



Gestion du cluster via l'interface de ligne de commandes

ONTAP 9

NetApp
April 24, 2024

Sommaire

Gestion du cluster via l'interface de ligne de commandes	1
Présentation de l'administration avec l'interface de ligne de commande	1
Administrateurs Cluster et SVM	1
Accès au cluster via l'interface de ligne de commandes (administrateurs de cluster uniquement)	3
Utilisez l'interface de ligne de commandes ONTAP	11
Gérer les sessions CLI	26
Gestion du cluster (administrateurs du cluster uniquement)	27
Gérer des nœuds	32
Configuration du réseau SP/BMC	56
Gérez les nœuds à distance à l'aide du processeur de service/contrôleur BMC	63
Gestion de l'heure du cluster (administrateurs du cluster uniquement)	96
Gérer la bannière et la MOTD	99
Gestion des tâches et planification	108
Sauvegarde et restauration des configurations de cluster (administrateurs de cluster uniquement)	112
Gestion des « core dumps » (administrateurs du cluster uniquement)	121

Gestion du cluster via l'interface de ligne de commandes

Présentation de l'administration avec l'interface de ligne de commande

Vous pouvez administrer les systèmes ONTAP via l'interface de ligne de commandes. Vous pouvez utiliser les interfaces de gestion ONTAP, accéder au cluster, gérer les nœuds et bien plus encore.

Vous devez utiliser ces procédures dans les circonstances suivantes :

- Vous voulez connaître la gamme de fonctionnalités d'administration ONTAP.
- Vous souhaitez utiliser l'interface de ligne de commandes, et non System Manager ou un outil de script automatisé.

Informations associées

Pour plus d'informations sur la syntaxe et l'utilisation de l'interface de ligne de commande, reportez-vous au ["Référence de page du manuel ONTAP 9" documentation](#) :

Administrateurs Cluster et SVM

Administrateurs Cluster et SVM

Les administrateurs du cluster administrent le cluster entier et les machines virtuelles de stockage (SVM, anciennement appelées vServers) qu'ils contiennent. Les administrateurs SVM n'administrent que leurs propres SVM de données.

Les administrateurs du cluster peuvent administrer l'ensemble du cluster et ses ressources. Ils peuvent également configurer des SVM de données et déléguer l'administration des SVM aux administrateurs des SVM. Les fonctionnalités spécifiques des administrateurs du cluster dépendent de leurs rôles de contrôle d'accès. Par défaut, un administrateur de cluster avec le nom de compte ou de rôle « admin » dispose de toutes les fonctionnalités de gestion du cluster et des SVM.

Les administrateurs du SVM ne peuvent gérer que leurs propres ressources de stockage et réseau SVM, telles que les volumes, les protocoles, les LIF et les services. Les fonctionnalités spécifiques des administrateurs SVM dépendent des rôles de contrôle d'accès qui sont attribués par les administrateurs du cluster.



L'interface de ligne de commande (CLI) ONTAP continue d'utiliser le terme *Vserver* dans la sortie, et `vserver` comme une commande ou un nom de paramètre n'a pas changé.

Gérez l'accès à System Manager

Vous pouvez activer ou désactiver l'accès d'un navigateur Web à System Manager. Vous pouvez également afficher le journal de System Manager.

Vous pouvez contrôler l'accès d'un navigateur Web à System Manager à l'aide de `vserver services web`

```
modify -name sysmgr -vserver cluster_name -enabled[true|false].
```

La journalisation de System Manager est enregistrée dans le `/mroot/etc/log/mlog/sysmgr.log` Fichiers du nœud qui héberge la LIF de gestion du cluster au moment où System Manager est accessible. Vous pouvez afficher les fichiers journaux à l'aide d'un navigateur. Le journal de System Manager est également inclus dans les messages AutoSupport.

Qu'est-ce que le serveur de gestion du cluster

Le serveur de gestion de cluster, également appelé *adminSVM*, est une implémentation SVM spécialisée qui présente le cluster comme une seule entité gérable. Outre les services faisant office de domaine d'administration de niveau le plus élevé, le serveur de gestion du cluster possède des ressources qui n'appartiennent pas de façon logique à un SVM de données.

Le serveur de gestion du cluster est toujours disponible sur le cluster. Vous pouvez accéder au serveur de gestion du cluster par le biais de la console ou du LIF de gestion du cluster.

En cas de défaillance de son port réseau local, la LIF de gestion du cluster bascule automatiquement vers un autre nœud du cluster. En fonction des caractéristiques de connectivité du protocole de gestion que vous utilisez, vous risquez de remarquer ou non le basculement. Si vous utilisez un protocole sans connexion (par exemple, SNMP) ou que vous disposez d'une connexion limitée (par exemple, HTTP), il est peu probable que vous remarquiez le basculement. Cependant, si vous utilisez une connexion à long terme (par exemple, SSH), vous devrez vous reconnecter au serveur de gestion du cluster après le basculement.

Lorsque vous créez un cluster, toutes les caractéristiques de la LIF de gestion du cluster sont configurées, y compris son adresse IP, son masque de réseau, sa passerelle et son port.

Contrairement à un SVM de données ou à un SVM de nœuds, un serveur de gestion du cluster ne possède pas de volume root ni de volumes utilisateur hôte (bien qu'il puisse héberger les volumes du système). En outre, un serveur de gestion du cluster ne peut avoir que des LIFs du type cluster management.

Si vous exécutez le `vserver show` commande, le serveur de gestion du cluster apparaît dans la liste de sortie de cette commande.

Types de SVM

Un cluster se compose de quatre types de SVM, ce qui facilite la gestion du cluster, ainsi que de ses ressources et de l'accès aux données aux clients et aux applications.

Un cluster contient les types suivants de SVM :

- SVM d'administration

Le processus d'installation du cluster crée automatiquement le SVM d'admin pour le cluster. Le SVM admin représente le cluster.

- SVM de nœuds

Un SVM de nœud est créé lorsque le nœud rejoint le cluster, et le SVM de nœud représente les différents nœuds du cluster.

- System SVM (avancé)

Un SVM système est automatiquement créé pour les communications au niveau du cluster dans un IPspace.

- SVM de données

Un SVM de données représente le service des SVM de données. Une fois le cluster setup, un administrateur de cluster doit créer des SVM de données et ajouter des volumes à ces SVM afin de faciliter l'accès aux données depuis le cluster.

Un cluster doit disposer d'au moins un SVM de données pour transmettre des données à ses clients.



Sauf indication contraire, le terme SVM désigne un SVM de données (service de données).

Dans l'interface de ligne de commandes, les SVM sont affichés comme vServers.

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

Accéder au cluster via le port série

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

Étapes

1. Sur la console, appuyez sur entrée.

Le système répond avec l'invite de connexion.

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

Pour accéder au cluster avec...	Entrez le nom de compte suivant...
Compte de cluster par défaut	admin
Un autre compte d'utilisateur administratif	<i>username</i>

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

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

Accéder au cluster via SSH

Vous pouvez émettre des requêtes SSH au cluster pour effectuer des tâches d'administration. SSH est activé par défaut.

Ce dont vous avez besoin

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

Le `-application` paramètre du `security login` les commandes spécifie la méthode d'accès pour un

compte utilisateur. Le security login "[pages de manuel](#)" contiennent des informations supplémentaires.

- Si vous utilisez un compte d'utilisateur de domaine Active Directory (AD) pour accéder au cluster, un tunnel d'authentification pour le cluster doit avoir été configuré via une VM de stockage compatible CIFS et votre compte d'utilisateur de domaine AD doit également avoir été ajouté au cluster avec `ssh` comme méthode d'accès et `domain` comme méthode d'authentification.
- Si vous utilisez des connexions IPv6, vous devez déjà configurer et activer IPv6 sur le cluster, et les politiques de pare-feu doivent déjà être configurées avec des adresses IPv6.

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

Description de la tâche

- Vous devez utiliser un client OpenSSH 5.7 ou version ultérieure.
- Seul le protocole SSH v2 est pris en charge ; SSH v1 n'est pas pris en charge.
- ONTAP prend en charge un maximum de 64 sessions SSH simultanées par nœud.

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

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

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

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

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

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

Options d'authentification SSH

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

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

- À partir de ONTAP 9.4, vous pouvez "[Activez l'authentification multifacteur SSH](#)" Pour les utilisateurs distants LDAP et NIS.

- À partir de ONTAP 9.13.1, vous pouvez éventuellement ajouter la validation du certificat au processus d'authentification SSH afin d'améliorer la sécurité de la connexion. Pour ce faire, "[Associer un certificat X.509 à la clé publique](#)" qu'un compte utilise. Si vous vous connectez à l'aide de SSH avec une clé publique SSH et un certificat X.509, ONTAP vérifie la validité du certificat X.509 avant de vous authentifier à l'aide de la clé publique SSH. La connexion SSH est refusée si le certificat a expiré ou a été révoqué et si la clé publique SSH est automatiquement désactivée.
- À partir de ONTAP 9.14.1, vous pouvez éventuellement ajouter l'authentification à deux facteurs Cisco Duo au processus d'authentification SSH pour améliorer la sécurité de la connexion. Lors de la première connexion après avoir activé l'authentification Cisco Duo, les utilisateurs doivent inscrire un périphérique pour qu'il serve d'authentificateur pour les sessions SSH. Reportez-vous à la section "[Configurez Cisco Duo 2FA pour les connexions SSH](#)". Pour plus d'informations sur la configuration de l'authentification SSH Cisco Duo pour ONTAP.

Étapes

1. À partir d'un hôte d'administration, entrez le `ssh` commande dans l'un des formats suivants :

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

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

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

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

Exemples de requêtes SSH

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

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

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

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

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

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

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

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


Sécurité de connexion SSH

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

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

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



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

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

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

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

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

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

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

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

Exemples d'informations de sécurité de la connexion SSH

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

- Ce message s'affiche après chaque connexion réussie :

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

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

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

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

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

Activer l'accès Telnet ou RSH au cluster

En tant que pratique recommandée pour la sécurité, Telnet et RSH sont désactivés dans la politique de pare-feu de gestion prédéfinie (`mgmt`). Pour permettre au cluster d'accepter les requêtes Telnet ou RSH, vous devez créer une nouvelle politique de pare-feu de gestion pour laquelle Telnet ou RSH est activé, puis associer la nouvelle politique avec la LIF de gestion du cluster.

Description de la tâche

ONTAP vous empêche de modifier des politiques de pare-feu prédéfinies, mais vous pouvez créer une nouvelle politique en clonant les règles prédéfinies `mgmt` Politique de pare-feu de gestion, puis activation de Telnet ou RSH dans le cadre de la nouvelle politique. Cependant, Telnet et RSH ne sont pas des protocoles sécurisés, vous devez donc envisager d'utiliser SSH pour accéder au cluster. SSH fournit un shell distant sécurisé et une session réseau interactive.

Effectuez les étapes suivantes pour activer l'accès Telnet ou RSH aux clusters :

Étapes

1. Saisissez le mode de privilège avancé :
set advanced
2. Activer un protocole de sécurité (RSH ou Telnet) :
security protocol modify -application security_protocol -enabled true
3. Créez une nouvelle politique de pare-feu de gestion basée sur le `mgmt` politique de pare-feu de gestion :
system services firewall policy clone -policy mgmt -destination-policy policy-name
4. Activer Telnet ou RSH dans la nouvelle politique de pare-feu de gestion :
system services firewall policy create -policy policy-name -service security_protocol -action allow -ip-list ip_address/netmask

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

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

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

Accéder au cluster à l'aide de Telnet

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

Ce dont vous avez besoin

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

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

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

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

Par défaut, Telnet est désactivé. Le `system services firewall policy show` commande avec `-service telnet` Paramètre indique si Telnet a été activé dans une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section `system services firewall policy` pages de manuel.

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

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

Description de la tâche

- Telnet n'est pas un protocole sécurisé.

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

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

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

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

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

Étapes

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

telnet *hostname_or_IP*

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

Exemple de requête Telnet

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

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

Accéder au cluster à l'aide de RSH

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

Ce dont vous avez besoin

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

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

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

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

Par défaut, RSH est désactivé. Le `system services firewall policy show` commande avec `-service rsh` Le paramètre indique si le RSH a été activé dans une stratégie de pare-feu. Pour plus d'informations, reportez-vous à la section `system services firewall policy` pages de manuel.

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

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

Description de la tâche

- RSH n'est pas un protocole sécurisé.

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

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

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

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

Étapes

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

```
rsh hostname_or_IP -l username:passwordcommand
```

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

command Est la commande que vous souhaitez exécuter sur RSH.

Exemple de demande de RSH

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

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

Node	Health	Eligibility
node1	true	true
node2	true	true

2 entries were displayed.

```
admin_host$
```

Utilisez l'interface de ligne de commandes ONTAP

Utilisation de l'interface de ligne de commandes ONTAP

L'interface de ligne de commande ONTAP fournit une vue basée sur les commandes de l'interface de gestion. Vous saisissez les commandes à l'invite du système de stockage et les résultats des commandes s'affichent dans un texte.

L'invite de commande CLI est représentée sous la forme `cluster_name::>`.

Si vous définissez le niveau de privilège (c'est-à-dire, le `-privilege` paramètre du `set` commande) à `advanced`, l'invite comprend un astérisque (*), par exemple :

```
cluster_name::*>
```

À propos des différents shells pour la présentation des commandes CLI (administrateurs de cluster uniquement)

Le cluster a trois shells différents pour les commandes CLI, le *clustershell*, le *nodeshell* et le *systemshell*. Les coques sont à des fins différentes, et elles ont chacune un jeu de commandes différent.

- Le clustershell est le shell natif qui démarre automatiquement lorsque vous vous connectez au cluster.

Il fournit toutes les commandes dont vous avez besoin pour configurer et gérer le cluster. L'aide CLI clustershell (déclenchée par ? à l'invite clustershell) affiche les commandes clustershell disponibles. Le `man command_name` commande dans le clustershell affiche la page man pour la commande clustershell spécifiée.

- Le nodeshell est un shell spécial pour les commandes qui prennent effet uniquement au niveau du nœud.

Le nodeshell est accessible via le `system node run` commande.

Aide de l'interface de ligne de commande du nodeshell (déclenchée par ? ou `help` à l'invite nodeshell) affiche les commandes disponibles du nodeshell. Le `man command_name` la commande dans le nodeshell affiche la page man pour la commande nodeshell spécifiée.

De nombreuses commandes et options de nodeshell couramment utilisées sont regroupées ou alitées dans le clustershell et peuvent également être exécutées à partir du clustershell.

- Le systemshell est un shell de bas niveau qui est utilisé uniquement pour le diagnostic et la résolution de problèmes.

Le systemshell et le compte "diag" associé sont destinés à des fins de diagnostic de bas niveau. Leur accès requiert le niveau de privilège de diagnostic et est réservé uniquement au support technique pour effectuer les tâches de dépannage.

Accès aux commandes et options du nodeshell dans le clustershell

Les commandes et options de Nodeshell sont accessibles via le nodeshell:

```
system node run -node nodename
```

De nombreuses commandes et options de nodeshell couramment utilisées sont regroupées ou alitées dans le clustershell et peuvent également être exécutées à partir du clustershell.

Les options Nodeshell prises en charge dans le clustershell sont accessibles à l'aide du `vserver options clustershell` commande. Pour voir ces options, vous pouvez effectuer l'une des opérations suivantes :

- Interroger la CLI clustershell avec `vserver options -vserver nodename_or_clustername -option-name ?`
- Accédez au `vserver options` Page man dans la CLI clustershell avec `man vserver options`

Si vous saisissez une commande ou une option nodeshell ou hérité dans le clustershell et que la commande ou l'option a une commande clustershell équivalente, ONTAP vous informe de la commande clustershell à utiliser.

Si vous entrez une commande ou une option de nodeshell ou hérité qui n'est pas prise en charge dans le

clustershell, ONTAP vous informe de l'état « non pris en charge » pour la commande ou l'option.

Affiche les commandes nodeshell disponibles

Vous pouvez obtenir la liste des commandes du nodeshell disponibles en utilisant l'aide de la CLI du nodeshell.

Étapes

1. Pour accéder au nodeshell, entrez la commande suivante à l'invite du système du clustershell :

```
system node run -node {nodename|local}
```

`local` est le nœud que vous utilisez pour accéder au cluster.



Le `system node run` la commande a une commande alias, `run`.

2. Entrez la commande suivante dans le nodeshell pour voir la liste des commandes disponibles du nodeshell :

```
[commandname] help
```

`_commandname_` est le nom de la commande dont vous souhaitez afficher la disponibilité. Si vous n'incluez pas `_commandname_`, La CLI affiche toutes les commandes du nodeshell disponibles.

Vous entrez `exit` Ou tapez `Ctrl-d` pour revenir à la CLI clustershell.

Exemple d'affichage des commandes de nodeshell disponibles

L'exemple suivant accède au nodeshell d'un nœud nommé `node2` et affiche les informations relatives à la commande nodeshell `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
      [status] [shelf [<adapter>[.<shelf-number>]]] |
      [status] [shelf_log] |
      [status] [shelf_stats] |
      [status] [shelf_power_status] |
      [status] [chassis [all | list-sensors | Temperature | PSU 1 |
PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

Méthodes de navigation dans les répertoires de commandes CLI

Les commandes de l'interface de ligne de commande sont organisées en hiérarchie par

répertoires de commandes. Vous pouvez exécuter des commandes dans la hiérarchie en entrant le chemin de commande complet ou en parcourant la structure du répertoire.

Lorsque vous utilisez l'interface de ligne de commande, vous pouvez accéder à un répertoire de commandes en saisissant le nom du répertoire à l'invite, puis en appuyant sur entrée. Le nom du répertoire est alors inclus dans le texte d'invite pour indiquer que vous interagissez avec le répertoire de commande approprié. Pour aller plus loin dans la hiérarchie de commandes, entrez le nom d'un sous-répertoire de commandes, puis appuyez sur entrée. Le nom du sous-répertoire est alors inclus dans le texte d'invite et le contexte passe à ce sous-répertoire.

Vous pouvez naviguer dans plusieurs répertoires de commandes en entrant la commande entière. Par exemple, vous pouvez afficher des informations sur les disques en entrant dans le `storage disk show` commande à l'invite. Vous pouvez également exécuter la commande en parcourant un seul répertoire de commandes à la fois, comme illustré dans l'exemple suivant :

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

Vous pouvez abrégier les commandes en n'entrant que le nombre minimal de lettres dans une commande qui rend la commande unique au répertoire courant. Par exemple, pour abrégier la commande dans l'exemple précédent, vous pouvez entrer `st d sh`. Vous pouvez également utiliser la touche Tab pour développer des commandes abrégées et afficher les paramètres d'une commande, y compris les valeurs des paramètres par défaut.

Vous pouvez utiliser le `top` commande pour accéder au niveau supérieur de la hiérarchie de commandes et au `up` commande ou `..` commande permettant d'atteindre un niveau dans la hiérarchie de commandes.



Les commandes et les options de commande précédées d'un astérisque (*) dans l'interface de ligne de commande ne peuvent être exécutées qu'au niveau de privilège avancé ou supérieur.

Règles d'indication des valeurs dans l'interface de ligne de commandes

La plupart des commandes comprennent un ou plusieurs paramètres obligatoires ou facultatifs. De nombreux paramètres exigent que vous spécifiez une valeur pour eux. Un certain nombre de règles doivent être respectées dans l'interface de ligne de commandes.

- Une valeur peut être un nombre, un spécificateur booléen, une sélection dans une liste de valeurs prédéfinies énumérées ou une chaîne de texte.

Certains paramètres acceptent une liste séparée par des virgules de deux valeurs ou plus. Les listes de valeurs séparées par des virgules n'ont pas besoin d'être entre guillemets (" "). Chaque fois que vous spécifiez du texte, un espace ou un caractère de requête (s'il ne s'agit pas d'une requête ou d'un texte commençant par un symbole inférieur ou supérieur à), vous devez inclure l'entité entre guillemets.

- L'ILC interprète une marque d'interrogation ("»?»") comme commande permettant d'afficher les informations d'aide pour une commande particulière.
- Certains textes que vous entrez dans l'interface de ligne de commande, par exemple les noms des commandes, les paramètres et certaines valeurs, ne sont pas sensibles à la casse.

Par exemple, lorsque vous saisissez des valeurs de paramètre pour le `vserver cifs` les commandes, majuscules sont ignorées. Cependant, la plupart des valeurs de paramètres, telles que les noms des nœuds, des serveurs virtuels de stockage (SVM), des agrégats, des volumes et des interfaces logiques, sont sensibles à la casse.

- Si vous souhaitez effacer la valeur d'un paramètre qui prend une chaîne ou une liste, vous devez spécifier un ensemble vide de guillemets ("") ou un tiret ("-").
- Le signe dièse ("#"), également appelé signe dièse, indique un commentaire pour une entrée de ligne de commande; s'il est utilisé, il doit apparaître après le dernier paramètre d'une ligne de commande.

La CLI ignore le texte entre ""#"" et la fin de la ligne.

Dans l'exemple suivant, un SVM est créé avec un commentaire texte. Le SVM est ensuite modifié pour supprimer le commentaire :

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

Dans l'exemple suivant, un commentaire de ligne de commande utilisant le signe ""#"" indique ce que fait la commande.

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

Méthodes d'affichage de l'historique des commandes et de réémission des commandes

Chaque session de l'interface de ligne de commande conserve un historique de toutes les commandes qui y sont émises. Vous pouvez afficher l'historique des commandes de la session dans laquelle vous vous trouvez. Vous pouvez également réémettre des commandes.

Pour afficher l'historique des commandes, vous pouvez utiliser le `history` commande.

Pour réémettre une commande, vous pouvez utiliser le `redo` commande avec l'un des arguments suivants :

- Chaîne correspondant à une partie d'une commande précédente

Par exemple, si le seul volume la commande que vous avez exécutée est `volume show`, vous pouvez utiliser l' `redo volume` pour réexécuter la commande.

- L'ID numérique d'une commande précédente, comme indiqué par le `history` commande

Par exemple, vous pouvez utiliser le `redo 4` commande permettant de réémettre la quatrième commande dans la liste de l'historique.

- Décalage négatif par rapport à la fin de la liste d'historique

Par exemple, vous pouvez utiliser le `redo -2` commande pour réémettre la commande que vous avez exécutée il y a deux commandes.

Par exemple, pour rétablir la commande troisième depuis la fin de l'historique des commandes, entrez la commande suivante :

```
cluster1:> redo -3
```

Raccourcis clavier pour la modification des commandes CLI

La commande à l'invite de commande en cours est la commande active. L'utilisation des raccourcis clavier vous permet de modifier rapidement la commande active. Ces raccourcis clavier sont similaires à ceux du shell `tcsh` UNIX et de l'éditeur Emacs.

Le tableau suivant répertorie les raccourcis clavier permettant de modifier les commandes de l'interface de ligne de commande. « Ctrl- » indique que vous maintenez la touche Ctrl enfoncée tout en tapant le caractère spécifié après. « Échap- » indique que vous appuyez sur la touche Échap et relâchez-la, puis saisissez le caractère spécifié après.

Les fonctions que vous recherchez...	Utilisez le raccourci clavier suivant...
Déplacez le curseur d'un caractère vers l'arrière	Ctrl-B
Flèche vers l'arrière	Déplacez le curseur d'un caractère vers l'avant
Ctrl-F	Flèche vers l'avant
Déplacez le curseur d'un mot vers l'arrière	ESC-B
Déplacez le curseur d'un mot vers l'avant	ESC-F
Déplacez le curseur au début de la ligne	Ctrl-A
Déplacez le curseur jusqu'à la fin de la ligne	Ctrl-E
Supprimez le contenu de la ligne de commande du début de la ligne jusqu'au curseur et enregistrez-le dans le tampon de coupe. La mémoire tampon de coupure agit comme une mémoire temporaire, similaire à ce que l'on appelle un <i>presse-papiers</i> dans certains programmes.	Ctrl-U

Les fonctions que vous recherchez...	Utilisez le raccourci clavier suivant...
Supprimez le contenu de la ligne de commande du curseur jusqu'à la fin de la ligne et enregistrez-le dans le tampon de découpe	Ctrl-K
Supprimez le contenu de la ligne de commande du curseur jusqu'à la fin du mot suivant et enregistrez-le dans le tampon de découpe	ESC-D
Supprimez le mot devant le curseur et enregistrez-le dans le tampon de coupe	Ctrl-W
Ank le contenu du tampon de coupe, et le pousser dans la ligne de commande au niveau du curseur	Ctrl + y
Supprimer le caractère avant le curseur	Ctrl-H
Retour arrière	Supprimez le caractère où se trouve le curseur
Ctrl-D.	Effacez la ligne
Ctrl-C	Effacez l'écran
Ctrl-L	Remplacez le contenu actuel de la ligne de commande par l'entrée précédente de la liste d'historique. À chaque répétition du raccourci clavier, le curseur historique se déplace vers l'entrée précédente.
Ctrl-P	ESC-P
Flèche vers le haut	Remplacez le contenu actuel de la ligne de commande par l'entrée suivante de la liste de l'historique. À chaque répétition du raccourci clavier, le curseur historique se déplace vers l'entrée suivante.
Ctrl-N	ESC-N
Flèche vers le bas	Développer une commande partiellement saisie ou répertorier une entrée valide à partir de la position d'édition actuelle
Onglet	Ctrl-I
Afficher l'aide contextuelle	?

Les fonctions que vous recherchez...	Utilisez le raccourci clavier suivant...
Échapper à la cartographie spéciale de la marque de question ("»?") character. For instance, to enter a question mark into a command's argument, press Esc and then the "»" caractère.	ESC- ?
Démarrez la sortie TTY	Ctrl-Q
Arrêter la sortie TTY	Ctrl-S

Utilisation des niveaux de privilège administratif

Les commandes et paramètres ONTAP sont définis à trois niveaux de privilèges : *admin*, *Advanced* et *diagnostic*. Les niveaux de privilège reflètent les niveaux de compétence requis pour exécuter les tâches.

- **admin**

La plupart des commandes et des paramètres sont disponibles à ce niveau. Ils sont utilisés pour les tâches courantes ou de routine.

- **avancé**

Les commandes et les paramètres à ce niveau sont rarement utilisés, nécessitent des connaissances avancées et peuvent causer des problèmes s'ils sont utilisés de façon inappropriée.

Vous utilisez des commandes ou des paramètres avancés uniquement avec les conseils du personnel de support.

- **diagnostic**

Les paramètres et les commandes de diagnostic sont potentiellement sources de perturbation. Ils sont utilisés uniquement par le personnel de support pour diagnostiquer et corriger les problèmes.

Définissez le niveau de privilège dans l'interface de ligne de commandes

Vous pouvez définir le niveau de privilège dans l'interface de ligne de commandes en utilisant la `set` commande. Les modifications apportées aux paramètres de niveau de privilège s'appliquent uniquement à la session dans laquelle vous vous trouvez. Elles ne sont pas persistantes d'une session à l'autre.

Étapes

1. Pour définir le niveau de privilège dans l'interface de ligne de commandes, utilisez le `set` commande avec `-privilege` paramètre.

Exemple de définition du niveau de privilège

L'exemple suivant définit le niveau de privilège sur avancé, puis sur admin :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1:*> set -privilege admin
```

Définissez les préférences d’affichage dans la CLI

Vous pouvez définir les préférences d’affichage d’une session CLI à l’aide de `set` commande et `rows` commande. Les préférences définies s’appliquent uniquement à la session dans laquelle vous vous trouvez. Elles ne sont pas persistantes d’une session à l’autre.

Description de la tâche

Vous pouvez définir les préférences d’affichage CLI suivantes :

- Niveau de privilège de la session de commande
- Indique si des confirmations sont émises pour des commandes potentiellement perturbatrices
- Si `show` les commandes affichent tous les champs
- Le ou les caractères à utiliser comme séparateur de champ
- Unité par défaut lors du reporting des tailles de données
- Le nombre de lignes que l’écran affiche dans la session CLI en cours avant que l’interface n’interrompt la sortie

Si le nombre de rangées préféré n’est pas spécifié, il est automatiquement ajusté en fonction de la hauteur réelle du terminal. Si la hauteur réelle n’est pas définie, le nombre de lignes par défaut est 24.

- Le nœud ou la machine virtuelle de stockage par défaut
- Si une commande continue doit s’arrêter s’il rencontre une erreur

Étapes

1. Pour définir les préférences d’affichage CLI, utilisez le `set` commande.

Pour définir le nombre de lignes que l’écran affiche dans la session CLI en cours, vous pouvez également utiliser le `rows` commande.

Pour plus d’informations, consultez les pages de manuel du `set` commande et `rows` commande.

Exemple de définition des préférences d’affichage dans l’interface de ligne de commande

L’exemple suivant définit une virgule comme étant le séparateur de champ, définit GB comme unité de taille de données par défaut, et définit le nombre de lignes sur 50 :

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

Méthodes d'utilisation des opérateurs de requête

L'interface de gestion prend en charge les requêtes, les modèles de style UNIX et les caractères génériques pour vous permettre de faire correspondre plusieurs valeurs dans les arguments de paramètres de commande.

Le tableau suivant décrit les opérateurs de requête pris en charge :

Opérateur	Description
*	Caractère générique correspondant à toutes les entrées. Par exemple, la commande <code>volume show -volume *tmp*</code> affiche la liste de tous les volumes dont le nom inclut la chaîne <code>tmp</code> .
!	PAS opérateur. Indique une valeur qui ne doit pas être comparée ; par exemple, <code>!vs0</code> indique de ne pas correspondre à la valeur <code>vs0</code> .
OU opérateur .	<code>vs2*</code> correspond soit à <code>vs0</code> , soit à <code>vs2</code> . Vous pouvez spécifier plusieurs instructions OU ; par exemple, <code>`a</code> Sépare deux valeurs à comparer , par exemple <code>`*vs0</code>
b*	<code>*c*</code> correspond à l'entrée <code>a</code> , toute entrée commençant par <code>b</code> , et toute entrée qui inclut <code>c</code> .
..	Opérateur de gamme. Par exemple : <code>5..10</code> correspond à n'importe quelle valeur de 5 à 10, inclus.
<	Moins que l'opérateur. Par exemple : <code><20</code> correspond à toute valeur inférieure à 20.
>	Opérateur supérieur à. Par exemple : <code>>5</code> correspond à toute valeur supérieure à 5.
<=	Inférieur ou égal à l'opérateur. Par exemple : <code>≤5</code> correspond à toute valeur inférieure ou égale à 5.

Opérateur	Description
>=	Supérieur à ou égal à l'opérateur. Par exemple : <code>>=5</code> correspond à toute valeur supérieure ou égale à 5.
{query}	Requête étendue. Une requête étendue doit être spécifiée comme premier argument après le nom de la commande, avant tout autre paramètre. Par exemple, la commande <code>volume modify {-volume *tmp*} -state offline</code> définit hors ligne tous les volumes dont le nom inclut la chaîne <code>tmp</code> .

Si vous voulez analyser les caractères de requête en tant que littéraux, vous devez les inclure entre guillemets (par exemple, "<10", "0..100", "*abc*", ou "a|b") pour que les résultats corrects soient renvoyés.

Vous devez inclure des noms de fichiers bruts entre guillemets pour empêcher l'interprétation des caractères spéciaux. Cela s'applique également aux caractères spéciaux utilisés par le cluster shell.

Vous pouvez utiliser plusieurs opérateurs de requête dans une seule ligne de commande. Par exemple, la commande `volume show -size >1GB -percent-used <50 -vserver !vs1` Affiche tous les volumes dont la taille est supérieure à 1 Go, inférieurs à 50 % utilisés et non sur la machine virtuelle de stockage (SVM) nommée « vs1 ».

Informations associées

["Raccourcis clavier pour la modification des commandes CLI"](#)

Méthodes d'utilisation des requêtes étendues

Vous pouvez utiliser des requêtes étendues pour faire correspondre et exécuter des opérations sur des objets ayant des valeurs spécifiées.

Vous spécifiez les requêtes étendues en les enfermant entre crochets (`{}`). Une requête étendue doit être spécifiée comme premier argument après le nom de la commande, avant tout autre paramètre. Par exemple, pour mettre hors ligne tous les volumes dont le nom inclut la chaîne `tmp`, vous exécutez la commande dans l'exemple suivant :

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Les requêtes étendues ne sont généralement utiles qu'avec `modify` et `delete` commandes. Ils n'ont aucun sens en `create` ou `show` commandes.

La combinaison de requêtes et d'opérations de modification est un outil utile. Toutefois, il peut être source de confusion et d'erreurs si la mise en œuvre est incorrecte. Par exemple, à l'aide du (privilège avancé) `system node image modify` commande permettant de définir automatiquement l'image logicielle par défaut d'un nœud définit l'autre image logicielle comme non la valeur par défaut. La commande dans l'exemple suivant est effectivement une opération nulle :

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

Cette commande définit l'image par défaut actuelle comme image non par défaut, puis définit la nouvelle image par défaut (l'image précédente non par défaut) sur l'image non par défaut, ce qui entraîne la conservation des paramètres par défaut d'origine. Pour effectuer l'opération correctement, vous pouvez utiliser la commande comme indiqué dans l'exemple suivant :

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

Méthodes de personnalisation de la commande show à l'aide des champs

Lorsque vous utilisez le `-instance` paramètre avec un `show` commande pour afficher les détails, le résultat peut être long et inclure plus d'informations qu'il ne vous en faut. Le `-fields` paramètre de la `show` vous permet d'afficher uniquement les informations que vous spécifiez.

Par exemple, en cours d'exécution `volume show -instance` est susceptible de donner lieu à plusieurs écrans d'information. Vous pouvez utiliser `volume show -fields fieldname[,fieldname...]` pour personnaliser la sortie de sorte qu'elle inclut uniquement le ou les champs spécifiés (en plus des champs par défaut qui sont toujours affichés). Vous pouvez utiliser `-fields ?` pour afficher des champs valides pour un `show` commande.

L'exemple suivant montre la différence de sortie entre le `-instance` paramètre et le `-fields` paramètre :


```

cluster1::> volume show -instance

Vserver Name: cluster1-1
Volume Name: vol0
Aggregate Name: aggr0
Volume Size: 348.3GB
Volume Data Set ID: -
Volume Master Data Set ID: -
Volume State: online
Volume Type: RW
Volume Style: flex
...
Space Guarantee Style: volume
Space Guarantee in Effect: true
...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume  space-guarantee  space-guarantee-enabled
-----  -
cluster1-1 vol0    volume           true
cluster1-2 vol0    volume           true
vs1      root_vol
          volume           true
vs2      new_vol
          volume           true
vs2      root_vol
          volume           true
...
cluster1::>

```

A propos des paramètres de position

Vous pouvez utiliser la fonctionnalité des paramètres de position de l'interface de ligne de commande ONTAP pour améliorer l'efficacité de l'entrée de commande. Vous pouvez interroger une commande pour identifier les paramètres qui sont de position pour la commande.

Définition d'un paramètre de position

- Un paramètre de position est un paramètre qui ne vous demande pas de spécifier le nom du paramètre avant de spécifier la valeur du paramètre.

- Un paramètre de position peut être intercalé avec des paramètres non positionnels dans l'entrée de commande, tant qu'il observe sa séquence relative avec d'autres paramètres de position dans la même commande, comme indiqué dans l' **`command_name ?`** sortie.
- Un paramètre de position peut être un paramètre obligatoire ou facultatif pour une commande.
- Un paramètre peut être positionné pour une commande mais non positionnel pour une autre.



L'utilisation de la fonctionnalité des paramètres de position dans les scripts n'est pas recommandée, en particulier lorsque les paramètres de position sont facultatifs pour la commande ou si des paramètres facultatifs sont répertoriés avant eux.

Identifiez un paramètre de position

Vous pouvez identifier un paramètre de position dans l' **`command_name ?`** sortie de la commande. Un paramètre de position comporte des crochets autour de son nom de paramètre, dans l'un des formats suivants :

- `[-parameter_name] parameter_value` affiche un paramètre requis qui est positionnel.
- `[[[-parameter_name] parameter_value]` affiche un paramètre facultatif qui est positionnel.

Par exemple, lorsqu'il s'affiche comme suit dans le **`command_name ?`** sortie, le paramètre est positionné pour la commande dans laquelle il apparaît :

- `[-lif] <lif-name>`
- `[[[-lif] <lif-name>]`

Toutefois, lorsqu'il est affiché comme suit, le paramètre n'est pas positionné pour la commande dans laquelle il apparaît :

- `-lif <lif-name>`
- `[-lif <lif-name>]`

Exemples d'utilisation de paramètres de position

Dans l'exemple suivant, le **`volume create ?`** le résultat indique que trois paramètres sont en position pour la commande : `-volume`, `-aggregate`, et `-size`.

```

cluster1::> volume create ?
    -vserver <vserver name>                Vserver Name
    [-volume] <volume name>                Volume Name
    [-aggregate] <aggregate name>          Aggregate Name
    [[-size] {<integer>[KB|MB|GB|TB|PB]]]  Volume Size
    [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                           Volume State (default: online)
    [ -type {RW|DP|DC} ]                   Volume Type (default: RW)
    [ -policy <text> ]                     Export Policy
    [ -user <user name> ]                 User ID
    ...
    [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
    [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
    ...

```

Dans l'exemple suivant, le `volume create` la commande est spécifiée sans utiliser la fonctionnalité des paramètres de position :

```

cluster1::> volume create -vserver svml -volume voll -aggregate aggr1 -size 1g
-percent-snapshot-space 0

```

Les exemples suivants utilisent la fonctionnalité des paramètres de position pour augmenter l'efficacité de l'entrée de commande. Les paramètres de position sont entrelatés avec des paramètres non positionnels dans `volume create` la commande et les valeurs des paramètres de position sont spécifiées sans les noms des paramètres. Les paramètres de position sont spécifiés dans la même séquence que celle indiquée par le **volume create ?** sortie. C'est-à-dire la valeur de `-volume` est spécifié avant celle de `-aggregate`, qui est à son tour spécifié avant celle de `-size`.

```

cluster1::> volume create vol2 aggr1 1g -vserver svml -percent-snapshot-space 0

```

```

cluster1::> volume create -vserver svml vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none

```

Méthodes d'accès aux pages de manuel ONTAP

Les pages de manuel ONTAP expliquent comment utiliser les commandes de l'interface de ligne de commande ONTAP. Ces pages sont disponibles sur la ligne de commande et sont également publiées dans *command references* spécifique à la version.

Sur la ligne de commande ONTAP, utilisez `man command_name` pour afficher la page man de la commande spécifiée. Si vous ne spécifiez pas de nom de commande, l'index de page manuelle s'affiche. Vous pouvez utiliser le `man man` pour afficher les informations relatives à man commande elle-même. Vous pouvez quitter une page man en entrant `q`.

Reportez-vous à la [Référence des commandes pour votre version de ONTAP 9](#) Pour en savoir plus sur les commandes ONTAP de niveau administrateur et avancé disponibles dans votre version.

Gérer les sessions CLI

Vous pouvez enregistrer une session CLI dans un fichier dont le nom et la taille sont définis, puis télécharger le fichier vers une destination FTP ou HTTP. Vous pouvez également afficher ou supprimer des fichiers dans lesquels vous avez déjà enregistré des sessions CLI.

Enregistrez une session CLI

Un enregistrement d'une session CLI se termine lorsque vous arrêtez l'enregistrement ou que vous mettez fin à la session CLI, ou lorsque le fichier atteint la limite de taille spécifiée. La taille de fichier par défaut est de 1 Mo. La taille maximale des fichiers est de 2 Go.

L'enregistrement d'une session CLI est utile, par exemple, si vous dépannez un problème et souhaitez enregistrer des informations détaillées ou si vous souhaitez créer un enregistrement permanent de l'utilisation de l'espace à un moment donné.

Étapes

1. Démarrer l'enregistrement de la session CLI en cours dans un fichier :

```
system script start
```

Pour plus d'informations sur l'utilisation du `system script start` voir la page man.

ONTAP commence à enregistrer votre session CLI dans le fichier spécifié.

2. Passez à la session CLI.
3. Lorsque vous avez terminé, arrêtez l'enregistrement de la session :

```
system script stop
```

Pour plus d'informations sur l'utilisation du `system script stop` voir la page man.

ONTAP arrête l'enregistrement de votre session CLI.

Commandes permettant de gérer les enregistrements des sessions CLI

Vous utilisez le `system script` Commandes permettant de gérer les enregistrements des sessions CLI.

Les fonctions que vous recherchez...	Utilisez cette commande...
Démarrez l'enregistrement de la session CLI en cours dans un fichier spécifié	<code>system script start</code>
Arrêter l'enregistrement de la session CLI en cours	<code>system script stop</code>
Affiche des informations sur les enregistrements des sessions CLI	<code>system script show</code>

Les fonctions que vous recherchez...	Utilisez cette commande...
Télécharger un enregistrement d'une session CLI vers une destination FTP ou HTTP	<code>system script upload</code>
Supprimer un enregistrement d'une session CLI	<code>system script delete</code>

Informations associées

["Commandes de ONTAP 9"](#)

Commandes permettant de gérer la période de temporisation automatique des sessions de l'interface de ligne de commande

La valeur du délai d'attente spécifie la durée pendant laquelle une session de l'interface de ligne de commande reste inactive avant d'être automatiquement arrêtée. La valeur du délai d'expiration de l'interface de ligne de commandes correspond à l'ensemble du cluster C'est-à-dire que chaque nœud d'un cluster utilise la même valeur de temporisation de l'interface de ligne de commandes.

Par défaut, le délai d'expiration automatique des sessions de l'interface de ligne de commande est de 30 minutes.

Vous utilisez le `system timeout` Commandes permettant de gérer la période de temporisation automatique des sessions de l'interface de ligne de commande.

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche la période de temporisation automatique pour les sessions CLI	<code>system timeout show</code>
Modifier la période de temporisation automatique pour les sessions de l'interface de ligne de commande	<code>system timeout modify</code>

Informations associées

["Commandes de ONTAP 9"](#)

Gestion du cluster (administrateurs du cluster uniquement)

Affiche des informations relatives aux nœuds dans un cluster

Vous pouvez afficher les noms des nœuds, que les nœuds soient sains et si ils sont éligibles au cluster. Au niveau de privilège avancé, vous pouvez également afficher si un nœud contient epsilon.

Étapes

1. Pour afficher des informations sur les nœuds d'un cluster, utilisez le `cluster show` commande.

Si vous souhaitez que la sortie indique si un nœud contient epsilon, lancer la commande au niveau de privilège avancé.

Exemples d’affichage des nœuds dans un cluster

L’exemple suivant affiche des informations sur tous les nœuds d’un cluster à quatre nœuds :

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
node3                true   true
node4                true   true
```

L’exemple suivant affiche des informations détaillées sur le nœud nommé « node1 » au niveau de privilège avancé :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

      Node: node1
Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
  Epsilon: false
Eligibility: true
    Health: true
```

Afficher les attributs du cluster

Vous pouvez afficher l’identifiant unique d’un cluster (UUID), son nom, son numéro de série, son emplacement et ses informations de contact.

Étapes

1. Pour afficher les attributs d’un cluster, utilisez le `cluster identity show` commande.

Exemple d’affichage des attributs du cluster

L’exemple suivant affiche le nom, le numéro de série, l’emplacement et les informations de contact d’un cluster.

```
cluster1::> cluster identity show
```

```
Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
Cluster Name: cluster1
Cluster Serial Number: 1-80-123456
Cluster Location: Sunnyvale
Cluster Contact: jsmith@example.com
```

Modifier les attributs du cluster

Vous pouvez modifier les attributs d'un cluster, comme le nom du cluster, l'emplacement et les informations de contact.

Description de la tâche

Vous ne pouvez pas modifier l'UUID d'un cluster, qui est défini lors de sa création.

Étapes

1. Pour modifier les attributs du cluster, utilisez le `cluster identity modify` commande.

Le `-name` le paramètre spécifie le nom du cluster. Le `cluster identity modify` la page man décrit les règles à respecter lorsque vous spécifiez le nom du cluster.

Le `-location` le paramètre spécifie l'emplacement pour le cluster.

Le `-contact` paramètre spécifie les informations de contact telles qu'un nom ou une adresse e-mail.

Exemple de changement de nom d'un cluster

La commande suivante renomme le cluster actuel (« cluster1 ») en « cluster2 » :

```
cluster1::> cluster identity modify -name cluster2
```

Afficher l'état des anneaux de réplication de cluster

Vous pouvez afficher l'état des anneaux de réplication du cluster pour vous aider à diagnostiquer les problèmes au niveau du cluster. Si votre cluster rencontre des problèmes, le personnel de support peut vous demander d'effectuer cette tâche afin de vous aider dans les opérations de dépannage.

Étapes

1. Pour afficher l'état des anneaux de réplication de cluster, utilisez le `cluster ring show` commande au niveau de privilège avancé.

Exemple d'affichage de l'état de réplication-anneau du cluster

L'exemple suivant affiche l'état de l'anneau de réplication VLDB sur un nœud nommé node0 :

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
      Node: node0
    Unit Name: vldb
      Status: master
        Epoch: 5
Master Node: node0
  Local Node: node0
      DB Epoch: 5
DB Transaction: 56
  Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412

```

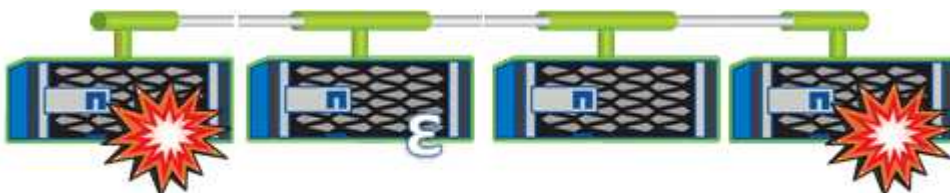
À propos du quorum et de l'épsilon

Le quorum et l'épsilon sont des mesures importantes de l'état de santé du cluster et des fonctions qui indiquent ensemble que les clusters répondent aux problèmes potentiels de communication et de connectivité.

Quorum est une condition préalable à un cluster pleinement opérationnel. Lorsqu'un cluster est au quorum, une simple majorité de nœuds sont en bon état et peuvent communiquer entre eux. En cas de perte du quorum, le cluster n'a plus la possibilité d'effectuer des opérations normales sur le cluster. Un seul ensemble de nœuds peut avoir le quorum à la fois car tous les nœuds partagent collectivement une vue unique des données. Par conséquent, si deux nœuds qui ne communiquent pas sont autorisés à modifier les données de manière divergentes, il n'est plus possible de réconcilier les données en une seule vue de données.

Chaque nœud du cluster participe à un protocole de vote qui sélectionne un nœud *master* ; chaque nœud restant est un *Secondary*. Le nœud maître est chargé de synchroniser les informations sur le cluster. Lorsque le quorum est formé, il est maintenu par vote continu. Si le nœud maître se met hors ligne et que le cluster est encore au quorum, un nouveau maître est élu par les nœuds qui restent en ligne.

Étant donné qu'il y a la possibilité d'une TIE dans un cluster qui a un nombre pair de nœuds, un nœud a un poids fractionnaire supplémentaire appelé *epsilon*. Si la connectivité entre deux portions égales d'un grand cluster tombe en panne, le groupe de nœuds contenant epsilon maintient le quorum, en supposant que tous les nœuds sont en bon état. Par exemple, l'illustration suivante montre un cluster à quatre nœuds où deux des nœuds ont échoué. Cependant, comme l'un des nœuds survivants contient epsilon, le cluster reste dans le quorum même s'il n'y a pas une simple majorité de nœuds sains.



Epsilon est automatiquement affecté au premier nœud lors de la création du cluster. Si le nœud qui contient epsilon devient défectueux, prend le relais de son partenaire haute disponibilité ou est repris par son partenaire haute disponibilité, puis il est automatiquement réaffecté à un nœud saine dans une paire haute disponibilité différente.

La mise hors ligne d'un nœud peut affecter la capacité du cluster à rester dans le quorum. Par conséquent, ONTAP émet un message d'avertissement si vous tentez une opération qui détiendra le cluster du quorum ou qui le mettra hors service de la perte du quorum. Vous pouvez désactiver les messages d'avertissement de quorum à l'aide du `cluster quorum-service options modify` commande au niveau de privilège avancé.

De manière générale, en supposant une connectivité fiable entre les nœuds du cluster, un cluster plus grand est plus stable qu'un cluster plus petit. Le quorum nécessaire à une simple majorité de moitié des nœuds plus epsilon est plus facile à maintenir dans un cluster de 24 nœuds que dans un cluster de deux nœuds.

Un cluster à deux nœuds présente des défis uniques pour le maintien du quorum. Les clusters à deux nœuds utilisent *cluster HA*, dans lesquels aucun nœud ne contient epsilon ; les deux nœuds sont plutôt interrogés en continu afin de s'assurer que si un nœud tombe en panne, l'autre dispose d'un accès en lecture/écriture complet aux données, ainsi que de l'accès aux interfaces logiques et aux fonctions de gestion.

De quels volumes système sont-ils

Les volumes système sont des volumes FlexVol qui contiennent des métadonnées spéciales, comme les métadonnées pour les journaux d'audit des services de fichiers. Ces volumes sont visibles dans le cluster, de sorte que vous puissiez entièrement prendre en compte l'utilisation du stockage dans votre cluster.

Les volumes système sont détenus par le serveur de gestion de cluster (également appelé SVM d'administration) et ils sont créés automatiquement lorsque l'audit des services de fichiers est activé.

Vous pouvez afficher les volumes système à l'aide du `volume show` mais la plupart des autres opérations de volume ne sont pas autorisées. Par exemple, vous ne pouvez pas modifier un volume système à l'aide de `volume modify` commande.

Cet exemple présente quatre volumes système sur le SVM d'administration, qui ont été automatiquement créés lorsque les audits de services de fichiers ont été activés pour un SVM de données dans le cluster :

```
cluster1::> volume show -vserver cluster1
```

Vserver	Volume	Aggregate	State	Type	Size	Available
Used%						
-----	-----	-----	-----	-----	-----	-----

cluster1	MDV_aud_1d0131843d4811e296fc123478563412	aggr0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_8be27f813d7311e296fc123478563412	root_vs0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_9dc4ad503d7311e296fc123478563412	aggr1	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_a4b887ac3d7311e296fc123478563412	aggr2	online	RW	2GB	1.90GB
5%						

4 entries were displayed.

Gérer des nœuds

Ajout de nœuds au cluster

Une fois le cluster créé, vous pouvez le développer en ajoutant des nœuds. Vous n'ajoutez qu'un seul nœud à la fois.

Ce dont vous avez besoin

- Si vous ajoutez des nœuds à un cluster à plusieurs nœuds, tous les nœuds existants du cluster doivent être en bon état (indiqué par la `cluster show`).
- Si vous ajoutez des nœuds à un cluster sans commutateur à deux nœuds, vous devez convertir le cluster sans commutateur à deux nœuds en cluster à connexion par commutateur à l'aide d'un commutateur de cluster pris en charge par NetApp.

La fonctionnalité de cluster sans commutateur n'est prise en charge que dans un cluster à deux nœuds.

- Si vous ajoutez un second nœud à un cluster à un seul nœud, le second nœud doit avoir été installé et le réseau de clusters doit avoir été configuré.
- Si la configuration automatique du processeur de service est activée sur le cluster, le sous-réseau spécifié pour le processeur de service doit disposer de ressources disponibles pour permettre au nœud de jonction d'utiliser le sous-réseau spécifié pour configurer automatiquement le processeur de service.
- Vous devez avoir collecté les informations suivantes pour le LIF de gestion des nœuds du nouveau nœud :
 - Port
 - Adresse IP
 - Masque de réseau

- Passerelle par défaut

Description de la tâche

Les nœuds doivent être numériques de manière à pouvoir former des paires haute disponibilité. Une fois que vous avez commencé à ajouter un nœud au cluster, vous devez terminer le processus. Le nœud doit faire partie du cluster avant de pouvoir ajouter un autre nœud.

Étapes

1. Mettez le nœud que vous souhaitez ajouter au cluster sous tension.

Le nœud démarre et l'assistant de configuration du nœud démarre sur la console.

```
Welcome to node setup.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
  Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.

Enter the node management interface port [e0M]:
```

2. Quittez l'assistant de configuration des nœuds : `exit`

L'assistant de configuration du nœud se ferme et une invite de connexion s'affiche, vous avertissant que vous n'avez pas terminé les tâches de configuration.

3. Connectez-vous au compte admin à l'aide de `admin` nom d'utilisateur.
4. Démarrez l'assistant de configuration du cluster :

cluster setup

```
::> cluster setup
```

Welcome to the cluster setup wizard.

You can enter the following commands at any time:

"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing
`https://<node_mgmt_or_e0M_IP_address>`

Otherwise, press Enter to complete cluster setup using the
command line interface:



Pour plus d'informations sur la configuration d'un cluster à l'aide de l'interface graphique de configuration, consultez le ["System Manager" aide en ligne](#).

5. Appuyez sur entrée pour effectuer cette tâche à l'aide de l'interface de ligne de commande. Lorsque vous êtes invité à créer un cluster ou à vous joindre à un cluster existant, entrez **join**.

```
Do you want to create a new cluster or join an existing cluster?  
{create, join}:  
join
```

Si la version de ONTAP exécutée sur le nouveau nœud est différente de celle exécutée sur le cluster existant, le système signale un `System checks Error: Cluster join operation cannot be performed at this time` erreur. Il s'agit du comportement attendu. Pour continuer, exécutez le `add-node -allow-mixed-version-join new_node_name` au niveau de privilège avancé à partir d'un nœud existant dans le cluster.

6. Suivez les invites pour configurer le nœud et le joindre au cluster :
 - Pour accepter la valeur par défaut d'une invite, appuyez sur entrée.
 - Pour saisir votre propre valeur pour une invite, entrez la valeur, puis appuyez sur entrée.
7. Répétez les étapes précédentes pour chaque nœud ajouté.

Une fois que vous avez terminé

Une fois les nœuds ajoutés au cluster, il est conseillé d'activer le basculement du stockage pour chaque paire haute disponibilité.

Informations associées

Retirer des nœuds du cluster

Vous pouvez supprimer les nœuds non souhaités d'un cluster ou d'un nœud à la fois. Après avoir supprimé un nœud, vous devez également supprimer son partenaire de basculement. Si vous supprimez un nœud, ses données deviennent inaccessibles ou effacées.

Avant de commencer

Les conditions suivantes doivent être remplies avant de supprimer des nœuds du cluster :

- Plus de la moitié des nœuds du cluster doivent être en bon état.
- Toutes les données du nœud que vous souhaitez supprimer doivent avoir été évacuées.
 - Cela peut inclure ["purge des données d'un volume chiffré"](#).
- Tous les volumes non-root ont été ["déplacé"](#) à partir d'agrégats détenus par le nœud.
- Tous les agrégats non racines ont été ["supprimé"](#) à partir du nœud.
- Si le nœud est propriétaire de disques FIPS (Federal Information Processing Standards) ou de disques à autocryptage (SED), ["le chiffrement de disque a été supprimé"](#) en retournant les disques en mode non protégé.
 - Pour aller plus avant ["Procédez à la suppression des disques FIPS ou des disques SED"](#).
- Les LIF de données l'ont été ["supprimé"](#) ou ["déplacé"](#) à partir du nœud.
- Les LIF de Cluster Management ont été ["déplacé"](#) à partir du nœud et des ports de rattachement modifiés.
- Toutes les LIFs intercluster ont été ["supprimé"](#).
 - Lorsque vous supprimez les LIFs intercluster, un avertissement qui peut être ignoré est affiché.
- Le basculement du stockage a été effectué ["désactivé"](#) pour le nœud.
- Toutes les règles de basculement LIF ont été ["modifié"](#) pour supprimer les ports sur le nœud.
- Tous les VLAN sur le nœud ont été ["supprimé"](#).
- Si vous souhaitez supprimer des LUN sur le nœud, vous devez ["Modifiez la liste des nœuds de rapport SLM \(Selective LUN Map\)"](#) avant de supprimer le nœud.

Si vous ne supprimez pas le nœud et son partenaire HA de la liste des nœuds-rapports SLM, l'accès aux LUN précédemment sur le nœud peut être perdu, même si les volumes contenant les LUN ont été déplacés vers un autre nœud.

Il est recommandé d'émettre un message AutoSupport pour informer le support technique NetApp que la suppression de nœud est en cours.

Remarque : vous ne devez pas effectuer d'opérations telles que `cluster remove-node`, `cluster unjoin`, et `node rename` Lorsqu'une mise à niveau automatisée de ONTAP est en cours.

Description de la tâche

- Si vous exécutez un cluster à versions mixtes, vous pouvez supprimer le dernier nœud à version faible à l'aide de l'une des commandes de privilège avancées commençant par ONTAP 9.3 :
 - ONTAP 9.3 : `cluster unjoin -skip-last-low-version-node-check`

- ONTAP 9.4 et versions ultérieures : `cluster remove-node -skip-last-low-version-node -check`

- Si vous dissociez 2 nœuds d'un cluster à 4 nœuds, la haute disponibilité du cluster est automatiquement activée sur les deux nœuds restants.



Toutes les données système et utilisateur de tous les disques connectés au nœud doivent être inaccessibles aux utilisateurs avant de supprimer un nœud du cluster. Si un nœud n'a pas été correctement rejoint à partir d'un cluster, contactez le support NetApp pour obtenir de l'aide concernant les options de restauration.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Vérifier si un nœud sur le cluster contient epsilon :

```
cluster show -epsilon true
```

3. Si un nœud sur le cluster contient epsilon et que ce nœud va être rejoint, déplacer epsilon vers un nœud qui ne va pas être dissocié :

- a. Déplacer epsilon depuis le nœud qui va être désrejoint

```
cluster modify -node <name_of_node_to_be_unjoined> -epsilon false
```

- b. Déplacer epsilon vers un nœud qui ne va pas être dissocié :

```
cluster modify -node <node_name> -epsilon true
```

4. Identifiez le nœud maître actuel :

```
cluster ring show
```

Le nœud maître est le nœud qui contient des processus tels que «mgmt», «vldb», «vifmgr», «bcomd» et «crs».

5. Si le nœud que vous souhaitez supprimer est le nœud maître actuel, activez un autre nœud du cluster pour qu'il soit choisi comme nœud maître :

- a. Rendre le nœud maître actuel inéligible pour participer au cluster :

```
cluster modify - node <node_name> -eligibility false
```

Lorsque le nœud maître devient inéligible, l'un des nœuds restants est choisi par le quorum du cluster comme nouveau maître.

- b. Rendez le nœud maître précédent éligible pour participer à nouveau au cluster :

```
cluster modify - node <node_name> -eligibility true
```

6. Connectez-vous à la LIF de Remote node management ou à la LIF cluster-management sur un autre nœud que celui en cours de suppression.
7. Supprimer le nœud du cluster :

Pour cette version ONTAP...	Utilisez cette commande...
ONTAP 9.3	<pre>cluster unjoin</pre>
ONTAP 9.4 et versions ultérieures	<pre>cluster remove-node*</pre>

Si vous avez une version mixte de cluster et que vous supprimez le dernier nœud inférieur, utilisez le `-skip-last-low-version-node-check` paramètre avec ces commandes.

Le système vous informe des informations suivantes :

- Vous devez également supprimer le partenaire de basculement du nœud du cluster.
- Après avoir retiré le nœud et avant de le réintégrer, vous devez utiliser l'option du menu de démarrage (4) nettoyer la configuration et initialiser tous les disques ou l'option (9) configurer le partitionnement de disque avancé pour effacer la configuration du nœud et initialiser tous les disques.

Un message de panne est généré si des conditions que vous devez traiter avant de supprimer le nœud. Par exemple, le message peut indiquer que le nœud dispose de ressources partagées que vous devez supprimer ou que le nœud se trouve dans une configuration de basculement du stockage ou de la configuration haute disponibilité du cluster que vous devez désactiver.

Si le nœud est le maître de quorum, le cluster sera brièvement perdu et reviendra ensuite au quorum. Cette perte de quorum est temporaire et n'affecte aucune opération de données.

8. Si un message d'erreur indique des conditions d'erreur, traitez ces conditions et relancez le `cluster remove-node` ou `cluster unjoin` commande.

Le nœud est redémarré automatiquement après sa suppression réussie du cluster.

9. Si vous requalifiez le nœud, effacez la configuration du nœud et initialisez tous les disques :
- Pendant le processus de démarrage, appuyez sur Ctrl-C pour afficher le menu de démarrage lorsque vous y êtes invité.
 - Sélectionner l'option de menu d'amorçage (4) nettoyer la configuration et initialiser tous les disques.
10. Retour au niveau de privilège admin :

```
set -privilege admin
```

11. Répétez la procédure précédente pour supprimer le partenaire de basculement du cluster.

Accédez aux fichiers log, core dump et MIB d'un nœud à l'aide d'un navigateur Web

L'infrastructure du processeur de service (`spi`) Le service web est activé par défaut pour permettre à un navigateur web d'accéder aux fichiers log, core dump et MIB d'un nœud du cluster. Les fichiers restent accessibles même lorsque le nœud est en panne, à condition que le nœud soit pris en charge par son partenaire.

Ce dont vous avez besoin

- La LIF de cluster management doit être active.

Vous pouvez utiliser la LIF de gestion du cluster ou un nœud pour accéder à la `spi` service web. Toutefois, il est recommandé d'utiliser la LIF de gestion du cluster.

Le `network interface show` La commande affiche le statut de toutes les LIFs du cluster.

- Vous devez utiliser un compte utilisateur local pour accéder à l' `spi` service web, les comptes utilisateur de domaine ne sont pas pris en charge.
- Si votre compte utilisateur n'a pas le rôle « admin » (qui a accès à l' `spi` service web par défaut), votre rôle de contrôle d'accès doit avoir accès au système `spi` service web.

Le `vserver services web access show` commande affiche les rôles auxquels les services web ont accès.

- Si vous n'utilisez pas le compte d'utilisateur « admin » (qui inclut `http` méthode d'accès par défaut), votre compte utilisateur doit être configuré avec le `http` méthode d'accès.

Le `security login show` la commande affiche les méthodes d'accès et de connexion des comptes utilisateur ainsi que leurs rôles de contrôle d'accès.

- Si vous souhaitez utiliser HTTPS pour un accès Web sécurisé, SSL doit être activé et un certificat numérique doit être installé.

Le `system services web show` la commande affiche la configuration du moteur de protocole web au niveau du cluster.

Description de la tâche

Le `spi` le service web est activé par défaut et le service peut être désactivé manuellement (`vserver services web modify -vserver * -name spi -enabled false`).

Le rôle « admin » est accordé à l' `spi` le service web par défaut peut être désactivé manuellement (`services web access delete -vserver cluster_name -name spi -role admin`).

Étapes

1. Pointez le navigateur Web sur `spi` URL du service web dans l'un des formats suivants :

- `http://cluster-mgmt-LIF/spi/`
- `https://cluster-mgmt-LIF/spi/`

`cluster-mgmt-LIF` Est l'adresse IP de la LIF de management du cluster.

2. Lorsque le navigateur vous y invite, entrez votre compte utilisateur et votre mot de passe.

Une fois votre compte authentifié, le navigateur affiche des liens vers le `/mroot/etc/log/`, `/mroot/etc/crash/`, et `/mroot/etc/mib/` répertoires de chaque nœud du cluster.

Accéder à la console système d'un nœud

Si un nœud est suspendu au menu de démarrage ou à l'invite de l'environnement de démarrage, vous pouvez y accéder uniquement via la console système (également appelée *série console*). Vous pouvez accéder à la console système d'un nœud depuis une connexion SSH vers le processeur de service du nœud ou vers le cluster.

Description de la tâche

Le processeur de service et ONTAP proposent des commandes qui vous permettent d'accéder à la console système. Toutefois, depuis le processeur de service, vous pouvez accéder uniquement à la console système de son propre nœud. Dans le cluster, vous pouvez accéder à la console système de n'importe quel nœud du cluster.

Étapes

1. Accéder à la console système d'un nœud :

Si vous êtes dans le...	Entrez cette commande...
Interface de ligne de commandes du processeur de service du nœud	<code>system console</code>
INTERFACE DE LIGNE DE COMMANDES DE ONTAP	<code>system node run-console</code>

2. Connectez-vous à la console du système lorsque vous y êtes invité.
3. Pour quitter la console du système, appuyez sur Ctrl-D.

Exemples d'accès à la console du système

L'exemple suivant montre le résultat de la saisie du `system console` Commande à l'invite "Enregistrer node2". La console système indique que le nœud 2 est suspendu à l'invite de l'environnement d'amorçage. Le `boot_ontap` La commande est entrée sur la console pour démarrer le nœud sur ONTAP. Ctrl-D est ensuite enfoncé pour quitter la console et retourner au processeur de service.

```

SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap

...
*****
*
* Press Ctrl-C for Boot Menu. *
*
*****
...

```

(La touche Ctrl-D est enfoncée pour quitter la console du système.)

```

Connection to 123.12.123.12 closed.
SP node2>

```

L'exemple suivant montre le résultat de la saisie du `system node run-console` Commande provenant de ONTAP pour accéder à la console système du nœud 2, qui est suspendue à l'invite de l'environnement de démarrage. Le `boot_ontap` La commande a été saisie au niveau de la console pour démarrer le nœud 2 vers ONTAP. Appuyez ensuite sur Ctrl-D pour quitter la console et revenir à ONTAP.

```

cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap

...
*****
*
* Press Ctrl-C for Boot Menu. *
*
*****
...

```

(La touche Ctrl-D est enfoncée pour quitter la console du système.)

```

Connection to 123.12.123.12 closed.
cluster1::>

```

Gestion des volumes root et des agrégats root des nœuds

Le volume racine d'un nœud est un volume FlexVol installé en usine ou par le logiciel d'installation. Il est réservé aux fichiers système, aux fichiers journaux et aux fichiers core. Le nom du répertoire est `/mroot`, qui n'est accessible que via le systemshell par le support technique. La taille minimale du volume racine d'un nœud dépend du modèle de plateforme.

Présentation des règles qui régissent les volumes racine des nœuds et les agrégats racine

Le volume racine d'un nœud contient des répertoires et des fichiers spéciaux pour ce nœud. L'agrégat root contient le volume root. Quelques règles régissent le volume racine d'un nœud et l'agrégat racine.

- Les règles suivantes régissent le volume racine du nœud :
 - À moins d'en recevoir l'instruction du support technique, ne modifiez pas la configuration ou le contenu du volume racine.
 - Ne stockez pas les données utilisateur sur le volume racine.

Le stockage des données utilisateur dans le volume racine augmente le temps de rétablissement du stockage entre les nœuds d'une paire haute disponibilité.

- Vous pouvez déplacer le volume root vers un autre agrégat. Voir [\[relocate-root\]](#).
- L'agrégat root est dédié uniquement au volume root du nœud.

ONTAP vous empêche de créer d'autres volumes dans l'agrégat racine.

"NetApp Hardware Universe"

Libérez de l'espace sur le volume racine d'un nœud

Un message d'avertissement s'affiche lorsque le volume racine d'un nœud est saturé ou presque plein. Le nœud ne peut pas fonctionner correctement lorsque son volume racine est plein. Vous pouvez libérer de l'espace sur le volume racine d'un nœud en supprimant les fichiers « core dump », les fichiers de trace des paquets et les copies Snapshot de volume racine.

Étapes

1. Afficher les fichiers core dump du nœud et leur nom :

```
system node coredump show
```

2. Supprimez les fichiers core dump indésirables du nœud :

```
system node coredump delete
```

3. Accès au nodeshell :

```
system node run -node nodename
```

nodename est le nom du nœud dont vous souhaitez libérer l'espace du volume racine.

4. Passez au niveau de privilège avancé du nodeshell à partir du nodeshell :

priv set advanced

5. Afficher et supprimer les fichiers de trace des paquets du nœud via le nodeshell :

a. Afficher tous les fichiers dans le volume root du nœud :

```
ls /etc
```

b. Si des fichiers de trace de paquets sont enregistrés (*.trc) sont dans le volume racine du nœud, supprimez-les individuellement :

```
rm /etc/log/packet_traces/file_name.trc
```

6. Identifiez et supprimez les copies Snapshot du volume racine du nœud via le nodeshell :

a. Identifiez le nom du volume root :

```
vol status
```

Le volume racine est indiqué par le mot « root » dans la colonne « Options » du `vol status` sortie de la commande.

Dans l'exemple suivant, le volume root est `vol0`:

```
node1*> vol status
```

Volume	State	Status	Options
vol0	online	raid_dp, flex 64-bit	root, nvfail=on

a. Afficher les copies Snapshot du volume racine :

```
snap list root_vol_name
```

b. Supprimez les copies Snapshot de volume racine non souhaitées :

```
snap delete root_vol_namesnapshot_name
```

7. Quittez le nodeshell et retournez au clustershell :

```
exit
```

Transfert des volumes racines vers de nouveaux agrégats

La procédure de remplacement racine migre l'agrégat racine actuel vers un autre jeu de disques sans interruption.

Description de la tâche

Le basculement du stockage doit être activé pour transférer les volumes root. Vous pouvez utiliser le `storage failover modify -node nodename -enable true` commande permettant d'activer le basculement.

Vous pouvez modifier l'emplacement du volume root vers un nouvel agrégat dans les scénarios suivants :

- Lorsque les agrégats racines ne sont pas sur le disque de votre choix
- Lorsque vous souhaitez réorganiser les disques connectés au nœud
- Lorsque vous effectuez un remplacement des tiroirs disques EOS

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set privilege advanced
```

2. Transférer l'agrégat racine :

```
system node migrate-root -node nodename -disklist disklist -raid-type raid-type
```

- **-noeud**

Spécifie le nœud qui possède l'agrégat racine que vous souhaitez migrer.

- **-disklist**

Spécifie la liste des disques sur lesquels le nouvel agrégat racine sera créé. Tous les disques doivent être des disques de secours et appartenir au même nœud. Le nombre minimum de disques requis dépend du type RAID.

- **-raid-type**

Spécifie le type RAID de l'agrégat racine. La valeur par défaut est `raid-dp`.

3. Surveiller la progression de la tâche :

```
job show -id jobid -instance
```

Résultats

Si toutes les vérifications préalables ont réussi, la commande démarre un travail de remplacement de volume racine et se ferme. Le nœud devrait redémarrer.

Démarrer ou arrêter la présentation d'un nœud

Pour des raisons de maintenance ou de dépannage, vous pouvez avoir besoin de démarrer ou d'arrêter un nœud. Vous pouvez le faire via l'interface de ligne de commandes de ONTAP, l'invite de l'environnement de démarrage ou l'interface de ligne de commandes du processeur de service.

Utilisation de la commande de l'interface de ligne de commandes du processeur `system power off` ou `system power cycle` Pour mettre hors/sous tension un nœud peut provoquer un arrêt inapproprié du nœud (également appelé *shutdown*) et n'a pas vocation à remplacer un arrêt normal à l'aide du ONTAP `system node halt` commande.

Redémarrez un nœud à l'invite du système

Vous pouvez redémarrer un nœud en mode normal depuis l'invite du système. Un nœud est configuré pour démarrer à partir du périphérique d'amorçage, tel qu'une carte CompactFlash pour PC.

Étapes

1. Si le cluster contient quatre nœuds ou plus, vérifier que le nœud à redémarrer ne contient pas epsilon :

- a. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- b. Déterminer quel nœud contient epsilon :

```
cluster show
```

L'exemple suivant montre que « node1 » possède epsilon :

```
cluster1::*> cluster show
Node                Health  Eligibility  Epsilon
-----
node1                true    true         true
node2                true    true         false
node3                true    true         false
node4                true    true         false
4 entries were displayed.
```

- a. Si le nœud à redémarrer contient epsilon, retirer epsilon du nœud :

```
cluster modify -node node_name -epsilon false
```

- b. Assigner epsilon à un nœud différent qui demeurera en service :

```
cluster modify -node node_name -epsilon true
```

- c. Retour au niveau de privilège admin :

```
set -privilege admin
```

2. Utilisez le `system node reboot` commande permettant de redémarrer le nœud.

Si vous ne spécifiez pas le `-skip-lif-migration` Paramètre, la commande tente de migrer les LIF de gestion du cluster et des données de manière synchrone vers un autre nœud avant le redémarrage. Si la migration de LIF échoue ou se trouve en dehors des délais, le processus de redémarrage est interrompu et ONTAP affiche une erreur pour indiquer l'échec de la migration de LIF.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

Le processus de redémarrage du nœud démarre. L'invite de connexion ONTAP apparaît, indiquant que le processus de redémarrage est terminé.

Démarrez ONTAP à l'invite de l'environnement de démarrage

Vous pouvez démarrer la version actuelle ou la version de sauvegarde de ONTAP lorsque vous êtes à l'invite d'environnement d'amorçage d'un nœud.

Étapes

1. Accédez à l'invite de l'environnement d'initialisation à partir de l'invite du système de stockage à l'aide de la `system node halt` commande.

La console du système de stockage affiche l'invite de l'environnement de démarrage.

2. À l'invite de l'environnement de démarrage, entrez l'une des commandes suivantes :

Pour démarrer...	Entrer...
La dernière version de ONTAP	<code>boot_ontap</code>
Image principale ONTAP à partir du périphérique de démarrage	<code>boot_primary</code>
Image de sauvegarde ONTAP à partir du périphérique de démarrage	<code>boot_backup</code>

Si vous n'êtes pas certain de l'image à utiliser, vous devez utiliser `boot_ontap` dans la première instance.

Arrêtez un nœud

Vous pouvez arrêter un nœud s'il ne répond plus, ou si le personnel de support vous y dirige, dans le cadre des opérations de dépannage.

Étapes

1. Si le cluster contient quatre nœuds ou plus, vérifier que le nœud à arrêter ne contient pas epsilon :

- a. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

- b. Déterminer quel nœud contient epsilon :

```
cluster show
```

L'exemple suivant montre que « node1 » possède epsilon :

```
cluster1::*> cluster show
Node           Health Eligibility  Epsilon
-----
node1          true   true       true
node2          true   true       false
node3          true   true       false
node4          true   true       false
4 entries were displayed.
```

a. Si le nœud à arrêter contient epsilon, retirer epsilon du nœud :

```
cluster modify -node node_name -epsilon false
```

b. Assigner epsilon à un nœud différent qui demeurera en service :

```
cluster modify -node node_name -epsilon true
```

c. Retour au niveau de privilège admin :

```
set -privilege admin
```

2. Utilisez le `system node halt` commande permettant d'arrêter le nœud.

Si vous ne spécifiez pas le `-skip-lif-migration` Paramètre, la commande tente de migrer les LIF de gestion des données et du cluster de manière synchrone vers un autre nœud avant l'arrêt. Si la migration de LIF échoue ou se trouve en dehors des délais, le processus d'arrêt est interrompu et ONTAP affiche une erreur pour indiquer l'échec de la migration de LIF.

Vous pouvez déclencher manuellement un « core dump » avec l'arrêt en utilisant les deux `-dump` paramètre.

L'exemple suivant arrête le nœud nommé « node1 » pour la maintenance matérielle :

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

Gérer un nœud à l'aide du menu de démarrage

Vous pouvez utiliser le menu de démarrage pour corriger les problèmes de configuration sur un nœud, réinitialiser le mot de passe d'administration, initialiser les disques, réinitialiser la configuration du nœud et restaurer les informations de configuration du nœud sur le périphérique d'amorçage.



Si une paire haute disponibilité est utilisée "[Cryptage SAS ou disques NVMe \(SED, NSE, FIPS\)](#)", vous devez suivre les instructions de la rubrique "[Retour d'un lecteur FIPS ou SED en mode non protégé](#)" Pour tous les disques de la paire HA avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

Étapes

- 1. Redémarrez le nœud pour accéder au menu de démarrage à l'aide de `system node reboot` commande à l'invite du système.

Le processus de redémarrage du nœud démarre.

- 2. Pendant le processus de redémarrage, appuyez sur Ctrl-C pour afficher le menu de démarrage lorsque vous y êtes invité.

Le nœud affiche les options suivantes pour le menu de démarrage :


```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```



Option de menu d'amorçage (2) l'amorçage sans `/etc/rc` est obsolète et n'a aucun effet sur le système.

- 3. Sélectionnez l'une des options suivantes en saisissant le numéro correspondant :

Pour...	Sélectionner...
Continuer à démarrer le nœud en mode normal	1) démarrage normal
Modifier le mot de passe du noeud, qui est aussi le mot de passe du compte ""admin""	3) modification du mot de passe

Pour...	Sélectionner...
Initialiser les disques du nœud et créer un volume racine pour le nœud	<p>4) nettoyer la configuration et initialiser tous les disques</p> <div>  <p>Cette option de menu efface toutes les données sur les disques du nœud et réinitialise la configuration par défaut de votre nœud.</p> </div> <p>Sélectionnez cette option de menu uniquement après que le nœud a été supprimé d'un cluster (non joint) et qu'il n'est pas joint à un autre cluster.</p> <p>Dans le cas d'un nœud avec des tiroirs disques internes ou externes, le volume racine des disques internes est initialisé. S'il n'y a pas de tiroirs disques internes, le volume root sur les disques externes est initialisé.</p> <p>Dans le cas d'un système exécutant la virtualisation FlexArray avec des tiroirs disques internes ou externes, les LUN de baie ne sont pas initialisées. Tout disque natif sur des tiroirs internes ou externes est initialisé.</p> <p>Dans le cas d'un système exécutant la virtualisation FlexArray avec uniquement DES LUN de baie et aucun tiroir disque interne ou externe, le volume racine DES LUN de la baie de stockage est initialisé, voir "Installation de FlexArray".</p> <p>Si le nœud que vous souhaitez initialiser contient des disques qui sont partitionnés pour le partitionnement données-racines, les disques doivent être départitionnés avant que le nœud puisse être initialisé, voir 9) configurer le partitionnement de disque avancé et "Gestion des disques et des agrégats".</p>
Opérations de maintenance des agrégats et des disques pour obtenir des informations détaillées sur les agrégats et les disques	<p>5) démarrage du mode maintenance</p> <p>Pour quitter le mode Maintenance, utilisez le <code>halt</code> commande.</p>
Restaurez les informations de configuration à partir du volume racine du nœud vers le périphérique d'amorçage, par exemple une carte CompactFlash pour PC	<p>6) mettre à jour la mémoire flash à partir de la configuration de sauvegarde</p> <p>ONTAP stocke des informations de configuration des nœuds sur le périphérique de démarrage. Au redémarrage du nœud, les informations du périphérique de démarrage sont automatiquement sauvegardées sur le volume racine du nœud. Si le périphérique d'amorçage est corrompu ou doit être remplacé, vous devez utiliser cette option de menu pour restaurer les informations de configuration du volume racine du nœud vers le périphérique d'amorçage.</p>

Pour...	Sélectionner...
Installez le nouveau logiciel sur le nœud	<p>7) installer le nouveau logiciel en premier</p> <p>Si le logiciel ONTAP du périphérique d'amorçage n'inclut pas la prise en charge de la matrice de stockage que vous souhaitez utiliser pour le volume racine, vous pouvez utiliser cette option de menu pour obtenir une version du logiciel qui prend en charge votre matrice de stockage et l'installer sur le nœud.</p> <p>Cette option de menu permet uniquement d'installer une version plus récente du logiciel ONTAP sur un nœud sur lequel aucun volume racine n'est installé. Do <i>NOT</i> utiliser cette option de menu pour mettre à niveau ONTAP.</p>
Redémarrez le nœud	8) redémarrez le nœud
Départitionner tous les disques et supprimer leurs informations de propriété ou nettoyer la configuration et initialiser le système avec des disques entiers ou partitionnés	<p>9) Configuration du partitionnement de disque avancé</p> <p>Depuis ONTAP 9.2, l'option de partitionnement de disque avancé fournit des fonctionnalités de gestion supplémentaires pour les disques configurés pour le partitionnement données-racines ou données-racines. Les options suivantes sont disponibles à partir de l'option de démarrage 9 :</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>(9a) Unpartition all disks and remove their ownership information.</p> <p>(9b) Clean configuration and initialize system with partitioned disks.</p> <p>(9c) Clean configuration and initialize system with whole disks.</p> <p>(9d) Reboot the node.</p> <p>(9e) Return to main boot menu.</p> </div>

Affiche les attributs du nœud

Vous pouvez afficher les attributs d'un ou plusieurs nœuds du cluster, par exemple le nom, le propriétaire, l'emplacement, numéro de modèle, numéro de série, durée pendant laquelle le nœud s'exécute, état de santé et éligibilité à un cluster.

Étapes

1. Pour afficher les attributs d'un nœud spécifié ou à propos de tous les nœuds d'un cluster, utilisez le `system node show` commande.

Exemple d'affichage des informations relatives à un nœud

L'exemple suivant affiche des informations détaillées sur le nœud 1 :

```
cluster1::> system node show -node node1
      Node: node1
      Owner: Eng IT
      Location: Lab 5
      Model: model_number
      Serial Number: 12345678
      Asset Tag: -
      Uptime: 23 days 04:42
      NVRAM System ID: 118051205
      System ID: 0118051205
      Vendor: NetApp
      Health: true
      Eligibility: true
      Differentiated Services: false
      All-Flash Optimized: true
      Capacity Optimized: false
      QLC Optimized: false
      All-Flash Select Optimized: false
      SAS2/SAS3 Mixed Stack Support: none
```

Modifier les attributs du nœud

Vous pouvez modifier les attributs d'un nœud si nécessaire. Les attributs que vous pouvez modifier incluent les informations sur le propriétaire du nœud, les informations d'emplacement, le numéro d'inventaire et l'éligibilité à participer au cluster.

Description de la tâche

L'éligibilité d'un nœud à participer au cluster peut être modifiée au niveau de privilège avancé à l'aide de `-eligibility` paramètre du `system node modify` ou `cluster modify` commande. Si vous définissez l'éligibilité d'un nœud sur `false`, le nœud est inactif dans le cluster.



Vous ne pouvez pas modifier l'éligibilité des nœuds localement. Il doit être modifié depuis un autre nœud. L'éligibilité des nœuds ne peut pas non plus être modifiée avec une configuration haute disponibilité du cluster.



Vous ne devez pas définir l'éligibilité d'un nœud sur `false`, à l'exception de cas tels que la restauration de la configuration de nœuds ou la maintenance prolongée des nœuds. L'accès aux données SAN et NAS au nœud peut être affecté lorsque ce dernier n'est pas éligible.

Étapes

1. Utilisez le `system node modify` commande permettant de modifier les attributs d'un nœud.

Exemple de modification des attributs du nœud

La commande suivante modifie les attributs du nœud « node1 ». Le propriétaire du nœud est défini sur « Joe Smith » et son numéro d'inventaire est défini sur « js1234 » :

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag  
js1234
```

Renommez un nœud

Vous pouvez modifier le nom d'un nœud si nécessaire.

Étapes

1. Pour renommer un nœud, utilisez `system node rename` commande.

Le `-newname` paramètre spécifie le nouveau nom pour le nœud. Le `system node rename` la page man décrit les règles à respecter lorsque vous spécifiez le nom du nœud.

Si vous souhaitez renommer plusieurs nœuds du cluster, vous devez exécuter la commande de chaque nœud séparément.



Le nom du nœud ne peut pas être « tous » car « tous » est un nom réservé au système.

Exemple de modification du nom d'un nœud

La commande suivante renomme le nœud « node1 » en « node1a » :

```
cluster1::> system node rename -node node1 -newname node1a
```

Gérez des clusters à un seul nœud

Un cluster à un seul nœud est une implémentation spéciale d'un cluster exécuté sur un nœud autonome. Les clusters à un seul nœud ne sont pas recommandés, car ils n'offrent pas de redondance. En cas de panne du nœud, l'accès aux données est perdu.



Pour la tolérance aux pannes et la continuité de l'activité, il est fortement recommandé de configurer votre cluster avec "[Haute disponibilité \(paires haute disponibilité\)](#)".

Si vous choisissez de configurer ou de mettre à niveau un cluster à un seul nœud, vous devez connaître les points suivants :

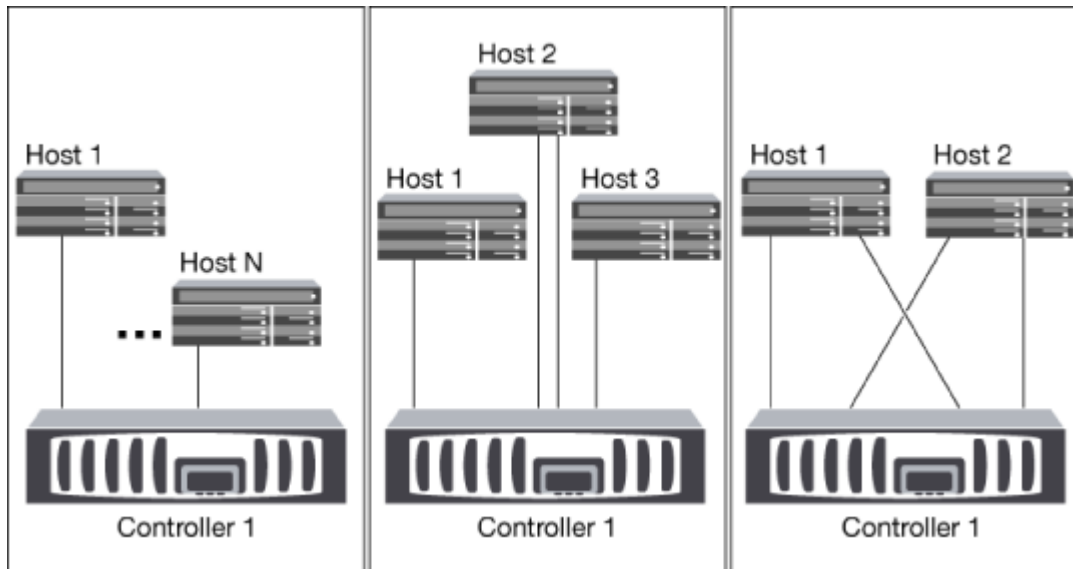
- Le chiffrement du volume racine n'est pas pris en charge sur les clusters à un seul nœud.
- Si vous supprimez des nœuds devant disposer d'un cluster à un seul nœud, vous devez modifier les ports de cluster pour transmettre le trafic de données en modifiant les ports de cluster en tant que ports de données, puis en créant des LIFs de données sur les ports de données.
- Pour les clusters à un seul nœud, vous pouvez spécifier la destination de sauvegarde de la configuration lors de l'installation du logiciel. Une fois l'installation effectuée, ces paramètres peuvent être modifiés à l'aide des commandes ONTAP.
- Si plusieurs hôtes se connectent au nœud, chaque hôte peut être configuré avec un système d'exploitation différent, tel que Windows ou Linux. Si plusieurs chemins s'offrent à l'hôte vers le contrôleur, ALUA doit être activé sur l'hôte.

Méthodes de configuration des hôtes SAN iSCSI avec des nœuds uniques

Vous pouvez configurer des hôtes SAN iSCSI pour qu'ils se connectent directement à un seul nœud ou via un ou plusieurs commutateurs IP. Le nœud peut avoir plusieurs connexions iSCSI au commutateur.

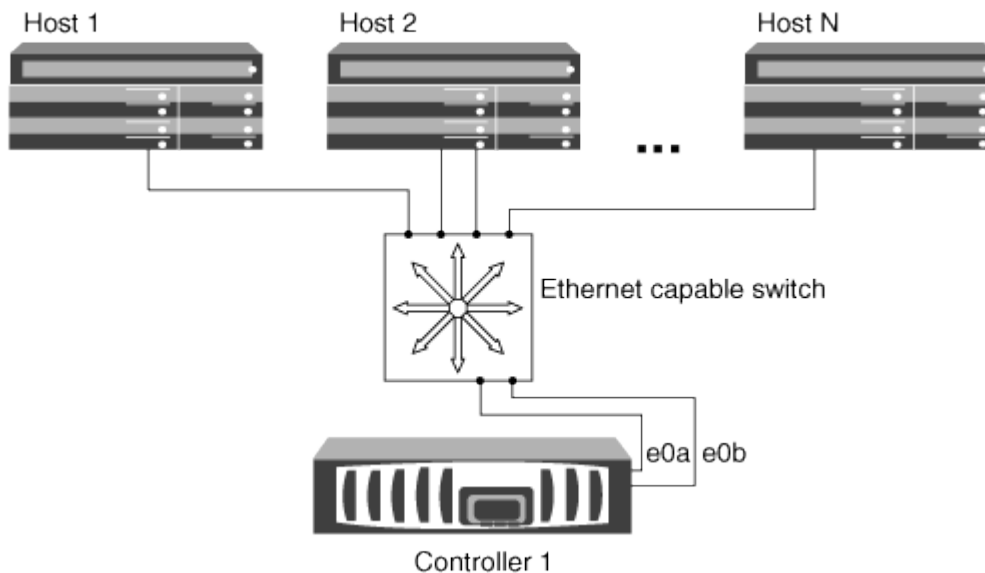
Configurations à un seul nœud en attachement direct

Dans les configurations à un seul nœud à connexion directe, un ou plusieurs hôtes sont directement connectés au nœud.



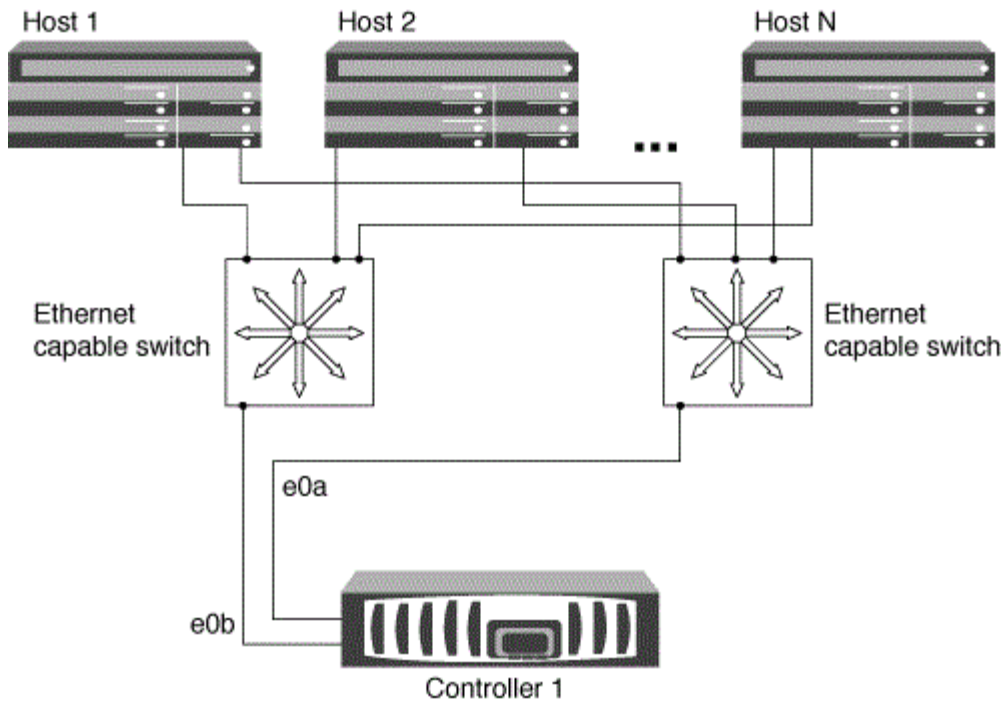
Configurations à un seul réseau sans nœud

Dans les configurations à un seul réseau et à un seul nœud, un commutateur connecte un seul nœud à un ou plusieurs hôtes. Comme il y a un seul commutateur, cette configuration n'est pas entièrement redondante.



Configurations à nœud unique multi-réseau

Dans les configurations à un nœud multi-réseau, deux commutateurs ou plus connectent un nœud à un ou plusieurs hôtes. Étant donné qu'il y a plusieurs commutateurs, cette configuration est totalement redondante.



Méthodes de configuration des hôtes SAN FC et FC-NVMe avec des nœuds uniques

Vous pouvez configurer des hôtes SAN FC et FC-NVMe avec des nœuds uniques via une ou plusieurs structures. La virtualisation NPIV (N-Port ID Virtualization) est requise et doit être activée sur tous les commutateurs FC de la structure. Vous ne pouvez pas relier directement des hôtes SAN FC ou FC-NVMe aux nœuds uniques sans utiliser de commutateur FC.

Configurations à 1 nœud et structure unique

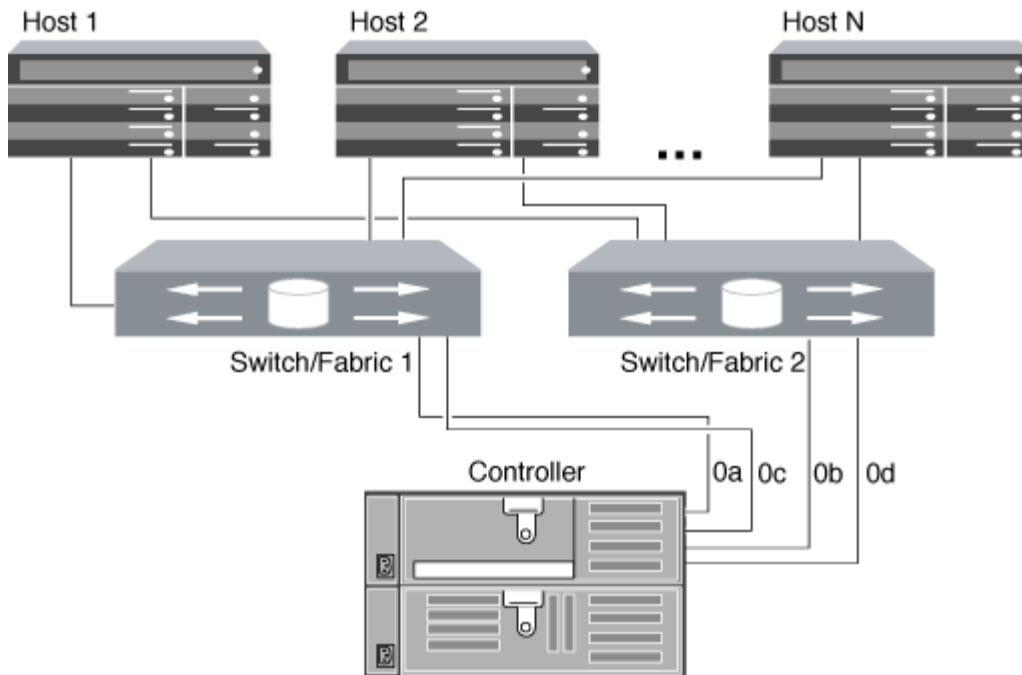
Dans les configurations à un seul nœud de la structure unique, un commutateur connecte un seul nœud à un ou plusieurs hôtes. Comme il y a un seul commutateur, cette configuration n'est pas entièrement redondante.

Dans les configurations à un seul nœud de la structure unique, vous n'avez pas besoin de logiciels de chemins d'accès multiples si vous disposez uniquement d'un chemin d'accès unique de l'hôte vers le nœud.

Configurations multifabriques à un nœud

Dans les configurations multifabriques à un nœud, il existe deux commutateurs ou plus qui connectent un nœud à un ou plusieurs hôtes. Dans une optique de simplicité, la figure suivante présente une configuration multistrukture à un seul nœud avec seulement deux fabriques. Elle présente également au moins deux fabrics dans une configuration multi-fabric. Dans cette figure, le contrôleur de stockage est monté dans le châssis supérieur et le châssis inférieur peut être vide ou comporter un module IOMX, comme dans cet exemple.

Les ports cibles FC (0a, 0C, 0b, 0d) dans les illustrations sont des exemples. Les numéros de port réels varient selon le modèle de votre nœud de stockage et si vous utilisez des adaptateurs d'extension.



Informations associées

["Rapport technique NetApp 4684 : implémentation et configuration de SAN modernes avec NVMe-of"](#)

Mise à niveau de ONTAP pour un cluster à un seul nœud

Depuis la version ONTAP 9.2, vous pouvez utiliser l'interface de ligne de commandes ONTAP pour effectuer une mise à jour automatisée d'un cluster à un seul nœud. Les clusters à un seul nœud ne manquent pas de redondance. Les mises à jour restent donc toujours perturbantes. Les mises à niveau entraînant des interruptions ne peuvent pas être réalisées avec System Manager.

Avant de commencer

Vous devez terminer la mise à niveau ["préparation"](#) étapes.

Étapes

1. Supprimez le pack logiciel ONTAP précédent :

```
cluster image package delete -version previous_package_version
```

2. Téléchargez le pack logiciel ONTAP cible :

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz
```

```
Package download completed.
Package processing completed.
```


3. Vérifiez que le pack logiciel est disponible dans le référentiel du package de cluster :

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
-----
9.7              M/DD/YYYY 10:32:15
```

4. Vérifiez que le cluster est prêt à être mis à niveau :

```
cluster image validate -version package_version_number
```

```
cluster1::> cluster image validate -version 9.7
```

```
WARNING: There are additional manual upgrade validation checks that must
be performed after these automated validation checks have completed...
```

5. Surveiller la progression de la validation :

```
cluster image show-update-progress
```

6. Effectuez toutes les actions requises identifiées par la validation.

7. Générer une estimation de mise à niveau logicielle si vous le souhaitez :

```
cluster image update -version package_version_number -estimate-only
```

L'estimation de la mise à niveau logicielle affiche des détails sur chaque composant à mettre à jour, ainsi que la durée estimée de la mise à niveau.

8. Effectuez la mise à niveau logicielle :

```
cluster image update -version package_version_number
```



En cas de problème, la mise à jour s'interrompt et vous êtes invité à prendre les mesures correctives nécessaires. Vous pouvez utiliser la commande `cluster image show-update-progress` pour afficher les détails de tous les problèmes et la progression de la mise à jour. Après avoir résolu le problème, vous pouvez reprendre la mise à jour à l'aide de la commande `cluster image resume-update`.

9. Afficher la progression de la mise à jour du cluster :

```
cluster image show-update-progress
```

Le nœud est redémarré dans le cadre de la mise à jour et ne peut pas être accédé durant le redémarrage.

10. Déclencher une notification :

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

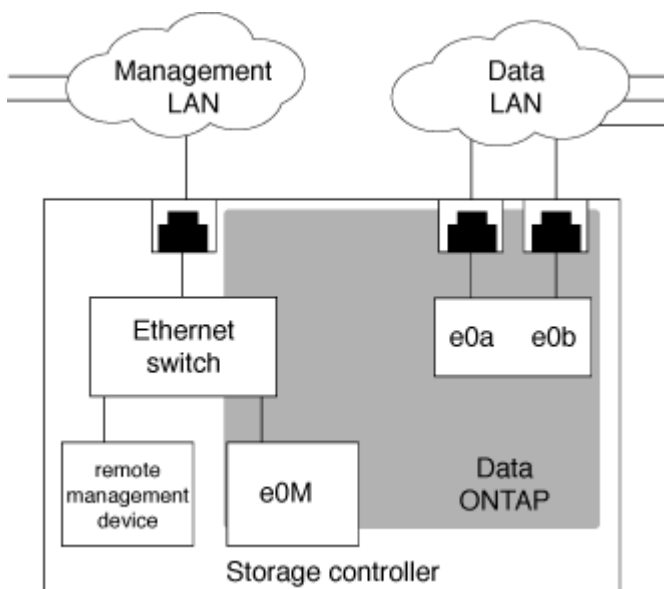
Si votre cluster n'est pas configuré pour envoyer des messages, une copie de la notification est enregistrée localement.

Configuration du réseau SP/BMC

Isolez le trafic du réseau de gestion

Il est recommandé de configurer le processeur de service/BMC et l'interface de gestion e0M sur un sous-réseau dédié au trafic de gestion. L'exécution du trafic de données sur le réseau de gestion peut entraîner des problèmes de dégradation des performances et de routage.

Le port Ethernet de gestion de la plupart des contrôleurs de stockage (indiqué par une icône de clé anglaise à l'arrière du châssis) est connecté à un commutateur Ethernet interne. Le commutateur interne fournit la connectivité au SP/BMC et à l'interface de gestion e0M, que vous pouvez utiliser pour accéder au système de stockage via les protocoles TCP/IP tels que Telnet, SSH et SNMP.



Si vous prévoyez d'utiliser à la fois le périphérique de gestion à distance et le e0M, vous devez les configurer sur le même sous-réseau IP. Étant donné qu'il s'agit d'interfaces à faible bande passante, il est recommandé de configurer le processeur de service/BMC et e0M sur un sous-réseau dédié au trafic de gestion.

Si vous ne pouvez pas isoler le trafic de gestion ou si votre réseau de gestion dédié est exceptionnellement grand, vous devez essayer de maintenir le volume de trafic réseau le plus bas possible. Un trafic de diffusion ou de multidiffusion excessif peut dégrader les performances du SP/BMC.



Certains contrôleurs de stockage, comme le AFF A800, disposent de deux ports externes, l'un pour BMC et l'autre pour e0M. Pour ces contrôleurs, il n'est pas nécessaire de configurer BMC et e0M sur le même sous-réseau IP.

Considérations relatives à la configuration réseau SP/BMC

Vous pouvez activer une configuration réseau automatique au niveau du cluster pour le processeur de service (recommandé). Vous pouvez également désactiver la configuration réseau automatique du processeur de service (par défaut) et gérer manuellement la configuration réseau du processeur de service au niveau du nœud. Il existe quelques considérations pour chaque cas.



Cette rubrique s'applique à la fois au processeur de service et au contrôleur BMC.

La configuration réseau automatique du processeur de service permet au processeur de service d'utiliser les ressources d'adresse (y compris l'adresse IP, le masque de sous-réseau et l'adresse de passerelle) du sous-réseau spécifié pour configurer automatiquement son réseau. Grâce à la configuration réseau automatique du processeur de service, vous n'avez pas besoin d'attribuer manuellement des adresses IP au processeur de service de chaque nœud. Par défaut, la configuration réseau automatique du processeur de service est désactivée, car l'activation de la configuration nécessite que le sous-réseau soit d'abord défini dans le cluster.

Si vous activez la configuration réseau automatique du processeur de service, les scénarios et considérations suivants s'appliquent :

- Si le processeur de service n'a jamais été configuré, le réseau du processeur de service est configuré automatiquement en fonction du sous-réseau spécifié pour la configuration réseau automatique du processeur de service.
- Si le processeur de service a déjà été configuré manuellement, ou si la configuration réseau du processeur de service existante est basée sur un autre sous-réseau, le réseau SP de tous les nœuds du cluster est reconfiguré en fonction du sous-réseau que vous spécifiez dans la configuration réseau automatique du processeur de service.

La reconfiguration peut affecter une autre adresse au processeur de service, ce qui peut avoir un impact sur votre configuration DNS et sa capacité à résoudre les noms d'hôtes du processeur de service. Par conséquent, vous devrez peut-être mettre à jour votre configuration DNS.

- Un nœud qui rejoint le cluster utilise le sous-réseau spécifié pour configurer automatiquement son réseau SP.
- Le `system service-processor network modify` La commande ne vous permet pas de modifier l'adresse IP du processeur de service.

Lorsque la configuration réseau automatique du processeur de service est activée, la commande ne vous permet que d'activer ou de désactiver l'interface réseau du processeur de service.

- Si la configuration réseau automatique du processeur de service était auparavant activée, la désactivation de l'interface réseau du processeur de service entraîne la libération de la ressource d'adresse attribuée et son renvoi au sous-réseau.

- Si vous désactivez l'interface réseau du processeur de service, puis le réactivez, il est possible que le processeur de service soit reconfiguré à une adresse différente.

Si la configuration réseau automatique du processeur de service est désactivée (par défaut), les scénarios et considérations suivants s'appliquent :

- Si le processeur de service n'a jamais été configuré, la configuration réseau IPv4 du processeur de service utilise par défaut DHCP IPv4 et IPv6 est désactivé.

Un nœud qui rejoint le cluster utilise également le DHCP IPv4 pour sa configuration réseau du processeur de service par défaut.

- Le `system service-processor network modify` Commande vous permet de configurer l'adresse IP du processeur de service d'un nœud.

Un message d'avertissement apparaît lorsque vous tentez de configurer manuellement le réseau du processeur de service avec des adresses allouées à un sous-réseau. Si vous ignorez l'avertissement et que vous procédez à l'attribution manuelle d'adresse, vous risquez d'entraîner un scénario avec des adresses en double.

Si la configuration réseau automatique du processeur de service est désactivée après avoir été activée précédemment, les scénarios et considérations suivants s'appliquent :

- Si la configuration réseau automatique du processeur de service possède la famille d'adresses IPv4 désactivée, le réseau IPv4 du processeur de service utilise par défaut DHCP, et le `system service-processor network modify` La commande vous permet de modifier la configuration IPv4 du processeur de service pour les nœuds individuels.
- Si la famille d'adresses IPv6 est désactivée dans la configuration réseau automatique du processeur de service, le réseau IPv6 du processeur de service est également désactivé et le `system service-processor network modify` Vous permet d'activer et de modifier la configuration IPv6 du processeur de service pour les nœuds individuels.

Activez la configuration réseau automatique SP/BMC

Pour permettre au processeur de service d'utiliser la configuration réseau automatique, il est préférable de ne pas configurer le réseau du processeur de service manuellement. Étant donné que la configuration réseau automatique du processeur de service est à l'échelle du cluster, vous n'avez pas besoin de gérer manuellement le réseau du processeur de service pour les nœuds individuels.



Cette tâche s'applique à la fois au processeur de service et au contrôleur BMC.

- Le sous-réseau que vous souhaitez utiliser pour la configuration réseau automatique du processeur de service doit déjà être défini dans le cluster et ne doit pas avoir de conflit de ressources avec l'interface réseau du processeur de service.

Le `network subnet show` la commande affiche les informations de sous-réseau du cluster.

Le paramètre qui force l'association de sous-réseau (le `-force-update-lif-associations` paramètre du `network subnet` Commandes) est pris en charge uniquement sur les LIFs réseau et non sur l'interface réseau du processeur de service.

- Si vous souhaitez utiliser des connexions IPv6 pour le processeur de service, IPv6 doit déjà être configuré et activé pour ONTAP.

Le `network options ipv6 show` Commande affiche l'état actuel des paramètres IPv6 pour ONTAP.

Étapes

1. Spécifiez la famille d'adresses IPv4 ou IPv6 et le nom du sous-réseau que vous souhaitez que le processeur de service utilise `system service-processor network auto-configuration enable` commande.
2. Affiche la configuration réseau automatique du processeur de service à l'aide de `system service-processor network auto-configuration show` commande.
3. Si vous souhaitez par la suite désactiver ou réactiver l'interface réseau IPv4 ou IPv6 du processeur de service pour tous les nœuds qui se trouvent dans le quorum, utilisez le `system service-processor network modify` commande avec `-address-family [IPv4|IPv6]` et `-enable [true|false]` paramètres.

Lorsque la configuration réseau automatique du processeur de service est activée, vous ne pouvez pas modifier l'adresse IP du processeur de service pour un nœud qui se trouve au quorum. Vous pouvez activer ou désactiver uniquement l'interface réseau IPv4 ou IPv6 du processeur de service.

Si un nœud est hors quorum, vous pouvez modifier la configuration réseau du processeur de service du nœud, y compris l'adresse IP du processeur de service, en exécutant `system service-processor network modify` Depuis le nœud et confirmer que vous souhaitez remplacer la configuration réseau automatique du processeur de service pour le nœud. Cependant, lorsque le nœud rejoint le quorum, la reconfiguration automatique du processeur de service est effectuée pour le nœud en fonction du sous-réseau spécifié.

Configurez le réseau SP/BMC manuellement

Si vous ne disposez pas d'une configuration réseau automatique définie pour le processeur de service, vous devez configurer manuellement le réseau SP d'un nœud pour que ce dernier soit accessible via une adresse IP.

Ce dont vous avez besoin

Si vous souhaitez utiliser des connexions IPv6 pour le processeur de service, IPv6 doit déjà être configuré et activé pour ONTAP. Le `network options ipv6` Les commandes gèrent les paramètres IPv6 pour ONTAP.



Cette tâche s'applique à la fois au processeur de service et au contrôleur BMC.

Vous pouvez configurer le processeur de service pour qu'il utilise IPv4, IPv6 ou les deux. La configuration IPv4 du processeur de service prend en charge l'adressage statique et DHCP, et la configuration IPv6 du processeur de service prend uniquement en charge l'adressage statique.

Si la configuration réseau automatique du processeur de service a été configurée, vous n'avez pas besoin de configurer manuellement le réseau SP pour des nœuds individuels, et le `system service-processor network modify` La commande vous permet d'activer ou de désactiver uniquement l'interface réseau du processeur de service.

Étapes

1. Configurez le réseau du processeur de service d'un nœud en utilisant le `system service-processor`

`network modify` commande.

- Le `-address-family` Le paramètre spécifie si la configuration IPv4 ou IPv6 du processeur de service doit être modifiée.
- Le `-enable` Paramètre active l'interface réseau de la famille d'adresses IP spécifiée.
- Le `-dhcp` Paramètre indique si la configuration réseau doit être utilisée depuis le serveur DHCP ou l'adresse réseau que vous fournissez.

Vous pouvez activer DHCP (par paramètre) `-dhcp à v4`) Uniquement si vous utilisez IPv4. Vous ne pouvez pas activer DHCP pour les configurations IPv6.

- Le `-ip-address` Le paramètre spécifie l'adresse IP publique pour le processeur de service.

Un message d'avertissement apparaît lorsque vous tentez de configurer manuellement le réseau du processeur de service avec des adresses allouées à un sous-réseau. L'omission de l'avertissement et la poursuite de l'attribution manuelle d'adresse peuvent entraîner une affectation d'adresse en double.

- Le `-netmask` Le paramètre spécifie le masque de réseau du processeur de service (si vous utilisez IPv4).
- Le `-prefix-length` Paramètre spécifie la longueur du préfixe réseau du masque de sous-réseau pour le processeur de service (si vous utilisez IPv6).
- Le `-gateway` Le paramètre spécifie l'adresse IP de passerelle pour le processeur de service.

2. Configurez le réseau SP pour les nœuds restants du cluster en répétant l'étape 1.

3. Affiche la configuration réseau du processeur de service et vérifie le statut de configuration du processeur de service à l'aide de `system service-processor network show` commande avec `-instance` ou `-field setup-status` paramètres.

Le statut de configuration du processeur de service d'un nœud peut être l'un des suivants :

- `not-setup` — non configuré
- `succeeded` — Configuration réussie
- `in-progress` — Configuration en cours
- `failed` — Echec de la configuration

Exemple de configuration du réseau du processeur de service

L'exemple suivant configure le processeur de service d'un nœud pour utiliser IPv4, active le processeur de service et affiche la configuration réseau du processeur de service pour vérifier les paramètres :

```

cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

Node: node1
Address Type: IPv4
Interface Enabled: true
Type of Device: SP
Status: online
Link Status: up
DHCP Status: none
IP Address: 192.168.123.98
MAC Address: ab:cd:ef:fe:ed:02
Netmask: 255.255.255.0
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: 192.168.123.1
Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
Subnet Name: -
Enable IPv6 Router Assigned Address: -
SP Network Setup Status: succeeded
SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>

```

Modifiez la configuration du service d'API du processeur de service

L'API du processeur de service est une API réseau sécurisée qui permet à ONTAP de communiquer avec le processeur de service sur le réseau. Vous pouvez modifier le port utilisé par le service API SP, renouveler les certificats que le service utilise pour les communications internes ou désactiver entièrement le service. Vous ne devez modifier la configuration que dans de rares cas.

Description de la tâche

- Le service d'API du processeur de service utilise le port 50000 par défaut.

Vous pouvez modifier la valeur du port si, par exemple, vous êtes dans un paramètre réseau où port 50000 Est utilisé pour la communication par une autre application réseau ou pour différencier le trafic des autres applications et le trafic généré par le service API SP.

- Les certificats SSL et SSH utilisés par le service API du processeur de service sont internes au cluster et

ne sont pas distribués en externe.

Dans le cas peu probable où les certificats sont compromis, vous pouvez les renouveler.

- Le service API du processeur de service est activé par défaut.

Il vous suffit de désactiver le service API du processeur de service dans de rares cas, par exemple dans un LAN privé où le processeur de service n'est pas configuré ou utilisé et que vous souhaitez désactiver ce service.

Si le service d'API du processeur de service est désactivé, l'API n'accepte aucune connexion entrante. En outre, des fonctionnalités telles que les mises à jour de micrologiciel SP basées sur le réseau et la collecte de journaux de SP « `down system` » basée sur le réseau deviennent indisponibles. Le système passe à l'aide de l'interface série.

Étapes

1. Passez au niveau de privilège avancé à l'aide du `set -privilege advanced` commande.
2. Modifiez la configuration du service d'API du processeur de service :

Les fonctions que vous recherchez...	Utiliser la commande suivante...
Modifiez le port utilisé par le service d'API du processeur de service	<code>system service-processor api-service modify</code> avec le <code>-port {49152..`65535`paramètre }</code>
Renouvelez les certificats SSL et SSH utilisés par le service API SP pour les communications internes	<ul style="list-style-type: none">• Pour ONTAP 9.5 ou une utilisation ultérieure <code>system service-processor api-service renew-internal-certificate</code>• Pour ONTAP 9.4 et une utilisation antérieure <code>system service-processor api-service renew-certificates</code> <p>Si aucun paramètre n'est spécifié, seuls les certificats d'hôte (y compris les certificats client et serveur) sont renouvelés.</p> <p>Si le <code>-renew-all true</code> Le paramètre est spécifié, les certificats d'hôte et le certificat d'autorité de certification racine sont renouvelés.</p>
comm	
Désactivez ou réactivez le service API du processeur de service	<code>system service-processor api-service modify</code> avec le <code>-is-enabled {true</code>

3. Affichez la configuration du service API du processeur de service à l'aide de `system service-processor api-service show` commande.

Gérez les nœuds à distance à l'aide du processeur de service/contrôleur BMC

Gérez un nœud à distance à l'aide de la présentation SP/BMC

Vous pouvez gérer un nœud à distance à l'aide d'un contrôleur intégré, appelé processeur de service (SP) ou contrôleur BMC (Baseboard Management Controller). Ce contrôleur de gestion à distance est inclus dans tous les modèles de plate-forme actuels. Le contrôleur reste opérationnel quel que soit l'état de fonctionnement du nœud.

Les plates-formes suivantes prennent en charge BMC au lieu de SP :

- FAS 8700
- FAS 8300
- Prise de l'extension
- AFF A800
- AFF A700s
- AFF A400
- A320 de AFF
- AVEC AFF A220
- Baie AFF C190

À propos du processeur de service

Le processeur de service (SP) est un périphérique de gestion à distance qui vous permet d'accéder à, de contrôler et de dépanner un nœud à distance.

Le processeur de service offre les fonctionnalités suivantes :

- Le processeur de service permet d'accéder à un nœud à distance pour diagnostiquer, arrêter, mettre hors/sous tension ou redémarrer le nœud, quel que soit l'état du contrôleur.

Le processeur de service est alimenté par une tension de veille, disponible tant qu'au moins une de ses alimentations est alimentée.

Vous pouvez vous connecter au processeur de service à l'aide d'une application cliente Secure Shell sur un hôte d'administration. Vous pouvez ensuite utiliser l'interface de ligne de commande du processeur de service pour surveiller et dépanner le nœud à distance. Vous pouvez également utiliser le processeur de service pour accéder à la console série et exécuter des commandes ONTAP à distance.

Vous pouvez accéder au processeur de service à partir de la console série de ou accéder à la console série à partir du processeur de service. Le processeur de service vous permet d'ouvrir simultanément une session d'interface de ligne de commandes du processeur de service et une autre session de console.

Par exemple, lorsqu'un capteur de température devient critique ou faible, ONTAP déclenche l'arrêt normal du processeur de service de la carte mère. La console série ne répond plus, mais vous pouvez tout de même utiliser la combinaison de touches Ctrl-G sur la console pour accéder à l'interface de ligne de commandes du processeur de service. Vous pouvez ensuite utiliser le `system power on` ou `system`

`power cycle` Commande du processeur de service pour mettre le nœud sous tension ou hors tension.

- Le processeur de service surveille les capteurs environnementaux et les journaux d'événements pour vous aider à prendre des mesures de service efficaces et en temps opportun.

Le processeur de service surveille les capteurs environnementaux tels que les températures des nœuds, les tensions, les courants et la vitesse des ventilateurs. Lorsqu'un capteur environnemental a atteint un état anormal, le processeur de service consigne les lectures anormales, informe ONTAP du problème et envoie des alertes et des notifications « système propre » si nécessaire via un message AutoSupport, que le nœud puisse envoyer des messages AutoSupport ou non.

Le processeur de service consigne également des événements tels que la progression du démarrage, les modifications des unités remplaçables sur site, les événements générés par ONTAP et l'historique des commandes du processeur de service. Vous pouvez appeler manuellement un message AutoSupport pour inclure les fichiers journaux du processeur de service collectés à partir d'un nœud spécifié.

Autre que la génération de ces messages pour le compte d'un nœud qui est en panne et la connexion d'informations de diagnostic supplémentaires aux messages AutoSupport, le processeur de service n'a aucun impact sur la fonctionnalité AutoSupport. Les paramètres de configuration de AutoSupport et le comportement du contenu des messages sont hérités de ONTAP.



Le processeur de service ne repose pas sur le `-transport` paramètre du `system node autosupport modify` commande permettant d'envoyer des notifications. Le processeur de service utilise uniquement le protocole SMTP (simple Mail transport Protocol) et requiert la configuration AutoSupport de son hôte pour inclure les informations relatives à l'hôte de messagerie.

Si le protocole SNMP est activé, le processeur de service génère des interruptions SNMP vers des hôtes d'interruption configurés pour tous les événements "système propriétaire".

- Le processeur de service dispose d'un tampon de mémoire non volatile qui stocke jusqu'à 4,000 événements dans un journal des événements du système (SEL) pour vous aider à diagnostiquer les problèmes.

Le journal des événements système enregistre chaque entrée du journal d'audit en tant qu'événement d'audit. Il est stocké dans la mémoire flash intégrée sur le processeur de service. La liste des événements du journal des événements est automatiquement envoyée par le processeur de service aux destinataires spécifiés via un message AutoSupport.

Le journal des événements du système contient les informations suivantes :

- Événements matériels détectés par le processeur de service --par exemple, statut d'un capteur concernant les alimentations, la tension ou d'autres composants
 - Erreurs détectées par le processeur de service—par exemple, une erreur de communication, une panne de ventilateur ou une erreur de la mémoire ou de l'UC
 - Événements logiciels critiques envoyés au SP par le nœud—par exemple, une panique, une panne de communication, une panne de démarrage ou un "système propre" déclenché par l'utilisateur à la suite de l'émission du SP `system reset` ou `system power cycle` commande
- Le processeur de service surveille la console série, que les administrateurs soient connectés ou non à la console, que ce soit.

Lorsque des messages sont envoyés à la console, le processeur de service les stocke dans le journal de la console. Le journal de la console est conservé tant que le processeur de service est alimenté à partir

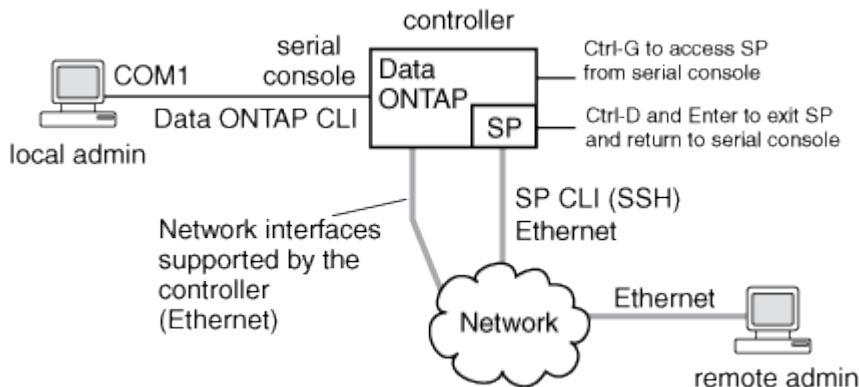
d'une des alimentations du nœud. Du fait que le processeur de service fonctionne avec une alimentation de veille, il demeure disponible même lorsque le nœud est mis hors tension puis sous tension ou lorsqu'il est arrêté.

- Le basculement assisté par matériel est disponible si le SP est configuré.
- Le service d'API du processeur de service permet à ONTAP de communiquer avec le processeur de service sur le réseau.

Le service améliore la gestion ONTAP du processeur de service en prenant en charge des fonctionnalités réseau telles que l'interface réseau de la mise à jour du firmware du processeur de service, ce qui permet à un nœud d'accéder à la fonctionnalité du processeur de service ou à la console système d'un autre nœud, et de charger le journal du processeur de service à partir d'un autre nœud.

Vous pouvez modifier la configuration du service API SP en modifiant le port utilisé par le service, en renouvelant les certificats SSL et SSH utilisés par le service pour une communication interne ou en désactivant entièrement le service.

Le schéma suivant illustre l'accès à ONTAP et au processeur de service d'un nœud. L'interface du processeur de service est accessible via le port Ethernet (indiqué par une icône de clé anglaise à l'arrière du châssis) :



Rôle du contrôleur de gestion de la carte mère

Depuis ONTAP 9.1, sur certaines plateformes matérielles, le logiciel est personnalisé pour prendre en charge un nouveau contrôleur intégré dans le contrôleur BMC (Baseboard Management Controller). Le contrôleur BMC dispose de commandes d'interface de ligne de commande (CLI) que vous pouvez utiliser pour gérer le périphérique à distance.

Le contrôleur BMC fonctionne de la même manière que le processeur de service et utilise plusieurs des mêmes commandes. Le BMC vous permet de faire les opérations suivantes :

- Configurez les paramètres réseau du contrôleur BMC.
- Accéder à un nœud à distance et effectuer des tâches de gestion de nœud, telles que diagnostiquer, arrêter, mettre hors/sous tension ou redémarrer le nœud.

Il existe certaines différences entre le processeur de service et le contrôleur BMC :

- Le contrôleur BMC contrôle entièrement la surveillance environnementale des éléments d'alimentation, des éléments de refroidissement, des capteurs de température, des capteurs de tension et des capteurs

de courant. Le contrôleur BMC signale les informations relatives aux capteurs à ONTAP via IPMI.

- Certaines des commandes de stockage et de haute disponibilité sont différentes.
- Le contrôleur BMC n'envoie pas de messages AutoSupport.

Des mises à jour automatiques du firmware sont également disponibles lors de l'exécution de ONTAP 9.2 GA ou version ultérieure avec les conditions suivantes :

- La version 1.15 ou ultérieure du micrologiciel BMC doit être installée.



Une mise à jour manuelle est nécessaire pour mettre à niveau le micrologiciel du contrôleur BMC de la version 1.12 à la version 1.15 ou ultérieure.

- BMC redémarre automatiquement une fois la mise à jour du micrologiciel terminée.



Les opérations de nœud ne sont pas affectées lors du redémarrage de BMC.

Méthodes de gestion des mises à jour du micrologiciel SP/BMC

ONTAP inclut une image du micrologiciel du processeur de service appelée *baseline image*. Si une nouvelle version du firmware du processeur de service est disponible par la suite, vous pouvez la télécharger et mettre à jour le firmware du processeur de service vers la version téléchargée sans mettre à niveau la version ONTAP.



Cette rubrique s'applique à la fois au processeur de service et au contrôleur BMC.

ONTAP propose les méthodes suivantes pour gérer les mises à jour du firmware du processeur de service :

- La fonctionnalité de mise à jour automatique du processeur de service est activée par défaut, ce qui permet la mise à jour automatique du firmware du processeur de service dans les scénarios suivants :
 - Lorsque vous effectuez une mise à niveau vers une nouvelle version de ONTAP

Le processus de mise à niveau du ONTAP inclut automatiquement la mise à jour du firmware du processeur de service, à condition que la version du firmware du processeur de service fournie avec ONTAP soit plus récente que la version du processeur de service exécutée sur le nœud.



ONTAP détecte une mise à jour automatique du processeur de service défectueuse et déclenche une action corrective pour retry la mise à jour automatique du processeur de service jusqu'à trois fois. Si les trois tentatives échouent, consultez le lien de l'article de la base de connaissances : [Health Monitor SPAutoUpgradeFailedMajorAlert la mise à niveau du SP échoue - message AutoSupport](#).

- Lorsque vous téléchargez une version du firmware du processeur de service depuis le site de support NetApp et que la version téléchargée est plus récente que celle actuellement exécutée par le processeur de service
- Lorsque vous rétrogradez ou restaurez à une version antérieure de ONTAP

Le micrologiciel du processeur de service est automatiquement mis à jour vers la dernière version compatible prise en charge par la version ONTAP que vous avez rétablie ou rétrogradée. Une mise à jour manuelle du firmware du processeur de service n'est pas requise.

Vous pouvez désactiver la fonctionnalité de mise à jour automatique du processeur de service à l'aide de `system service-processor image modify` commande. Toutefois, il est recommandé de ne pas activer cette fonctionnalité. La désactivation de cette fonctionnalité peut entraîner des combinaisons sous-optimales ou non qualifiées entre l'image ONTAP et l'image du firmware du processeur de service.

- ONTAP vous permet de déclencher manuellement une mise à jour du processeur de service et de spécifier comment la mise à jour doit avoir lieu à l'aide du `system service-processor image update` commande.

Vous pouvez spécifier les options suivantes :

- Le pack du firmware du processeur de service à utiliser (`-package`)

Vous pouvez mettre à jour le firmware du processeur de service sur un pack téléchargé en indiquant le nom du fichier d'image. L'avance `system image package show` La commande affiche tous les fichiers d'image (y compris les fichiers du pack du firmware du processeur de service) disponibles sur un nœud.

- Indique si vous souhaitez utiliser le pack du firmware du processeur de service de base pour la mise à jour du processeur de service (`-baseline`)

Vous pouvez mettre à jour le firmware du processeur de service vers la version de base fournie avec la version en cours d'exécution de ONTAP.



Si vous utilisez certaines des options ou paramètres de mise à jour les plus avancés, les paramètres de configuration du contrôleur BMC peuvent être temporairement effacés. Après le redémarrage, ONTAP peut restaurer la configuration du contrôleur BMC pendant 10 minutes.

- ONTAP vous permet d'afficher l'état de la dernière mise à jour du firmware du processeur de service déclenchée par ONTAP à l'aide de `system service-processor image update-progress show` commande.

Toute connexion existante au processeur de service est interrompue lors de la mise à jour du firmware du processeur de service. Voici si la mise à jour du firmware du processeur de service est automatique ou déclenchée manuellement.

Informations associées

["Téléchargements NetApp : firmware système et diagnostics"](#)

Lorsque le SP/BMC utilise l'interface réseau pour les mises à jour du micrologiciel

Une mise à jour du firmware du processeur de service déclenchée par ONTAP avec le processeur de service qui exécute les versions 1.5, 2.5, 3.1 ou ultérieures prend en charge l'utilisation d'un mécanisme de transfert de fichiers IP sur l'interface réseau du processeur de service.



Cette rubrique s'applique à la fois au processeur de service et au contrôleur BMC.

La mise à jour du firmware du processeur de service sur l'interface réseau est plus rapide qu'une mise à jour via l'interface série. Il réduit la fenêtre de maintenance pendant laquelle le firmware du processeur de service est mis à jour, et le fonctionnement de la ONTAP ne génère aucune interruption. Des versions du processeur

de service qui prennent en charge cette fonctionnalité sont incluses avec ONTAP. Ils sont également disponibles sur le site de support NetApp et peuvent être installés sur les contrôleurs qui exécutent une version compatible de ONTAP.

Lorsque vous exécutez SP version 1.5, 2.5, 3.1 ou ultérieure, les comportements de mise à niveau du micrologiciel suivants s'appliquent :

- Une mise à jour du firmware du processeur de service qui est *automatiquement* déclenchée par ONTAP par défaut par l'utilisation de l'interface réseau pour la mise à jour. Toutefois, le processeur de service passe à l'utilisation de l'interface série pour la mise à jour du firmware si l'une des conditions suivantes se produit :
 - L'interface réseau du processeur de service n'est pas configurée ou n'est pas disponible.
 - Le transfert de fichier IP échoue.
 - Le service API du processeur de service est désactivé.

Quelle que soit la version du processeur de service que vous exécutez, une mise à jour du firmware du processeur de service déclenchée par l'interface de ligne de commandes du processeur de service utilise toujours l'interface réseau du processeur de service pour la mise à jour.

Informations associées

["Téléchargements NetApp : firmware système et diagnostics"](#)

Comptes pouvant accéder au processeur de service

Lorsque vous tentez d'accéder au processeur de service, vous êtes invité à fournir des informations d'identification. Comptes utilisateurs du cluster créés avec le `service-processor` Le type d'application a accès à l'interface de ligne de commandes du processeur de service sur n'importe quel nœud du cluster. Les comptes utilisateurs du processeur de service sont gérés à partir de ONTAP et authentifiés par mot de passe. Depuis ONTAP 9.9.1, les comptes utilisateurs de SP doivent avoir le `admin` rôle.

Les comptes utilisateurs permettant d'accéder au processeur de service sont gérés à partir de ONTAP au lieu de l'interface de ligne de commandes du processeur de service. Un compte utilisateur du cluster peut accéder au processeur de service s'il est créé avec le `-application` paramètre du `security login create` commande définie sur `service-processor` et le `-authmethod` paramètre défini sur `password`. Le processeur de service prend uniquement en charge l'authentification par mot de passe.

Vous devez spécifier le `-role` Paramètre lors de la création d'un compte utilisateur du processeur de service.

- Dans ONTAP 9.9.1 et versions ultérieures, vous devez spécifier `admin` pour le `-role` et toute modification d'un compte nécessite le `admin` rôle. Les autres rôles ne sont plus autorisés pour des raisons de sécurité.
 - Si vous effectuez une mise à niveau vers ONTAP 9.9.1 ou une version ultérieure, reportez-vous à la section ["Modifier les comptes utilisateur pouvant accéder au Service Processor"](#).
 - Si vous rétablir ONTAP 9.8 ou des versions antérieures, consultez ["Vérifiez les comptes utilisateurs pouvant accéder au Service Processor"](#).
- Dans ONTAP 9.8 et les versions antérieures, tout rôle peut accéder au processeur de service, mais `admin` est recommandé.

Par défaut, le compte d'utilisateur du cluster nommé « admin » inclut le `service-processor` Le type d'application et a accès au processeur de service.

ONTAP vous empêche de créer des comptes utilisateur avec des noms réservés au système (tels que « root » et « naroot »). Vous ne pouvez pas utiliser un nom réservé système pour accéder au cluster ou au processeur de service.

Vous pouvez afficher les comptes utilisateurs actuels du processeur de service à l'aide de `-application service-processor` paramètre du `security login show` commande.

Accéder au SP/BMC à partir d'un hôte d'administration

Vous pouvez vous connecter au processeur de service d'un nœud à partir d'un hôte d'administration pour effectuer des tâches de gestion des nœuds à distance.

Ce dont vous avez besoin

Les conditions suivantes doivent être remplies :

- L'hôte d'administration que vous utilisez pour accéder au processeur de service doit prendre en charge SSHv2.
- Votre compte utilisateur doit déjà être configuré pour l'accès au processeur de service.

Pour accéder au processeur de service, votre compte utilisateur doit avoir été créé avec le `-application` paramètre du `security login create` commande définie sur `service-processor` et le `-authmethod` paramètre défini sur `password`.



Cette tâche s'applique à la fois au processeur de service et au contrôleur BMC.

Si le processeur de service est configuré pour utiliser une adresse IPv4 ou IPv6 et si cinq tentatives de connexion SSH d'un hôte échouent consécutivement en 10 minutes, le processeur de service rejette les demandes de connexion SSH et suspend la communication avec l'adresse IP de l'hôte pendant 15 minutes. La communication reprend au bout de 15 minutes, et vous pouvez essayer de vous reconnecter au processeur de service.

ONTAP vous empêche de créer ou d'utiliser des noms réservés au système (tels que « root » et « naroot ») pour accéder au cluster ou au processeur de service.

Étapes

1. Depuis l'hôte d'administration, connectez-vous au processeur de service :

```
ssh username@SP_IP_address
```

2. Lorsque vous êtes invité, saisissez le mot de passe pour `username`.

L'invite du processeur de service apparaît, indiquant que vous avez accès à l'interface de ligne de commandes du processeur de service.

Exemples d'accès au processeur de service à partir d'un hôte d'administration

L'exemple suivant montre comment vous connecter au processeur de service avec un compte utilisateur `joe`, Qui a été configuré pour accéder au processeur de service.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

Les exemples suivants montrent comment utiliser l'adresse globale IPv6 ou l'adresse annoncée du routeur IPv6 pour vous connecter au processeur de service sur un nœud sur lequel SSH est configuré pour IPv6 et le processeur de service configuré pour IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

Accédez au processeur de service/BMC à partir de la console système

Vous pouvez accéder au processeur de service à partir de la console système (également appelée *console série*) pour effectuer des tâches de surveillance ou de dépannage.

Description de la tâche

Cette tâche s'applique à la fois au processeur de service et au contrôleur BMC.

Étapes

1. Accédez à l'interface de ligne de commandes du processeur de service à partir de la console système en appuyant sur Ctrl-G à l'invite de.
2. Connectez-vous à l'interface de ligne de commandes du processeur de service lorsque vous êtes invité.

L'invite du processeur de service apparaît, indiquant que vous avez accès à l'interface de ligne de commandes du processeur de service.

3. Quittez l'interface de ligne de commandes du processeur de service et revenez à la console du système en appuyant sur Ctrl-D, puis appuyez sur entrée.

Exemple d'accès à l'interface de ligne de commandes du processeur de service à partir de la console système

L'exemple suivant montre le résultat d'une pression sur Ctrl-G depuis la console système pour accéder à l'interface de ligne de commandes du processeur de service. Le `help system power` La commande est entrée à l'invite du processeur de service, suivie d'une pression sur Ctrl-D, puis entrée pour revenir à la console du système.

```
cluster1::>
```


(Appuyez sur Ctrl-G pour accéder à l'interface de ligne de commandes du processeur de service.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Appuyez sur Ctrl-D, puis entrée pour revenir à la console du système.)

```
cluster1::>
```

Relations entre l'interface de ligne de commandes du processeur de service, la console du processeur de service et les sessions de console système

Vous pouvez ouvrir une session de l'interface de ligne de commandes du processeur de service afin de gérer un nœud à distance et d'ouvrir une session de console distincte du processeur de service pour accéder à la console du nœud. La session de la console du processeur de service met en miroir les valeurs de sortie affichées dans une session de console système simultanée. Le processeur de service et la console du système disposent d'environnements shell indépendants avec une authentification de connexion indépendante.

La présentation de la façon dont les sessions de l'interface de ligne de commandes du processeur de service, de la console du processeur de service et de la console système sont associées permet de gérer un nœud à distance. Voici une description de la relation entre les sessions :

- Un seul administrateur peut se connecter à la session de l'interface de ligne de commandes du processeur de service à la fois. Toutefois, le processeur de service vous permet d'ouvrir simultanément une session de l'interface de ligne de commandes du processeur de service et une autre session de console du processeur de service.

L'interface de ligne de commandes du processeur de service est indiquée avec l'invite du processeur de service (SP>). Dans une session de l'interface de ligne de commandes du processeur de service, vous pouvez utiliser ce dernier `system console` Commande pour lancer une session de console du processeur de service. En même temps, vous pouvez démarrer une session de l'interface de ligne de commandes du processeur de service distincte via SSH. Si vous appuyez sur Ctrl-D pour quitter la session de console du processeur de service, vous revenez automatiquement à la session de l'interface de ligne de commandes du processeur de service. Si une session de l'interface de ligne de commandes du processeur de service existe déjà, un message vous demande si vous souhaitez mettre fin à la session de l'interface de ligne de commandes du processeur de service existante. Si vous saisissez « y », la session de l'interface de ligne de commandes du processeur de service existante est interrompue, ce qui vous

permet de revenir de la console du processeur de service à l'interface de ligne de commandes du processeur de service. Cette action est enregistrée dans le journal des événements du processeur de service.

Dans une session de l'interface de ligne de commandes ONTAP connectée via SSH, vous pouvez basculer sur la console système d'un nœud en exécutant `ONTAP system node run-console` commande provenant d'un autre nœud.

- Pour des raisons de sécurité, la session de l'interface de ligne de commandes du processeur de service et la session de console du système ont une authentification de connexion indépendante.

Lorsque vous lancez une session de console du processeur de service à partir de l'interface de ligne de commandes du processeur de service (en utilisant le processeur de service) `system console` commande), vous êtes invité à fournir les informations d'identification de la console du système. Lorsque vous accédez à l'interface de ligne de commandes du processeur de service à partir d'une session de console système (en appuyant sur Ctrl-G), vous êtes invité à fournir les informations d'identification de l'interface de ligne de commandes du processeur de service.

- La session de console du processeur de service et la session de console du système ont des environnements de shell indépendants.

La session de la console du processeur de service met en miroir les valeurs de sortie affichées dans une session de console simultanée du système. Cependant, la session de console simultanée du système ne met pas en miroir la session de console du processeur de service.

La session de la console du processeur de service ne met pas en miroir les valeurs de sortie des sessions SSH simultanées.

Gérez les adresses IP pouvant accéder au processeur de service

Par défaut, le processeur de service accepte les requêtes de connexion SSH des hôtes d'administration de n'importe quelle adresse IP. Vous pouvez configurer le processeur de service pour qu'il accepte les requêtes de connexion SSH depuis uniquement les hôtes d'administration qui possèdent les adresses IP que vous spécifiez. Les modifications que vous apportez s'appliquent à l'accès SSH au processeur de service de n'importe quel nœud du cluster.

Étapes

1. Accordez au processeur de service l'accès aux adresses IP que vous spécifiez via le `system service-processor ssh add-allowed-addresses` commande avec `-allowed-addresses` paramètre.

- La valeur du `-allowed-addresses` le paramètre doit être spécifié au format de `address/netmask`, et multiple `address/netmask` les paires doivent être séparées par des virgules, par exemple `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

Réglage du `-allowed-addresses` paramètre à `0.0.0.0/0, ::/0` Permet à toutes les adresses IP d'accéder au processeur de service (par défaut).

- Lorsque vous modifiez la valeur par défaut en limitant l'accès au SP aux adresses IP que vous spécifiez, ONTAP vous invite à confirmer que vous souhaitez que les adresses IP spécifiées remplacent le paramètre par défaut « Autoriser tous » (`0.0.0.0/0, ::/0`).
- Le `system service-processor ssh show` La commande affiche les adresses IP pouvant

accéder au processeur de service.

2. Si vous souhaitez bloquer l'accès au processeur de service à une adresse IP spécifiée, utilisez le `system service-processor ssh remove-allowed-addresses` commande avec `-allowed-addresses` paramètre.

Si vous bloquez l'accès à toutes les adresses IP, le processeur de service devient inaccessible depuis n'importe quel hôte d'administration.

Exemples de gestion des adresses IP pouvant accéder au processeur de service

Les exemples suivants montrent le paramètre par défaut pour l'accès SSH au processeur de service, modifiez la valeur par défaut en limitant l'accès du processeur de service aux adresses IP spécifiées, en supprimant les adresses IP spécifiées de la liste d'accès, puis en restaurant l'accès du processeur de service pour toutes les adresses IP :

```

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
      with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
      addresses will be denied access. To restore the "allow all"
default,
      use the "system service-processor ssh add-allowed-addresses
      -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
      {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

```

Utilisez l'aide en ligne de la CLI SP/BMC

L'aide en ligne affiche les commandes et options de la CLI du processeur de service/BMC.

Description de la tâche

Cette tâche s'applique à la fois au processeur de service et au contrôleur BMC.

Étapes

1. Pour afficher les informations d'aide pour les commandes SP/BMC, entrez les suivantes :

Pour accéder à l'aide du processeur de service...	Pour accéder à l'aide de BMC...
Type <code>help</code> À l'invite du processeur de service.	Type <code>system</code> À l'invite BMC.

L'exemple suivant montre l'aide en ligne de l'interface de ligne de commandes du processeur de service.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

L'exemple suivant montre l'aide en ligne de BMC CLI.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. Pour afficher les informations d'aide relatives à l'option d'une commande SP/BMC, entrez `help` Avant ou après la commande SP/BMC.

L'exemple suivant montre l'aide en ligne de l'interface de ligne de commandes du processeur de service pour le processeur de service `events` commande.

```
SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

L'exemple suivant montre l'aide en ligne de BMC CLI pour le BMC `system power` commande.

```
BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>
```

Commandes permettant de gérer à distance un nœud

Vous pouvez gérer un nœud à distance en accédant à son processeur de service et en exécutant des commandes de l'interface de ligne de commandes du processeur de service afin d'effectuer des tâches de gestion des nœuds. Dans le cas de plusieurs tâches courantes de gestion des nœuds à distance, vous pouvez également utiliser les commandes ONTAP d'un autre nœud du cluster. Certaines commandes du processeur de service sont spécifiques à la plateforme et peuvent ne pas être disponibles sur votre plateforme.


Les fonctions que vous recherchez...	Utilisez cette commande du processeur de service...	Utilisez cette commande BMC...	Ou cette commande ONTAP ...
Affiche les commandes ou sous-commandes du processeur de service disponibles d'une commande SP spécifiée	<code>help [command]</code>		
Affiche le niveau de privilège actuel pour l'interface de ligne de commandes du processeur de service	<code>priv show</code>		


Les fonctions que vous recherchez...	Utilisez cette commande du processeur de service...	Utilisez cette commande BMC...	Ou cette commande ONTAP ...
Définissez le niveau de privilège pour accéder au mode spécifié pour l'interface de ligne de commandes du processeur de service	<code>priv set {admin</code>	<code>advanced</code>	<code>diag}</code>
		Afficher la date et l'heure du système	<code>date</code>
	<code>date</code>	Affiche les événements consignés par le processeur de service	<code>events {all</code>
<code>info</code>	<code>newest number</code>	<code>oldest number</code>	<code>search keyword}</code>
		Affiche l'état du processeur de service et les informations de configuration réseau	<code>sp status [-v</code>
<code>-d]</code> Le <code>-v</code> Option affiche les statistiques du processeur de service sous forme détaillée. Le <code>-d</code> Option ajoute le journal de débogage du processeur de service à l'affichage.	<code>bmc status [-v</code>	<code>-d]</code> Le <code>-v</code> Option affiche les statistiques du processeur de service sous forme détaillée. Le <code>-d</code> Option ajoute le journal de débogage du processeur de service à l'affichage.	<code>system service-processor show</code>
Affiche la durée de mise en service du processeur de service et le nombre moyen de tâches de la file d'attente d'exécution au cours des 1, 5 et 15 dernières minutes	<code>sp uptime</code>	<code>bmc uptime</code>	
Affiche les journaux de la console du système	<code>system log</code>		
Affiche les archives du journal du processeur de service ou les fichiers d'une archive	<code>sp log history show [-archive {latest</code>	<code>{all</code>	<code>archive-name}] [-dump {all</code>

Les fonctions que vous recherchez...	Utilisez cette commande du processeur de service...	Utilisez cette commande BMC...	Ou cette commande ONTAP ...
file-name}}	bmc log history show [-archive {latest	{all	archive-name}} [-dump {all
file-name}}		Affiche l'état de mise sous tension du contrôleur d'un nœud	system power status
	system node power show	Afficher les informations sur la batterie	system battery show
		Affiche les informations ACP ou l'état des capteurs du module d'extension	system acp [show
sensors show]			Répertorier toutes les unités remplaçables sur site et leurs ID
system fru list			Affiche les informations produit pour l'unité remplaçable sur site spécifiée
system fru show fru_id			Affiche le journal d'historique des données FRU
system fru log show (niveau de privilège avancé)			Affiche le statut des capteurs environnementaux, y compris leurs États et leurs valeurs actuelles
system sensors ou system sensors show		system node environment sensors show	Affiche l'état et les détails du capteur spécifié

Les fonctions que vous recherchez...	Utilisez cette commande du processeur de service...	Utilisez cette commande BMC...	Ou cette commande ONTAP ...
<code>system sensors get sensor_name</code> Vous pouvez obtenir <code>sensor_name</code> à l'aide du <code>system sensors</code> ou le <code>system sensors show</code> commande.			Affiche les informations de version du firmware du processeur de service
<code>version</code>		<code>system service-processor image show</code>	Affiche l'historique des commandes du processeur de service
<code>sp log audit</code> (niveau de privilège avancé)	<code>bmc log audit</code>		Affiche les informations de débogage du processeur de service
<code>sp log debug</code> (niveau de privilège avancé)	<code>bmc log debug</code> (niveau de privilège avancé)		Affiche le fichier des messages du processeur de service
<code>sp log messages</code> (niveau de privilège avancé)	<code>bmc log messages</code> (niveau de privilège avancé)		Affiche les paramètres de collecte d'analyses système lors d'un événement de réinitialisation de la surveillance, affiche les informations d'analyse système recueillies lors d'un événement de réinitialisation de la surveillance ou efface les informations d'analyse système recueillies
<code>system forensics [show</code>	<code>log dump</code>	<code>log clear]</code>	
	Connectez-vous à la console du système	<code>system console</code>	

Les fonctions que vous recherchez...	Utilisez cette commande du processeur de service...	Utilisez cette commande BMC...	Ou cette commande ONTAP ...
system node run-console	Vous devez appuyer sur Ctrl-D pour quitter la session de console du système.	Mise sous tension ou hors tension du nœud, ou réalisation d'une mise hors/sous tension (mise hors tension, puis remise sous tension)	system power on
	system node power on (niveau de privilège avancé)	system power off	
	system power cycle		

Les fonctions que vous recherchez...	Utilisez cette commande du processeur de service...	Utilisez cette commande BMC...	Ou cette commande ONTAP ...
<p>L'alimentation de veille reste allumée pour maintenir le processeur de service en fonctionnement sans interruption. Pendant la mise hors/sous tension, une brève pause se produit avant de remettre l'alimentation en marche.</p> <div data-bbox="167 1014 220 1066">  </div> <p>À l'aide de ces commandes, la mise hors/sous tension du nœud peut provoquer un arrêt incorrect du nœud (également appelé <i>shutdown</i>) et ne remplace pas un arrêt normal à l'aide de ONTAP <code>system node halt</code> commande.</p>	<p>Créer un « core dump » et réinitialiser le nœud</p>	<p><code>system core [-f]</code></p> <p>Le <code>-f</code> option force la création d'un « core dump » et la réinitialisation du nœud.</p>	

Les fonctions que vous recherchez...	Utilisez cette commande du processeur de service...	Utilisez cette commande BMC...	Ou cette commande ONTAP ...
<p>system node coredump trigger</p> <p>(niveau de privilège avancé)</p>	<p>Ces commandes ont le même effet que d'appuyer sur le bouton non masquable Interrupt (NMI) d'un nœud, provoquant un arrêt non planifié du nœud et forçant un vidage des fichiers core lors de l'arrêt du nœud. Ces commandes sont utiles lorsque ONTAP sur le nœud est arrêté ou ne répond pas aux commandes telles que system node shutdown. Les fichiers core dump générés sont affichés dans la sortie du system node coredump show commande. Le processeur de service reste opérationnel tant que l'alimentation en entrée du nœud n'est pas interrompue.</p>	<p>Redémarrez le nœud à l'aide d'une image du micrologiciel du BIOS (primaire, de sauvegarde ou de courant) spécifiée en option pour effectuer une restauration suite à des problèmes tels qu'une image corrompue du périphérique d'amorçage du nœud</p>	<p>system reset {primary}</p>
<p>backup</p>	<p>current}</p>		<p>system node reset avec le -firmware {primary}</p>
<p>backup</p>	<p>current} paramètre (niveau de privilège avancé)</p> <p>system node reset</p>	<div>  <p>Cette opération provoque un arrêt non planifié du nœud.</p> </div> <p>Si aucune image du micrologiciel du BIOS n'est spécifiée, l'image actuelle est utilisée pour le redémarrage. Le processeur de service reste opérationnel tant que l'alimentation en entrée du nœud n'est pas interrompue.</p>	<p>Affiche l'état de la mise à jour automatique du firmware des batteries ou active ou désactive la mise à jour automatique du firmware des batteries lors du prochain démarrage du SP</p>

Les fonctions que vous recherchez...	Utilisez cette commande du processeur de service...	Utilisez cette commande BMC...	Ou cette commande ONTAP ...
system battery auto_update [status]	enable	disable] (niveau de privilège avancé)	
	Comparez l'image actuelle du micrologiciel de la batterie à une image de micrologiciel spécifiée	system battery verify [image_URL] (niveau de privilège avancé) Si image_URL n'est pas spécifié, l'image du micrologiciel de la batterie par défaut est utilisée pour la comparaison.	
	Mettez à jour le micrologiciel de la batterie à partir de l'image à l'emplacement spécifié	system battery flash image_URL (niveau de privilège avancé) Vous utilisez cette commande si le processus de mise à niveau automatique du micrologiciel de la batterie a échoué pour une raison quelconque.	
	Mettez à jour le firmware du processeur de service en utilisant l'image à l'emplacement spécifié	sp update image_URL image_URL il ne doit pas dépasser 200 caractères.	bmc update image_URL image_URL il ne doit pas dépasser 200 caractères.
system service-processor image update	Redémarre le processeur de service	sp reboot	

Les fonctions que vous recherchez...	Utilisez cette commande du processeur de service...	Utilisez cette commande BMC...	Ou cette commande ONTAP ...
system service-processor reboot-sp	Effacez le contenu Flash de la mémoire NVRAM	system nvram flash clear (niveau de privilège avancé) Cette commande ne peut pas être démarrée lorsque le contrôleur est hors tension (system power off).	
	Quittez l'interface de ligne de commandes du processeur de service	exit	

À propos des mesures du capteur du processeur de service à seuil et des valeurs d'état du résultat de la commande des capteurs du système

Les capteurs à seuils prélèvent des mesures périodiques des différents composants du système. Le processeur de service compare la mesure d'un capteur à seuil par rapport aux limites de seuil prédéfinies qui définissent les conditions de fonctionnement acceptables d'un composant.

En fonction de la mesure du capteur, le processeur de service affiche l'état du capteur pour vous aider à contrôler l'état du composant.

Les capteurs de température, de tension, de courant et de vitesse des ventilateurs du système sont des exemples de capteurs à seuils. La liste spécifique des capteurs à seuils dépend de la plateforme.

Les seuils des capteurs à seuils sont les suivants, affichés dans le résultat du processeur de service `system sensors` commande :

- Valeur critique inférieure (LCR)
- Valeur non critique inférieure (LNC)
- Valeur non critique supérieure (UNC)
- Valeur critique supérieure (UCR)

Une mesure de capteur entre LNC et LCR ou entre UNC et UCR indique des signes d'un problème et une panne du système. Par conséquent, vous devez prévoir rapidement un entretien du composant.

Une mesure de capteur inférieure à LCR ou supérieure à UCR indique un dysfonctionnement du composant et une panne imminente du système. Le composant requiert donc une intervention immédiate.

Le schéma suivant illustre les plages de gravité spécifiées par les seuils :



La mesure d'un capteur à seuil se trouve sous le `Current` dans le `system sensors` sortie de la commande. Le `system sensors get sensor_name` la commande affiche des détails supplémentaires pour le capteur spécifié. Lorsque la mesure d'un capteur à seuil franchit les plages de seuils non critique et critique, le capteur signale un problème d'augmentation de la gravité. Lorsque la mesure dépasse une limite de seuil, l'état du capteur dans le `system sensors` la sortie de la commande change de `ok` à `nc` (non critique) ou `cr` (Critique) selon le seuil dépassé et un message d'événement est enregistré dans le journal des événements du journal des événements du système.

Certains capteurs à seuils ne possèdent pas les quatre niveaux de seuil. Les seuils manquants indiquent concernant ces capteurs `na` comme leurs limites dans le `system sensors`. Le résultat de la commande, indiquant que le capteur particulier n'a aucune limite ou problème de gravité pour le seuil donné, et que le processeur de service ne surveille pas le capteur pour ce seuil.

Exemple de sortie de la commande System Sensors

L'exemple suivant montre certaines des informations affichées par `system sensors` Commande dans l'interface de ligne de commandes du processeur de service :

```
SP node1> system sensors
```

Sensor Name	Current	Unit	Status	LCR	LNC
UNC	UCR				
-----+-----+-----+-----+-----+					
-----+-----+-----					
CPU0_Temp_Margin	-55.000	degrees C	ok	na	na
-5.000	0.000				
CPU1_Temp_Margin	-56.000	degrees C	ok	na	na
-5.000	0.000				
In_Flow_Temp	32.000	degrees C	ok	0.000	10.000
42.000	52.000				
Out_Flow_Temp	38.000	degrees C	ok	0.000	10.000
59.000	68.000				
CPU1_Error	0x0	discrete	0x0180	na	na
na	na				
CPU1_Therm_Trip	0x0	discrete	0x0180	na	na
na	na				
CPU1_Hot	0x0	discrete	0x0180	na	na
na	na				
IO_Mid1_Temp	30.000	degrees C	ok	0.000	10.000
55.000	64.000				
IO_Mid2_Temp	30.000	degrees C	ok	0.000	10.000
55.000	64.000				
CPU_VTT	1.106	Volts	ok	1.028	1.048
1.154	1.174				
CPU0_VCC	1.154	Volts	ok	0.834	0.844
1.348	1.368				
3.3V	3.323	Volts	ok	3.053	3.116
3.466	3.546				
5V	5.002	Volts	ok	4.368	4.465
5.490	5.636				
STBY_1.8V	1.794	Volts	ok	1.678	1.707
1.892	1.911				
...					

Exemple de sortie de la commande `sensor_name` des capteurs système pour un capteur à seuils

L'exemple suivant montre le résultat de la saisie `system sensors get sensor_name` Dans l'interface de ligne de commandes du processeur de service pour le capteur à seuil 5V :


```

SP node1> system sensors get 5V

Locating sensor record...
Sensor ID           : 5V (0x13)
Entity ID           : 7.97
Sensor Type (Analog) : Voltage
Sensor Reading       : 5.002 (+/- 0) Volts
Status               : ok
Lower Non-Recoverable : na
Lower Critical        : 4.246
Lower Non-Critical    : 4.490
Upper Non-Critical    : 5.490
Upper Critical        : 5.758
Upper Non-Recoverable : na
Assertion Events      :
Assertions Enabled    : lnc- lcr- ucr+
Deassertions Enabled : lnc- lcr- ucr+

```

Informations sur les valeurs d'état du capteur SP discrètes du résultat de la commande des capteurs du système

Les capteurs discrets ne possèdent pas de seuils. Leurs relevés, affichés sous le `Current` Dans l'interface de ligne de commandes du processeur de service `system sensors` La sortie de la commande, ne portent pas de significations réelles et sont ainsi ignorées par le processeur de service. Le `Status` dans le `system sensors` le résultat de la commande affiche les valeurs d'état des capteurs discrets au format hexadécimal.

Les capteurs de panne des ventilateurs, des unités d'alimentation et du système sont des exemple de capteurs discrets. La liste spécifique des capteurs discrets dépend de la plateforme.

Vous pouvez utiliser l'interface de ligne de commandes du processeur de service `system sensors get sensor_name` commande d'aide à l'interprétation des valeurs d'état de la plupart des capteurs discrets. Les exemples suivants montrent les résultats de la saisie `system sensors get sensor_name` Pour les capteurs discrets `CPU0_Error` et `IO_Slot1_PRESENT` :

```

SP node1> system sensors get CPU0_Error

Locating sensor record...
Sensor ID           : CPU0_Error (0x67)
Entity ID           : 7.97
Sensor Type (Discrete): Temperature
States Asserted      : Digital State
                     [State Deasserted]

```

```

SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID           : IO_Slot1_Present (0x74)
Entity ID           : 11.97
Sensor Type (Discrete): Add-in Card
States Asserted      : Availability State
                      [Device Present]

```

Bien que le `system sensors get sensor_name` La commande affiche les informations d'état de la plupart des capteurs discrets ; elle ne fournit pas d'informations d'état pour les capteurs discrets `System_FW_Status`, `System_Watchdog`, `PSU1_Input_Type` et `PSU2_Input_Type`. Vous pouvez utiliser les informations suivantes pour interpréter les valeurs d'état de ces capteurs.

System_FW_Status

L'état du capteur `System_FW_Status` s'affiche sous la forme de `0xAABB`. Vous pouvez combiner les informations de `AA` et `BB` pour déterminer l'état du capteur.

`AA` peut avoir l'une des valeurs suivantes :

Valeurs	État du capteur
01	Erreur du firmware du système
02	Blocage du firmware du système
04	Progression du firmware du système

`BB` peut avoir l'une des valeurs suivantes :

Valeurs	État du capteur
00	Le logiciel système s'est arrêté correctement
01	Initialisation de la mémoire en cours
02	Initialisation de la NVMEM en cours (lorsque la mémoire NVMEM est présente)
04	Restauration des valeurs du concentrateur du contrôleur de mémoire (MCH) (lorsque NVMEM est présent)
05	L'utilisateur a accédé à la configuration

Valeurs	État du capteur
13	Démarrage du système d'exploitation ou DU CHARGEUR
1F	Le BIOS est en cours de démarrage
20	LE CHARGEUR est en cours d'exécution
21	LE CHARGEUR programme le firmware du BIOS principal. Vous ne devez pas mettre le système hors tension.
22	LE CHARGEUR programme l'autre firmware du BIOS. Vous ne devez pas mettre le système hors tension.
2E	ONTAP est en cours d'exécution
60	Le processeur de service est hors tension du système
61	Le processeur de service est mis sous tension sur le système
62	Le processeur de service a réinitialisé le système
63	Cycle d'alimentation du chien de garde du processeur de service
64	Réinitialisation à froid du processeur de service

Par exemple, l'état du capteur System_FW_Status 0x042F signifie « progression du micrologiciel du système (04), ONTAP est en cours d'exécution (2F) ».

Surveillance_système

Le capteur System_Watchdog peut avoir l'une des conditions suivantes :

- **0x0080**

L'état de ce capteur n'a pas changé

Valeurs	État du capteur
0x0081	Interruption du temporisateur
0x0180	Temporisation expirée

Valeurs	État du capteur
0x0280	Réinitialisation matérielle
0x0480	Hors tension
0x0880	Cycle d'alimentation

Par exemple, l'état 0x0880 du capteur System_Watchdog indique qu'un délai de surveillance est expiré et provoque un cycle d'alimentation du système.

PSU1_Input_Type et PSU2_Input_Type

Pour les alimentations à courant continu (CC), les capteurs PSU1_Input_Type et PSU2_Input_Type ne s'appliquent pas. Pour les alimentations à courant alternatif (CA), l'état des capteurs peut avoir l'une des valeurs suivantes :

Valeurs	État du capteur
0x01 xx	Type d'alimentation 220 V
0x02 xx	Type d'alimentation 110 V

Par exemple, l'état du capteur PSU1_Input_Type 0x0280 indique que le capteur indique que le type d'alimentation est 110 V.

Commandes de gestion du processeur de service à partir de ONTAP

ONTAP fournit des commandes de gestion du processeur de service, y compris la configuration réseau du processeur de service, l'image du firmware du processeur de service, l'accès SSH au processeur de service et l'administration générale du processeur de service.

Commandes permettant de gérer la configuration réseau du processeur de service


Les fonctions que vous recherchez...	Exécuter cette commande ONTAP...
Activez la configuration réseau automatique du processeur de service pour que ce dernier utilise la famille d'adresse IPv4 ou IPv6 du sous-réseau spécifié	<code>system service-processor network auto-configuration enable</code>
Désactivez la configuration réseau automatique du processeur de service pour la famille d'adresses IPv4 ou IPv6 du sous-réseau spécifié pour le processeur de service	<code>system service-processor network auto-configuration disable</code>

Les fonctions que vous recherchez...	Exécuter cette commande ONTAP...
Affiche la configuration réseau automatique du processeur de service	system service-processor network auto-configuration show
<p>Configurez manuellement le réseau du processeur de service d'un nœud, y compris les éléments suivants :</p> <ul style="list-style-type: none"> • La famille d'adresses IP (IPv4 ou IPv6) • Indique si l'interface réseau de la famille d'adresses IP spécifiée doit être activée • Si vous utilisez IPv4, que vous utilisiez la configuration réseau depuis le serveur DHCP ou l'adresse réseau que vous spécifiez • Adresse IP publique du processeur de service • Le masque de réseau du processeur de service (si vous utilisez IPv4) • Longueur du préfixe réseau du masque de sous-réseau pour le processeur de service (en cas d'utilisation d'IPv6) • Adresse IP de la passerelle pour le processeur de service 	system service-processor network modify
<p>Affichage de la configuration réseau du processeur de service, y compris les éléments suivants :</p> <ul style="list-style-type: none"> • La famille d'adresses configurée (IPv4 ou IPv6) et si elle est activée ou non • Type de périphérique de gestion à distance • État actuel du processeur de service et état de la liaison • Configuration du réseau, comme l'adresse IP, l'adresse MAC, le masque de réseau, la longueur du préfixe du masque de sous-réseau, l'adresse IP attribuée par le routeur, l'adresse IP locale de liaison et l'adresse IP de la passerelle • Heure à laquelle le processeur de service a été mis à jour pour la dernière fois • Nom du sous-réseau utilisé pour la configuration automatique du processeur de service • Indique si l'adresse IP attribuée par le routeur IPv6 est activée • État de configuration du réseau du processeur de service • Raison de l'échec de configuration réseau du processeur de service 	<p>system service-processor network show</p> <p>L'affichage des détails complets du réseau du processeur de service nécessite le -instance paramètre.</p>

Les fonctions que vous recherchez...	Exécuter cette commande ONTAP...
<p>Modifiez la configuration du service API du processeur de service, notamment :</p> <ul style="list-style-type: none"> • Modification du port utilisé par le service d'API du processeur de service • Activation ou désactivation du service API du processeur de service 	<pre>system service-processor api-service modify</pre> <p>(niveau de privilège avancé)</p>
<p>Affiche la configuration du service API du processeur de service</p>	<pre>system service-processor api-service show</pre> <p>(niveau de privilège avancé)</p>
<p>Renouvelez les certificats SSL et SSH utilisés par le service API SP pour les communications internes</p>	<ul style="list-style-type: none"> • Pour ONTAP 9.5 ou version ultérieure : <pre>system service-processor api-service renew-internal-certificates</pre> • Pour ONTAP 9.4 ou version antérieure : <pre>system service-processor api-service renew-certificates</pre> <p>(niveau de privilège avancé)</p>

Commandes permettant de gérer l'image du firmware du processeur de service

Les fonctions que vous recherchez...	Exécuter cette commande ONTAP...
<p>Afficher les détails de l'image du firmware du processeur de service actuellement installée, y compris les éléments suivants :</p> <ul style="list-style-type: none"> • Type de périphérique de gestion à distance • Image (principale ou de sauvegarde) à partir de laquelle le processeur de service démarre, son état et la version du firmware • Indique si la mise à jour automatique du micrologiciel est activée et que l'état de la dernière mise à jour est activé 	<pre>system service-processor image show</pre> <p>Le <code>-is-current</code> Paramètre indique l'image (principale ou de sauvegarde) à partir de laquelle le processeur de service est actuellement démarré, pas si la version du firmware installée est la plus récente.</p>

Les fonctions que vous recherchez...	Exécuter cette commande ONTAP...
Activez ou désactivez la mise à jour automatique du firmware du processeur de service	<pre>system service-processor image modify</pre> <p>Par défaut, le firmware du processeur de service est automatiquement mis à jour avec la mise à jour du ONTAP ou lorsqu'une nouvelle version du firmware du processeur de service est téléchargée manuellement. La désactivation de la mise à jour automatique n'est pas recommandée, car cela peut entraîner des combinaisons sous-optimales ou non qualifiées entre l'image ONTAP et l'image du firmware du processeur de service.</p>
Téléchargez manuellement une image du firmware du processeur de service sur un nœud	<pre>system node image get</pre> <div>  <p>Avant d'exécuter le <code>system node image</code> commandes, vous devez définir le niveau de privilège sur avancé (<code>set -privilege advanced</code>), saisissez y lorsque vous êtes invité à continuer.</p> </div> <p>L'image du firmware du processeur de service est fournie avec ONTAP. Vous n'avez pas besoin de télécharger manuellement le firmware du processeur de service, sauf si vous souhaitez utiliser une version du firmware du processeur de service différente de celle fournie avec ONTAP.</p>
<p>Affichez le statut de la dernière mise à jour du firmware du processeur de service déclenchée par ONTAP, y compris les informations suivantes :</p> <ul style="list-style-type: none"> • Heure de début et de fin de la dernière mise à jour du firmware du processeur de service • Indique si une mise à jour est en cours et le pourcentage terminé 	<pre>system service-processor image update-progress show</pre>

Commandes permettant de gérer l'accès SSH au processeur de service

Les fonctions que vous recherchez...	Exécuter cette commande ONTAP...
Accordez au SP un accès uniquement aux adresses IP spécifiées	<pre>system service-processor ssh add-allowed-addresses</pre>
Bloc les adresses IP spécifiées pour l'accès au processeur de service	<pre>system service-processor ssh remove-allowed-addresses</pre>

Les fonctions que vous recherchez...	Exécuter cette commande ONTAP...
Affiche les adresses IP pouvant accéder au processeur de service	<code>system service-processor ssh show</code>

Commandes d'administration générale du processeur de service

Les fonctions que vous recherchez...	Exécuter cette commande ONTAP...
<p>Affichage des informations générales sur le processeur de service, notamment :</p> <ul style="list-style-type: none"> • Type de périphérique de gestion à distance • État actuel du processeur de service • Indique si le réseau du processeur de service est configuré ou non • Informations sur le réseau, telles que l'adresse IP publique et l'adresse MAC • Version du firmware du processeur de service et version de l'interface IPMI (Intelligent Platform Management interface) • Indique si la mise à jour automatique du firmware du processeur de service est activée 	<p><code>system service-processor show</code> L'affichage des informations complètes du processeur de service nécessite le <code>-instance</code> paramètre.</p>
Redémarre le processeur de service sur un nœud	<code>system service-processor reboot-sp</code>
Générez et envoyez un message AutoSupport qui inclut les fichiers journaux du processeur de service collectés à partir d'un nœud spécifié	<code>system node autosupport invoke-splog</code>
Affiche la carte d'allocation des fichiers journaux du processeur de service collectés dans le cluster, y compris les numéros de séquence des fichiers journaux du processeur de service qui résident dans chaque nœud de collecte	<code>system service-processor log show-allocations</code>

Informations associées

["Commandes de ONTAP 9"](#)

Commandes ONTAP pour la gestion BMC

Ces commandes ONTAP sont prises en charge sur le contrôleur BMC (Baseboard Management Controller).

Le BMC utilise certaines des mêmes commandes que le processeur de service. Les commandes suivantes du processeur de service sont prises en charge sur le contrôleur BMC.

Les fonctions que vous recherchez...	Utilisez cette commande
Affiche les informations BMC	<code>system service-processor show</code>
Afficher/modifier la configuration réseau du BMC	<code>system service-processor network show/modify</code>
Réinitialisez le contrôleur BMC	<code>system service-processor reboot-sp</code>
Affiche/modifie les détails de l'image du micrologiciel BMC actuellement installée	<code>system service-processor image show/modify</code>
Mettre à jour le micrologiciel du contrôleur BMC	<code>system service-processor image update</code>
Affiche l'état de la dernière mise à jour du micrologiciel du contrôleur BMC	<code>system service-processor image update-progress show</code>
Activez la configuration réseau automatique pour que le contrôleur BMC utilise une adresse IPv4 ou IPv6 sur le sous-réseau spécifié	<code>system service-processor network auto-configuration enable</code>
Désactivez la configuration réseau automatique pour une adresse IPv4 ou IPv6 sur le sous-réseau spécifié pour le contrôleur BMC	<code>system service-processor network auto-configuration disable</code>
Afficher la configuration réseau automatique du contrôleur BMC	<code>system service-processor network auto-configuration show</code>

Pour les commandes qui ne sont pas prises en charge par le micrologiciel du contrôleur BMC, le message d'erreur suivant est renvoyé.

```
::> Error: Command not supported on this platform.
```

Commandes BMC CLI

Vous pouvez vous connecter au contrôleur BMC à l'aide de SSH. Les commandes suivantes sont prises en charge à partir de la ligne de commande BMC.

Commande	Fonction
systeme	Affiche la liste de toutes les commandes.
console systeme	Effectue la connexion à la console du système. Utiliser <code>Ctrl+D</code> pour quitter la session.

Commande	Fonction
cœur du système	Vide le « core » du système et effectue une réinitialisation.
cycle de mise sous tension du système	Mettez le système hors tension, puis sous tension.
le système est hors tension	Mettez le système hors tension.
le système est sous tension	Mettez le système sous tension.
état de l'alimentation du système	État de l'alimentation du système d'impression.
réinitialisation du système	Réinitialisez le système.
journal système	Imprimer les journaux de la console du système
affichage des fru du système [id]	Vidage des informations sur l'unité remplaçable sur site (FRU) sélectionnée.

Gestion de l'heure du cluster (administrateurs du cluster uniquement)

Les problèmes peuvent survenir lorsque l'heure du cluster est incorrecte. Bien que ONTAP vous permet de définir manuellement le fuseau horaire, la date et l'heure sur le cluster, vous devez configurer les serveurs NTP (Network Time Protocol) pour synchroniser l'heure du cluster.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

NTP est toujours activé. Toutefois, la synchronisation du cluster avec une source de temps externe nécessite toujours une configuration. ONTAP vous permet de gérer la configuration NTP du cluster de l'une des manières suivantes :

- Vous pouvez associer un maximum de 10 serveurs NTP externes au cluster (`cluster time-service ntp server create`).
 - Pour la redondance et la qualité du service de temps, vous devez associer au moins trois serveurs NTP externes au cluster.
 - Vous pouvez spécifier un serveur NTP à l'aide de son adresse IPv4 ou IPv6 ou de son nom d'hôte complet.
 - Vous pouvez spécifier manuellement la version NTP (v3 ou v4) à utiliser.

Par défaut, ONTAP sélectionne automatiquement la version NTP prise en charge pour un serveur NTP externe donné.

Si la version NTP que vous spécifiez n'est pas prise en charge pour le serveur NTP, le service de change ne peut pas avoir lieu.

- Au niveau de privilège avancé, vous pouvez spécifier un serveur NTP externe associé au cluster comme source de temps principale pour corriger et ajuster l'heure du cluster.
- Vous pouvez afficher les serveurs NTP associés au cluster (`cluster time-service ntp server show`).
- Vous pouvez modifier la configuration NTP du cluster (`cluster time-service ntp server modify`).
- Vous pouvez dissocier le cluster d'un serveur NTP externe (`cluster time-service ntp server delete`).
- Au niveau de privilège avancé, vous pouvez réinitialiser la configuration en désactivant toute association de serveurs NTP externes au cluster (`cluster time-service ntp server reset`).

Un nœud qui rejoint un cluster adopte automatiquement la configuration NTP du cluster.

Outre l'utilisation du protocole NTP, ONTAP vous permet également de gérer manuellement l'heure du cluster. Cette fonctionnalité est utile pour corriger une heure erronée (par exemple, l'heure d'un nœud est devenue très incorrecte après un redémarrage). Dans ce cas, vous pouvez indiquer une heure approximative du cluster jusqu'à ce que NTP puisse se synchroniser avec un serveur de temps externe. Le temps que vous définissez manuellement prend effet sur tous les nœuds du cluster.

Vous pouvez gérer manuellement l'heure du cluster des manières suivantes :

- Vous pouvez définir ou modifier le fuseau horaire, la date et l'heure sur le cluster (`cluster date modify`).
- Vous pouvez afficher les paramètres actuels du fuseau horaire, de date et d'heure du cluster (`cluster date show`).



Les planifications des tâches ne s'adaptent pas aux modifications manuelles de la date et de l'heure du cluster. Ces travaux sont planifiés pour s'exécuter en fonction de l'heure actuelle du cluster au moment de la création du travail ou de l'exécution du travail le plus récent. Par conséquent, si vous modifiez manuellement la date ou l'heure du cluster, vous devez utiliser le `job show` et `job history show` commandes permettant de vérifier que tous les travaux planifiés sont mis en file d'attente et terminés en fonction de vos besoins.



Commandes de gestion de l'heure du cluster

Vous utilisez le `cluster time-service ntp server` Commandes permettant de gérer les serveurs NTP du cluster. Vous utilisez le `cluster date` commandes permettant de gérer manuellement l'heure du cluster.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

Les commandes suivantes vous permettent de gérer les serveurs NTP du cluster :

Les fonctions que vous recherchez...	Utilisez cette commande...
Associez le cluster à un serveur NTP externe sans authentification symétrique	<code>cluster time-service ntp server create -server server_name</code>

Les fonctions que vous recherchez...	Utilisez cette commande...
Associez le cluster à un serveur NTP externe avec une authentification symétrique disponible dans ONTAP 9.5 ou version ultérieure	<pre>cluster time-service ntp server create -server server_ip_address -key-id key_id</pre> <div>  <p>Le <code>key_id</code> doit faire référence à une clé partagée existante configurée avec « clé ntp de service de cluster ».</p> </div>
<p>Activer l'authentification symétrique pour un serveur NTP existant le serveur NTP existant peut être modifié pour activer l'authentification en ajoutant l'ID de clé requis</p> <p>Disponible dans ONTAP 9.5 ou version ultérieure</p>	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
Désactiver l'authentification symétrique	<pre>cluster time-service ntp server modify -server server_name -is-authentication -enabled false</pre>
Configurez une clé NTP partagée	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>Les clés partagées sont désignées par un ID. L'ID, son type et la valeur doivent être identiques sur le nœud et le serveur NTP</p> </div>
Affiche les informations relatives aux serveurs NTP associés au cluster	<pre>cluster time-service ntp server show</pre>
Modifier la configuration d'un serveur NTP externe associé au cluster	<pre>cluster time-service ntp server modify</pre>
Dissociez un serveur NTP du cluster	<pre>cluster time-service ntp server delete</pre>
Réinitialise la configuration en désactivant l'association de tous les serveurs NTP externes au cluster	<pre>cluster time-service ntp server reset</pre> <div>  <p>Cette commande nécessite le niveau de privilège avancé.</p> </div>

Les commandes suivantes vous permettent de gérer manuellement l'heure du cluster :

Les fonctions que vous recherchez...	Utilisez cette commande...
Définissez ou modifiez le fuseau horaire, la date et l'heure	<code>cluster date modify</code>
Affiche les paramètres de fuseau horaire, de date et d'heure du cluster	<code>cluster date show</code>

Informations associées

["Commandes de ONTAP 9"](#)

Gérer la bannière et la MOTD

Gérer la bannière et la vue d'ensemble de la MOTD

ONTAP vous permet de configurer une bannière de connexion ou un message du jour (MOTD) pour communiquer des informations administratives aux utilisateurs de l'interface de ligne de commande du cluster ou de la machine virtuelle de stockage (SVM).

Une bannière s'affiche dans une session de console (pour l'accès au cluster uniquement) ou dans une session SSH (pour l'accès au cluster ou au SVM) avant qu'un utilisateur soit invité à authentification par exemple. Par exemple, vous pouvez utiliser la bannière pour afficher un message d'avertissement comme les éléments suivants à une personne qui tente de se connecter au système :

```
$ ssh admin@cluster1-01
```

```
This system is for authorized users only. Your IP Address has been logged.
```

```
Password:
```

Une MOTD s'affiche dans une session de console (pour l'accès au cluster uniquement) ou une session SSH (pour l'accès au cluster ou au SVM) après l'authentification d'un utilisateur, mais avant l'affichage de l'invite `clustershell`. Par exemple, vous pouvez utiliser le MOTD pour afficher un message d'accueil ou d'information comme les éléments suivants que seuls les utilisateurs authentifiés verront :

```
$ ssh admin@cluster1-01
```

```
Password:
```

```
Greetings. This system is running ONTAP 9.0.
```

```
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015  
from 10.72.137.28.
```

Vous pouvez créer ou modifier le contenu de la bannière ou de la MOTD en utilisant le `security login banner modify` ou `security login motd modify` les commandes, respectivement, de l'une des

manières suivantes :

- Vous pouvez utiliser la CLI de manière interactive ou non interactive pour spécifier le texte à utiliser pour la bannière ou la MOTD.

Le mode interactif, lancé lorsque la commande est utilisée sans l' `-message` ou `-uri` paramètre, vous permet d'utiliser des nouvelles lignes (également appelées fin de lignes) dans le message.

Le mode non interactif, qui utilise le `-message` paramètre pour spécifier la chaîne de message, ne prend pas en charge les nouvelles lignes.

- Vous pouvez télécharger du contenu à partir d'un emplacement FTP ou HTTP à utiliser pour la bannière ou le MOTD.
- Vous pouvez configurer le MOTD pour qu'il affiche du contenu dynamique.

Voici des exemples de ce que vous pouvez configurer le MOTD pour qu'il s'affiche de façon dynamique :

- Nom du cluster, nom de nœud ou nom SVM
- Date et heure du cluster
- Nom de l'utilisateur connecté
- Dernière connexion de l'utilisateur sur n'importe quel nœud du cluster
- Nom ou adresse IP du périphérique de connexion
- Nom du système d'exploitation
- Version du logiciel
- Chaîne de version effective du cluster

Le `security login motd modify` La page man décrit les séquences d'échappement que vous pouvez utiliser pour permettre au MOTD d'afficher du contenu généré dynamiquement.

La bannière ne prend pas en charge le contenu dynamique.

Vous pouvez gérer la bannière et la MOTD au niveau du cluster ou du SVM :

- Les faits suivants s'appliquent à la bannière :
 - La bannière configurée pour le cluster est également utilisée pour tous les SVM qui ne possèdent pas de message de bannière défini.
 - Une bannière SVM peut être configurée pour chaque SVM.

Si une bannière au niveau du cluster a été configurée, elle est remplacée par la bannière SVM-level pour la SVM donnée.

- Les faits suivants s'appliquent à la MOTD :
 - Par défaut, la MOTD configurée pour le cluster est également activée pour tous les SVM.
 - En outre, un MOTD au niveau d'un SVM peut être configuré pour chaque SVM.

Dans ce cas, les utilisateurs qui se connectent à la SVM verront deux MOTDS, l'un défini au niveau du cluster et l'autre au niveau du SVM.

- La fonction MOTD au niveau du cluster peut être activée ou désactivée par SVM par l'administrateur du cluster.

Si l'administrateur du cluster désactive la MOTD au niveau du cluster pour un SVM, un utilisateur qui se connecte à la SVM ne voit pas la MOTD au niveau du cluster.

Créez une bannière

Vous pouvez créer une bannière pour afficher un message à quelqu'un qui tente d'accéder au cluster ou à un SVM. La bannière s'affiche dans une session de console (pour l'accès au cluster uniquement) ou dans une session SSH (pour l'accès au cluster ou SVM) avant qu'un utilisateur soit invité à s'authentifier.

Étapes

1. Utilisez le `security login banner modify` Commande pour créer une bannière pour le cluster ou le SVM :

Les fonctions que vous recherchez...	Alors...
Spécifiez un message à une seule ligne	Utilisez le <code>-message «text" paramètre pour spécifier le texte.</code>
Inclure les nouvelles lignes (également appelées fin de lignes) dans le message	Utiliser la commande sans <code>-message</code> ou <code>-uri</code> paramètre pour lancer le mode interactif d'édition de la bannière.
Téléchargez le contenu depuis un emplacement pour l'utiliser pour la bannière	Utilisez le <code>-uri</code> Paramètre pour spécifier l'emplacement FTP ou HTTP du contenu.

La taille maximale d'une bannière est de 2,048 octets, y compris les newlines.

Bannière créée à l'aide du `-uri` paramètre statique. Elle n'est pas mise à jour automatiquement pour refléter les modifications ultérieures du contenu source.

La bannière créée pour le cluster est également affichée pour tous les SVM qui ne disposent pas de bannière existante. Toute bannière créée pour un SVM remplace la bannière de niveau cluster pour ce SVM. Spécification du `-message` paramètre avec un tiret dans les guillemets doubles ("`-`") Pour la SVM réinitialise le SVM pour l'utilisation de la bannière cluster.

2. Vérifiez que la bannière a été créée en l'affichant avec le `security login banner show` commande.

Spécification du `-message` paramètre avec une chaîne vide ("`"`") affiche des bannières qui n'ont pas de contenu.

Spécification du `-message` paramètre avec "`-`" Affiche tous les SVM (admin ou data) ne disposant pas de bannière configurée.

Exemples de bannières de création

L'exemple suivant utilise le mode non interactif pour créer une bannière pour le cluster « cluster1 » :

```
cluster1::> security login banner modify -message "Authorized users only!"  
  
cluster1::>
```

L'exemple suivant utilise le mode interactif pour créer une bannière pour le SVM "svm1":

```
cluster1::> security login banner modify -vserver svm1  
  
Enter the message of the day for Vserver "svm1".  
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to  
abort.  
0          1          2          3          4          5          6          7  
8  
12345678901234567890123456789012345678901234567890123456789012345678901234  
567890  
The svm1 SVM is reserved for authorized users only!  
  
cluster1::>
```

L'exemple suivant montre les bannières créées :

```
cluster1::> security login banner show  
Vserver: cluster1  
Message  
-----  
---  
Authorized users only!  
  
Vserver: svm1  
Message  
-----  
---  
The svm1 SVM is reserved for authorized users only!  
  
2 entries were displayed.  
  
cluster1::>
```

Informations associées

[Gestion de la bannière](#)

Gestion de la bannière

Vous pouvez gérer la bannière au niveau du cluster ou de la SVM. La bannière configurée pour le cluster est également utilisée pour tous les SVM qui ne possèdent pas de message de bannière défini. Une bannière créée par la suite pour un SVM remplace la bannière de cluster pour ce SVM.

Choix

- Gérez la bannière au niveau du cluster :

Les fonctions que vous recherchez...	Alors...
Créez une bannière à afficher pour toutes les sessions de connexion de l'interface de ligne de commande	Définissez une bannière au niveau du cluster : <code>*security login banner modify -vserver cluster_name { [-message "text"]</code>
<code>[-uri ftp_or_http_addr] }</code>	Supprimer la bannière pour toutes les connexions (cluster et SVM)
Définissez la bannière sur une chaîne vide ("") : <code>security login banner modify -vserver * -message ""</code>	Remplacer une bannière créée par un administrateur du SVM
Modifier le message de la bannière SVM : <code>*security login banner modify -vserver svm_name { [-message "text"]</code>	<code>[-uri ftp_or_http_addr] }</code>

- Gestion de la bannière au niveau du SVM :

Spécification `-vserver svm_name` N'est pas requis dans le contexte SVM.

Les fonctions que vous recherchez...	Alors...
Remplacer la bannière fournie par l'administrateur du cluster avec une autre bannière pour le SVM	Créer une bannière pour le SVM : <code>*security login banner modify -vserver svm_name { [-message "text"]</code>
<code>[-uri ftp_or_http_addr] }</code>	Supprime la bannière fournie par l'administrateur du cluster afin qu'aucune bannière ne s'affiche pour la SVM

Les fonctions que vous recherchez...	Alors...
Définir la bannière SVM sur une chaîne vide pour le SVM :	Utilisez la bannière cluster lorsque le SVM utilise actuellement une bannière de niveau SVM
security login banner modify -vserver svm_name -message ""	

Créer un MOTD

Vous pouvez créer un message du jour (MOTD) pour communiquer des informations aux utilisateurs authentifiés de CLI. Le mot MOTD s'affiche dans une session de console (pour l'accès au cluster uniquement) ou dans une session SSH (pour l'accès au cluster ou SVM) après l'authentification d'un utilisateur, mais avant l'affichage de l'invite clustershell.

Étapes

1. Utilisez le `security login motd modify` Commande pour créer un MOTD pour le cluster ou le SVM :

Les fonctions que vous recherchez...	Alors...
Spécifiez un message à une seule ligne	Utilisez le <code>-message «text" paramètre pour spécifier le texte.</code>
Inclure les nouvelles lignes (également appelée fin de lignes)	Utiliser la commande sans <code>-message</code> ou <code>-uri</code> Paramètre pour lancer le mode interactif pour modifier le MOTD.
Téléchargez le contenu à partir d'un emplacement pour le MOTD	Utilisez le <code>-uri</code> Paramètre pour spécifier l'emplacement FTP ou HTTP du contenu.

La taille maximale d'un MOTD est de 2,048 octets, y compris les nouvelles lignes.

Le `security login motd modify` La page man décrit les séquences d'échappement que vous pouvez utiliser pour permettre au MOTD d'afficher du contenu généré dynamiquement.

Un MOTD créé à l'aide du `-uri` paramètre statique. Elle n'est pas mise à jour automatiquement pour refléter les modifications ultérieures du contenu source.

Un MOTD créé pour le cluster est également affiché pour toutes les connexions de SVM par défaut, ainsi qu'un MOTD de niveau SVM que vous pouvez créer séparément pour un SVM donné. Réglage du `-is -cluster-message-enabled` paramètre à `false` Pour un SVM, il n'est pas possible de visualiser la MOTD niveau du cluster pour ce SVM.

2. Vérifiez que le MOTD a été créé en l'affichant avec le `security login motd show` commande.

Spécification du `-message` paramètre avec une chaîne vide ("") Affiche les MOTDS qui ne sont pas configurés ou n'ont pas de contenu.

Voir la "[code de connexion de sécurité motd modifier](#)" Page de manuel de commande pour une liste de paramètres à utiliser pour permettre au MOTD d'afficher le contenu généré dynamiquement. Assurez-vous de consulter la page de manuel spécifique à votre version de ONTAP.

Exemples de création de MOTDS

L'exemple suivant utilise le mode non interactif pour créer un MOTD pour le cluster « cluster1 » :

```
cluster1::> security login motd modify -message "Greetings!"
```

L'exemple suivant utilise le mode interactif pour créer un MOTD pour le SVM "svm1" qui utilise les séquences d'échappement pour afficher le contenu généré dynamiquement :

```
cluster1::> security login motd modify -vserver svm1
```

Enter the message of the day for Vserver "svm1".

Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to abort.

0 1 2 3 4 5 6 7
8

123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890
567890

Welcome to the \n SVM. Your user ID is '\N'. Your last successful login was \L.

L'exemple suivant affiche les MOTDS qui ont été créés :

```
cluster1::> security login motd show
```

Vserver: cluster1

Is the Cluster MOTD Displayed?: true

Message

Greetings!

Vserver: svm1

Is the Cluster MOTD Displayed?: true

Message

Welcome to the \n SVM. Your user ID is '\N'. Your last successful login was \L.

2 entries were displayed.

Gérer la DPE

Vous pouvez gérer le message du jour (MOTD) au niveau du cluster ou de la SVM. Par défaut, la MOTD configurée pour le cluster est également activée pour tous les SVM. En outre, un MOTD au niveau d'un SVM peut être configuré pour chaque SVM. La fonction MOTD au niveau du cluster peut être activée ou désactivée pour chaque SVM par l'administrateur du cluster.

Pour obtenir la liste des séquences d'échappement pouvant être utilisées pour générer dynamiquement du contenu pour le MOTD, reportez-vous au ["référence de commande"](#).

Choix

- Gérer la DPE au niveau du cluster :

Les fonctions que vous recherchez...	Alors...
Créez un MOTD pour toutes les connexions lorsqu'il n'existe pas de MOTD	Définir un mot de travail au niveau du cluster : <code>`*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"]</code>
<code>[-uri <i>ftp_or_http_addr</i>] }*</code>	Modifiez le MOTD pour toutes les connexions lorsqu'aucun MOTD au niveau des SVM n'est configuré
Modifier la DPE au niveau du cluster : <code>`*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"] }</code>	<code>[-uri <i>ftp_or_http_addr</i>] }*</code>
Supprimer le MOTD pour toutes les connexions lorsqu'aucun MOTD au niveau des SVM n'est configuré	Définissez le mot-symbole MOTD au niveau du cluster sur une chaîne vide ("") : <code>security login motd modify -vserver <i>cluster_name</i> -message ""</code>
Demandez à chaque SVM d'afficher la MOTD au niveau du cluster au lieu d'utiliser la MOTD au niveau du SVM	Définissez un MOTD au niveau du cluster, puis définissez tous les MOTD au niveau du SVM sur une chaîne vide lorsque le MOTD au niveau du cluster est activé : a. <code>`*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"]</code>
<code>[-uri <i>ftp_or_http_addr</i>] }*</code> <code>.. security login motd modify { -vserver !"cluster_name" } -message "" -is -cluster-message-enabled true</code>	Avoir un MOTD affiché uniquement pour les SVM sélectionnés et n'utiliser aucun MOTD au niveau du cluster

Les fonctions que vous recherchez...	Alors...
<p>Définissez la MOTD au niveau du cluster sur une chaîne vide, puis définissez les MOTDS au niveau du SVM pour les SVM sélectionnés :</p> <p>a. security login motd modify -vserver <i>cluster_name</i> -message ""</p> <p>b. *security login motd modify -vserver <i>svm_name</i> { [-message "<i>text</i>"]</p>	<p>[-uri <i>ftp_or_http_addr</i>] }* + Vous pouvez répéter cette étape pour chaque SVM si nécessaire.</p>
<p>Utilisez la même MOTD au niveau du SVM pour toutes les SVM (données et admin</p>	<p>Définir le cluster et tous les SVM afin d'utiliser le même MOTD :</p> <p>*security login motd modify -vserver * { [-message "<i>text</i>"]</p>
<p>[-uri <i>ftp_or_http_addr</i>] }*</p> <p>[NOTE] ==== Si vous utilisez le mode interactif, la CLI vous invite à entrer la MOTD individuellement pour le cluster et chaque SVM. Vous pouvez coller le même MOTD dans chaque instance lorsque vous êtes invité à le faire. =====</p>	<p>Disposer d'une MOTD au niveau du cluster disponible en option pour tous les SVM, mais ne pas vouloir que la MOTD soit affichée pour les connexions de cluster</p>
<p>Définissez un MOTD au niveau du cluster, mais désactivez son affichage pour le cluster :</p> <p>*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"]</p>	<p>[-uri <i>ftp_or_http_addr</i>] } -is-cluster-message-enabled false*</p>
<p>Supprimer tous les MOTD au niveau du cluster et des SVM lorsque seuls certains SVM ont des MOTD au niveau du cluster et des SVM</p>	<p>Définissez le cluster et tous les SVM de manière à utiliser une chaîne vide pour le MOTD :</p> <p>security login motd modify -vserver * -message ""</p>
<p>Modifiez la MOTD uniquement pour les SVM qui ont une chaîne non vide, lorsque d'autres SVM utilisent une chaîne vide, et lorsqu'un autre MOTD est utilisé au niveau du cluster</p>	<p>Utilisez les requêtes étendues pour modifier la MOTD de façon sélective :</p> <p>*security login motd modify { -vserver !"cluster_name" -message !"" } { [-message "<i>text</i>"]</p>

Les fonctions que vous recherchez...	Alors...
<code>[-uri ftp_or_http_addr] }</code>	Afficher tous les MOTD contenant du texte spécifique (par exemple, « janvier » suivi de « 2015 ») n'importe où dans un message unique ou multiligne, même si le texte est divisé entre différentes lignes
Utilisez une requête pour afficher les MOTDS : security login motd show -message *"January"*"2015"*	Créer de manière interactive un MOTD qui inclut plusieurs nouvelles lignes consécutives (également appelées fin de lignes, ou EOLs)

- Gestion de la MOTD au niveau de la SVM :

Spécification `-vserver svm_name` N'est pas requis dans le contexte SVM.

Les fonctions que vous recherchez...	Alors...
Utilisez une DPE différente au niveau du SVM lorsque le SVM possède déjà une DPE au niveau du SVM	Modifier la MOTD au niveau du SVM : <code>*security login motd modify -vserver svm_name { [-message "text"]</code>
<code>[-uri ftp_or_http_addr] }</code>	Utiliser uniquement la MOTD de niveau cluster pour le SVM, lorsque le SVM possède déjà une MOTD de niveau SVM
Définir la MOTD au niveau du SVM sur une chaîne vide, puis faire activer la MOTD au niveau du cluster pour la SVM : a. security login motd modify -vserver svm_name -message "" b. (Pour l'administrateur du cluster) security login motd modify -vserver svm_name -is-cluster-message-enabled true	Pas que le SVM n'affiche de DPE, lorsque les DPE au niveau du cluster et du SVM sont actuellement affichées pour la SVM

Gestion des tâches et planification

Les travaux sont placés dans une file d'attente de travaux et exécutés en arrière-plan lorsque des ressources sont disponibles. Si une tâche consomme trop de ressources de cluster, vous pouvez l'arrêter ou le mettre en pause jusqu'à ce que la demande sur le cluster soit moins élevée. Vous pouvez également surveiller et redémarrer les travaux.

Catégories de travail

Il existe trois catégories de travaux que vous pouvez gérer : affilié au serveur, affilié au cluster et privé.

Un travail peut se trouver dans l'une des catégories suivantes :

- **Travaux affiliés au serveur**

Ces travaux sont mis en file d'attente par l'infrastructure de gestion vers un nœud spécifique à exécuter.

- **Emplois affiliés à un groupe**

Ces travaux sont mis en file d'attente par l'infrastructure de gestion vers n'importe quel nœud du cluster à exécuter.

- **Emplois privés**

Ces jobs sont spécifiques à un nœud et n'utilisent pas la base de données répliquée (RDB) ou tout autre mécanisme du cluster. Les commandes qui gèrent les travaux privés nécessitent un niveau de privilège avancé ou supérieur.

Commandes de gestion des travaux

Lorsque vous entrez une commande qui appelle un travail, généralement, la commande vous informe que le travail a été mis en file d'attente, puis revient à l'invite de commande CLI. Toutefois, certaines commandes indiquent plutôt la progression du travail et ne reviennent pas à l'invite de commande CLI tant que le travail n'a pas été terminé. Dans ce cas, vous pouvez appuyer sur Ctrl-C pour déplacer le travail en arrière-plan.

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche des informations sur tous les travaux	<code>job show</code>
Affiche des informations sur les travaux par nœud	<code>job show bynode</code>
Affiche des informations sur les travaux affiliés à un cluster	<code>job show-cluster</code>
Affiche des informations sur les tâches terminées	<code>job show-completed</code>
Affiche des informations sur l'historique des travaux	<code>job history show</code> Jusqu'à 25,000 enregistrements de tâche sont stockés pour chaque nœud du cluster. Par conséquent, toute tentative d'affichage de l'historique complet du travail peut prendre beaucoup de temps. Pour éviter les temps d'attente potentiellement longs, il est conseillé d'afficher les tâches par nœud, machine virtuelle de stockage ou ID d'enregistrement.
Affiche la liste des travaux privés	<code>job private show</code> (niveau de privilège avancé)
Affiche des informations sur les travaux privés terminés	<code>job private show-completed</code> (niveau de privilège avancé)

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche des informations sur l'état d'initialisation des gestionnaires de travaux	<code>job initstate show</code> (niveau de privilège avancé)
Surveiller la progression d'une tâche	<code>job watch-progress</code>
Surveiller la progression d'un travail privé	<code>job private watch-progress</code> (niveau de privilège avancé)
Interrompre un travail	<code>job pause</code>
Interrompre un travail privé	<code>job private pause</code> (niveau de privilège avancé)
Reprendre un travail en pause	<code>job resume</code>
Reprendre un travail privé en pause	<code>job private resume</code> (niveau de privilège avancé)
Arrêter un travail	<code>job stop</code>
Arrêter un travail privé	<code>job private stop</code> (niveau de privilège avancé)
Supprimer un travail	<code>job delete</code>
Supprimer un travail privé	<code>job private delete</code> (niveau de privilège avancé)
Dissociez un travail affilié à un cluster avec un nœud non disponible qui le possède, de sorte qu'un autre nœud puisse prendre possession de ce travail	<code>job unclaim</code> (niveau de privilège avancé)



Vous pouvez utiliser le `event log show` commande permettant de déterminer le résultat d'un travail terminé.

Informations associées

["Commandes de ONTAP 9"](#)

Commandes de gestion des planifications de travaux

De nombreuses tâches, par exemple, les copies Snapshot de volume, peuvent être configurées pour s'exécuter sur des planifications spécifiées. Les planifications qui s'exécutent à des heures spécifiques sont appelées *cron* planifications (similaires à UNIX) *cron* planifications). Les horaires exécutés à intervalles sont appelés *interval* planifications. Vous utilisez le `job schedule` commandes permettant de gérer les planifications de tâches.

Les planifications de tâches ne s'adaptent pas aux modifications manuelles apportées à la date et à l'heure du cluster. Ces travaux sont planifiés pour s'exécuter en fonction de l'heure actuelle du cluster au moment de la

création du travail ou de l'exécution du travail le plus récent. Par conséquent, si vous modifiez manuellement la date ou l'heure du cluster, vous devez utiliser le `job show` et `job history show` commandes permettant de vérifier que tous les travaux planifiés sont mis en file d'attente et terminés en fonction de vos besoins.

Si le cluster fait partie d'une configuration MetroCluster, la planification de tâches sur les deux clusters doit être identique. Par conséquent, si vous créez, modifiez ou supprimez un Job planning, vous devez effectuer la même opération sur le cluster distant.

Les fonctions que vous recherchez...	Utilisez cette commande...
Affiche des informations sur tous les horaires	<code>job schedule show</code>
Affiche la liste des travaux par planning	<code>job schedule show-jobs</code>
Affiche des informations sur les planifications cron	<code>job schedule cron show</code>
Affiche des informations sur les plannings d'intervalles	<code>job schedule interval show</code>
Créez une planification cron	<code>job schedule cron create</code> À partir de ONTAP 9.10.1, vous pouvez inclure le SVM pour votre planification de tâches.
Créer un planning d'intervalles	<code>job schedule interval create</code> Vous devez spécifier au moins un des paramètres suivants : <code>-days</code> , <code>-hours</code> , <code>-minutes</code> , ou <code>-seconds</code> .
Modifier une planification cron	<code>job schedule cron modify</code>
Modifier un planning d'intervalles	<code>job schedule interval modify</code>
Supprimer un planning	<code>job schedule delete</code>
Supprimez une planification cron	<code>job schedule cron delete</code>
Supprimer un planning d'intervalles	<code>job schedule interval delete</code>

Informations associées

["Commandes de ONTAP 9"](#)

Sauvegarde et restauration des configurations de cluster (administrateurs de cluster uniquement)

Quels sont les fichiers de sauvegarde de configuration

Les fichiers de sauvegarde de configuration sont des fichiers d'archive (.7z) qui contiennent des informations sur toutes les options configurables qui sont nécessaires pour que le cluster et les nœuds qu'il contient fonctionnent correctement.

Ces fichiers stockent la configuration locale de chaque nœud, plus la configuration répliquée au niveau du cluster. Vous utilisez les fichiers de sauvegarde de configuration pour sauvegarder et restaurer la configuration de votre cluster.

Il existe deux types de fichiers de sauvegarde de configuration :

- **Fichier de sauvegarde de configuration de nœud**

Chaque nœud sain du cluster inclut un fichier de sauvegarde de configuration de nœud, qui contient toutes les informations de configuration et les métadonnées nécessaires au fonctionnement du nœud sur le cluster.

- **Fichier de sauvegarde de configuration de cluster**

Ces fichiers incluent une archive de tous les fichiers de sauvegarde de configuration des nœuds du cluster, ainsi que des informations de configuration du cluster répliqué (base de données répliquée ou fichier RDB). Les fichiers de sauvegarde de configuration de cluster vous permettent de restaurer la configuration de tout le cluster ou de tout nœud du cluster. Les planifications de sauvegarde de configuration de cluster créent ces fichiers automatiquement et les stockent sur plusieurs nœuds du cluster.



Les fichiers de sauvegarde de configuration contiennent uniquement des informations sur la configuration. Elles n'incluent aucune donnée utilisateur. Pour plus d'informations sur la restauration des données utilisateur, reportez-vous à la section "[La protection des données](#)".

Sauvegarde automatique des configurations de nœuds et de clusters

Trois planifications distinctes créent automatiquement les fichiers de sauvegarde des configurations de cluster et de nœud et les répliquent entre les nœuds du cluster.

Les fichiers de sauvegarde de configuration sont automatiquement créés en fonction des planifications suivantes :



- Toutes les 8 heures
- Tous les jours
- Hebdomadaire

À chaque fois, un fichier de sauvegarde de configuration de nœud est créé sur chaque nœud en bon état du cluster. Tous ces fichiers de sauvegarde de configuration de nœud sont ensuite rassemblés dans un fichier de sauvegarde de configuration de cluster unique avec la configuration de cluster répliquée et enregistrés sur un ou plusieurs nœuds du cluster.

Commandes de gestion des planifications de sauvegarde de configuration

Vous pouvez utiliser le `system configuration backup settings` commandes permettant de gérer les planifications de sauvegarde de configuration.

Ces commandes sont disponibles au niveau de privilège avancé.


Les fonctions que vous recherchez...	Utilisez cette commande...
<p>Modifiez les paramètres d'un planning de sauvegarde de configuration :</p> <ul style="list-style-type: none">• Spécifiez une URL distante (HTTP, HTTPS, FTP, FTPS ou TFTP) où les fichiers de sauvegarde de configuration seront chargés en plus des emplacements par défaut dans le cluster• Spécifiez un nom d'utilisateur à utiliser pour se connecter à l'URL distante• Définissez le nombre de sauvegardes à conserver pour chaque planning de sauvegarde de configuration	<p><code>system configuration backup settings modify</code></p> <p>Lorsque vous utilisez HTTPS dans l'URL distante, utilisez le <code>-validate-certification</code> option permettant d'activer ou de désactiver la validation de certificats numériques. La validation du certificat est désactivée par défaut.</p> <div><p>Le serveur Web sur lequel vous téléchargez le fichier de sauvegarde de configuration doit avoir ACTIVÉ les opérations HTTP et LES opérations DE POST activées pour HTTPS. Pour plus d'informations, consultez la documentation de votre serveur Web.</p></div>
<p>Définissez le mot de passe à utiliser pour vous connecter à l'URL distante</p>	<p><code>system configuration backup settings set-password</code></p>
<p>Afficher les paramètres du programme de sauvegarde de la configuration</p>	<p><code>system configuration backup settings show</code></p> <div><p>Vous définissez le <code>-instance</code> paramètre pour afficher le nom d'utilisateur et le nombre de sauvegardes à conserver pour chaque planning.</p></div>


Commandes de gestion des fichiers de sauvegarde de configuration

Vous utilisez le `system configuration backup` commandes permettant de gérer les fichiers de sauvegarde de la configuration du cluster et des nœuds.

Ces commandes sont disponibles au niveau de privilège avancé.

Les fonctions que vous recherchez...	Utilisez cette commande...
<p>Créer un nouveau fichier de sauvegarde de configuration de nœud ou de cluster</p>	<p><code>system configuration backup create</code></p>

Les fonctions que vous recherchez...	Utilisez cette commande...
Copiez un fichier de sauvegarde de configuration d'un nœud vers un autre nœud du cluster	<code>system configuration backup copy</code>
Charger un fichier de sauvegarde de configuration à partir d'un nœud du cluster vers une URL distante (FTP, HTTP, HTTPS, TFTP ou FTPS)	<p><code>system configuration backup upload</code></p> <p>Lorsque vous utilisez HTTPS dans l'URL distante, utilisez le <code>-validate-certification</code> option permettant d'activer ou de désactiver la validation de certificats numériques. La validation du certificat est désactivée par défaut.</p> <div>  <p>Le serveur Web sur lequel vous téléchargez le fichier de sauvegarde de configuration doit avoir ACTIVÉ les opérations HTTP et LES opérations DE POST activées pour HTTPS. Certains serveurs Web peuvent nécessiter l'installation d'un module supplémentaire. Pour plus d'informations, consultez la documentation de votre serveur Web. Les formats d'URL pris en charge varient en fonction de la version d'ONTAP. Consultez l'aide en ligne de commandes de votre version ONTAP.</p> </div>
Téléchargez un fichier de sauvegarde de configuration à partir d'une URL distante vers un nœud du cluster et, si spécifié, validez le certificat numérique	<p><code>system configuration backup download</code></p> <p>Lorsque vous utilisez HTTPS dans l'URL distante, utilisez le <code>-validate-certification</code> option permettant d'activer ou de désactiver la validation de certificats numériques. La validation du certificat est désactivée par défaut.</p>
Renommez un fichier de sauvegarde de configuration sur un nœud du cluster	<code>system configuration backup rename</code>
Afficher les fichiers de sauvegarde de configuration de nœud et de cluster pour un ou plusieurs nœuds du cluster	<code>system configuration backup show</code>

Les fonctions que vous recherchez...	Utilisez cette commande...
Supprime un fichier de sauvegarde de configuration sur un nœud	<pre>system configuration backup delete</pre> <div>  <p>Cette commande supprime le fichier de sauvegarde de configuration sur le nœud spécifié uniquement. Si le fichier de sauvegarde de configuration existe également sur d'autres nœuds du cluster, il reste sur ces nœuds.</p> </div>

Recherchez un fichier de sauvegarde de configuration à utiliser pour restaurer un nœud

Vous utilisez un fichier de sauvegarde de configuration situé sur une URL distante ou sur un nœud du cluster pour restaurer une configuration de nœud.

Description de la tâche

Vous pouvez utiliser un fichier de sauvegarde de configuration de cluster ou de nœud pour restaurer une configuration de nœud.

Étape

1. Rendez le fichier de sauvegarde de configuration disponible pour le nœud pour lequel vous devez restaurer la configuration.

Si le fichier de sauvegarde de configuration se trouve...	Alors...
Sur une URL distante	Utilisez le <code>system configuration backup download</code> commande au niveau de privilège avancé pour le télécharger sur le nœud restauré.
Sur un nœud du cluster	<ol style="list-style-type: none"> a. Utilisez le <code>system configuration backup show</code> commande au niveau de privilège avancé pour afficher la liste des fichiers de sauvegarde de configuration disponibles dans le cluster contenant la configuration du nœud de restauration. b. Si le fichier de sauvegarde de configuration que vous identifiez n'existe pas sur le nœud de récupération, utilisez le <code>system configuration backup copy</code> commande de copie sur le nœud restauré.

Si vous avez précédemment recréé-crée le cluster, vous devez choisir un fichier de sauvegarde de configuration qui a été créé après la création du cluster. Si vous devez utiliser un fichier de sauvegarde de configuration qui a été créé avant le regroupement de loisirs, après avoir restauré le nœud, vous devez recréer le cluster.

Restaurez la configuration du nœud à l'aide d'un fichier de sauvegarde de configuration

Vous restaurez la configuration du nœud à l'aide du fichier de sauvegarde de configuration que vous avez identifié et mis à la disposition du nœud de récupération.

Description de la tâche

Vous ne devez effectuer cette tâche que pour effectuer une restauration suite à un incident entraînant la perte des fichiers de configuration locale du nœud.

Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Si le nœud fonctionne correctement, utilisez le au niveau de privilège avancé d'un autre nœud `cluster modify` commande avec `-node` et `-eligibility` paramètres pour le signaler non éligible et l'isoler du cluster.

Si le nœud n'est pas sain, ignorez cette étape.

Dans cet exemple, le nœud 2 est modifié pour ne pas participer au cluster afin que sa configuration puisse être restaurée :

```
cluster1::*> cluster modify -node node2 -eligibility false
```

3. Utilisez le `system configuration recovery node restore` commande au niveau de privilège avancé pour restaurer la configuration du nœud à partir d'un fichier de sauvegarde de configuration.

Si le nœud a perdu son identité, y compris son nom, vous devez utiliser le `-nodename-in-backup` paramètre pour spécifier le nom du nœud dans le fichier de sauvegarde de configuration.

Cet exemple restaure la configuration du nœud à l'aide de l'un des fichiers de sauvegarde de configuration stockés sur le nœud :

```
cluster1::*> system configuration recovery node restore -backup  
cluster1.8hour.2011-02-22.18_15_00.7z
```

```
Warning: This command overwrites local configuration files with  
files contained in the specified backup file. Use this  
command only to recover from a disaster that resulted  
in the loss of the local configuration files.  
The node will reboot after restoring the local configuration.  
Do you want to continue? {y|n}: y
```

La configuration est restaurée et le nœud redémarre.

4. Si vous avez indiqué que le nœud n'est pas éligible, utilisez le `system configuration recovery`

`cluster sync` commande pour marquer le nœud comme éligible et le synchroniser avec le cluster.

5. Si vous travaillez dans un environnement SAN, utilisez le `system node reboot` Commande permettant de redémarrer le nœud et de rétablir le quorum SAN.

Une fois que vous avez terminé

Si vous avez précédemment recréés le cluster, et si vous restaurez la configuration du nœud à l'aide d'un fichier de sauvegarde de configuration créé avant la recréation du cluster, vous devez recréer le cluster.

Recherchez une configuration à utiliser pour la récupération d'un cluster

Vous utilisez la configuration à partir d'un nœud du cluster ou d'un fichier de sauvegarde de configuration de cluster pour restaurer un cluster.

Étapes

1. Choisissez un type de configuration pour restaurer le cluster.

- Un nœud dans le cluster

Si le cluster se compose de plusieurs nœuds et que l'un des deux nœuds dispose d'une configuration de cluster depuis laquelle le cluster était dans la configuration souhaitée, vous pouvez restaurer le cluster à l'aide de la configuration stockée sur ce nœud.

Dans la plupart des cas, le nœud contenant l'anneau de réplication avec l'ID de transaction le plus récent est le nœud le plus adapté à la restauration de la configuration du cluster. Le `cluster ring show` la commande au niveau de privilège avancé vous permet d'afficher la liste des anneaux répliqués disponibles sur chaque nœud du cluster.

- Fichier de sauvegarde de la configuration du cluster

Si vous ne pouvez pas identifier un nœud avec la configuration de cluster appropriée ou si le cluster est composé d'un seul nœud, vous pouvez utiliser un fichier de sauvegarde de configuration de cluster pour restaurer le cluster.

Si vous récupérez le cluster à partir d'un fichier de sauvegarde de configuration, toute modification de configuration effectuée depuis la sauvegarde sera perdue. Après la restauration, vous devez résoudre tout écart entre le fichier de sauvegarde de configuration et la configuration actuelle. Consultez l'article de la base de connaissances "[Guide de résolution des sauvegardes de configuration ONTAP](#)" pour des conseils de dépannage.

2. Si vous choisissez d'utiliser un fichier de sauvegarde de configuration de cluster, mettez le fichier à disposition du nœud que vous prévoyez d'utiliser pour restaurer le cluster.

Si le fichier de sauvegarde de configuration se trouve...	Alors...
Sur une URL distante	Utilisez le <code>system configuration backup download</code> commande au niveau de privilège avancé pour le télécharger sur le nœud restauré.

Si le fichier de sauvegarde de configuration se trouve...	Alors...
Sur un nœud du cluster	<p>a. Utilisez le <code>system configuration backup show</code> commande au niveau de privilège avancé pour trouver un fichier de sauvegarde de la configuration du cluster qui a été créé lorsque le cluster était dans la configuration souhaitée.</p> <p>b. Si le fichier de sauvegarde de configuration de cluster n'est pas situé sur le nœud que vous souhaitez utiliser pour restaurer le cluster, utilisez le <code>system configuration backup copy</code> commande de copie sur le nœud restauré.</p>

Restaurer une configuration de cluster à partir d'une configuration existante

Pour restaurer une configuration de cluster à partir d'une configuration existante après une défaillance de cluster, vous devez recréer le cluster à l'aide de la configuration de cluster que vous avez choisie et mise à disposition du nœud de récupération, puis vous devez relier chaque nœud supplémentaire au nouveau cluster.

Description de la tâche

Vous ne devez effectuer cette tâche que pour effectuer une restauration après un incident ayant entraîné la perte de la configuration du cluster.



Si vous créez à nouveau le cluster à partir d'un fichier de sauvegarde de configuration, vous devez contacter le support technique pour résoudre tout écart entre le fichier de sauvegarde de configuration et la configuration présente dans le cluster.

Si vous récupérez le cluster à partir d'un fichier de sauvegarde de configuration, toute modification de configuration effectuée depuis la sauvegarde sera perdue. Après la restauration, vous devez résoudre tout écart entre le fichier de sauvegarde de configuration et la configuration actuelle. Consultez l'article de la base de connaissances ["Guide de résolution des sauvegardes de configuration ONTAP pour des conseils de dépannage"](#).

Étapes

1. Désactiver le basculement du stockage pour chaque paire haute disponibilité :

```
storage failover modify -node node_name -enabled false
```

Il n'est nécessaire de désactiver qu'une seule fois le basculement du stockage pour chaque paire haute disponibilité. Lorsque vous désactivez le basculement du stockage pour un nœud, le basculement du stockage est également désactivé sur le partenaire du nœud.

2. Arrêtez chaque nœud sauf pour le nœud qui récupère :

```
system node halt -node node_name -reason "text"
```



```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

4. Sur le nœud de récupération, utilisez **system configuration recovery cluster recreate** commande pour recréer le cluster.

Cet exemple recrée du cluster à l'aide des informations de configuration stockées sur le nœud lors de la restauration :

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
        rebuild a new single-node cluster consisting of this node
        and its current configuration. This feature should only be
        used to recover from a disaster. Do not perform any other
        recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

Un nouveau cluster est créé sur le nœud restauré.

5. Si vous recréez le cluster à partir d'un fichier de sauvegarde de configuration, vérifiez que le cluster Recovery est toujours en cours :

```
system configuration recovery cluster show
```

Il n'est pas nécessaire de vérifier l'état de restauration du cluster si vous recréez le cluster à partir d'un nœud sain.

```
cluster1::*> system configuration recovery cluster show
Recovery Status: in-progress
Is Recovery Status Persisted: false
```

6. Démarrez chaque nœud qui doit être rejoint au cluster recréé-crée.

Vous devez redémarrer les nœuds un par un.

7. Pour chaque nœud qui doit être joint au cluster recréé-crée, procédez comme suit :

- a. A partir d'un nœud sain sur le cluster recréé-crée, rejoignez le nœud cible :

```
system configuration recovery cluster rejoin -node node_name
```

Cet exemple rejoint le nœud cible « node2 » au cluster recréé-crée :

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
cluster, potentially overwriting critical cluster
configuration files. This command should only be used
to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress.
This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

Le nœud cible redémarre, puis rejoint le cluster.

- b. Vérifier que le nœud cible est en bon état et qu'il a formé le quorum avec le reste des nœuds du cluster :

```
cluster show -eligibility true
```

Le nœud cible doit rejoindre à nouveau le cluster créé avant de pouvoir rejoindre un autre nœud.

```
cluster1::*> cluster show -eligibility true
Node           Health Eligibility Epsilon
-----
node0           true   true      false
node1           true   true      false
2 entries were displayed.
```

8. Si vous avez créé à nouveau le cluster à partir d'un fichier de sauvegarde de configuration, définissez l'état de restauration sur terminé :

```
system configuration recovery cluster modify -recovery-status complete
```

9. Retour au niveau de privilège admin :

```
set -privilege admin
```

10. Si le cluster comprend seulement deux nœuds, utilisez le **cluster ha modify** Commande pour réactiver le cluster HA.
11. Utilisez le **storage failover modify** Commande permettant de réactiver le basculement du stockage pour chaque paire haute disponibilité.

Une fois que vous avez terminé

Si le cluster a des relations de pairs SnapMirror, vous devez également les recréer. Pour plus d'informations, voir ["La protection des données"](#).

Synchroniser un nœud avec le cluster

Si le quorum au niveau du cluster est atteint mais qu'un ou plusieurs nœuds ne sont pas synchronisés avec le cluster, il faut synchroniser le nœud pour restaurer la base de données répliquée (RDB) sur le nœud et la mettre au quorum.

Étape

1. Depuis un nœud sain, utilisez le `system configuration recovery cluster sync` commande au niveau de privilège avancé pour synchroniser le nœud qui est hors synchronisation avec la configuration du cluster.

Cet exemple synchronise un nœud (*node2*) avec le reste du cluster :

```
cluster1::*> system configuration recovery cluster sync -node node2
```

```
Warning: This command will synchronize node "node2" with the cluster
configuration, potentially overwriting critical cluster
configuration files on the node. This feature should only be
used to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress. This
command will cause all the cluster applications on node
"node2" to restart, interrupting administrative CLI and Web
interface on that node.
```

```
Do you want to continue? {y|n}: y
```

```
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

Résultat

Le RDB est répliqué sur le nœud et le nœud devient éligible au cluster.

Gestion des « core dumps » (administrateurs du cluster uniquement)

Lorsqu'un nœud fonctionne de façon incohérente, un « core dump » se produit et le système crée un fichier « core dump » que le support technique peut utiliser pour résoudre le problème. Vous pouvez configurer ou afficher les attributs de core dump. Vous pouvez également enregistrer, afficher, segmenter, charger ou supprimer un fichier de vidage de mémoire.

Vous pouvez gérer des « core dumps » des manières suivantes :

- Configuration des « core dumps » et affichage des paramètres de configuration
- Affichage des informations de base, de l'état et des attributs des « core dumps »

Les fichiers core dump et les rapports sont stockés dans le `/mroot/etc/crash/` répertoire d'un nœud. Vous pouvez afficher le contenu du répertoire à l'aide du `system node coredump` commandes ou un

navigateur web.

- Enregistrement du contenu du core dump et chargement du fichier enregistré à un emplacement spécifié ou au support technique


ONTAP vous empêche de lancer l'enregistrement d'un fichier « core dump » lors d'un basculement, d'un transfert d'agrégat ou d'un rétablissement.

- Suppression des fichiers « core dump » qui ne sont plus nécessaires

Commandes pour la gestion des « core dumps »

Vous utilisez le `system node coredump config` commandes permettant de gérer la configuration des « core dumps », le `system node coredump` commandes pour gérer les fichiers « core dump » et `system node coredump reports` commandes permettant de gérer les rapports de base de l'application.

Les fonctions que vous recherchez...	Utilisez cette commande...
Configurer les « core dumps »	<code>system node coredump config modify</code>
Affiche les paramètres de configuration des « core dumps »	<code>system node coredump config show</code>
Affiche les informations de base relatives aux « core dumps »	<code>system node coredump show</code>
Déclenche manuellement un « core dump » lorsque vous redémarrez un nœud	<code>system node reboot</code> avec les deux <code>-dump</code> et <code>-skip-lif-migration-before-reboot</code> paramètres  Le lien: https://docs.netapp.com/us-en/ontap-cli-9141/system-node-reboot.html#parameters[skip-lif-migration-before-reboot] Le paramètre spécifie que la migration de LIF avant un redémarrage sera ignorée.
Déclenche manuellement un « core dump » lorsque vous arrêtez un nœud	<code>system node halt</code> avec les deux <code>-dump</code> et <code>-skip-lif-migration-before-shutdown</code> paramètres  Le lien: https://docs.netapp.com/us-en/ontap-cli-9141/system-node-halt.html#parameters[skip-lif-migration-before-shutdown] Le paramètre spécifie que la migration de LIF avant un arrêt sera ignorée.
Enregistrer un « core dump » spécifié	<code>system node coredump save</code>

Les fonctions que vous recherchez...	Utilisez cette commande...
Enregistrez tous les « core dumps » non enregistrés sur un nœud spécifié	<code>system node coredump save-all</code>
Générez et envoyez un message AutoSupport avec un fichier « core dump » que vous spécifiez	<div> <div>  </div> <div> <p>Le <code>-uri</code> Le paramètre facultatif indique une destination alternative pour le message AutoSupport.</p> </div> </div> <div> <code>system node autosupport invoke-core-upload</code> </div>
Affiche les informations d'état relatives aux « core dumps »	<code>system node coredump status</code>
Supprime un « core dump » spécifié	<code>system node coredump delete</code>
Supprimez tous les « core dumps » non enregistrés ou tous les fichiers « core » enregistrés sur un nœud	<code>system node coredump delete-all</code>
Affiche les rapports de vidage de mémoire de l'application	<code>system node coredump reports show</code>
Supprimer un rapport de vidage de mémoire de l'application	<code>system node coredump reports delete</code>

Informations associées

["Commandes de ONTAP 9"](#)

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.