
- À "créer un nouveau rôle NetApp HCC" Vous devez d'abord configurer un nouveau compte utilisateur dans vCenter, créer un rôle NetApp HCC, puis attribuer les autorisations à l'utilisateur.
- Pour les configurations d'hôtes NetApp ESXi, vous devez mettre à jour le compte utilisateur créé par NDE avec le nouveau rôle NetApp HCC :
 - Utiliser "cette option" si votre hôte NetApp ESXi ne se trouve pas dans un cluster d'hôtes vCenter
 - Utiliser "cette option" si votre hôte NetApp ESXi se trouve à l'intérieur d'un cluster d'hôtes vCenter
- Tu peux "configurer une ressource de contrôleur" qui existe déjà sur le nœud de gestion.
- Utilisez le nouveau rôle NetApp HCC pour "ajouter un actif" au nœud de gestion.

Créer un nouveau rôle NetApp HCC

Configurez un nouveau compte utilisateur dans vCenter, créez un rôle NetApp HCC, puis attribuez les autorisations à l'utilisateur.

Créez un nouveau compte utilisateur dans vCenter.

Pour créer un nouveau compte utilisateur dans vCenter, procédez comme suit.

Étapes

1. Connectez-vous au client Web vSphere en tant que `administrator@vsphere.local` ou équivalent.
2. Dans le menu, sélectionnez **Administration**.
3. Dans la section **Authentification unique**, sélectionnez **Utilisateurs et Groupes**.
4. Dans la liste **Domaine**, sélectionnez `vsphere.local` ou votre domaine LDAP.
5. Sélectionnez **Ajouter un utilisateur**.
6. Remplissez le formulaire **Ajouter un utilisateur**.

Créez un nouveau rôle NetApp HCC dans vCenter.

Pour créer un nouveau rôle NetApp HCC dans vCenter, procédez comme suit.

Étapes

1. Sélectionnez **Modifier le rôle** et attribuez les autorisations requises.
2. Dans le volet de navigation de gauche, sélectionnez **Global**.
3. Sélectionnez **Diagnostics et Licences**.
4. Dans le volet de navigation de gauche, sélectionnez **Hôtes**.
5. Sélectionnez **Maintenance, Alimentation, Configuration de la partition de stockage et Micrologiciel**.
6. Enregistrer sous **NetApp Role**.

Attribuer des autorisations utilisateur à vCenter

Pour attribuer les autorisations utilisateur au nouveau rôle NetApp HCC dans vCenter, procédez comme suit.

Étapes

1. Dans le menu, sélectionnez **Hôtes et Clusters**.
2. Dans le volet de navigation de gauche, sélectionnez l'une des options suivantes :
 - Le vCenter de niveau supérieur.
 - Votre vCenter souhaité si vous êtes en mode lié.
 - À partir du plug-in NetApp Element pour vCenter Server 5.0, pour utiliser "[Mode lié vCenter](#)", vous enregistrez le plug-in Element à partir d'un nœud de gestion distinct pour chaque serveur vCenter qui gère les clusters de stockage NetApp SolidFire (recommandé).
 - Utilisation du plug-in NetApp Element pour vCenter Server 4.10 et versions antérieures afin de gérer les ressources du cluster à partir d'autres serveurs vCenter. "[Mode lié vCenter](#)" est limité aux clusters de stockage locaux uniquement.

3. Dans le volet de navigation de droite, sélectionnez **Permissions**.

4. Sélectionnez l'icône **+** pour ajouter le nouvel utilisateur.

Ajoutez les informations suivantes dans la fenêtre **Ajouter une autorisation** :

- a. Sélectionner `vsphere.local` ou votre domaine LDAP
- b. Utilisez la recherche pour trouver le nouvel utilisateur que vous avez créé dans [Créez un nouveau compte utilisateur dans vCenter](#).
- c. Sélectionner **NetApp Role**.



Ne sélectionnez **PAS Propager aux enfants**.

Add Permission

satyabra-vcenter01.mgmt.ict.openengla... X

User

vsphere.local

netapp

Role

NetApp Role

Propagate to children

CANCEL

OK

Attribuer des autorisations utilisateur au centre de données

Pour attribuer les autorisations utilisateur au centre de données dans vCenter, procédez comme suit.

Étapes

1. Dans le volet de gauche, sélectionnez **Centre de données**.
2. Dans le volet de navigation de droite, sélectionnez **Permissions**.
3. Sélectionnez l'icône **+** pour ajouter le nouvel utilisateur.

Ajoutez les informations suivantes dans la fenêtre **Ajouter une autorisation** :

- a. Sélectionner **vsphere.local** ou votre domaine LDAP.
- b. Utilisez la recherche pour trouver le nouvel utilisateur HCC que vous avez créé dans [Créez un nouveau compte utilisateur dans vCenter](#).
- c. Sélectionner **ReadOnly** role.



Ne sélectionnez **PAS Propager aux enfants**.

Attribuer des autorisations utilisateur aux banques de données NetApp HCI

Pour attribuer les autorisations utilisateur aux banques de données NetApp HCI dans vCenter, procédez comme suit.

Étapes

1. Dans le volet de gauche, sélectionnez **Centre de données**.

2. Créez un nouveau dossier de stockage. Faites un clic droit sur **Datacenter** et sélectionnez **Créer un dossier de stockage**.
 3. Transférez tous les datastores NetApp HCI du cluster de stockage et du nœud de calcul local vers le nouveau dossier de stockage.
 4. Sélectionnez le nouveau dossier de stockage.
 5. Dans le volet de navigation de droite, sélectionnez **Permissions**.
 6. Sélectionnez l'icône **+** pour ajouter le nouvel utilisateur.
- Ajoutez les informations suivantes dans la fenêtre **Ajouter une autorisation** :
- a. Sélectionner `vsphere.local` ou votre domaine LDAP.
 - b. Utilisez la recherche pour trouver le nouvel utilisateur HCC que vous avez créé dans [Créez un nouveau compte utilisateur dans vCenter](#).
 - c. Sélectionner `Administrator` role
 - d. Sélectionnez **Propager aux enfants**.

Attribuer des autorisations utilisateur à un cluster d'hôtes NetApp

Pour attribuer les autorisations utilisateur à un cluster d'hôtes NetApp dans vCenter, procédez comme suit.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez le cluster hôte NetApp .
2. Dans le volet de navigation de droite, sélectionnez **Permissions**.
3. Sélectionnez l'icône **+** pour ajouter le nouvel utilisateur.

Ajoutez les informations suivantes dans la fenêtre **Ajouter une autorisation** :

- a. Sélectionner `vsphere.local` ou votre domaine LDAP.
- b. Utilisez la recherche pour trouver le nouvel utilisateur HCC que vous avez créé dans [Créez un nouveau compte utilisateur dans vCenter](#).
- c. Sélectionner `NetApp Role` ou `Administrator`.
- d. Sélectionnez **Propager aux enfants**.

Configurations hôtes NetApp ESXi

Pour les configurations d'hôtes NetApp ESXi, vous devez mettre à jour le compte utilisateur créé par NDE avec le nouveau rôle NetApp HCC.

L'hôte NetApp ESXi n'existe pas dans un cluster d'hôtes vCenter.

Si l'hôte NetApp ESXi n'existe pas dans un cluster d'hôtes vCenter, vous pouvez utiliser la procédure suivante pour attribuer le rôle NetApp HCC et les autorisations utilisateur dans vCenter.

Étapes

1. Dans le menu, sélectionnez **Hôtes et Clusters**.
2. Dans le volet de navigation de gauche, sélectionnez l'hôte NetApp ESXi.
3. Dans le volet de navigation de droite, sélectionnez **Permissions**.

4. Sélectionnez l'icône + pour ajouter le nouvel utilisateur.

Ajoutez les informations suivantes dans la fenêtre **Ajouter une autorisation** :

- a. Sélectionner vsphere.local ou votre domaine LDAP.
- b. Utilisez la recherche pour trouver le nouvel utilisateur que vous avez créé dans [Créez un nouveau compte utilisateur dans vCenter](#).
- c. Sélectionner NetApp Role ou Administrator.

5. Sélectionnez **Propager aux enfants**.

L'hôte NetApp ESXi se trouve dans un cluster d'hôtes vCenter.

Si un hôte NetApp ESXi existe au sein d'un cluster d'hôtes vCenter avec d'autres hôtes ESXi de fournisseurs différents, vous pouvez utiliser la procédure suivante pour attribuer le rôle NetApp HCC et les autorisations utilisateur dans vCenter.

1. Dans le menu, sélectionnez **Hôtes et Clusters**.
2. Dans le volet de navigation de gauche, développez le cluster hôte souhaité.
3. Dans le volet de navigation de droite, sélectionnez **Permissions**.
4. Sélectionnez l'icône + pour ajouter le nouvel utilisateur.

Ajoutez les informations suivantes dans la fenêtre **Ajouter une autorisation** :

- a. Sélectionner vsphere.local ou votre domaine LDAP.
- b. Utilisez la recherche pour trouver le nouvel utilisateur que vous avez créé dans [Créez un nouveau compte utilisateur dans vCenter](#).
- c. Sélectionner NetApp Role .



Ne sélectionnez **PAS Propager aux enfants**.

5. Dans le volet de navigation de gauche, sélectionnez un hôte NetApp ESXi.
6. Dans le volet de navigation de droite, sélectionnez **Permissions**.
7. Sélectionnez l'icône + pour ajouter le nouvel utilisateur.

Ajoutez les informations suivantes dans la fenêtre **Ajouter une autorisation** :

- a. Sélectionner vsphere.local ou votre domaine LDAP.
 - b. Utilisez la recherche pour trouver le nouvel utilisateur que vous avez créé dans [Créez un nouveau compte utilisateur dans vCenter](#).
 - c. Sélectionner NetApp Role ou Administrator .
 - d. Sélectionnez **Propager aux enfants**.
8. Répétez l'opération pour les autres hôtes NetApp ESXi du cluster.

La ressource du contrôleur existe déjà sur le nœud de gestion.

Si une ressource de contrôleur existe déjà sur le nœud de gestion, procédez comme suit pour configurer le contrôleur en utilisant `PUT /assets/{asset_id}/controllers/{controller_id}` .

Étapes

1. Accédez à l'interface utilisateur de l'API du service mnode sur le nœud de gestion :

<https://<ManagementNodeIP>/mnode>

2. Sélectionnez **Autoriser** et saisissez les identifiants pour accéder aux appels API.
3. Sélectionner GET /assets pour obtenir l'identifiant du parent.
4. Sélectionner PUT /assets/{asset_id}/controllers/{controller_id}.
 - a. Saisissez les identifiants créés lors de la configuration du compte dans le corps de la requête.

Ajouter un actif au nœud de gestion

Si vous devez ajouter manuellement un nouvel élément après l'installation, utilisez le nouveau compte utilisateur HCC que vous avez créé dans [Créez un nouveau compte utilisateur dans vCenter](#). Pour plus d'informations, voir "[Ajouter une ressource de contrôleur au nœud de gestion](#)".

Trouver plus d'informations

- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation logicielle SolidFire et Element](#)"

Configurer un contrôleur d'interface réseau (NIC) de stockage

Si vous utilisez une carte réseau supplémentaire pour le stockage, vous pouvez vous connecter en SSH au nœud de gestion ou utiliser la console vCenter et exécuter une commande curl pour configurer une interface réseau étiquetée ou non étiquetée.

Avant de commencer

- Vous connaissez votre adresse IP eth0.
- Votre version de cluster exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
- Vous avez déployé un nœud de gestion 11.3 ou ultérieur.

Options de configuration

Choisissez l'option qui correspond à votre environnement :

- [Configurer un contrôleur d'interface réseau \(NIC\) de stockage pour une interface réseau non étiquetée](#)
- [Configurer un contrôleur d'interface réseau \(NIC\) de stockage pour une interface réseau étiquetée](#)

Configurer un contrôleur d'interface réseau (NIC) de stockage pour une interface réseau non étiquetée

Étapes

1. Ouvrez une console SSH ou vCenter.
2. Remplacez les valeurs dans le modèle de commande suivant et exécutez la commande :



Les valeurs sont représentées par \$ pour chacun des paramètres requis pour votre nouvelle interface réseau de stockage. Le cluster L'objet figurant dans le modèle suivant est obligatoire et peut être utilisé pour renommer le nom d'hôte du nœud de gestion. --insecure ou -k Ces options ne doivent pas être utilisées dans les environnements de production.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d '{
  "params": {
    "network": {
      "$eth1": {
        "#default" : false,
        "address" : "$storage_IP",
        "auto" : true,
        "family" : "inet",
        "method" : "static",
        "mtu" : "9000",
        "netmask" : "$subnet_mask",
        "status" : "Up"
      }
    },
    "cluster": {
      "name": "$mnode_host_name"
    }
  },
  "method": "SetConfig"
}'
```



Les valeurs sont représentées par \$ pour chacun des paramètres requis pour votre nouvelle interface réseau de stockage. Le cluster L'objet figurant dans le modèle suivant est obligatoire et peut être utilisé pour renommer le nom d'hôte du nœud de gestion. --insecure ou -k Ces options ne doivent pas être utilisées dans les environnements de production.

Configurer un contrôleur d'interface réseau (NIC) de stockage pour une interface réseau étiquetée

Étapes

1. Ouvrez une console SSH ou vCenter.
2. Remplacez les valeurs dans le modèle de commande suivant et exécutez la commande :

```

curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
    "params": {
        "network": {
            "$eth1": {
                "#default" : false,
                "address" : "$storage_IP",
                "auto" : true,
                "family" : "inet",
                "method" : "static",
                "mtu" : "9000",
                "netmask" : "$subnet_mask",
                "status" : "Up",
                "virtualNetworkTag" : "$vlan_id"
            }
        },
        "cluster": {
            "name": "$mnode_host_name",
            "cipi": "$eth1.$vlan_id",
            "sipi": "$eth1.$vlan_id"
        }
    },
    "method": "SetConfig"
}
'

```

Pour en savoir plus, consultez les informations disponibles.

- ["Ajouter une ressource de contrôleur au nœud de gestion"](#)
- ["Module d'extension NetApp Element pour vCenter Server"](#)
- ["Documentation logicielle SolidFire et Element"](#)

Récupérer un nœud de gestion

Vous pouvez récupérer et redéployer manuellement le nœud de gestion de votre cluster exécutant le logiciel NetApp Element si votre nœud de gestion précédent utilisait des volumes persistants.

Vous pouvez déployer un nouvel OVA et exécuter un script de redéploiement pour récupérer les données de configuration d'un nœud de gestion précédemment installé exécutant la version 11.3 ou ultérieure.

Ce dont vous aurez besoin

- Votre nœud de gestion précédent exécutait le logiciel NetApp Element version 11.3 ou ultérieure avec "Volumes persistants" Fonctionnalité activée.
- Vous connaissez le MVIP et le SVIP du cluster contenant les volumes persistants.
- Votre version de cluster exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
- Votre installation utilise IPv4. Le nœud de gestion 11.3 ne prend pas en charge IPv6.
- Vous êtes autorisé à télécharger des logiciels depuis le site d'assistance NetApp .
- Vous avez identifié le type d'image de nœud de gestion qui convient à votre plateforme :

Plate-forme	type d'image d'installation
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

Étapes

1. [Téléchargez l'ISO ou l'OVA et déployez la machine virtuelle.](#)
2. [Configurer le réseau](#)
3. [Configurer la synchronisation de l'heure](#)
4. [Configurer le nœud de gestion](#)

Téléchargez l'ISO ou l'OVA et déployez la machine virtuelle.

1. Téléchargez le fichier OVA ou ISO pour votre installation depuis le site web. "Logiciel Element" page sur le site d'assistance NetApp .
 - a. Sélectionnez **Télécharger la dernière version** et acceptez le CLUF.
 - b. Sélectionnez l'image du nœud de gestion que vous souhaitez télécharger.
2. Si vous avez téléchargé le fichier OVA, suivez ces étapes :
 - a. Déployez l'OVA.
 - b. Si votre cluster de stockage se trouve sur un sous-réseau distinct de votre nœud de gestion (eth0) et que vous souhaitez utiliser des volumes persistants, ajoutez un deuxième contrôleur d'interface réseau (NIC) à la VM sur le sous-réseau de stockage (par exemple, eth1) ou assurez-vous que le réseau de gestion peut router vers le réseau de stockage.
3. Si vous avez téléchargé l'ISO, suivez ces étapes :
 - a. Créez une nouvelle machine virtuelle 64 bits à partir de votre hyperviseur avec la configuration suivante :
 - Six processeurs virtuels
 - 24 Go de RAM
 - Disque virtuel de 400 Go, provisionnement dynamique
 - Une interface réseau virtuelle avec accès internet et accès au stockage MVIP.
 - (Optionnel pour le stockage 100% flash SolidFire) Une interface réseau virtuelle avec accès

réseau de gestion au cluster de stockage. Si votre cluster de stockage se trouve sur un sous-réseau distinct de votre nœud de gestion (eth0) et que vous souhaitez utiliser des volumes persistants, ajoutez un deuxième contrôleur d'interface réseau (NIC) à la VM sur le sous-réseau de stockage (eth1) ou assurez-vous que le réseau de gestion peut router vers le réseau de stockage.



N'allumez pas la machine virtuelle avant l'étape qui vous invitera à le faire plus loin dans cette procédure.

b. Attachez l'image ISO à la machine virtuelle et démarrez sur l'image d'installation .iso.



L'installation d'un nœud de gestion à l'aide de cette image peut entraîner un délai de 30 secondes avant l'affichage de l'écran de démarrage.

4. Mettez sous tension la machine virtuelle du nœud de gestion une fois l'installation terminée.

Configurer le réseau

1. À l'aide de l'interface utilisateur du terminal (TUI), créez un utilisateur administrateur de nœud de gestion.



Pour naviguer dans les options du menu, appuyez sur les touches fléchées Haut ou Bas. Pour naviguer entre les boutons, appuyez sur Tab. Pour passer des boutons aux champs, appuyez sur la touche Tab. Pour naviguer entre les champs, appuyez sur les touches fléchées Haut ou Bas.

2. Configurez le réseau du nœud de gestion (eth0).



Si vous avez besoin d'une carte réseau supplémentaire pour isoler le trafic de stockage, consultez les instructions relatives à la configuration d'une autre carte réseau : ["Configurer un contrôleur d'interface réseau \(NIC\) de stockage"](#).

Configurer la synchronisation de l'heure

1. Vérifiez que l'heure est synchronisée entre le nœud de gestion et le cluster de stockage à l'aide de NTP :



À partir de l'élément 12.3.1, les sous-étapes (a) à (e) sont exécutées automatiquement. Pour le nœud de gestion 12.3.1 ou version ultérieure, passez à la section suivante : [sous-étape \(f\)](#) pour terminer la configuration de la synchronisation horaire.

1. Connectez-vous au nœud de gestion en utilisant SSH ou la console fournie par votre hyperviseur.

2. Stop NTPD :

```
sudo service ntpd stop
```

3. Modifier le fichier de configuration NTP /etc/ntp.conf :

a. Commentez les serveurs par défaut(`server 0.gentoo.pool.ntp.org`) en ajoutant un # devant chacun.

b. Ajoutez une nouvelle ligne pour chaque serveur de temps par défaut que vous souhaitez ajouter. Les serveurs de temps par défaut doivent être les mêmes serveurs NTP que ceux utilisés sur le cluster de

stockage que vous utiliserez dans un "étape ultérieure".

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

c. Enregistrez le fichier de configuration une fois terminé.

4. Forcez une synchronisation NTP avec le serveur nouvellement ajouté.

```
sudo ntpd -gq
```

5. Redémarrez NTPD.

```
sudo service ntpd start
```

6. Désactiver la synchronisation de l'heure avec l'hôte via l'hyperviseur (voici un exemple VMware) :



Si vous déployez le mNode dans un environnement d'hyperviseur autre que VMware, par exemple à partir de l'image .iso dans un environnement Openstack, reportez-vous à la documentation de l'hyperviseur pour connaître les commandes équivalentes.

a. Désactiver la synchronisation horaire périodique :

```
vmware-toolbox-cmd timesync disable
```

b. Afficher et confirmer l'état actuel du service :

```
vmware-toolbox-cmd timesync status
```

c. Dans vSphere, vérifiez que la **Synchronize guest time with host** La case correspondante est décochée dans les options de la machine virtuelle.



Ne pas activer cette option si vous apportez des modifications ultérieures à la machine virtuelle.



Ne modifiez pas le protocole NTP après avoir terminé la configuration de la synchronisation horaire, car cela affectera le protocole NTP lors de son exécution. [commande de redéploiement](#) sur le nœud de gestion.

Configurer le nœud de gestion

1. Créez un répertoire de destination temporaire pour le contenu du bundle de services de gestion :

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. Téléchargez le module de services de gestion (version 2.15.28 ou ultérieure) précédemment installé sur le nœud de gestion existant et enregistrez-le dans le répertoire suivant : /sf/etc/mnode/ annuaire.
3. Extrayez le paquet téléchargé à l'aide de la commande suivante, en remplaçant la valeur entre crochets [] (crochets compris) par le nom du fichier du paquet :

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle file]
```

4. Extrayez le fichier résultant vers le /sf/etc/mnode-archive annuaire:

```
tar -C /sf/etc/mnode/mnode-archive -xvf /sf/etc/mnode/services_deploy_bundle.tar.gz
```

5. Créez un fichier de configuration pour les comptes et les volumes :

```
echo '{"trident": true, "mvip": "[mvip IP address]", "account_name": "[persistent volume account name]"}' | sudo tee /sf/etc/mnode/mnode-archive/management-services-metadata.json
```

- a. Remplacez la valeur entre crochets [] (crochets compris) pour chacun des paramètres obligatoires suivants :

- **[Adresse IP mvip]** : L'adresse IP virtuelle de gestion du cluster de stockage. Configurez le nœud de gestion avec le même cluster de stockage que celui que vous avez utilisé lors de ["configuration des serveurs NTP"](#).
- **[nom du compte de volume persistant]** : Le nom du compte associé à tous les volumes persistants dans ce cluster de stockage.

1. Configurez et exécutez la commande de redéploiement du nœud de gestion pour vous connecter aux volumes persistants hébergés sur le cluster et démarrer les services avec les données de configuration précédentes du nœud de gestion :



Vous serez invité à saisir vos mots de passe dans une fenêtre sécurisée. Si votre cluster se trouve derrière un serveur proxy, vous devez configurer les paramètres du proxy pour pouvoir accéder à un réseau public.

```
sudo /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
```

- a. Remplacez la valeur entre crochets [] (crochets compris) par le nom d'utilisateur du compte administrateur du nœud de gestion. Il s'agit probablement du nom d'utilisateur du compte utilisateur que vous avez utilisé pour vous connecter au nœud de gestion.



Vous pouvez ajouter le nom d'utilisateur ou laisser le script vous demander ces informations.

- b. Exécutez la `redeploy-mnode` commande. Le script affiche un message de réussite une fois le redéploiement terminé.
- c. Si vous accédez aux interfaces Web d'Element (telles que le nœud de gestion ou NetApp Hybrid Cloud Control) en utilisant le nom de domaine pleinement qualifié (FQDN) du système, "[reconfigurer l'authentification pour le nœud de gestion](#)" .



capacité SSH qui fournit "[Accès à la session du tunnel d'assistance à distance \(RST\) de NetApp Support](#)" est désactivé par défaut sur les nœuds de gestion exécutant les services de gestion 2.18 et versions ultérieures. Si vous aviez précédemment activé la fonctionnalité SSH sur le nœud de gestion, vous pourriez avoir besoin de "[désactiver SSH à nouveau](#)" sur le nœud de gestion récupéré.

Pour en savoir plus, consultez les informations disponibles.

- "[Volumes persistants](#)"
- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation logicielle SolidFire et Element](#)"

Accédez au nœud de gestion

À partir de la version 11.3 du logiciel NetApp Element , le nœud de gestion contient deux interfaces utilisateur : une interface utilisateur pour la gestion des services basés sur REST et une interface utilisateur par nœud pour la gestion des paramètres réseau et de cluster ainsi que des tests et utilitaires du système d'exploitation.

Pour les clusters exécutant la version 11.3 ou ultérieure du logiciel Element, vous pouvez utiliser l'une des deux interfaces suivantes :

- En utilisant l'interface utilisateur du nœud de gestion(`https:// [mNode IP] :442`), vous pouvez modifier les paramètres réseau et de cluster, exécuter des tests système ou utiliser les utilitaires système.
- En utilisant l'interface utilisateur de l'API REST intégrée(`https:// [mNode IP] /mnode`), vous pouvez exécuter ou comprendre les API relatives aux services du nœud de gestion, notamment la configuration du serveur proxy, les mises à jour du niveau de service ou la gestion des actifs.

Accéder à l'interface utilisateur du nœud de gestion

Depuis l'interface utilisateur de chaque nœud, vous pouvez accéder aux paramètres réseau et de cluster et utiliser les tests et utilitaires système.

Étapes

1. Accédez à l'interface utilisateur du nœud de gestion en saisissant l'adresse IP du nœud de gestion suivie de :442

https://[IP address]:442

The screenshot shows the 'Network Settings - Management' configuration page. The 'Management' tab is selected. The configuration fields are as follows:

- Method: static
- Link Speed: 1000
- IPv4 Address: 10.117.148.209
- IPv4 Subnet Mask: 255.255.148.0
- IPv4 Gateway Address: 10.117.148.254
- IPv6 Address: (empty)
- IPv6 Gateway Address: (empty)
- MTU: 1500
- DNS Servers: 10.117.205.40, 10.116.103.40
- Search Domains: den.academy.net, cme.den.academy
- Status: UpAndRunning

Below the configuration area, there is a 'Routes' section with an 'Add' button. At the bottom are 'Reset Changes' and 'Save Changes' buttons.

2. Saisissez le nom d'utilisateur et le mot de passe du nœud de gestion lorsque vous y êtes invité.

Accédez à l'interface utilisateur de l'API REST du nœud de gestion

Depuis l'interface utilisateur de l'API REST, vous pouvez accéder à un menu d'API liées aux services qui contrôlent les services de gestion sur le nœud de gestion.

Étapes

1. Pour accéder à l'interface utilisateur de l'API REST pour les services de gestion, saisissez l'adresse IP du nœud de gestion suivie de /mnode :

https://[IP address]/mnode

MANAGEMENT SERVICES API 1.0

[Base URL : /mnodel]

<https://10.117.1.1/mnode/swagger.json>

The configuration REST service for MANAGEMENT SERVICES

NetApp - Website

NetApp Commercial Software License

[Authorize](#)

logs Log service

GET /logs Get logs from the MNODE service(s)

assets Asset service

POST /assets Add a new asset

GET /assets Get all assets

GET /assets/compute-nodes Get all compute nodes

GET /assets/compute-nodes/{compute_node_id} Get a specific compute node by ID

GET /assets/controllers Get all controllers

GET /assets/controllers/{controller_id} Get a specific controller by ID

GET /assets/storage-clusters Get all storage clusters

GET /assets/storage-clusters/{storage_cluster_id} Get a specific storage cluster by ID

PUT /assets/{asset_id} Modify an asset with a specific ID

DELETE /assets/{asset_id} Delete an asset with a specific ID

GET /assets/{asset_id} Get an asset by it's ID

POST /assets/{asset_id}/compute-nodes Add a compute asset

GET /assets/{asset_id}/compute-nodes Get compute assets

PUT /assets/{asset_id}/compute-nodes/{compute_id} Update a specific compute node asset

DELETE /assets/{asset_id}/compute-nodes/{compute_id} Delete a specific compute node asset

2. Sélectionnez **Autoriser** ou toute icône de verrouillage et saisissez les identifiants d'administrateur du cluster pour obtenir les autorisations d'utilisation des API.

Pour en savoir plus, consultez les informations disponibles.

- "Activer la surveillance Active IQ et NetApp"
 - "Module d'extension NetApp Element pour vCenter Server"
 - "Documentation logicielle SolidFire et Element"

Modifier le certificat SSL par défaut du nœud de gestion

Vous pouvez modifier le certificat SSL par défaut et la clé privée du nœud de gestion à l'aide de l'API NetApp Element .

Lorsque vous configurez un nœud de gestion, celui-ci crée un certificat SSL (Secure Sockets Layer) auto-signé unique et une clé privée qui sont utilisés pour toutes les communications HTTPS via l'interface utilisateur Element, l'interface utilisateur par nœud ou les API. Le logiciel Element prend en charge les certificats auto-

signés ainsi que les certificats émis et vérifiés par une autorité de certification (AC) de confiance.

Vous pouvez utiliser les méthodes API suivantes pour obtenir plus d'informations sur le certificat SSL par défaut et y apporter des modifications.

- **Obtenir le certificat SSL du nœud**

Vous pouvez utiliser le "[Méthode GetNodeSSLCertificate](#)" pour récupérer des informations sur le certificat SSL actuellement installé, y compris tous les détails du certificat.

- **Définir le certificat SSL du nœud**

Vous pouvez utiliser le "[méthode SetNodeSSLCertificate](#)" pour configurer les certificats SSL du cluster et par nœud avec le certificat et la clé privée que vous fournissez. Le système valide le certificat et la clé privée afin d'empêcher l'application d'un certificat invalide.

- **Supprimer le certificat SSL du nœud**

Ce "[Méthode RemoveNodeSSLCertificate](#)" Supprime le certificat SSL et la clé privée actuellement installés. Le cluster génère ensuite un nouveau certificat auto-signé et une nouvelle clé privée.

Trouver plus d'informations

- "[Modifier le certificat SSL par défaut du logiciel Element](#)"
- "[Quelles sont les exigences relatives à la configuration de certificats SSL personnalisés dans Element Software ?](#)"
- "[Documentation logicielle SolidFire et Element](#)"
- "[Module d'extension NetApp Element pour vCenter Server](#)"

Utiliser l'interface utilisateur du nœud de gestion

Aperçu de l'interface utilisateur du nœud de gestion

Avec l'interface utilisateur du nœud de gestion(<https://<ManagementNodeIP>:442>), vous pouvez modifier les paramètres réseau et de cluster, exécuter des tests système ou utiliser les utilitaires système.

Tâches que vous pouvez effectuer avec l'interface utilisateur du nœud de gestion :

- "[Configurer la surveillance des alertes](#)"
- "[Modifier et tester les paramètres du réseau, du cluster et du système du nœud de gestion](#)"
- "[Exécuter les utilitaires système à partir du nœud de gestion](#)"

Trouver plus d'informations

- "[Accédez au nœud de gestion](#)"
- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation logicielle SolidFire et Element](#)"

Configurer la surveillance des alertes

Les outils de surveillance des alertes sont configurés pour la surveillance des alertes NetApp HCI . Ces outils ne sont ni configurés ni utilisés pour le stockage 100 % flash SolidFire . L'exécution des outils pour ces clusters génère l'erreur 405 suivante, ce qui est normal compte tenu de la configuration : webUIParseError : Invalid response from server. 405

Pour plus d'informations sur la configuration de la surveillance des alertes pour NetApp HCI, consultez "[Configurer la surveillance des alertes](#)"

Modifier et tester les paramètres du réseau, du cluster et du système du nœud de gestion

Vous pouvez modifier et tester les paramètres du réseau, du cluster et du système du nœud de gestion.

- [Paramètres réseau du nœud de gestion des mises à jour](#)
- [Paramètres du cluster de nœuds de gestion des mises à jour](#)
- [Tester les paramètres du nœud de gestion](#)

Paramètres réseau du nœud de gestion des mises à jour

Dans l'onglet Paramètres réseau de l'interface utilisateur du nœud de gestion par nœud, vous pouvez modifier les champs de l'interface réseau du nœud de gestion.

1. Ouvrez l'interface utilisateur de gestion par nœud.
2. Sélectionnez l'onglet **Paramètres réseau**.
3. Afficher ou saisir les informations suivantes :
 - a. **Méthode** : Choisissez l'une des méthodes suivantes pour configurer l'interface :
 - **loopback**: À utiliser pour définir l'interface de bouclage IPv4.
 - **manual**: Permet de définir des interfaces pour lesquelles aucune configuration n'est effectuée par défaut.
 - **dhop**: À utiliser pour obtenir une adresse IP via DHCP.
 - **static**: À utiliser pour définir des interfaces Ethernet avec des adresses IPv4 allouées statiquement.
 - b. **Vitesse de liaison** : La vitesse négociée par la carte réseau virtuelle.
 - c. **Adresse IPv4** : L'adresse IPv4 du réseau eth0.
 - d. **Masque de sous-réseau IPv4** : Subdivisions d'adresses du réseau IPv4.
 - e. **Adresse de la passerelle IPv4** : Adresse réseau du routeur permettant d'envoyer les paquets hors du réseau local.
 - f. **Adresse IPv6** : L'adresse IPv6 du réseau eth0.
 - g. **Adresse de passerelle IPv6** : Adresse réseau du routeur permettant d'envoyer les paquets hors du réseau local.



Les options IPv6 ne sont pas prises en charge pour les versions 11.3 et ultérieures du nœud de gestion.

- h. **MTU** : Taille maximale des paquets qu'un protocole réseau peut transmettre. Doit être supérieur ou égal à 1500. Si vous ajoutez une deuxième carte réseau de stockage, la valeur doit être de 9000.
- i. **Serveurs DNS** : Interface réseau utilisée pour la communication du cluster.
- j. **Recherche de domaines** : Rechercher les adresses MAC supplémentaires disponibles pour le système.
- k. **Statut** : Valeurs possibles :
 - UpAndRunning
 - Down
 - Up
- l. **Routes** : Routes statiques vers des hôtes ou des réseaux spécifiques via l'interface associée que les routes sont configurées pour utiliser.

Paramètres du cluster de nœuds de gestion des mises à jour

Dans l'onglet Paramètres du cluster de l'interface utilisateur par nœud du nœud de gestion, vous pouvez modifier les champs d'interface du cluster lorsqu'un nœud est dans les états Disponible, En attente, En attente actif et Actif.

1. Ouvrez l'interface utilisateur de gestion par nœud.
2. Sélectionnez l'onglet **Paramètres du cluster**.
3. Afficher ou saisir les informations suivantes :
 - **Rôle** : Rôle du nœud de gestion dans le cluster. Valeur possible : Management .
 - **Version** : Version du logiciel Element exécutée sur le cluster.
 - **Interface par défaut** : Interface réseau par défaut utilisée pour la communication du nœud de gestion avec le cluster exécutant le logiciel Element.

Tester les paramètres du nœud de gestion

Après avoir modifié les paramètres de gestion et de réseau du nœud de gestion et validé les modifications, vous pouvez exécuter des tests pour valider les changements apportés.

1. Ouvrez l'interface utilisateur de gestion par nœud.
2. Dans l'interface utilisateur du nœud de gestion, sélectionnez **Tests système**.
3. Complétez l'une des tâches suivantes :
 - a. Pour vérifier que les paramètres réseau que vous avez configurés sont valides pour le système, sélectionnez **Tester la configuration réseau**.
 - b. Pour tester la connectivité réseau à tous les nœuds du cluster sur les interfaces 1G et 10G à l'aide de paquets ICMP, sélectionnez **Test Ping**.
4. Afficher ou saisir les informations suivantes :
 - **Hôtes** : Spécifiez une liste d'adresses ou de noms d'hôtes de périphériques à interroger, séparés par des virgules.

- **Tentatives** : Spécifiez le nombre de fois où le système doit répéter le test ping. Valeur par défaut : 5.
- **Taille du paquet** : Spécifiez le nombre d'octets à envoyer dans le paquet ICMP envoyé à chaque adresse IP. Le nombre d'octets doit être inférieur à la MTU maximale spécifiée dans la configuration réseau.
- **Délai d'attente en mSec** : Spécifiez le nombre de millisecondes à attendre pour chaque réponse ping. Valeur par défaut : 500 ms.
- **Délai d'attente total (s)** : Spécifiez la durée en secondes pendant laquelle le ping doit attendre une réponse du système avant d'effectuer la tentative de ping suivante ou de mettre fin au processus. Valeur par défaut : 5.
- **Interdire la fragmentation** : Activez l'indicateur DF (ne pas fragmenter) pour les paquets ICMP.

Pour en savoir plus, consultez les informations disponibles.

- ["Module d'extension NetApp Element pour vCenter Server"](#)
- ["Documentation logicielle SolidFire et Element"](#)

Exécutez les utilitaires système à partir du nœud de gestion

Vous pouvez utiliser l'interface utilisateur par nœud du nœud de gestion pour créer ou supprimer des ensembles de support de cluster, réinitialiser les paramètres de configuration du nœud ou redémarrer le réseau.

Étapes

1. Ouvrez l'interface utilisateur de gestion par nœud en utilisant les identifiants d'administrateur du nœud de gestion.
2. Sélectionnez **Utilitaires système**.
3. Sélectionnez le bouton correspondant à l'utilitaire que vous souhaitez exécuter :
 - a. **Contrôle de l'alimentation** : Redémarre, met hors tension ou éteint le nœud. Spécifiez l'une des options suivantes.



Cette opération entraîne une perte temporaire de connectivité réseau.

- **Action** : Les options incluent `Restart` et `Halt` (coupure du courant).
- **Délai de réveil** : Tout temps supplémentaire avant que le nœud ne soit de nouveau en ligne.
- b. **Créer un bundle de support de cluster** : Crée le bundle de support de cluster pour aider le support NetApp à évaluer le diagnostic d'un ou plusieurs nœuds d'un cluster. Spécifiez les options suivantes :
 - **Nom du pack** : Nom unique pour chaque pack de support créé. Si aucun nom n'est fourni, alors « `supportbundle` » et le nom du nœud sont utilisés comme nom de fichier.
 - **Mvip** : Le MVIP du cluster. Les paquets sont collectés à partir de tous les nœuds du cluster. Ce paramètre est obligatoire si le paramètre `Nodes` n'est pas spécifié.
 - **Nœuds** : Les adresses IP des nœuds à partir desquels collecter les paquets. Utilisez soit `Nodes`, soit `Mvip`, mais pas les deux, pour spécifier les nœuds à partir desquels rassembler les paquets. Ce paramètre est obligatoire si `Mvip` n'est pas spécifié.
 - **Nom d'utilisateur** : Le nom d'utilisateur de l'administrateur du cluster.
 - **Mot de passe** : Le mot de passe de l'administrateur du cluster.

- **Autoriser les opérations incomplètes** : Permet au script de continuer à s'exécuter si les paquets ne peuvent pas être collectés à partir d'un ou plusieurs nœuds.
- **Arguments supplémentaires** : Ce paramètre est transmis à `sf_make_support_bundle` scénario. Ce paramètre ne doit être utilisé qu'à la demande du support NetApp .
- c. **Supprimer tous les modules de support** : Supprime tous les modules de support actuellement présents sur le nœud de gestion.
- d. **Réinitialiser le nœud** : Réinitialise le nœud de gestion à une nouvelle image d'installation. Cela rétablit tous les paramètres par défaut, à l'exception de la configuration réseau. Spécifiez les options suivantes :
 - **Build** : URL d'une image logicielle Element distante vers laquelle le nœud sera réinitialisé.
 - **Options** : Spécifications pour l'exécution des opérations de réinitialisation. Des détails supplémentaires seront fournis par le support NetApp , si nécessaire.



Cette opération entraîne une perte temporaire de connectivité réseau.

- e. **Redémarrage du réseau** : Redémarre tous les services réseau sur le nœud de gestion.



Cette opération entraîne une perte temporaire de connectivité réseau.

Pour en savoir plus, consultez les informations disponibles.

- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation logicielle SolidFire et Element](#)"

Utilisez l'API REST du nœud de gestion

Présentation de l'interface utilisateur de l'API REST du nœud de gestion

En utilisant l'interface utilisateur de l'API REST

intégrée(<https://<ManagementNodeIP>/mnode>), vous pouvez exécuter ou comprendre les API relatives aux services du nœud de gestion, notamment la configuration du serveur proxy, les mises à jour du niveau de service ou la gestion des actifs.

Tâches que vous pouvez effectuer avec les API REST :

Autorisation

- "[Obtenir l'autorisation d'utiliser les API REST](#)"

Configuration des actifs

- "[Activer la surveillance Active IQ et NetApp](#)"
- "[Configurer un serveur proxy pour le nœud de gestion](#)"
- "[Configurer NetApp Hybrid Cloud Control pour plusieurs vCenters](#)"
- "[Ajouter une ressource de contrôleur au nœud de gestion](#)"

- "Créer et gérer des ressources de cluster de stockage"

Gestion d'actifs

- "Afficher ou modifier les ressources de contrôleur existantes"
- "Créer et gérer des ressources de cluster de stockage"
- "Utilisez l'API REST pour collecter les journaux système Element."
- "Vérifier les versions du système d'exploitation et des services du nœud de gestion"
- "Récupération des journaux des services de gestion"

Trouver plus d'informations

- "Accédez au nœud de gestion"
- "Module d'extension NetApp Element pour vCenter Server"
- "Documentation logicielle SolidFire et Element"

Obtenir l'autorisation d'utiliser les API REST

Vous devez vous authentifier avant de pouvoir utiliser les API pour les services de gestion dans l'interface utilisateur de l'API REST. Pour cela, vous devez obtenir un jeton d'accès.

Pour obtenir un jeton, vous devez fournir les identifiants d'administrateur du cluster et un ID client. Chaque jeton dure environ dix minutes. Une fois le jeton expiré, vous pouvez vous authentifier à nouveau pour obtenir un nouveau jeton d'accès.

La fonctionnalité d'autorisation est configurée pour vous lors de l'installation et du déploiement du nœud de gestion. Le service de jetons est basé sur le cluster de stockage que vous avez défini lors de la configuration.

Avant de commencer

- Votre version de cluster doit exécuter le logiciel NetApp Element 11.3 ou une version ultérieure.
- Vous auriez dû déployer un nœud de gestion exécutant la version 11.3 ou ultérieure.

Commande API

```
TOKEN=`curl -k -X POST https://MVIP/auth/connect/token -F client_id=mnode-client -F grant_type=password -F username=CLUSTER_ADMIN -F password=CLUSTER_PASSWORD|awk -F':|'{print $2}'|awk -F','|'{print $1}'|sed s/\"/`
```

Étapes de l'interface utilisateur de l'API REST

1. Accédez à l'interface utilisateur de l'API REST du service en saisissant l'adresse IP du nœud de gestion suivie du nom du service, par exemple : /mnode/ :

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

2. Sélectionnez **Autoriser**.



Vous pouvez également sélectionner l'icône de verrouillage à côté de chaque API de service.

3. Complétez ce qui suit :

- a. Saisissez le nom d'utilisateur et le mot de passe du cluster.
- b. Saisissez l'identifiant du client comme `mnode-client`.
- c. Ne saisissez pas de valeur pour le secret client.
- d. Sélectionnez **Autoriser** pour démarrer une session.

4. Fermez la boîte de dialogue **Autorisations disponibles**.



Si vous essayez d'exécuter une commande après l'expiration du jeton, une `401 Error: UNAUTHORIZED` Un message apparaît. Si vous voyez ce message, veuillez vous authentifier à nouveau.

Trouver plus d'informations

- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation logicielle SolidFire et Element](#)"

Activer la surveillance Active IQ et NetApp

Vous pouvez activer la surveillance du stockage Active IQ si vous ne l'avez pas déjà fait lors de l'installation ou de la mise à niveau. Vous pourriez avoir besoin d'utiliser cette procédure si vous n'avez pas configuré SolidFire Active IQ lors de l'installation d'un système de stockage 100 % flash SolidFire .

Le service de collecte Active IQ transmet les données de configuration et les indicateurs de performance du cluster basés sur le logiciel Element à SolidFire Active IQ pour la création de rapports historiques et la surveillance des performances en quasi temps réel. Le service de surveillance NetApp permet de transmettre les pannes des clusters de stockage à vCenter pour notification d'alerte.

Avant de commencer

- Certaines fonctions d' Active IQ, par exemple la qualité de service (QoS), nécessitent Element 11.3 ou une version ultérieure pour fonctionner correctement. Pour confirmer que vous êtes en mesure d'utiliser toutes les fonctions Active IQ , NetApp recommande ce qui suit :
 - Votre cluster de stockage exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
 - Vous avez déployé un nœud de gestion exécutant la version 11.3 ou ultérieure.
- Vous avez accès à Internet. Le service de collecte Active IQ ne peut pas être utilisé depuis des sites isolés dépourvus de connectivité externe.

Étapes

1. Obtenez l'identifiant de l'actif de base pour l'installation :

- a. Ouvrez l'interface utilisateur de l'API REST du service d'inventaire sur le nœud de gestion :

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Sélectionnez **Autoriser** et complétez les informations suivantes :
 - i. Saisissez le nom d'utilisateur et le mot de passe du cluster.
 - ii. Saisissez l'identifiant du client comme `mnode-client`.
 - iii. Sélectionnez **Autoriser** pour démarrer une session.
 - iv. Ferme la fenêtre.
- c. Dans l'interface utilisateur de l'API REST, sélectionnez **GET /installations**.
- d. Sélectionnez **Essayer**.
- e. Sélectionnez **Exécuter**.
- f. À partir du corps de la réponse code 200, copiez le `id` pour l'installation.

```
{
  "installations": [
    {
      "_links": {
        "collection": "https://10.111.211.111/inventory/1/installations",
        "self": "https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```



Votre installation possède une configuration de ressources de base qui a été créée lors de l'installation ou de la mise à niveau.

2. Activer la télémétrie :

- a. Accédez à l'interface utilisateur de l'API du service `mnode` sur le nœud de gestion en saisissant l'adresse IP du nœud de gestion suivie de `/mnode` :

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

- b. Sélectionnez **Autoriser** ou toute icône de verrouillage et procédez comme suit :
 - i. Saisissez le nom d'utilisateur et le mot de passe du cluster.
 - ii. Saisissez l'identifiant du client comme `mnode-client`.
 - iii. Sélectionnez **Autoriser** pour démarrer une session.
 - iv. Ferme la fenêtre.
- c. Configurer la ressource de base :

- i. Sélectionnez **PUT /assets/{asset_id}**.
- ii. Sélectionnez **Essayer**.
- iii. Saisissez les éléments suivants dans la charge utile JSON :

```
{
  "telemetry_active": true
  "config": {}
}
```

- iv. Saisissez l'identifiant de base de l'étape précédente dans **asset_ID**.
- v. Sélectionnez **Exécuter**.

Le service Active IQ redémarre automatiquement à chaque modification des ressources. La modification des ressources entraîne un court délai avant l'application des paramètres.

3. Si vous ne l'avez pas déjà fait, ajoutez un élément de contrôleur vCenter pour NetApp Hybrid Cloud Control aux ressources connues du nœud de gestion :



Un contrôleur est nécessaire pour les services de surveillance NetApp .

- a. Sélectionnez **POST /assets/{asset_id}/controllers** pour ajouter un sous-élément de contrôleur.
- b. Sélectionnez **Essayer**.
- c. Saisissez l'identifiant de l'actif de base parent que vous avez copié dans votre presse-papiers dans le champ **asset_id**.
- d. Saisissez les valeurs de charge utile requises avec `type` comme `vCenter` et les identifiants vCenter.

```
{
  "username": "string",
  "password": "string",
  "ip": "string",
  "type": "vCenter",
  "host_name": "string",
  "config": {}
}
```



`ip` est l'adresse IP de vCenter.

- e. Sélectionnez **Exécuter**.

Trouver plus d'informations

- ["Module d'extension NetApp Element pour vCenter Server"](#)
- ["Documentation logicielle SolidFire et Element"](#)

Configurer NetApp Hybrid Cloud Control pour plusieurs vCenters

Vous pouvez configurer NetApp Hybrid Cloud Control pour gérer les ressources de deux vCenters ou plus qui n'utilisent pas le mode lié.

Vous devriez utiliser cette procédure après votre installation initiale lorsque vous devez ajouter des ressources pour une installation récemment mise à l'échelle ou lorsque de nouvelles ressources n'ont pas été ajoutées automatiquement à votre configuration. Utilisez ces API pour ajouter des ressources récemment ajoutées à votre installation.

Ce dont vous aurez besoin

- Votre version de cluster exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
- Vous avez déployé un nœud de gestion exécutant la version 11.3 ou ultérieure.

Étapes

1. ["Ajouter de nouveaux vCenters en tant qu'actifs de contrôleur"](#) à la configuration du nœud de gestion.
2. Actualisez l'API du service d'inventaire sur le nœud de gestion :

```
https://<ManagementNodeIP>/inventory/1/
```



Vous pouvez également attendre 2 minutes que l'inventaire se mette à jour dans l'interface utilisateur de NetApp Hybrid Cloud Control.

- a. Sélectionnez **Autoriser** et complétez les informations suivantes :
 - i. Saisissez le nom d'utilisateur et le mot de passe du cluster.
 - ii. Saisissez l'identifiant du client comme `mnode-client`.
 - iii. Sélectionnez **Autoriser** pour démarrer une session.
 - iv. Ferme la fenêtre.
- b. Dans l'interface utilisateur de l'API REST, sélectionnez **GET /installations**.
- c. Sélectionnez **Essayer**.
- d. Sélectionnez **Exécuter**.
- e. À partir de la réponse, copiez l'identifiant de l'actif d'installation.("id").
- f. Dans l'interface utilisateur de l'API REST, sélectionnez **GET /installations/{id}**.
- g. Sélectionnez **Essayer**.
- h. Définir l'actualisation sur `True` .
 - i. Collez l'identifiant de l'élément d'installation dans le champ **id**.
 - j. Sélectionnez **Exécuter**.

3. Actualisez le navigateur NetApp Hybrid Cloud Control pour voir les modifications.

Trouver plus d'informations

- ["Module d'extension NetApp Element pour vCenter Server"](#)
- ["Documentation logicielle SolidFire et Element"](#)

Ajouter une ressource de contrôleur au nœud de gestion

Vous pouvez ajouter une ressource de contrôleur à la configuration du nœud de gestion à l'aide de l'interface utilisateur de l'API REST.

Vous devrez peut-être ajouter une ressource si vous avez récemment mis à l'échelle votre installation et que les nouvelles ressources n'ont pas été ajoutées automatiquement à votre configuration. Utilisez ces API pour ajouter des ressources récemment ajoutées à votre installation.

Ce dont vous aurez besoin

- Votre version de cluster exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
- Vous avez déployé un nœud de gestion exécutant la version 11.3 ou ultérieure.
- Vous avez créé un nouveau rôle NetApp HCC dans vCenter afin de limiter la vue des services du nœud de gestion aux seules ressources NetApp. Voir "[Créez un rôle NetApp HCC dans vCenter.](#)"

Étapes

1. Obtenez l'identifiant de l'actif de base pour l'installation :

a. Ouvrez l'interface utilisateur de l'API REST du service d'inventaire sur le nœud de gestion :

```
https://<ManagementNodeIP>/inventory/1/
```

b. Sélectionnez **Autoriser** et complétez les informations suivantes :

- Saisissez le nom d'utilisateur et le mot de passe du cluster.
- Saisissez l'identifiant du client comme `mnode-client`.
- Sélectionnez **Autoriser** pour démarrer une session.
- Ferme la fenêtre.

c. Dans l'interface utilisateur de l'API REST, sélectionnez **GET /installations**.

d. Sélectionnez **Essayer**.

e. Sélectionnez **Exécuter**.

f. À partir du corps de la réponse code 200, copiez le `id` pour l'installation.

```
{
  "installations": [
    {
      "_links": {
        "collection": "https://10.111.211.111/inventory/1/installations",
        "self": "https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```



Votre installation possède une configuration de ressources de base qui a été créée lors de l'installation ou de la mise à niveau.

- g. Dans l'interface utilisateur de l'API REST, sélectionnez **GET /installations/{id}**.
- h. Sélectionnez **Essayer**.
 - i. Collez l'identifiant de l'élément d'installation dans le champ **id**.
 - j. Sélectionnez **Exécuter**.
- k. À partir de la réponse, copiez et enregistrez l'ID du contrôleur de cluster("controllerId") pour une utilisation ultérieure.

2. Pour ajouter un sous-actif de contrôleur à un actif de base existant, sélectionnez :

```
POST /assets/{asset_id}/controllers
```

- a. Ouvrez l'interface utilisateur de l'API REST du service mNode sur le nœud de gestion :

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

- b. Sélectionnez **Autoriser** et complétez les informations suivantes :
 - i. Saisissez le nom d'utilisateur et le mot de passe du cluster.
 - ii. Saisissez l'identifiant du client comme `mnode-client` .
 - iii. Sélectionnez **Autoriser** pour démarrer une session.
 - iv. Ferme la fenêtre.
- c. Sélectionnez **POST /assets/{asset_id}/controllers**.
- d. Sélectionnez **Essayer**.
- e. Saisissez l'identifiant de l'actif de base parent dans le champ **asset_id**.
- f. Ajoutez les valeurs requises à la charge utile.
- g. Sélectionnez **Exécuter**.

Trouver plus d'informations

- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation logicielle SolidFire et Element](#)"

Créer et gérer des ressources de cluster de stockage

Vous pouvez ajouter de nouveaux éléments de cluster de stockage au nœud de gestion, modifier les informations d'identification enregistrées pour les éléments de cluster de stockage connus et supprimer des éléments de cluster de stockage du nœud de gestion à l'aide de l'API REST.

Ce dont vous aurez besoin

- Assurez-vous que votre version de cluster de stockage exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
- Assurez-vous d'avoir déployé un nœud de gestion exécutant la version 11.3 ou ultérieure.

options de gestion des actifs du cluster de stockage

Choisissez l'une des options suivantes :

- [Récupérer l'ID d'installation et l'ID de cluster d'une ressource de cluster de stockage](#)
- [Ajouter un nouvel élément de cluster de stockage](#)
- [Modifier les informations d'identification enregistrées pour une ressource de cluster de stockage](#)
- [Supprimer un actif de cluster de stockage](#)

Récupérer l'ID d'installation et l'ID de cluster d'une ressource de cluster de stockage

Vous pouvez utiliser l'API REST pour obtenir l'ID d'installation et l'ID du cluster de stockage. Vous avez besoin de l'ID d'installation pour ajouter un nouvel élément de cluster de stockage, et de l'ID du cluster pour modifier ou supprimer un élément de cluster de stockage spécifique.

Étapes

1. Accédez à l'interface utilisateur de l'API REST du service d'inventaire en saisissant l'adresse IP du nœud de gestion, suivie de /inventory/1/ :

```
https://<ManagementNodeIP>/inventory/1/
```

2. Sélectionnez **Autoriser** ou toute icône de verrouillage et procédez comme suit :
 - a. Saisissez le nom d'utilisateur et le mot de passe du cluster.
 - b. Saisissez l'identifiant du client comme mnode-client .
 - c. Sélectionnez **Autoriser** pour démarrer une session.
 - d. Ferme la fenêtre.
3. Sélectionnez **GET /installations**.
4. Sélectionnez **Essayer**.
5. Sélectionnez **Exécuter**.

L'API renvoie la liste de toutes les installations connues.

6. À partir du corps de la réponse (code 200), enregistrez la valeur dans le `id` champ, que vous pouvez trouver dans la liste des installations. Il s'agit de l'identifiant d'installation. Par exemple:

```

"installations": [
  {
    "id": "1234a678-12ab-35dc-7b4a-1234a5b6a7ba",
    "name": "my-sf-installation",
    "_links": {
      "collection": "https://localhost/inventory/1/installations",
      "self": "https://localhost/inventory/1/installations/1234a678-12ab-35dc-7b4a-1234a5b6a7ba"
    }
  }
]

```

7. Accédez à l'interface utilisateur de l'API REST du service de stockage en saisissant l'adresse IP du nœud de gestion, suivie de /storage/1/ :

https://<ManagementNodeIP>/storage/1/

8. Sélectionnez **Autoriser** ou toute icône de verrouillage et procédez comme suit :

- Saisissez le nom d'utilisateur et le mot de passe du cluster.
- Saisissez l'identifiant du client comme `mnode-client`.
- Sélectionnez **Autoriser** pour démarrer une session.
- Ferme la fenêtre.

9. Sélectionnez **GET /clusters**.

10. Sélectionnez **Essayer**.

11. Saisissez l'identifiant d'installation que vous avez enregistré précédemment dans le champ prévu à cet effet. `installationId` paramètre.

12. Sélectionnez **Exécuter**.

L'API renvoie la liste de tous les clusters de stockage connus dans cette installation.

13. À partir du corps de la réponse (code 200), trouvez le cluster de stockage approprié et enregistrez la valeur dans ce cluster. `storageId` champ. Il s'agit de l'identifiant du cluster de stockage.

Ajouter un nouvel élément de cluster de stockage

Vous pouvez utiliser l'API REST pour ajouter un ou plusieurs nouveaux éléments de cluster de stockage à l'inventaire du nœud de gestion. Lorsque vous ajoutez une nouvelle ressource de cluster de stockage, celle-ci est automatiquement enregistrée auprès du nœud de gestion.

Ce dont vous aurez besoin

- Vous avez copié le **ID du cluster de stockage et ID d'installation** pour tous les clusters de stockage que vous souhaitez ajouter.
- Si vous ajoutez plusieurs nœuds de stockage, vous avez lu et compris les limitations de **"Groupe d'autorité"** et la prise en charge de plusieurs clusters de stockage.



Tous les utilisateurs définis sur le cluster faisant autorité sont définis comme utilisateurs sur tous les autres clusters liés à l'instance NetApp Hybrid Cloud Control.

Étapes

1. Accédez à l'interface utilisateur de l'API REST du service de stockage en saisissant l'adresse IP du nœud de gestion, suivie de /storage/1/ :

```
https://<ManagementNodeIP>/storage/1/
```

2. Sélectionnez **Autoriser** ou toute icône de verrouillage et procédez comme suit :

- Saisissez le nom d'utilisateur et le mot de passe du cluster.
- Saisissez l'identifiant du client comme mnode-client .
- Sélectionnez **Autoriser** pour démarrer une session.
- Ferme la fenêtre.

3. Sélectionnez **POST /clusters**.

4. Sélectionnez **Essayer**.

5. Saisissez les informations du nouveau cluster de stockage dans les paramètres suivants, dans le champ **Corps de la requête** :

```
{
  "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
  "mvip": "10.0.0.1",
  "password": "admin",
  "userId": "admin"
}
```

Paramètre	Type	Description
installationId	chaîne	L'installation dans laquelle ajouter le nouveau cluster de stockage. Saisissez l'identifiant d'installation que vous avez enregistré précédemment dans ce paramètre.
mvip	chaîne	L'adresse IP virtuelle de gestion IPv4 (MVIP) du cluster de stockage.
password	chaîne	Le mot de passe utilisé pour communiquer avec le cluster de stockage.

Paramètre	Type	Description
userId	chaîne	L'identifiant utilisateur utilisé pour communiquer avec le cluster de stockage (l'utilisateur doit disposer de priviléges d'administrateur).

6. Sélectionnez **Exécuter**.

L'API renvoie un objet contenant des informations sur la ressource de cluster de stockage nouvellement ajoutée, telles que le nom, la version et l'adresse IP.

Modifier les informations d'identification enregistrées pour une ressource de cluster de stockage

Vous pouvez modifier les informations d'identification enregistrées que le nœud de gestion utilise pour se connecter à un cluster de stockage. L'utilisateur que vous choisissez doit disposer d'un accès d'administrateur de cluster.



Assurez-vous d'avoir suivi les étapes dans [Récupérer l'ID d'installation et l'ID de cluster d'une ressource de cluster de stockage](#) avant de continuer.

Étapes

1. Accédez à l'interface utilisateur de l'API REST du service de stockage en saisissant l'adresse IP du nœud de gestion, suivie de /storage/1/ :

```
https://<ManagementNodeIP>/storage/1/
```

2. Sélectionnez **Autoriser** ou toute icône de verrouillage et procédez comme suit :

- Saisissez le nom d'utilisateur et le mot de passe du cluster.
- Saisissez l'identifiant du client comme mnode-client .
- Sélectionnez **Autoriser** pour démarrer une session.
- Ferme la fenêtre.

3. Sélectionnez **PUT /clusters/{storageId}**.

4. Sélectionnez **Essayer**.

5. Collez l'ID du cluster de stockage que vous avez copié précédemment dans le `storageId` paramètre.

6. Modifiez un ou les deux paramètres suivants dans le champ **Corps de la requête** :

```
{
  "password": "adminadmin",
  "userId": "admin"
}
```

Paramètre	Type	Description
password	chaîne	Le mot de passe utilisé pour communiquer avec le cluster de stockage.
userId	chaîne	L'identifiant utilisateur utilisé pour communiquer avec le cluster de stockage (l'utilisateur doit disposer de privilèges d'administrateur).

7. Sélectionnez **Exécuter**.

Supprimer un actif de cluster de stockage

Vous pouvez supprimer un élément de cluster de stockage si celui-ci n'est plus en service. Lorsque vous supprimez un élément de cluster de stockage, celui-ci est automatiquement désenregistré du nœud de gestion.



Assurez-vous d'avoir suivi les étapes dans [Récupérer l'ID d'installation et l'ID de cluster d'une ressource de cluster de stockage](#) avant de continuer.

Étapes

1. Accédez à l'interface utilisateur de l'API REST du service de stockage en saisissant l'adresse IP du nœud de gestion, suivie de /storage/1/ :

```
https://<ManagementNodeIP>/storage/1/
```

2. Sélectionnez **Autoriser** ou toute icône de verrouillage et procédez comme suit :
 - a. Saisissez le nom d'utilisateur et le mot de passe du cluster.
 - b. Saisissez l'identifiant du client comme `mnode-client`.
 - c. Sélectionnez **Autoriser** pour démarrer une session.
 - d. Ferme la fenêtre.
3. Sélectionnez **SUPPRIMER /clusters/{storageId}**.
4. Sélectionnez **Essayer**.
5. Saisissez l'ID du cluster de stockage que vous avez copié précédemment dans le `storageId` paramètre.
6. Sélectionnez **Exécuter**.

En cas de succès, l'API renvoie une réponse vide.

Trouver plus d'informations

- "[Groupe d'autorité](#)"
- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation logicielle SolidFire et Element](#)"

Afficher ou modifier les ressources de contrôleur existantes

Vous pouvez consulter et modifier les informations relatives aux contrôleurs VMware vCenter existants dans la configuration du nœud de gestion à l'aide de l'API REST. Les contrôleurs sont des instances VMware vCenter enregistrées sur le nœud de gestion de votre installation NetApp SolidFire .

Avant de commencer

- Assurez-vous que votre version de cluster exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
- Assurez-vous d'avoir déployé un nœud de gestion exécutant la version 11.3 ou ultérieure.

Accédez à l'API REST des services de gestion

Étapes

1. Accédez à l'interface utilisateur de l'API REST pour les services de gestion en saisissant l'adresse IP du nœud de gestion suivie de /vcenter/1/ :

```
https://<ManagementNodeIP>/vcenter/1/
```

2. Sélectionnez **Autoriser** ou toute icône de verrouillage et procédez comme suit :
 - a. Saisissez le nom d'utilisateur et le mot de passe du cluster.
 - b. Saisissez l'identifiant du client comme mnode-client .
 - c. Sélectionnez **Autoriser** pour démarrer une session.
 - d. Ferme la fenêtre.

Afficher les informations enregistrées concernant les contrôleurs existants

Vous pouvez lister les contrôleurs vCenter existants enregistrés auprès du nœud de gestion et consulter les informations stockées les concernant à l'aide de l'API REST.

Étapes

1. Sélectionnez **GET /compute/controllers**.
2. Sélectionnez **Essayer**.
3. Sélectionnez **Exécuter**.

L'API renvoie une liste de tous les contrôleurs vCenter connus, ainsi que l'adresse IP, l'ID du contrôleur, le nom d'hôte et l'ID utilisateur utilisés pour communiquer avec chaque contrôleur.

4. Si vous souhaitez connaître l'état de connexion d'un contrôleur particulier, copiez l'ID du contrôleur à partir de `id` copiez le champ de ce contrôleur dans votre presse-papiers et voyez [Afficher l'état d'un contrôleur existant](#) .

Afficher l'état d'un contrôleur existant

Vous pouvez consulter l'état de n'importe quel contrôleur vCenter existant enregistré auprès du nœud de gestion. L'API renvoie un statut indiquant si NetApp Hybrid Cloud Control peut se connecter au contrôleur vCenter, ainsi que la raison de ce statut.

Étapes

1. Sélectionnez **GET /compute/controllers/{controller_id}/status**.
2. Sélectionnez **Essayer**.
3. Saisissez l'ID du contrôleur que vous avez copié précédemment dans le `controller_id` paramètre.
4. Sélectionnez **Exécuter**.

L'API renvoie l'état de ce contrôleur vCenter particulier, ainsi que la raison de cet état.

Modifier les propriétés stockées d'un contrôleur

Vous pouvez modifier le nom d'utilisateur ou le mot de passe enregistré pour chacun des contrôleurs vCenter existants enregistrés auprès du nœud de gestion. Vous ne pouvez pas modifier l'adresse IP enregistrée d'un contrôleur vCenter existant.

Étapes

1. Sélectionnez **PUT /compute/controllers/{controller_id}**.
2. Saisissez l'ID du contrôleur vCenter dans le champ prévu à cet effet. `controller_id` paramètre.
3. Sélectionnez **Essayer**.
4. Modifiez l'un des paramètres suivants dans le champ **Corps de la requête** :

Paramètre	Type	Description
<code>userId</code>	chaîne	Modifiez l'identifiant utilisateur utilisé pour communiquer avec le contrôleur vCenter (l'utilisateur doit disposer de priviléges d'administrateur).
<code>password</code>	chaîne	Modifiez le mot de passe utilisé pour communiquer avec le contrôleur vCenter.

5. Sélectionnez **Exécuter**.

L'API renvoie des informations de contrôleur mises à jour.

Trouver plus d'informations

- "[Ajouter une ressource de contrôleur au nœud de gestion](#)"
- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation logicielle SolidFire et Element](#)"

Configurer un serveur proxy

Si votre cluster se trouve derrière un serveur proxy, vous devez configurer les paramètres du proxy afin de pouvoir accéder à un réseau public.

Un serveur proxy est utilisé pour la collecte des données de télémétrie et les connexions de tunnel inverse. Vous pouvez activer et configurer un serveur proxy à l'aide de l'interface utilisateur de l'API REST si vous n'en

avez pas déjà configuré un lors de l'installation ou de la mise à niveau. Vous pouvez également modifier les paramètres du serveur proxy existant ou désactiver un serveur proxy.

La commande permettant de configurer un serveur proxy met à jour puis renvoie les paramètres proxy actuels pour le nœud de gestion. Les paramètres de proxy sont utilisés par Active IQ, le service de surveillance NetApp , et d'autres utilitaires logiciels Element installés sur le nœud de gestion, y compris le tunnel de support inverse pour NetApp Support.

Avant de commencer

- Vous devez connaître les informations d'hôte et d'identification du serveur proxy que vous configurez.
- Assurez-vous que votre version de cluster exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
- Assurez-vous d'avoir déployé un nœud de gestion exécutant la version 11.3 ou ultérieure.
- (Nœud de gestion 12.0 et versions ultérieures) Vous avez mis à jour NetApp Hybrid Cloud Control vers la version 2.16 des services de gestion avant de configurer un serveur proxy.

Étapes

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

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

2. Sélectionnez **Autoriser** ou toute icône de verrouillage et procédez comme suit :

- a. Saisissez le nom d'utilisateur et le mot de passe du cluster.
- b. Saisissez l'identifiant du client comme mnode-client .
- c. Sélectionnez **Autoriser** pour démarrer une session.
- d. Ferme la fenêtre.

3. Sélectionnez **PUT /settings**.

4. Sélectionnez **Essayer**.

5. Pour activer un serveur proxy, vous devez configurer `use_proxy` à vrai. Saisissez l'adresse IP ou le nom d'hôte et les ports de destination du proxy.

Le nom d'utilisateur du proxy, le mot de passe du proxy et le port SSH sont facultatifs et doivent être omis s'ils ne sont pas utilisés.

```
{
  "proxy_ip_or_hostname": "[IP or name]",
  "use_proxy": [true/false],
  "proxy_username": "[username]",
  "proxy_password": "[password]",
  "proxy_port": [port value],
  "proxy_ssh_port": [port value: default is 443]
}
```

6. Sélectionnez **Exécuter**.



Selon votre environnement, vous devrez peut-être redémarrer votre nœud de gestion.

Trouver plus d'informations

- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation logicielle SolidFire et Element](#)"

Vérifier les versions du système d'exploitation et des services du nœud de gestion

Vous pouvez vérifier les numéros de version du système d'exploitation du nœud de gestion, du bundle de services de gestion et des services individuels exécutés sur le nœud de gestion à l'aide de l'API REST du nœud de gestion.

Ce dont vous aurez besoin

- Votre cluster exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
- Vous avez déployé un nœud de gestion exécutant la version 11.3 ou ultérieure.

Options

- [Commandes API](#)
- [Étapes de l'interface utilisateur de l'API REST](#)

Commandes API

- Obtenez des informations sur la version du système d'exploitation du nœud de gestion, du bundle de services de gestion et du service API du nœud de gestion (mnode-api) exécutés sur le nœud de gestion :

```
curl -X GET "https://<ManagementNodeIP>/mnode/about" -H "accept: application/json"
```

- Obtenez des informations sur la version des services individuels exécutés sur le nœud de gestion :

```
curl -X GET "https://<ManagementNodeIP>/mnode/services?status=running" -H "accept: */*" -H "Authorization: ${TOKEN}"
```



Vous pouvez trouver le porteur \${TOKEN} utilisé par la commande API lorsque vous "[autoriser](#)". Le porteur \${TOKEN} se trouve dans la réponse curl.

Étapes de l'interface utilisateur de l'API REST

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

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

2. Effectuez l'une des opérations suivantes :

- Obtenez des informations sur la version du système d'exploitation du nœud de gestion, du bundle de services de gestion et du service API du nœud de gestion (mnode-api) exécutés sur le nœud de gestion :

i. Sélectionnez **GET /about**.

ii. Sélectionnez **Essayer**.

iii. Sélectionnez **Exécuter**.

La version groupée des services de gestion("mnode_bundle_version"), version du système d'exploitation du nœud de gestion("os_version"), et la version de l'API du nœud de gestion("version") sont indiqués dans le corps de la réponse.

- Obtenez des informations sur la version des services individuels exécutés sur le nœud de gestion :

i. Sélectionnez **GET /services**.

ii. Sélectionnez **Essayer**.

iii. Sélectionnez l'état **En cours d'exécution**.

iv. Sélectionnez **Exécuter**.

Les services exécutés sur le nœud de gestion sont indiqués dans le corps de la réponse.

Trouver plus d'informations

- ["Module d'extension NetApp Element pour vCenter Server"](#)
- ["Documentation logicielle SolidFire et Element"](#)

Récupération des journaux des services de gestion

Vous pouvez récupérer les journaux des services exécutés sur le nœud de gestion à l'aide de l'API REST. Vous pouvez extraire les journaux de tous les services publics ou spécifier des services particuliers et utiliser des paramètres de requête pour mieux définir les résultats renvoyés.

Ce dont vous aurez besoin

- Votre version de cluster exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
- Vous avez déployé un nœud de gestion exécutant la version 11.3 ou ultérieure.

Étapes

1. Ouvrez l'interface utilisateur de l'API REST sur le nœud de gestion.

- À partir des services de gestion 2.21.61 :

```
https://<ManagementNodeIP>/mnode/4/
```

- Pour les services de gestion 2.20.69 ou antérieurs :

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

2. Sélectionnez **Autoriser** ou toute icône de verrouillage et procédez comme suit :

- Saisissez le nom d'utilisateur et le mot de passe du cluster.
- Saisissez l'identifiant client sous la forme mnode-client si cette valeur n'est pas déjà renseignée.
- Sélectionnez **Autoriser** pour démarrer une session.
- Ferme la fenêtre.

3. Sélectionnez **GET /logs**.

4. Sélectionnez **Essayer**.

5. Spécifiez les paramètres suivants :

- Lines: Entrez le nombre de lignes que vous souhaitez que le journal renvoie. Ce paramètre est un entier dont la valeur par défaut est 1000.



Évitez de demander l'historique complet du contenu du journal en définissant le nombre de lignes sur 0.

- since: Ajoute un horodatage ISO-8601 au point de départ des journaux de service.



Utilisez une méthode raisonnable since paramètre lors de la collecte de journaux sur des périodes plus longues.

- service-name: Veuillez saisir un nom de service.



Utilisez le GET /services commande permettant de lister les services sur le nœud de gestion.

- stopped: Définir sur true pour récupérer les journaux des services arrêtés.

6. Sélectionnez **Exécuter**.

7. Dans le corps de la réponse, sélectionnez **Télécharger** pour enregistrer la sortie du journal.

Pour en savoir plus, consultez les informations disponibles.

- ["Module d'extension NetApp Element pour vCenter Server"](#)
- ["Documentation logicielle SolidFire et Element"](#)

Gérer les connexions d'assistance

Accès aux nœuds de stockage via SSH pour le dépannage de base

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

avancé.

Le compte système sfreadonly permet d'exécuter des commandes de dépannage système et réseau Linux de base, notamment ping .

 Sauf avis contraire du support NetApp , toute modification apportée à ce système n'est pas prise en charge, annule votre contrat de support et peut 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 : Exécuter ssh-keygen à partir de Windows 10, MacOS ou Linux. Il s'agit d'une action ponctuelle permettant de créer une paire de clés utilisateur, réutilisable pour de futures sessions de dépannage. Vous pourriez utiliser des certificats associés aux comptes des employés, ce qui fonctionnerait également dans ce modèle.
- **Activer la fonctionnalité SSH sur le nœud de gestion** : Pour activer la fonctionnalité d'accès à distance en mode gestion, consultez "[ce sujet](#)" . Pour les services de gestion 2.18 et versions ultérieures, la possibilité 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, consultez "[ce sujet](#)" .
- **Configuration du pare-feu** : Si votre nœud de gestion se trouve derrière un serveur proxy, les ports TCP suivants sont requis dans le fichier sshd.config :

Port TCP	Description	Direction de connexion
443	Appels API/HTTPS pour la redirection de port inverse via un tunnel de support ouvert vers l'interface utilisateur web	nœud de gestion vers nœuds de stockage
22	accès de connexion SSH	Du nœud de gestion aux nœuds de stockage ou des nœuds de stockage au nœud de gestion

Options de dépannage

- [Dépannage d'un nœud de cluster](#)
- [Dépannage d'un nœud de cluster avec le support NetApp](#)
- [Dépannage d'un nœud qui ne fait pas partie du cluster](#)

Dépannage d'un nœud de cluster

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

Étapes

1. Connectez-vous au nœud de gestion via SSH en utilisant les identifiants de connexion du compte que vous avez sélectionnés lors de l'installation de la machine virtuelle du nœud de gestion.
2. Sur le nœud de gestion, accédez à /sf/bin .
3. Trouvez le script approprié pour votre système :

- SignSshKeys.ps1
- SignSshKeys.py
- SignSshKeys.sh

SignSshKeys.ps1 nécessite PowerShell 7 ou une version ultérieure et SignSshKeys.py nécessite Python 3.6.0 ou une version ultérieure. ["module de requêtes"](#).



Le SignSshKeys script écrit `user`, `user.pub`, et `user-cert.pub` fichiers dans le répertoire de travail actuel, qui seront ensuite utilisés par la `ssh` commande. Cependant, lorsqu'un fichier de clé publique est fourni au script, seul un `<public_key>` fichier (avec `<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 via le compte système `sfreadonly` sur tous les nœuds du cluster.

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

- Remplacez la valeur entre crochets [] (crochets compris) pour chacun des paramètres suivants :



Vous pouvez utiliser soit le paramètre abrégé, soit le paramètre complet.

- **--ip | -i [adresse IP]**: Adresse IP du nœud cible sur lequel l'API doit s'exécuter.
- **--user | -u [nom_utilisateur]**: Utilisateur du cluster utilisé pour exécuter l'appel API.
- **(Optionnel) --duration | -d [heures]**: La durée pendant laquelle une clé signée doit rester valide sous forme d'entier en heures. La valeur par défaut est de 24 heures.
- **(Optionnel) --publickey | -k [chemin de la clé publique]** : Le chemin vers une clé publique, si l'utilisateur choisit d'en fournir une.

- Comparez votre saisie avec 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
```

- Exécutez la commande.

- Connexion SSH aux adresses IP des nœuds :

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

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

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



Le protocole SSH reste activé sur le nœud de gestion si vous ne le désactivez pas. La configuration SSH activée persiste sur le nœud de gestion lors des mises à jour et des mises à niveau jusqu'à ce qu'elle soit désactivée manuellement.

Dépannage d'un nœud de cluster avec le support NetApp

L'assistance NetApp peut effectuer un dépannage avancé grâce à un compte système qui permet à un technicien d'exécuter des diagnostics Element plus approfondis.

Étapes

1. Connectez-vous au nœud de gestion via SSH en utilisant les identifiants de connexion du compte que vous avez sélectionnés 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>
```

L'assistance NetApp se connectera à votre nœud de gestion via le tunnel d'assistance.

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

`SignSshKeys.ps1` nécessite PowerShell 7 ou une version ultérieure et `SignSshKeys.py` nécessite Python 3.6.0 ou une version ultérieure. ["module de requêtes"](#) .



Le `SignSshKeys` script écrit `user`, `user.pub`, et `user-cert.pub` fichiers dans le répertoire de travail actuel, qui seront ensuite utilisés par la `ssh` commande. Cependant, lorsqu'un fichier de clé publique est fourni au script, seul un `<public_key>` fichier (avec `<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 le `--sfadmin` drapeau. Le script active SSH sur tous les nœuds.

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

Pour SSH comme --sfadmin Pour un nœud en cluster, vous devez générer le trousseau SSH à l'aide d'un --user avec supportAdmin accès sur le cluster.

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



- "Configurez l'accès « supportAdmin » à l'aide de l'interface utilisateur Element."
- Configure supportAdmin accès via des API et ajout "supportAdmin" comme le "access" saisissez le type dans la requête API :
 - "Configurer l'accès « supportAdmin » pour un nouveau compte"
 - "Configurer l'accès « supportAdmin » pour un compte existant"

Pour obtenir le clusterAdminID , vous pouvez utiliser le "[ListClusterAdmins](#)" API.

Pour ajouter supportAdmin Pour y accéder, vous devez disposer des priviléges d'administrateur de cluster ou d'administrateur.

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



Vous pouvez utiliser soit le paramètre abrégé, soit le paramètre complet.

- --ip | -i [adresse IP]: Adresse IP du nœud cible sur lequel l'API doit s'exécuter.
- --user | -u [nom_utilisateur]: Utilisateur du cluster utilisé pour exécuter l'appel API.
- (Optionnel) --duration | -d [heures]: La durée pendant laquelle une clé signée doit rester valide sous forme d'entier en heures. La valeur par défaut est de 24 heures.

b. Comparez votre saisie avec l'exemple de commande suivant. Dans cet exemple, 192.168.0.1 est l'adresse 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 l'accès au nœud de support NetApp pour le dépannage :

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

c. Exécutez la commande.

6. Connexion SSH aux adresses IP des nœuds :

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

7. Pour fermer le tunnel d'assistance à distance, saisissez les informations suivantes :

```
rst --killall
```

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



Le protocole SSH reste activé sur le nœud de gestion si vous ne le désactivez pas. La configuration SSH activée persiste sur le nœud de gestion lors des mises à jour et des mises à niveau jusqu'à ce qu'elle soit désactivée manuellement.

Dépannage d'un nœud qui ne fait pas partie du cluster

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

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

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

3. (Facultatif) Désactiver "[fonctionnalité d'accès à distance](#)" à nouveau une fois le dépannage terminé.



Le protocole SSH reste activé sur le nœud de gestion si vous ne le désactivez pas. La configuration SSH activée persiste sur le nœud de gestion lors des mises à jour et des mises à niveau jusqu'à ce qu'elle soit désactivée manuellement.

Trouver plus d'informations

- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation NetApp HCI](#)"

Démarrer une session d'assistance NetApp à distance

Si vous avez besoin d'assistance technique pour votre système de stockage 100 % flash SolidFire , l'assistance 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 Secure Shell (SSH) inversée vers votre environnement.

Vous pouvez ouvrir un port TCP pour une connexion tunnel SSH inverse 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 2.18 et versions ultérieures, la possibilité d'accès à distance est désactivée par défaut sur le nœud de gestion. Pour activer la fonctionnalité d'accès à distance, consultez "[Gérer la fonctionnalité SSH sur le nœud de gestion](#)" .
- Si votre nœud de gestion se trouve derrière un serveur proxy, les ports TCP suivants sont requis dans le fichier sshd.config :

Port TCP	Description	Direction de connexion
443	Appels API/HTTPS pour la redirection de port inverse via un tunnel de support ouvert vers l'interface utilisateur web	nœud de gestion vers nœuds de stockage
22	accès de connexion SSH	Du nœud de gestion aux nœuds de stockage ou des nœuds de stockage au nœud de gestion

Étapes

- Connectez-vous à votre nœud de gestion et ouvrez une session de terminal.

- À l'invite, saisissez les informations suivantes :

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

- Pour fermer le tunnel d'assistance à distance, saisissez les informations suivantes :

```
rst --killall
```

- (Facultatif) Désactiver "[fonctionnalité d'accès à distance](#)" encore.



Le protocole SSH reste activé sur le nœud de gestion si vous ne le désactivez pas. La configuration SSH activée persiste sur le nœud de gestion lors des mises à jour et des mises à niveau jusqu'à ce qu'elle soit désactivée manuellement.

Trouver plus d'informations

- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation logicielle SolidFire et Element](#)"

Gérer 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 (mNode) à l'aide de l'API REST. La capacité SSH qui fournit "[Accès à la session du tunnel d'assistance à distance \(RST\) de NetApp Support](#)" est désactivé par défaut sur les nœuds de gestion exécutant les services de gestion 2.18 ou ultérieurs.

À partir de Management Services 2.20.69, vous pouvez activer et désactiver la fonctionnalité SSH sur le nœud de gestion à l'aide de l'interface utilisateur de NetApp Hybrid Cloud Control.

Ce dont vous aurez besoin

- * Autorisations NetApp Hybrid Cloud Control* : Vous disposez des autorisations d'administrateur.
- **Permissions d'administrateur de cluster** : Vous disposez des autorisations d'administrateur sur le cluster de stockage.
- **Logiciel Element** : Votre cluster exécute le logiciel NetApp Element 11.3 ou une version ultérieure.
- **Nœud de gestion** : Vous avez déployé un nœud de gestion exécutant la version 11.3 ou ultérieure.
- **Mises à jour des services de gestion** :

- Pour utiliser l'interface utilisateur de NetApp Hybrid Cloud Control, vous devez mettre à jour votre "[ensemble de services de gestion](#)" à la version 2.20.69 ou ultérieure.
- Pour utiliser l'interface utilisateur de l'API REST, vous avez mis à jour votre "[ensemble de services de gestion](#)" à la version 2.17.

Options

- [Activez ou désactivez la fonctionnalité SSH sur le nœud de gestion à l'aide de l'interface utilisateur de NetApp Hybrid Cloud Control.](#)

Vous pouvez effectuer l'une des tâches suivantes après avoir "[authentifier](#)" :

- [Activer ou désactiver la fonctionnalité SSH sur le nœud de gestion à l'aide des API](#)
- [Déterminer l'état de la capacité SSH sur le nœud de gestion à l'aide des API](#)

Activez ou désactivez la fonctionnalité SSH sur le nœud de gestion à l'aide de l'interface utilisateur de NetApp Hybrid Cloud Control.

Vous pouvez désactiver ou réactiver la fonctionnalité SSH sur le nœud de gestion. capacité SSH qui fournit "[Accès à la session du tunnel d'assistance à distance \(RST\) de NetApp Support](#)" est désactivé par défaut sur les nœuds de gestion exécutant les services de gestion 2.18 ou ultérieurs. La désactivation de SSH ne met pas fin aux sessions client SSH existantes ni ne les déconnecte du nœud de gestion. Si vous désactivez SSH et choisissez de le réactiver ultérieurement, vous pouvez le faire à l'aide de l'interface utilisateur de NetApp Hybrid Cloud Control.



Pour activer ou désactiver l'accès au support via SSH pour un cluster de stockage, vous devez utiliser le "[page des paramètres du cluster Element UI](#)".

Étapes

1. Depuis le tableau de bord, sélectionnez le menu des options en haut à droite et sélectionnez **Configurer**.
2. Dans l'écran **Accès au support pour le nœud de gestion**, basculez le commutateur pour activer le SSH du nœud de gestion.
3. Une fois le dépannage terminé, dans l'écran **Accès au support pour le nœud de gestion**, basculez l'interrupteur pour désactiver le SSH du nœud de gestion.

Activer ou désactiver la fonctionnalité SSH sur le nœud de gestion à l'aide des API

Vous pouvez désactiver ou réactiver la fonctionnalité SSH sur le nœud de gestion. capacité SSH qui fournit "[Accès à la session du tunnel d'assistance à distance \(RST\) de NetApp Support](#)" est désactivé par défaut sur les nœuds de gestion exécutant les services de gestion 2.18 ou ultérieurs. La désactivation de SSH ne met pas fin aux sessions client SSH existantes ni ne les déconnecte du nœud de gestion. Si vous désactivez SSH et choisissez de le réactiver ultérieurement, vous pouvez le faire en utilisant la même API.

Commande API

Pour les services de gestion 2.18 ou ultérieurs :

```
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 2.17 ou antérieurs :

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



Vous pouvez trouver le porteur \${TOKEN} utilisé par la commande API lorsque vous ["autoriser"](#). Le porteur \${TOKEN} se trouve dans la réponse curl.

Étapes de l'interface utilisateur de l'API REST

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

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

2. Sélectionnez **Autoriser** et complétez les informations suivantes :

- Saisissez le nom d'utilisateur et le mot de passe du cluster.
 - Saisissez l'identifiant du client comme mnode-client .
 - Sélectionnez **Autoriser** pour démarrer une session.
 - Ferme la fenêtre.
3. Depuis l'interface utilisateur de l'API REST, sélectionnez **PUT /settings/ssh**.
- Sélectionnez **Essayer**.
 - Définissez le paramètre **activé** sur `false` pour désactiver SSH ou `true` pour réactiver la fonctionnalité SSH qui avait été précédemment désactivée.
 - Sélectionnez **Exécuter**.

Déterminer l'état de la capacité SSH sur le nœud de gestion à l'aide des 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 du nœud de gestion. Le protocole SSH est désactivé par défaut sur les nœuds de gestion exécutant les services de gestion 2.18 ou ultérieurs.

Commande API

Pour les services de gestion 2.18 ou ultérieurs :

```
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 2.17 ou antérieurs :

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



Vous pouvez trouver le porteur \${TOKEN} utilisé par la commande API lorsque vous "[autoriser](#)".
Le porteur \${TOKEN} se trouve dans la réponse curl...

Étapes de l'interface utilisateur de l'API REST

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

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

2. Sélectionnez **Autoriser** et complétez les informations suivantes :
 - a. Saisissez le nom d'utilisateur et le mot de passe du cluster.
 - b. Saisissez l'identifiant du client comme mnode-client .
 - c. Sélectionnez **Autoriser** pour démarrer une session.
 - d. Ferme la fenêtre.
3. Dans l'interface utilisateur de l'API REST, sélectionnez **GET /settings/ssh**.
 - a. Sélectionnez **Essayer**.
 - b. Sélectionnez **Exécuter**.

Trouver plus d'informations

- "[Module d'extension NetApp Element pour vCenter Server](#)"
- "[Documentation logicielle SolidFire et Element](#)"

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE 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.