Gestion du cluster via l'interface de ligne de commandes

ONTAP 9

NetApp
March 22, 2023

Table des matières

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 auhttp://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-cmpr/GUID-5CB10C70-AC11-41C0-8C16-B4D0DF916E9B.html["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 *admin*SVM, 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.

Principes de base de l'interface de gestion ONTAP

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

Accéder au cluster via le port série

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

Étapes

1. Sur la console, appuyez sur entrée.

   Le système répond avec l'invite de connexion.

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

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

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

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

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` les pages man contiennent des informations supplémentaires.

- Si vous utilisez un compte utilisateur de domaine Active Directory (AD) pour accéder au cluster, un tunnel d'authentification pour le cluster doit avoir été configuré via un SVM (Storage Virtual machine) compatible CIFS et votre compte utilisateur AD domain 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.

- Depuis ONTAP 9.3, vous pouvez activer 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.

- Depuis ONTAP 9.4, vous pouvez activer l'authentification multifacteur SSH pour les utilisateurs distants LDAP et NIS.

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.
```

Informations associées

"Authentification de l'administrateur et RBAC"

Sécurité de connexion SSH

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

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

- La dernière fois que votre nom de compte a été connecté.
- Nombre de tentatives de connexion infructueuses depuis la dernière connexion réussie.

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

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

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

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

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

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

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

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

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

Exemples d'informations de sécurité de la connexion SSH

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

- Ce message s'affiche après chaque connexion réussie :

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

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

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

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

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

Activer l'accès Telnet ou RSH au cluster

En tant que pratique 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 les commandes CLI (administrateurs de cluster uniquement)

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 abréger 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 abréger 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 *presse-papiers* dans certains programmes.	Ctrl-U
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

Les fonctions que vous recherchez…	Utilisez le raccourci clavier suivant…
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	?
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 technical support.
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 `volume show -volume *tmp*` affiche la liste de tous les volumes dont le nom inclut la chaîne `tmp`.
!	PAS opérateur. Indique une valeur qui ne doit pas être comparée ; par exemple, **`!vs0`** indique de ne pas correspondre à la valeur `vs0`.
OU opérateur . Sépare deux valeurs à comparer , par exemple `*vs0	vs2*` correspond soit à vs0, soit à vs2. Vous pouvez spécifier plusieurs instructions OU ; par exemple, `a
b*	*c*` correspond à l'entrée `a`, toute entrée commençant par `b`, et toute entrée qui inclut `c`.
..	Opérateur de gamme. Par exemple : **`5..10`** correspond à n'importe quelle valeur de `5` à `10`, inclus.
<	Moins que l'opérateur. Par exemple : **`<20`** correspond à toute valeur inférieure à `20`.
>	Opérateur supérieur à. Par exemple : **`>5`** correspond à toute valeur supérieure à `5`.
<=	Inférieur ou égal à l'opérateur. Par exemple : ⇐**`5`** correspond à toute valeur inférieure ou égale à `5`.
>=	Supérieur à ou égal à l'opérateur. Par exemple : **`>=5`** correspond à toute valeur supérieure ou égale à `5`.

Opérateur	Description
{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 `volume modify {-volume *tmp*} -state offline` définit hors ligne tous les volumes dont le nom inclut la chaîne `tmp`.

Si vous souhaitez analyser les caractères de requête en tant que littérales, vous devez inclure ces caractères dans des guillemets doubles (par exemple, « »^', «».", "*", or "$») pour les bons résultats à retourner.

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 ».

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 a `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 svm1 -volume vol1 -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 svm1 -percent-snapshot-space 0
```

```
cluster1::> volume create -vserver svm1 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 (administrateurs du cluster uniquement)

Gérer les enregistrements des sessions CLI

Présentation de la gestion des enregistrements des 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.

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.

Enregistrez une session CLI

Vous pouvez utiliser le `system script start` et `system script stop` Commandes permettant d'enregistrer une session CLI.

Étapes

1. Pour démarrer l'enregistrement de la session CLI en cours dans un fichier, utilisez le `system script start` commande.

   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. Pour arrêter l'enregistrement de la session, utilisez le `system script stop` commande.

   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	`system script start`
Arrêter l'enregistrement de la session CLI en cours	`system script stop`

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur les enregistrements des sessions CLI	`system script show`
Télécharger un enregistrement d'une session CLI vers une destination FTP ou HTTP	`system script upload`
Supprimer un enregistrement d'une session CLI	`system script delete`

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	`system timeout show`
Modifier la période de temporisation automatique pour les sessions de l'interface de ligne de commande	`system timeout modify`

Informations associées

"Commandes de ONTAP 9"

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 les commandes CLI (administrateurs de cluster uniquement)

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 abréger 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 abréger 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

Les fonctions que vous recherchez…	Utilisez le raccourci clavier suivant…
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 *presse-papiers* dans certains programmes.	Ctrl-U
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.

Les fonctions que vous recherchez…	Utilisez le raccourci clavier suivant…
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	?
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 technical support.
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 `volume show -volume *tmp*` affiche la liste de tous les volumes dont le nom inclut la chaîne `tmp`.
!	PAS opérateur. Indique une valeur qui ne doit pas être comparée ; par exemple, **`!vs0`** indique de ne pas correspondre à la valeur `vs0`.

Opérateur	Description
OU opérateur. Sépare deux valeurs à comparer, par exemple `*vs0	vs2*` correspond soit à vs0, soit à vs2. Vous pouvez spécifier plusieurs instructions OU ; par exemple, `a
b*	*c*` correspond à l'entrée `a`, toute entrée commençant par `b`, et toute entrée qui inclut `c`.
..	Opérateur de gamme. Par exemple : **`5..10`** correspond à n'importe quelle valeur de `5` à `10`, inclus.
<	Moins que l'opérateur. Par exemple : **`<20`** correspond à toute valeur inférieure à `20`.
>	Opérateur supérieur à. Par exemple : **`>5`** correspond à toute valeur supérieure à `5`.
<=	Inférieur ou égal à l'opérateur. Par exemple : ⇐**`5`** correspond à toute valeur inférieure ou égale à `5`.
>=	Supérieur à ou égal à l'opérateur. Par exemple : **`>=5`** 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 `volume modify {-volume *tmp*} -state offline` définit hors ligne tous les volumes dont le nom inclut la chaîne `tmp`.

Si vous souhaitez analyser les caractères de requête en tant que littérales, vous devez inclure ces caractères dans des guillemets doubles (par exemple, « »^', «».`", "*", or "$`») pour les bons résultats à retourner.

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 ».

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 a `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 svm1 -volume vol1 -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 svm1 -percent-snapshot-space 0
```

```
cluster1::> volume create -vserver svm1 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.

Notions de base sur la 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'epsilon

Le quorum et l'epsilon 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 noeuds survivants contient epsilon, le cluster reste dans le quorum même s'il n'y a pas une simple majorité de noeuds 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

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 noeud « 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
```

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, vous devez trouver l'état de santé de plus de la moitié des nœuds existants du cluster (indiqué par `cluster show`).
- Si vous ajoutez des nœuds à un cluster sans commutateur à deux nœuds, vous devez avoir installé et configuré les commutateurs de gestion et d'interconnexion du cluster avant d'ajouter des nœuds supplémentaires.

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

  Lorsqu'un cluster contient ou passe à plus de deux nœuds, la haute disponibilité du cluster n'est pas requise et est désactivée automatiquement.

- 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 le cluster est activé pour la configuration automatique du processeur de service, le sous-réseau spécifié pour que ce dernier puisse utiliser doit disposer de ressources disponibles pour le nœud d'arrivée.

  Un nœud qui rejoint le cluster utilise 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 [e0c]:
   ```

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://10.63.11.29

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
```

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.

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 ont été "déplacé" ou "supprimé" à partir d'agrégats détenus par le nœud.
- Tous les agrégats l'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" a 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 noeuds-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 noeud.

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`

Remarque : toutes les données système et utilisateur, de tous les disques connectés au nœud, doivent être rendues 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. Si le nœud que vous souhaitez supprimer est le nœud maître actuel, activez-le pour qu'un autre nœud du cluster soit élu comme nœud maître en changeant l'éligibilité du cluster du nœud maître à `false`:

   `cluster modify –eligibility false`

   Le noeud maître est le noeud qui contient des processus tels que «mgmt», «vldb», «vifmgr», «bcomd» et «crs». Le `cluster ring show` la commande avancée affiche le nœud maître actuel.

   ```
   cluster::*> cluster modify -node node1 -eligibility false
   ```

3. 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.
4. Supprimer le nœud du cluster :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.3	**`cluster unjoin`**
ONTAP 9.4 et versions ultérieures	**`cluster remove-node`**

   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.

5. 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.

6. Si vous requalifiez le nœud, effacez la configuration du nœud et initialisez tous les disques :
   a. Pendant le processus de démarrage, appuyez sur Ctrl-C pour afficher le menu de démarrage lorsque vous y êtes invité.

b. Sélectionner l'option de menu d'amorçage **(4) nettoyer la configuration et initialiser tous les disques**.

7. Retour au niveau de privilège admin :

```
set -privilege admin
```

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

Une fois que vous avez terminé

Si vous avez supprimé les nœuds pour disposer d'un cluster à un seul nœud, vous devez modifier les ports de cluster pour diffuser les données en modifiant les ports de cluster en tant que ports de données, puis en créant les LIFs de données sur les ports data.

Accédez aux fichiers log, core dump et MIB d'un noeud 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 noeud 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	`system console`
INTERFACE DE LIGNE DE COMMANDES DE ONTAP	`system node run-console`

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 noeud 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::>
```

Règles qui régissent les volumes racine des nœuds et les agrégats racine

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.

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.

- 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.

    Transfert des volumes racines vers de nouveaux agrégats
- 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"

Libérer 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 leurs noms en utilisant la `system node coredump show` commande.
2. Supprimez les fichiers core dump indésirables du nœud à l'aide de la `system node coredump delete` commande.
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     root, nvfail=on
                                64-bit
```

   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.

Démarre ou arrête un nœud

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	`boot_ontap`
Image principale ONTAP à partir du périphérique de démarrage	`boot_primary`
Image de sauvegarde ONTAP à partir du périphérique de démarrage	`boot_backup`

   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
Selection (1-9)?
```

   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	4) nettoyer la configuration et initialiser tous les disques Cette option de menu efface toutes les données sur les disques du nœud et réinitialise la configuration par défaut de votre nœud. 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. 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. 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. 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". 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".
Opérations de maintenance des agrégats et des disques pour obtenir des informations détaillées sur les agrégats et les disques	5) démarrage du mode maintenance Pour quitter le mode Maintenance, utilisez le `halt` commande.
Restaurez les informations de configuration à partir du volume racine du nœud vers le périphérique d'amorçage, par exemple une carte CompactFlash pour PC	6) mettre à jour la mémoire flash à partir de la configuration de sauvegarde 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.

Pour…	Sélectionner…
Installez le nouveau logiciel sur le nœud	7) installer le nouveau logiciel en premier 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. 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 *NOT* utilisez cette option de menu pour mettre à niveau ONTAP.
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	9) Configuration du partitionnement de disque avancé
	
	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 :
	
	`(9a) Unpartition all disks and remove their ownership information.`
	`(9b) Clean configuration and initialize system with partitioned disks.`
	`(9c) Clean configuration and initialize system with whole disks.`
	`(9d) Reboot the node.`
	`(9e) Return to main boot menu.`

Gérez un nœud à distance à l'aide du SP/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
- AFF A320
- AVEC AFF A220
- 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.

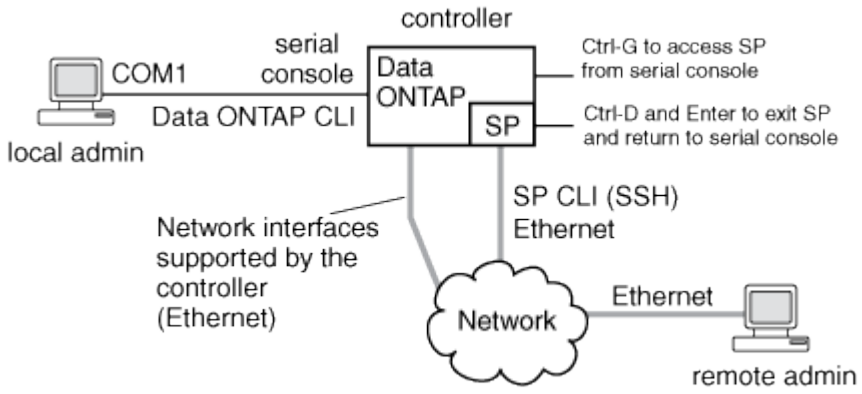
  Lorsque des messages sont envoyés à la console, le processeur de service les stocke dans le journal de la console. Le journal de la console est conservé tant que le processeur de service est alimenté à partir d'une des alimentations du nœud. Du fait que le processeur de service fonctionne avec une alimentation 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.

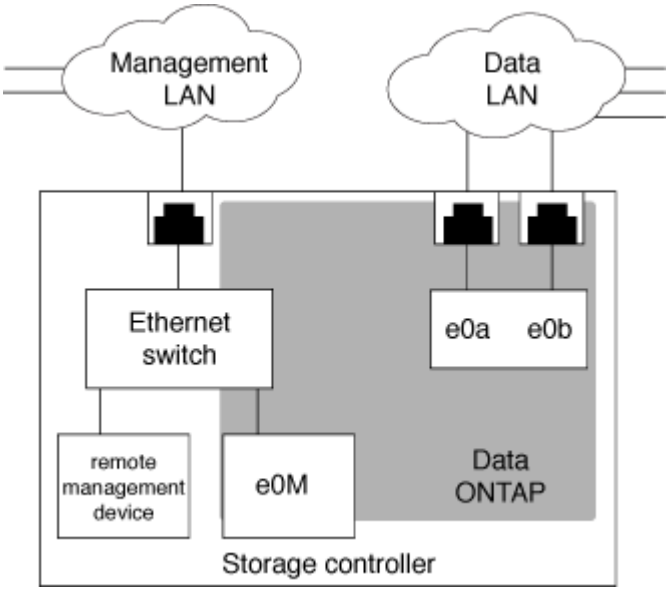
  Les opérations de nœud ne sont pas affectées lors du redémarrage de BMC.

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	`system service-processor api-service modify` avec le `-port` {`49152..`65535`paramètre }
Renouvelez les certificats SSL et SSH utilisés par le service API SP pour les communications internes	• Pour ONTAP 9.5 ou une utilisation ultérieure `system service-processor api-service renew-internal-certificate` • Pour ONTAP 9.4 et une utilisation antérieure • `system service-processor api-service renew-certificates` Si aucun paramètre n'est spécifié, seuls les certificats d'hôte (y compris les certificats client et serveur) sont renouvelés. Si le `-renew-all true` Le paramètre est spécifié, les certificats d'hôte et le certificat d'autorité de certification racine sont renouvelés.
comm	
Désactivez ou réactivez le service API du processeur de service	`system service-processor api-service modify` avec le `-is-enabled` {`true`

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

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 défaillante 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 échec de la mise à niveau du SP du moniteur SPAutoUpgradeFailedMajorAlert - 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"

Accéder au SP/BMC

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 `help` À l'invite du processeur de service.	Type `system` 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	`help` [`command`]		
Affiche le niveau de privilège actuel pour l'interface de ligne de commandes du processeur de service	`priv show`		

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	`priv set {admin`	`advanced`	`diag}`
		Afficher la date et l'heure du système	`date`
	`date`	Affiche les événements consignés par le processeur de service	`events {all`
`info`	`newest number`	`oldest number`	`search keyword}`
		Affiche l'état du processeur de service et les informations de configuration réseau	`sp status [-v`
`-d]` Le `-v` Option affiche les statistiques du processeur de service sous forme détaillée. Le `-d` Option ajoute le journal de débogage du processeur de service à l'affichage.	`bmc status [-v`	`-d]` Le `-v` Option affiche les statistiques du processeur de service sous forme détaillée. Le `-d` Option ajoute le journal de débogage du processeur de service à l'affichage.	`system service-processor show`
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	`sp uptime`	`bmc uptime`	
Affiche les journaux de la console du système	`system log`		
Affiche les archives du journal du processeur de service ou les fichiers d'une archive	`sp log history show [-archive {latest`	`{all`	`archive-name}] [-dump {all`

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 …
`system sensors get sensor_name` Vous pouvez obtenir `sensor_name` à l'aide du `system sensors` ou le `system sensors show` commande.			Affiche les informations de version du firmware du processeur de service
`version`		`system service-processor image show`	Affiche l'historique des commandes du processeur de service
`sp log audit` (niveau de privilège avancé)	`bmc log audit`		Affiche les informations de débogage du processeur de service
`sp log debug` (niveau de privilège avancé)	`bmc log debug` (niveau de privilège avancé)		Affiche le fichier des messages du processeur de service
`sp log messages` (niveau de privilège avancé)	`bmc log messages` (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
`system forensics` [`show`	`log dump`	`log clear`]	
	Connectez-vous à la console du système	`system console`	

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 …
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. À l'aide de ces commandes, la mise hors/sous tension du nœud peut provoquer un arrêt incorrect du nœud (également appelé *shutdown*) et ne remplace pas un arrêt normal à l'aide de ONTAP `system node halt` commande.	Créer un « core dump » et réinitialiser le nœud	`system core [-f]` Le `-f` option force la création d'un « core dump » et la réinitialisation du nœud.	

Les fonctions que vous recherchez…	Utilisez cette commande du processeur de service…	Utilisez cette commande BMC…	Ou cette commande ONTAP …
`system node coredump trigger` (niveau de privilège avancé)	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.	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	`system reset {primary`
`backup`	`current}`		`system node reset` avec le `-firmware {primary`
`backup`	`current}` paramètre (niveau de privilège avancé) `system node reset`	Cette opération provoque un arrêt non planifié du nœud. 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.	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

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.

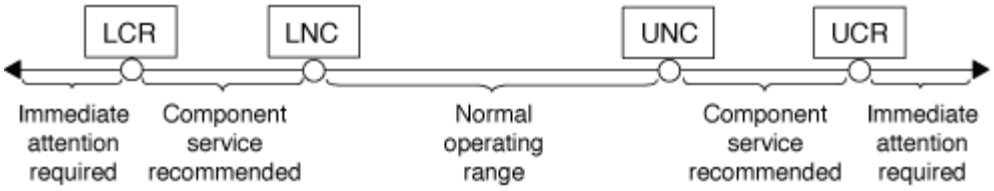
Les seuils des capteurs à seuils sont les suivants, affichés dans le résultat du processeur de service `system sensors` commande :

- 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 l' `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 system Sensors_name pour un capteur à seuil

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.
2F	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	`system service-processor network auto-configuration enable`
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	`system service-processor network auto-configuration disable`
Affiche la configuration réseau automatique du processeur de service	`system service-processor network auto-configuration show`

Les fonctions que vous recherchez…	Exécuter cette commande ONTAP…
Configurez manuellement le réseau du processeur de service d'un nœud, y compris les éléments suivants : • 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`
Affichage de la configuration réseau du processeur de service, y compris les éléments suivants : • 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	`system service-processor network show` L'affichage des détails complets du réseau du processeur de service nécessite le `-instance` paramètre.

Les fonctions que vous recherchez…	Exécuter cette commande ONTAP…
Modifiez la configuration du service API du processeur de service, notamment : • Modification du port utilisé par le service d'API du processeur de service • Activation ou désactivation du service API du processeur de service	`system service-processor api-service modify` (niveau de privilège avancé)
Affiche la configuration du service API du processeur de service	`system service-processor api-service show` (niveau de privilège avancé)
Renouvelez les certificats SSL et SSH utilisés par le service API SP pour les communications internes	• Pour ONTAP 9.5 ou version ultérieure : `system service-processor api-service renew-internal-certificates` • Pour ONTAP 9.4 ou version antérieure : `system service-processor api-service renew-certificates` (niveau de privilège avancé)

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

Les fonctions que vous recherchez…	Exécuter cette commande ONTAP…
Afficher les détails de l'image du firmware du processeur de service actuellement installée, y compris les éléments suivants : • 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	`system service-processor image show` Le `-is-current` 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.

Les fonctions que vous recherchez…	Exécuter cette commande ONTAP…
Activez ou désactivez la mise à jour automatique du firmware du processeur de service	`system service-processor image modify` 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.
Téléchargez manuellement une image du firmware du processeur de service sur un nœud	`system node image get` Avant d'exécuter le `system node image` commandes, vous devez définir le niveau de privilège sur avancé (`set -privilege advanced`), saisissez **y** lorsque vous êtes invité à continuer. 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.
Affichez le statut de la dernière mise à jour du firmware du processeur de service déclenchée par ONTAP, y compris les informations suivantes : • 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	`system service-processor image update-progress show`

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	`system service-processor ssh add-allowed-addresses`
Bloc les adresses IP spécifiées pour l'accès au processeur de service	`system service-processor ssh remove-allowed-addresses`

Les fonctions que vous recherchez…	Exécuter cette commande ONTAP…
Affiche les adresses IP pouvant accéder au processeur de service	`system service-processor ssh show`

Commandes d'administration générale du processeur de service

Les fonctions que vous recherchez…	Exécuter cette commande ONTAP…
Affichage des informations générales sur le processeur de service, notamment : • 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	`system service-processor show` L'affichage des informations complètes du processeur de service nécessite le `-instance` paramètre.
Redémarre le processeur de service sur un nœud	`system service-processor reboot-sp`
Générez et envoyez un message AutoSupport qui inclut les fichiers journaux du processeur de service collectés à partir d'un nœud spécifié	`system node autosupport invoke-splog`
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	`system service-processor log show-allocations`

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	**system service-processor show**
Afficher/modifier la configuration réseau du BMC	**system service-processor network show/modify**
Réinitialisez le contrôleur BMC	**system service-processor reboot-sp**
Affiche/modifie les détails de l'image du micrologiciel BMC actuellement installée	**system service-processor image show/modify**
Mettre à jour le micrologiciel du contrôleur BMC	**system service-processor image update**
Affiche l'état de la dernière mise à jour du micrologiciel du contrôleur BMC	**system service-processor image update-progress show**
Activez la configuration réseau automatique pour que le contrôleur BMC utilise une adresse IPv4 ou IPv6 sur le sous-réseau spécifié	**system service-processor network auto-configuration enable**
Désactivez la configuration réseau automatique pour une adresse IPv4 ou IPv6 sur le sous-réseau spécifié pour le contrôleur BMC	**system service-processor network auto-configuration disable**
Afficher la configuration réseau automatique du contrôleur BMC	**system service-processor network auto-configuration show**

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
système	Affiche la liste de toutes les commandes.
console système	Effectue la connexion à la console du système. Utiliser `Ctrl+D` 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 la journalisation des audits pour les activités de gestion

Mise en œuvre de la journalisation des audits par ONTAP

Les activités de gestion enregistrées dans le journal d'audit sont incluses dans les rapports AutoSupport standard et certaines activités de consignation sont incluses dans les messages EMS. Vous pouvez également transférer le journal d'audit aux destinations que vous spécifiez et afficher les fichiers journaux d'audit à l'aide de l'interface de ligne de commande ou d'un navigateur Web.

Depuis ONTAP 9.11.1, vous pouvez afficher le contenu des journaux d'audit à l'aide de System Manager.

Depuis 9.12.1, les journaux d'audit sont inviolables, c'est-à-dire tout fichier journal qui enregistre une action d'administration ne peut pas être modifié ou supprimé, même par les comptes d'administrateur de cluster.

ONTAP consigne les activités de gestion qui sont effectuées sur le cluster, par exemple la requête émise, l'utilisateur qui a déclenché la demande, la méthode d'accès de l'utilisateur et l'heure de la demande.

Les activités de gestion peuvent être de l'un des types suivants :

- DÉFINIR les demandes, qui s'appliquent généralement aux commandes ou opérations non affichées
  - Ces demandes sont émises lorsque vous exécutez un `create`, `modify`, ou `delete` commande, par exemple.
  - Les demandes de série sont consignées par défaut.
- OBTENIR les demandes, qui récupèrent les informations et les affichent dans l'interface de gestion

- Ces demandes sont émises lorsque vous exécutez un `show` commande, par exemple.
- Les demandes GET ne sont pas consignées par défaut, mais vous pouvez contrôler si LES demandes GET sont envoyées depuis l'interface de ligne de commande ONTAP (`-cliget`) Ou à partir des API ONTAP (`-ontapiget`) sont consignés dans le fichier.

ONTAP enregistre les activités de gestion dans `/mroot/etc/log/mlog/audit.log` fichier d'un nœud. Les commandes des trois shells pour les commandes CLI—le clustershell, le nodeshell et le systemshell non-interactif (les commandes du systemshell interactives ne sont pas consignées)--ainsi que les commandes d'API sont consignées ici. Les journaux d'audit incluent des horodatages pour indiquer si tous les nœuds d'un cluster sont synchronisés.

Le `audit.log` Le fichier est envoyé par l'outil AutoSupport aux destinataires spécifiés. Vous pouvez également transférer le contenu en toute sécurité vers des destinations externes que vous spécifiez (par exemple, un serveur Splunk ou syslog).

Le `audit.log` le fichier fait l'objet d'une rotation quotidienne. La rotation se produit également lorsqu'elle atteint 100 Mo et que les 48 copies précédentes sont conservées (avec un total maximum de 49 fichiers). Lorsque le fichier d'audit effectue sa rotation quotidienne, aucun message EMS n'est généré. Si le fichier d'audit tourne parce que sa taille limite de fichier est dépassée, un message EMS est généré.

Modifications de la journalisation des audits dans ONTAP 9

Avec ONTAP 9, le `command-history.log` le fichier est remplacé par `audit.log`, et le `mgwd.log` le fichier ne contient plus d'informations d'audit. Si vous effectuez une mise à niveau vers ONTAP 9, il est recommandé de consulter les scripts ou les outils qui font référence aux fichiers hérités et à leur contenu.

Après la mise à niveau vers ONTAP 9, existant `command-history.log` les fichiers sont conservés. Ils sont tournés vers l'extérieur (supprimés) comme nouveaux `audit.log` les fichiers sont pivotés dans (créés).

Outils et scripts qui vérifient le `command-history.log` le fichier peut continuer à fonctionner, car un lien logiciel de `command-history.log` à `audit.log` est créée lors de la mise à niveau. Cependant, les outils et les scripts qui vérifient le `mgwd.log` le fichier échoue, car ce fichier ne contient plus d'informations d'audit.

Les journaux d'audit dans ONTAP 9 et les versions ultérieures n'incluent plus les entrées suivantes, car elles ne sont pas considérées comme utiles et n'entraînent pas d'activité de journalisation inutile :

- Commandes internes exécutées par ONTAP (c'est-à-dire où username=root)
- Alias de commande (séparément de la commande à laquelle ils pointent)

Depuis ONTAP 9, vous pouvez transmettre les journaux d'audit de manière sécurisée vers des destinations externes à l'aide des protocoles TCP et TLS.

Afficher le contenu du journal d'audit

Vous pouvez afficher le contenu du cluster `/mroot/etc/log/mlog/audit.log` Fichiers via l'interface de ligne de commandes de ONTAP, System Manager ou un navigateur Web.

Les entrées du fichier journal du cluster sont les suivantes :

Temps

Horodatage de l'entrée du journal.

Client supplémentaire

Application utilisée pour se connecter au cluster. Voici des exemples de valeurs possibles `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, et `service-processor`.

Utilisateur

Nom d'utilisateur de l'utilisateur distant.

État

État actuel de la demande d'audit, qui pourrait être `success`, `pending`, ou `error`.

Messagerie

Champ facultatif qui peut contenir une erreur ou des informations supplémentaires sur l'état d'une commande.

ID de session

ID de session sur lequel la demande est reçue. Un ID de session est attribué à chaque session SSH *session*, tandis que chaque HTTP, ONTAPI ou SNMP *request* se voit attribuer un ID de session unique.

VM de stockage

SVM via lequel l'utilisateur a connecté.

Portée

S'affiche `svm` Lorsque la demande se trouve sur une machine virtuelle de stockage de données ; dans le cas contraire, s'affiche `cluster`.

ID de commande

ID de chaque commande reçue lors d'une session CLI. Cela vous permet de mettre en corrélation une demande et une réponse. Les requêtes ZAPI, HTTP et SNMP ne possèdent pas d'ID de commande.

Vous pouvez afficher les entrées des journaux du cluster depuis l'interface de ligne de commandes de ONTAP, depuis un navigateur Web et depuis ONTAP 9.11.1, depuis System Manager.

System Manager

- Pour afficher l'inventaire, sélectionnez **Evénements et travaux > journaux d'audit**. + chaque colonne dispose de contrôles pour filtrer, trier, rechercher, afficher et afficher les catégories d'inventaire. Les détails de l'inventaire peuvent être téléchargés sous forme de classeur Excel.
- Pour définir des filtres, cliquez sur le bouton **Filter** dans le coin supérieur droit, puis sélectionnez les champs souhaités. + vous pouvez également afficher toutes les commandes exécutées dans la session dans laquelle un échec s'est produit en cliquant sur le lien ID de session.

CLI

Pour afficher les entrées d'audit fusionnées à partir de plusieurs nœuds du cluster, entrez : `security audit log show` *`[parameters]`*

Vous pouvez utiliser le `security audit log show` commande permettant d'afficher les entrées d'audit de nœuds individuels ou fusionnées à partir de plusieurs nœuds du cluster. Vous pouvez également afficher le contenu du `/mroot/etc/log/mlog` répertoire sur un seul nœud à l'aide d'un navigateur web. Voir la page man pour plus de détails.

Navigateur Web

Vous pouvez afficher le contenu du `/mroot/etc/log/mlog` répertoire sur un seul nœud à l'aide d'un navigateur web. "Découvrez comment accéder aux fichiers log, core dump et MIB d'un nœud à l'aide d'un navigateur Web".

Gérer les paramètres de demande GET d'audit

Lorsque LES demandes DÉFINIES sont consignées par défaut, les demandes GET ne le sont pas. Cependant, vous pouvez contrôler si LES requêtes GET sont envoyées depuis ONTAP HTML (`-httpget`), l'interface de ligne de commande ONTAP (`-cliget`), ou à partir des API ONTAP (`-ontapiget`) sont consignés dans le fichier.

Vous pouvez modifier les paramètres de la journalisation des audits depuis l'interface de ligne de commandes de ONTAP et depuis ONTAP 9.11.1 depuis System Manager.

System Manager

1. Sélectionnez **événements et travaux > journaux d'audit**.
2. Cliquez sur ⚙ dans le coin supérieur droit, choisissez les demandes à ajouter ou à supprimer.

CLI

- Pour spécifier que les demandes GET depuis l'interface de ligne de commande ou les API ONTAP doivent être enregistrées dans le journal d'audit (fichier audit.log), en plus des demandes SET par défaut, entrez :
  `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Pour afficher les paramètres actuels, entrez :
  `security audit show`

Consultez les pages de manuel pour plus de détails.

Gérer les destinations du journal d'audit

Vous pouvez transférer le journal d'audit vers un maximum de 10 destinations. Par exemple, vous pouvez transférer le journal vers un serveur Splunk ou syslog à des fins de surveillance, d'analyse ou de sauvegarde.

Description de la tâche

Pour configurer le transfert, vous devez fournir l'adresse IP de l'hôte syslog ou Splunk, son numéro de port, un protocole de transmission et la fonction syslog à utiliser pour les journaux transférés. "En savoir plus sur les installations de syslog".

Vous pouvez sélectionner l'une des valeurs de transmission suivantes :

UDP non crypté
: Protocole de datagramme utilisateur sans sécurité (par défaut)

TCP non crypté
: Protocole de contrôle de transmission sans sécurité

TCP chiffré
: Protocole de contrôle de transmission avec TLS (transport Layer Security) + une option **Verify Server** est disponible lorsque le protocole TCP chiffré est sélectionné.

Vous pouvez transférer les journaux d'audit depuis l'interface de ligne de commandes de ONTAP et depuis ONTAP 9.11.1 depuis System Manager.

System Manager

- Pour afficher les destinations du journal d'audit, sélectionnez **Cluster > Paramètres**. + Un nombre de destinations de journaux est affiché dans la vignette **gestion des notifications**. Cliquez sur ⋮ pour afficher les détails.
- Pour ajouter, modifier ou supprimer des destinations du journal d'audit, sélectionnez **Evénements et travaux > journaux d'audit**, puis cliquez sur **gérer destinations d'audit** dans le coin supérieur droit de l'écran. + cliquez sur + Add ou cliquez sur ⋮ Dans la colonne **adresse hôte** pour modifier ou supprimer des entrées.

CLI

1. Pour chaque destination vers laquelle vous souhaitez transférer le journal d'audit, spécifiez l'adresse IP ou le nom d'hôte de destination et les options de sécurité.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - Si le `cluster log-forwarding create` la commande ne peut pas envoyer de requête ping à l'hôte de destination pour vérifier la connectivité, la commande échoue avec une erreur. Bien qu'il ne soit pas recommandé, utiliser le `-force` le paramètre utilisé avec la commande ignore la vérification de connectivité.
   - Lorsque vous définissez le `-verify-server` paramètre à `true`, l'identité de la destination de transfert de journal est vérifiée en validant son certificat. Vous pouvez définir la valeur sur `true` uniquement lorsque vous sélectionnez `tcp-encrypted` valeur dans le `-protocol` légale.

2. Vérifiez que les enregistrements de destination sont corrects à l'aide du `cluster log-forwarding show` commande.

```
cluster1::> cluster log-forwarding show

                                              Verify Syslog
Destination Host          Port   Protocol     Server Facility
------------------------- ------ -------- ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            514    tcp-encrypted   true   user
2 entries were displayed.
```

Consultez les pages de manuel pour plus de détails.

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	`cluster time-service ntp server create -server server_name`
Associez le cluster à un serveur NTP externe avec une authentification symétrique disponible dans ONTAP 9.5 ou version ultérieure	`cluster time-service ntp server create -server server_ip_address -key-id key_id` Le `key_id` doit faire référence à une clé partagée existante configurée avec « clé ntp de service de cluster ».
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 Disponible dans ONTAP 9.5 ou version ultérieure	`cluster time-service ntp server modify -server server_name -key-id key_id`
Désactiver l'authentification symétrique	`cluster time-service ntp server modify -server server_name -authentication disabled`

Les fonctions que vous recherchez…	Utilisez cette commande…
Configurez une clé NTP partagée	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` 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
Affiche les informations relatives aux serveurs NTP associés au cluster	`cluster time-service ntp server show`
Modifier la configuration d'un serveur NTP externe associé au cluster	`cluster time-service ntp server modify`
Dissociez un serveur NTP du cluster	`cluster time-service ntp server delete`
Réinitialise la configuration en désactivant l'association de tous les serveurs NTP externes au cluster	`cluster time-service ntp server reset` Cette commande nécessite le niveau de privilège avancé.

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	`cluster date modify`
Affiche les paramètres de fuseau horaire, de date et d'heure du cluster	`cluster date show`

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
- Version de cluster efficace chaîne de `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 `-message «text"` paramètre pour spécifier le texte.

Les fonctions que vous recherchez…	Alors…
Inclure les nouvelles lignes (également appelées fin de lignes) dans le message	Utiliser la commande sans `-message` ou `-uri` 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 `-uri` 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 : `*security login banner modify -vserver *cluster_name* { [-message "text"]
[*-uri ftp_or_http_addr*] }*`	Supprimer la bannière pour toutes les connexions (cluster et SVM)
Définissez la bannière sur une chaîne vide (`""`) : **`security login banner modify -vserver * -message ""`**	Remplacer une bannière créée par un administrateur du SVM
Modifier le message de la bannière SVM : `*security login banner modify -vserver *svm_name* { [-message "*text*"]	[-uri *ftp_or_http_addr*] }*`

- 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 : `*security login banner modify -vserver *svm_name* { [-message "text"]
[-uri ftp_or_http_addr] }*`	Supprime la bannière fournie par l'administrateur du cluster afin qu'aucune bannière ne s'affiche pour la SVM
Définir la bannière SVM sur une chaîne vide pour le SVM : **`security login banner modify -vserver *svm_name* -message ""`**	Utilisez la bannière cluster lorsque le SVM utilise actuellement une bannière de niveau SVM

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 `-message «text"` paramètre pour spécifier le texte.
Inclure les nouvelles lignes (également appelée fin de lignes)	Utiliser la commande sans `-message` ou `-uri` Paramètre pour lancer le mode interactif pour modifier le MOTD.
Téléchargez le contenu à partir d'un emplacement pour le MOTD	Utilisez le `-uri` 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
12345678901234567890123456789012345678901234567890123456789012345678901234
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.

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 : `*security login motd modify -vserver *cluster_name* { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*`	Modifiez le MOTD pour toutes les connexions lorsqu'aucun MOTD au niveau des SVM n'est configuré
Modifier la DPE au niveau du cluster : `*security login motd modify -vserver *cluster_name* { [-message "*text*"] }	[-uri ftp_or_http_addr] }*`
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 (`""`) : **`security login motd modify -vserver *cluster_name* -message ""`**
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. `*security login motd modify -vserver *cluster_name* { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*` .. **`security login motd modify { -vserver !"*cluster_name*" } -message "" -is -cluster-message-enabled true`**	Avoir un MOTD affiché uniquement pour les SVM sélectionnés et n'utiliser aucun MOTD au niveau du cluster
Définissez la MOTD au niveau du cluster sur une chaîne vide, puis définissez les MOTDS au niveau du SVM pour les SVM sélectionnés : a. **`security login motd modify -vserver *cluster_name* -message ""`** b. `*security login motd modify -vserver *svm_name* { [-message "*text*"]	[-uri *ftp_or_http_addr*] }*` + Vous pouvez répéter cette étape pour chaque SVM si nécessaire.
Utilisez la même MOTD au niveau du SVM pour toutes les SVM (données et admin	Définir le cluster et tous les SVM afin d'utiliser le même MOTD : `*security login motd modify *-vserver* * { [-message "*text*"]

Les fonctions que vous recherchez…	Alors…
[-uri *ftp_or_http_addr*] }*` [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. ====	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
Définissez un MOTD au niveau du cluster, mais désactivez son affichage pour le cluster : `*security login motd modify -vserver *cluster_name* { [-message "*text*"]	[-uri *ftp_or_http_addr*] } -is-cluster-message-enabled false*`
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	Définissez le cluster et tous les SVM de manière à utiliser une chaîne vide pour le MOTD : **`security login motd modify -vserver * -message ""`**
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	Utilisez les requêtes étendues pour modifier la MOTD de façon sélective : `*security login motd modify { -vserver !"*cluster_name*" -message !"" } { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*`	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 : `*security login motd modify -vserver *svm_name* { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*`	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 licences (administrateurs du cluster uniquement)

Gestion des licences Overview (administrateurs du cluster uniquement)

Une licence est un enregistrement d'un ou plusieurs droits logiciels. Dans ONTAP 8.2 à ONTAP 9.9.1, les clés de licence sont livrées sous forme de chaînes de 28 caractères, et une clé par fonctionnalité ONTAP est disponible. Un nouveau format de clé de licence appelé fichier de licence NetApp (NLF) a été introduit dans ONTAP 9.2 en ce qui concerne uniquement les fonctionnalités de cluster, telles que FabricPool.

À partir de ONTAP 9.10.1, toutes les licences sont fournies sous forme de NLF. Les licences NLF peuvent activer une ou plusieurs fonctionnalités ONTAP, selon votre achat. Vous pouvez récupérer des licences NLF sur le site de support NetApp en recherchant le numéro de série du système (contrôleur).

Vous trouverez les licences pour vos commandes logicielles initiales ou d'extension sur le site de support NetApp sous **My support** > **licences logicielles** (connexion requise). Pour plus d'informations sur les remplacements de licences, consultez l'article de la base de connaissances "Processus de remplacement post-carte mère pour la mise à jour des licences sur un système AFF/FAS".

ONTAP vous permet de gérer les licences des fonctions de l'une des manières suivantes :

- Affiche des informations sur les licences installées (`system license show`)
- Affiche les packs qui requièrent des licences et leur état actuel de licence sur le cluster (`system license status show`)
- Supprimez une licence du cluster ou d'un nœud dont vous spécifiez le numéro de série (`system license delete`)

- Afficher ou supprimer les licences expirées ou inutilisées (`system license clean-up`)

ONTAP vous permet de surveiller l'utilisation des fonctionnalités et le risque de licence de l'une des manières suivantes :

- Affiche un récapitulatif de l'utilisation des fonctionnalités dans le cluster par nœud (`system feature-usage show-summary`)

  Le résumé inclut des informations de compteur telles que le nombre de semaines pendant laquelle une fonction a été utilisée et la date et l'heure de la dernière utilisation de la fonction.

- Affiche l'état d'utilisation de la fonction dans le cluster par nœud et par semaine (`system feature-usage show-history`)

  L'état d'utilisation de la fonction peut être `not-used`, `configured`, ou `in-use`. Si les informations d'utilisation ne sont pas disponibles, l'état indique `not-available`.

- Affiche l'état du risque de droit de licence pour chaque package de licences (`system license entitlement-risk show`)

  L'état du risque peut être `low`, `medium`, `high`, `unlicensed`, ou `unknown`. L'état des risques est également inclus dans le message AutoSupport. Le risque de droit de licence ne s'applique pas au package de licences de base.

  Le risque d'autorisation de licence est évalué à l'aide d'un certain nombre de facteurs, qui peuvent inclure, sans s'y limiter, les éléments suivants :

  - État des licences de chaque package
  - Le type de chaque licence, son état d'expiration et l'uniformité des licences à travers le cluster
  - Utilisation des fonctionnalités associées au package de licences si le processus d'évaluation détermine que le cluster présente un risque de licence, le résultat de la commande suggère également une action corrective.

> Remarque : ONTAP 9.10.1 prend également en charge les clés de licence de 28 caractères avec System Manager ou l'interface de ligne de commandes. Cependant, si une licence NLF est installée pour une fonction, vous ne pouvez pas installer une clé de licence à 28 caractères sur la licence NLF pour la même fonction. Pour plus d'informations sur l'installation des NLF ou des clés de licence à l'aide de System Manager, reportez-vous à la section « Activer les nouvelles fonctionnalités ».

Informations associées

"Qu'est-ce qu'une présentation et des références des licences Data ONTAP 8.2 et 8.3 ?"

"Comment vérifier les autorisations de logiciel Data ONTAP et les clés de licence associées sur le site de support"

"FAQ : mises à jour des licences dans Data ONTAP 9.2"

"NetApp : état du risque Data ONTAP"

Types de licence et méthode sous licence

La compréhension des types de licence et la méthode sous licence vous aident à gérer les licences dans un cluster.

Types de licence

Un pack peut disposer d'un ou plusieurs des types de licence suivants installés dans le cluster. Le `system license show` commande affiche le ou les types de licence installés pour un package.

- Licence standard (`license`)

  Une licence standard est une licence verrouillée par un nœud. Il est émis pour un nœud avec un numéro de série système spécifique (également appelé *numéro de série du contrôleur*). Une licence standard n'est valide que pour le nœud qui possède le numéro de série correspondant.

  L'installation d'une licence standard verrouillée par un nœud donne droit à la fonctionnalité sous licence d'un nœud. Pour que le cluster utilise la fonctionnalité sous licence, au moins un nœud doit être sous licence pour cette fonctionnalité. Il se peut qu'il soit hors conformité pour utiliser la fonctionnalité sous licence sur un nœud qui ne dispose pas d'un droit pour la fonctionnalité.

- Licence de site (`site`)

  Une licence de site n'est pas liée à un numéro de série de système spécifique. Lorsque vous installez une licence de site, tous les nœuds du cluster ont droit à la fonctionnalité sous licence. Le `system license show` la commande affiche les licences du site sous le numéro de série du cluster.

  Si votre cluster dispose d'une licence de site et que vous supprimez un nœud du cluster, le nœud ne dispose pas de la licence de site et il n'est plus autorisé à utiliser la fonctionnalité sous licence. Si vous ajoutez un noeud à un cluster qui possède une licence de site, le noeud a automatiquement droit à la fonctionnalité accordée par la licence de site.

- Licence d'évaluation (`demo`)

  Une licence d'évaluation est une licence temporaire qui expire après une certaine période (indiquée par le `system license show` commande). Il vous permet d'essayer certaines fonctionnalités logicielles sans avoir à acheter un droit. Il s'agit d'une licence à l'échelle du cluster, qui n'est pas liée à un numéro de série spécifique d'un nœud.

  Si votre cluster dispose d'une licence d'évaluation pour un package et que vous supprimez un nœud du cluster, celui-ci ne supporte pas la licence d'évaluation.

Méthode sous licence

Il est possible d'installer une licence au niveau du cluster (`site` ou `demo` type) et une licence verrouillée par nœud (`license` type) pour un package. Par conséquent, un package installé peut avoir plusieurs types de licence au sein du cluster. Cependant, pour le cluster, il n'y a qu'une seule méthode *licensed* pour un package. Le `licensed method` champ du `system license status show` commande affiche le droit utilisé pour le pack. La commande détermine la méthode sous licence comme suit :

- Si un pack ne comporte qu'un seul type de licence installé dans le cluster, le type de licence installé est la méthode sous licence.

- Si aucune licence n'est installée dans le pack, la méthode sous licence est `none`.
- Si plusieurs types de licence sont installés sur un package, la méthode sous licence est déterminée dans l'ordre de priorité suivant du type de licence :-`site`, `license`, et `demo`.

  Par exemple :

  - Si vous disposez d'une licence de site, d'une licence standard et d'une licence d'évaluation pour un package, la méthode sous licence pour le package du cluster est `site`.
  - Si vous disposez d'une licence standard et d'une licence d'évaluation pour un package, la méthode sous licence pour le package du cluster est `license`.
  - Si vous ne disposez que d'une licence d'évaluation pour un package, la méthode sous licence pour le package du cluster est `demo`.

Commandes de gestion des licences

Vous utilisez le `system license` commandes permettant de gérer les licences des fonctions pour le cluster. Vous utilisez le `system feature-usage` commandes permettant de contrôler l'utilisation des fonctions.

Les fonctions que vous recherchez…	Utilisez cette commande…
Ajoutez une ou plusieurs licences	`system license add`
Affiche des informations sur les licences installées, par exemple : • Nom et description du package de licences • Type de licence (`site`, `license`, ou `demo`) • Date d'expiration, le cas échéant • Les clusters ou nœuds pour lesquels une licence est accordée par un pack • Indique si la licence a été installée avant Data ONTAP 8.2 (`legacy`) • ID client	`system license show` Certaines informations s'affichent uniquement lorsque vous utilisez le `-instance` paramètre.
Afficher tous les packages qui requièrent des licences et leur état actuel de licence, y compris les éléments suivants : • Nom du package • La méthode sous licence • La date d'expiration, le cas échéant	`system license status show`
Supprimez la licence d'un pack du cluster ou d'un nœud dont vous avez spécifié le numéro de série	`system license delete`

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher ou supprimer les licences expirées ou inutilisées	`system license clean-up`
Affiche un récapitulatif de l'utilisation des fonctionnalités dans le cluster par nœud	`system feature-usage show-summary`
Affiche l'état d'utilisation de la fonction dans le cluster par nœud et par semaine	`system feature-usage show-history`
Affiche l'état du risque de droit de licence pour chaque package de licences	`system license entitlement-risk show` Certaines informations s'affichent uniquement lorsque vous utilisez le `-detail` et `-instance` paramètres.

Informations associées

"Commandes de ONTAP 9"

Gérer les tâches et les plannings

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

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.

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	`job show`
Affiche des informations sur les travaux par nœud	`job show bynode`
Affiche des informations sur les travaux affiliés à un cluster	`job show-cluster`
Affiche des informations sur les tâches terminées	`job show-completed`
Affiche des informations sur l'historique des travaux	`job history show` 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	`job private show` (niveau de privilège avancé)
Affiche des informations sur les travaux privés terminés	`job private show-completed` (niveau de privilège avancé)
Affiche des informations sur l'état d'initialisation des gestionnaires de travaux	`job initstate show` (niveau de privilège avancé)
Surveiller la progression d'une tâche	`job watch-progress`
Surveiller la progression d'un travail privé	`job private watch-progress` (niveau de privilège avancé)
Interrompre un travail	`job pause`
Interrompre un travail privé	`job private pause` (niveau de privilège avancé)
Reprendre un travail en pause	`job resume`

Les fonctions que vous recherchez…	Utilisez cette commande…
Reprendre un travail privé en pause	`job private resume` (niveau de privilège avancé)
Arrêter un travail	`job stop`
Arrêter un travail privé	`job private stop` (niveau de privilège avancé)
Supprimer un travail	`job delete`
Supprimer un travail privé	`job private delete` (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	`job unclaim` (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	`job schedule show`
Affiche la liste des travaux par planning	`job schedule show-jobs`

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur les planifications cron	`job schedule cron show`
Affiche des informations sur les plannings d'intervalles	`job schedule interval show`
Créez une planification cron[1]	`job schedule cron create`
Créer un planning d'intervalles	`job schedule interval create` Vous devez spécifier au moins un des paramètres suivants : `-days`, `-hours`, `-minutes`, ou `-seconds`.
Modifier une planification cron	`job schedule cron modify`
Modifier un planning d'intervalles	`job schedule interval modify`
Supprimer un planning	`job schedule delete`
Supprimez une planification cron	`job schedule cron delete`
Supprimer un planning d'intervalles	`job schedule interval delete`

[1]à partir de ONTAP 9.10.1, lorsque vous créez un programme de travaux à l'aide du `job schedule cron create` Commande, vous pouvez inclure le vServer dans votre planification de tâches.

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".

Gérer les sauvegardes de configuration

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.

Pour les clusters à un seul nœud (y compris les systèmes Data ONTAP Edge), vous pouvez spécifier la destination de sauvegarde de configuration lors de la configuration du logiciel. Une fois l'installation effectuée, ces paramètres peuvent être modifiés à l'aide des commandes ONTAP.

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…
Modifiez les paramètres d'un planning de sauvegarde de configuration : • 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	`system configuration backup settings modify` Lorsque vous utilisez HTTPS dans l'URL distante, utilisez le `-validate-certification` option permettant d'activer ou de désactiver la validation de certificats numériques. La validation du certificat est désactivée par défaut. 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.
Définissez le mot de passe à utiliser pour vous connecter à l'URL distante	`system configuration backup settings set-password`
Afficher les paramètres du programme de sauvegarde de la configuration	`system configuration backup settings show` Vous définissez le `-instance` paramètre pour afficher le nom d'utilisateur et le nombre de sauvegardes à conserver pour chaque planning.

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…
Créer un nouveau fichier de sauvegarde de configuration de nœud ou de cluster	`system configuration backup create`
Copiez un fichier de sauvegarde de configuration d'un nœud vers un autre nœud du cluster	`system configuration backup copy`

Les fonctions que vous recherchez…	Utilisez cette commande…
Charger un fichier de sauvegarde de configuration à partir d'un nœud du cluster vers une URL distante (FTP, HTTP, HTTPS, TFTP ou FTPS)	`system configuration backup upload` Lorsque vous utilisez HTTPS dans l'URL distante, utilisez le `-validate-certification` option permettant d'activer ou de désactiver la validation de certificats numériques. La validation du certificat est désactivée par défaut. 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.
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	`system configuration backup download` Lorsque vous utilisez HTTPS dans l'URL distante, utilisez le `-validate-certification` option permettant d'activer ou de désactiver la validation de certificats numériques. La validation du certificat est désactivée par défaut.
Renommez un fichier de sauvegarde de configuration sur un nœud du cluster	`system configuration backup rename`
Afficher les fichiers de sauvegarde de configuration de nœud et de cluster pour un ou plusieurs nœuds du cluster	`system configuration backup show`
Supprime un fichier de sauvegarde de configuration sur un noeud	`system configuration backup delete` 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 noeuds du cluster, il reste sur ces noeuds.

Récupération d'une configuration de nœud

Recherchez un fichier de sauvegarde de configuration à utiliser pour restaurer un noeud

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 noeud pour lequel vous devez restaurer la configuration.

Si le fichier de sauvegarde de configuration se trouve…	Alors…
Sur une URL distante	Utilisez le `system configuration backup download` commande au niveau de privilège avancé pour le télécharger sur le nœud restauré.
Sur un nœud du cluster	a. Utilisez le `system configuration backup show` 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 `system configuration backup copy` commande de copie sur le nœud restauré.

Si vous avez précédemment recréé-créé le cluster, vous devez choisir un fichier de sauvegarde de configuration qui a été créé après le récréation 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.

Restaurer une configuration de 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 `system configuration backup download` commande au niveau de privilège avancé pour le télécharger sur le nœud restauré.
Sur un nœud du cluster	a. Utilisez le `system configuration backup show` 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. 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 `system configuration backup copy` commande de copie sur le nœud restauré.

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 recréé 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-créé.

   Vous devez redémarrer les nœuds un par un.

7. Pour chaque nœud qui doit être joint au cluster recréé-créé, procédez comme suit :

   a. A partir d'un nœud sain sur le cluster recréé-créé, rrejoignez le nœud cible :

      system configuration recovery cluster rejoin -node *node_name*

      Cet exemple rejoint le nœud cible « node2 » au cluster recréé-créé :

      ```
      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

> AFF A220, AFF A800, FAS2720, FAS2750 et versions ultérieures stockent les core dumps sur leur périphérique de démarrage. Lorsque NetApp Volume Encryption (NVE) ou NetApp Storage Encryption (NSE) sont activés sur ces systèmes, le « core dump » est également chiffré.

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 »	`system node coredump config modify`
Affiche les paramètres de configuration des « core dumps »	`system node coredump config show`
Affiche les informations de base relatives aux « core dumps »	`system node coredump show`
Déclenche manuellement un « core dump » lorsque vous redémarrez un nœud	`system node reboot` avec les deux `-dump` et `-skip-lif-migration` paramètres
Déclenche manuellement un « core dump » lorsque vous arrêtez un nœud	`system node halt` avec les deux `-dump` et `-skip-lif-migration` paramètres
Enregistrer un « core dump » spécifié	`system node coredump save`
Enregistrez tous les « core dumps » non enregistrés sur un nœud spécifié	`system node coredump save-all`
Générez et envoyez un message AutoSupport avec un fichier « core dump » que vous spécifiez	`system node autosupport invoke-core-upload` Le `-uri` Le paramètre facultatif indique une destination alternative pour le message AutoSupport.
Affiche les informations d'état relatives aux « core dumps »	`system node coredump status`
Supprime un « core dump » spécifié	`system node coredump delete`
Supprimez tous les « core dumps » non enregistrés ou tous les fichiers « core » enregistrés sur un nœud	`system node coredump delete-all`
Affiche les rapports de vidage de mémoire de l'application	`system node coredump reports show`

Les fonctions que vous recherchez…	Utilisez cette commande…
Supprimer un rapport de vidage de mémoire de l'application	`system node coredump reports delete`

Informations associées

"Commandes de ONTAP 9"

Surveillance d'un système de stockage

Utilisez AutoSupport et Active IQ Digital Advisor

Le composant AutoSupport de ONTAP collecte les données de télémétrie et les envoie pour analyse. Le conseiller digital Active IQ analyse les données d'AutoSupport et fournit un support proactif et une optimisation. Avec l'intelligence artificielle, Active IQ peut identifier les problèmes potentiels et vous aider à les résoudre avant qu'ils n'affectent votre activité.

Active IQ vous permet d'optimiser votre infrastructure de données dans l'ensemble de votre cloud hybride grâce à un portail cloud et à une application mobile qui offrent des analyses prédictives et un support proactif. Les informations et les recommandations basées sur les données de Active IQ sont accessibles à tous les clients NetApp qui possèdent un contrat SupportEdge actif (les fonctionnalités varient selon le produit et le niveau de support).

Voici quelques avantages que vous pouvez faire avec Active IQ :

- Planification des mises à niveau. Active IQ identifie les problèmes qui peuvent être résolus dans votre environnement en effectuant une mise à niveau vers la plus récente version d'ONTAP et le composant Upgrade Advisor vous aide à planifier une mise à niveau réussie.
- Voir le bien-être du système. Votre tableau de bord Active IQ signale tout problème éventuel et vous aide à le corriger. Surveillez la capacité du système pour vous assurer que votre espace de stockage est insuffisant. Consultez les dossiers de demande de support de votre système.
- Gestion des performances. Active IQ affiche les performances du système sur une période plus longue que ce que vous pouvez voir dans System Manager. Identifiez les problèmes de configuration et de système qui ont un impact sur les performances.
- Optimisez l'efficacité. Affichez les mesures de l'efficacité du stockage et identifiez des moyens de stocker plus de données dans moins d'espace.
- Voir l'inventaire et la configuration. Active IQ affiche des informations complètes sur l'inventaire et la configuration logicielle et matérielle. Voyez quand les contrats de service arrivent à expiration et renouvelez-les pour vous assurer que vous restez pris en charge.

Informations associées

"Documentation NetApp : conseiller digital Active IQ"

"Lancez Active IQ"

"Services SupportEdge"

Gérez les paramètres AutoSupport avec System Manager

System Manager permet d'afficher et de modifier les paramètres de votre compte AutoSupport.

Vous pouvez effectuer les opérations suivantes :

- Afficher les paramètres AutoSupport
- Générez et envoyez des données AutoSupport
- Testez la connexion à AutoSupport
- Activez ou désactivez le protocole AutoSupport
- Supprimez la génération des dossiers de demande de support
- Reprendre la génération des dossiers de demande de support
- Modifier les paramètres AutoSupport

Afficher les paramètres AutoSupport

Vous pouvez utiliser System Manager pour afficher les paramètres de votre compte AutoSupport.

Étapes

1. Dans System Manager, cliquez sur **Cluster > Paramètres**.

   Dans la section **AutoSupport**, les informations suivantes sont affichées :

   - État
   - Protocole de transport
   - Serveur proxy
   - De l'adresse e-mail
2. Dans la section **AutoSupport**, cliquez sur ⋮, Puis cliquez sur **plus d'options**.

   Des informations supplémentaires s'affichent sur la connexion AutoSupport et les paramètres de messagerie. De plus, l'historique des transferts de messages est répertorié.

Générez et envoyez des données AutoSupport

Dans System Manager, vous pouvez lancer la génération de messages AutoSupport et choisir entre le nœud de cluster ou les nœuds où les données sont collectées.

Étapes

1. Dans System Manager, cliquez sur **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, cliquez sur ⋮, Puis cliquez sur **générer et Envoyer**.
3. Saisissez un objet.
4. Cliquez sur la case à cocher sous **Collect Data from** pour spécifier les nœuds à partir desquels les données doivent être collectées.

Testez la connexion à AutoSupport

Depuis System Manager, vous pouvez envoyer un message de test pour vérifier la connexion à AutoSupport.

Étapes

1. Dans System Manager, cliquez sur **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, cliquez sur ⋮, Puis cliquez sur **Tester la connectivité**.
3. Saisissez un objet pour le message.

Activez ou désactivez le protocole AutoSupport

Dans System Manager, vous pouvez désactiver la fonction AutoSupport de surveillance de l'état de santé de votre système de stockage et vous envoyer des messages de notification. Vous pouvez à nouveau activer AutoSupport après sa désactivation.

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, cliquez sur ⋮, Puis cliquez sur **Désactiver**.
3. Si vous souhaitez à nouveau activer AutoSupport, dans la section **AutoSupport**, cliquez sur ⋮, Puis cliquez sur **Activer**.

Supprimez la génération des dossiers de demande de support

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour envoyer une demande à AutoSupport afin de supprimer la génération des dossiers de demande de support.

Description de la tâche

Pour supprimer la génération de dossiers de demande de support, vous spécifiez les nœuds et le nombre d'heures pour lesquels la suppression doit avoir lieu.

La suppression de dossiers de demande de support peut être particulièrement utile si vous ne souhaitez pas que AutoSupport crée des dossiers automatisés pendant que vous effectuez la maintenance de vos systèmes.

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, cliquez sur ⋮, Puis cliquez sur **Supress support case Generation**.
3. Saisissez le nombre d'heures pendant lesquelles vous souhaitez que la suppression se produise.
4. Sélectionnez les nœuds pour lesquels vous souhaitez que la suppression se produise.

Reprendre la génération des dossiers de demande de support

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour reprendre la génération d'demandes de support avec AutoSupport si elles ont été supprimées.

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, cliquez sur ⋮, Puis cliquez sur **reprendre la génération de cas de support**.
3. Sélectionnez les nœuds pour lesquels vous souhaitez que la génération reprenne.

Modifier les paramètres AutoSupport

System Manager permet de modifier les paramètres de connexion et de messagerie de votre compte AutoSupport.

Étapes

1. Cliquez sur **Cluster > Paramètres**.
2. Dans la section **AutoSupport**, cliquez sur ⋮, Puis cliquez sur **plus d'options**.
3. Dans la section **connexions** ou **Email**, cliquez sur Edit pour modifier le paramètre de l'une des sections.

Gérez AutoSupport avec l'interface de ligne de commandes

Présentation de Manage AutoSupport

AutoSupport est un mécanisme qui surveille de manière proactive l'état de votre système et envoie automatiquement des messages au support technique NetApp, à votre organisation de support interne et à un partenaire de support. Bien que les messages AutoSupport au support technique soient activés par défaut, vous devez définir les options correctes et disposer d'un hôte de messagerie valide pour que les messages soient envoyés à votre service de support interne.

Seul l'administrateur du cluster peut effectuer la gestion AutoSupport. L'administrateur du SVM (Storage Virtual machine) n'a pas accès à AutoSupport.

L'option AutoSupport est activée par défaut lorsque vous configurez votre système de stockage pour la première fois. L'AutoSupport envoie des messages au support technique sous 24 heures après l'activation de AutoSupport. Vous pouvez réduire cette période de 24 heures en mettant à niveau ou en restaurer le système, en modifiant la configuration AutoSupport ou en modifiant l'heure du système pour une période différente de 24 heures.

> ⓘ Vous pouvez désactiver AutoSupport à tout moment, mais vous devez l'activer. L'activation d'AutoSupport peut considérablement accélérer l'identification et la résolution des problèmes sur votre système de stockage. Par défaut, le système collecte les informations AutoSupport et les stocke localement, même si vous désactivez AutoSupport.

Pour en savoir plus sur AutoSupport, consultez le site de support NetApp.

Informations associées

- "Support NetApp"
- "Pour en savoir plus sur les commandes AutoSupport, consultez l'interface de ligne de commandes de ONTAP"

Quand et où les messages AutoSupport sont envoyés

AutoSupport envoie des messages à différents destinataires, en fonction du type de message. Savoir où et quand envoyer des messages AutoSupport peut vous aider à comprendre les messages que vous recevez par e-mail ou consultez le site Web Active IQ (anciennement My AutoSupport).

Sauf indication contraire, les paramètres dans les tableaux suivants sont des paramètres de l' `system node autosupport modify` commande.

Messages déclenchés par des événements

Lorsque des événements se produisent sur le système qui nécessitent une action corrective, AutoSupport envoie automatiquement un message déclenché par un événement.

Lorsque le message est envoyé	Où le message est envoyé
AutoSupport répond à un événement de déclenchement dans l'EMS	Adresses spécifiées dans `-to` et `-noteto`. (Seuls les événements critiques affectant le service sont envoyés.) Adresses spécifiées dans `-partner-address` Support technique, si `-support` est défini sur `enable`

Messages programmés

AutoSupport envoie automatiquement plusieurs messages selon un calendrier normal.

Lorsque le message est envoyé	Où le message est envoyé
Quotidien (par défaut, envoyé entre 12 h 00 et 1:00 en tant que message de journal)	Adresses spécifiées dans `-partner-address` Support technique, si `-support` est défini sur `enable`
Quotidien (par défaut, envoyé entre 12 h 00 et 1:00 comme un message de performance), si le `-perf` le paramètre est défini sur `true`	Adresses spécifiées dans -adresse-partenaire» Support technique, si `-support` est défini sur `enable`
Hebdomadaire (par défaut, envoyé le dimanche entre 12 h 00 et 1 h 00)	Adresses spécifiées dans `-partner-address` Support technique, si `-support` est défini sur `enable`

Messages déclenchés manuellement

Vous pouvez lancer ou renvoyer manuellement un message AutoSupport.

Lorsque le message est envoyé	Où le message est envoyé
Vous lancez manuellement un message à l'aide de `system node autosupport invoke` commande	Si un URI est spécifié à l'aide de `-uri` paramètre dans le `system node autosupport invoke` Commande, le message est envoyé à cet URI. Si `-uri` est omis, le message est envoyé aux adresses spécifiées dans `-to` et `-partner -address`. Le message est également envoyé au support technique si `-support` est défini sur `enable`.
Vous lancez manuellement un message à l'aide de `system node autosupport invoke-core-upload` commande	Si un URI est spécifié à l'aide de `-uri` paramètre dans le `system node autosupport invoke-core-upload` Commande, le message est envoyé à cet URI, et le fichier core dump est chargé sur l'URI. Si `-uri` est omis dans le `system node autosupport invoke-core-upload` commande, le message est envoyé au support technique et le fichier « core dump » est chargé sur le site du support technique. Cela est nécessaire dans les deux cas `-support` est défini sur `enable` et `-transport` est défini sur `https` ou `http`. En raison de la grande taille des fichiers core dump, le message n'est pas envoyé aux adresses spécifiées dans l' `-to` et `-partner-addresses` paramètres.
Vous lancez manuellement un message à l'aide de `system node autosupport invoke-performance-archive` commande	Si un URI est spécifié à l'aide de `-uri` paramètre dans le `system node autosupport invoke-performance-archive` Commande, le message est envoyé à cet URI, et le fichier d'archive de performances est chargé dans l'URI. Si `-uri` est omis dans le `system node autosupport invoke-performance-archive`, le message est envoyé au support technique et le fichier d'archive de performances est chargé sur le site de support technique. Cela est nécessaire dans les deux cas `-support` est défini sur `enable` et `-transport` est défini sur `https` ou `http`. En raison de la taille importante des fichiers d'archivage de performances, le message n'est pas envoyé aux adresses spécifiées dans l' `-to` et `-partner-addresses` paramètres.

Lorsque le message est envoyé	Où le message est envoyé
Vous renvoyez manuellement un message précédent à l'aide de `system node autosupport history retransmit` commande	Uniquement à l'URI que vous spécifiez dans le `-uri` paramètre du `system node autosupport history retransmit` commande

Messages déclenchés par le support technique

Le support technique peut demander des messages à AutoSupport avec la fonction AutoSupport OnDemand.

Lorsque le message est envoyé	Où le message est envoyé
Quand AutoSupport obtient les instructions de livraison pour générer de nouveaux messages AutoSupport	Adresses spécifiées dans `-partner-address` Support technique, si `-support` est défini sur `enable` et `-transport` est défini sur `https`
Quand AutoSupport obtient des instructions de livraison pour renvoyer les messages AutoSupport précédents	Support technique, si `-support` est défini sur `enable` et `-transport` est défini sur `https`
Quand AutoSupport obtient des instructions de livraison pour générer de nouveaux messages AutoSupport qui chargent des fichiers core dump ou d'archivage des performances	Support technique, si `-support` est défini sur `enable` et `-transport` est défini sur `https`. Le fichier « core dump » ou d'archivage des performances est téléchargé sur le site du support technique.

Comment AutoSupport crée et envoie des messages déclenchés par des événements

AutoSupport crée des messages AutoSupport déclenchés par les événements lorsque le système EMS traite un événement déclencheur. Un message AutoSupport déclenché par un événement alerte les destinataires des problèmes qui requièrent une action corrective et ne contient que des informations pertinentes pour le problème. Vous pouvez personnaliser le contenu à inclure et qui reçoit les messages.

AutoSupport utilise le processus suivant pour créer et envoyer des messages AutoSupport déclenchés par les événements :

1. Lorsque l'EMS traite un événement déclencheur, EMS envoie une requête à AutoSupport.

   Un événement déclencheur est un événement EMS avec une destination AutoSupport et un nom commençant par un `callhome.` préfixe.

2. AutoSupport crée un message AutoSupport déclenché par un événement.

   AutoSupport collecte des informations de base et de dépannage des sous-systèmes associés au déclencheur afin de créer un message contenant uniquement les informations pertinentes pour l'événement de déclenchement.

   Un ensemble de sous-systèmes par défaut est associé à chaque déclencheur. Cependant, vous pouvez

choisir d'associer des sous-systèmes supplémentaires à un déclencheur en utilisant le `system node autosupport trigger modify` commande.

3. AutoSupport envoie le message AutoSupport déclenché par l'événement aux destinataires définis par le `system node autosupport modify` commande avec `-to`, `-noteto`, `-partner-address`, et `-support` paramètres.

   Vous pouvez activer et désactiver la transmission de messages AutoSupport pour des déclencheurs spécifiques à l'aide de la `system node autosupport trigger modify` commande avec `-to` et `-noteto` paramètres.

Exemple de données envoyées pour un événement spécifique

Le `storage shelf PSU failed` L'événement EMS déclenche un message contenant des données de base provenant des fichiers obligatoires, journaux, stockage, RAID, HA, Sous-systèmes de plate-forme et de mise en réseau et données de dépannage des sous-systèmes obligatoire, fichiers journaux et stockage.

Vous souhaitez inclure des données à propos de NFS dans tout message AutoSupport envoyé en réponse à une future `storage shelf PSU failed` événement. Vous entrez la commande suivante pour activer les données de dépannage de NFS pour le `callhome.shlf.ps.fault` événement :

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Notez que le `callhome.` le préfixe est supprimé du `callhome.shlf.ps.fault` événement lorsque vous utilisez le `system node autosupport trigger` Commandes ou lorsqu'elles sont référencées par des événements AutoSupport et EMS dans l'interface de ligne de commande.

Types de messages AutoSupport et leur contenu

Les messages AutoSupport contiennent des informations d'état sur les sous-systèmes pris en charge. Découvrez ce que contiennent les messages AutoSupport pour vous aider à interpréter les messages que vous recevez par e-mail ou à consulter sur le site Web Active IQ (anciennement My AutoSupport).

Type de message	Type de données que le message contient
Événement déclenché	Fichiers contenant des données contextuelles sur le sous-système spécifique où l'événement s'est produit
Tous les jours	Fichiers journaux
Performance	Données de performance échantillonnées au cours des 24 heures précédentes
Hebdomadaire	Données de configuration et d'état

Type de message	Type de données que le message contient
Déclenché par le `system node autosupport invoke` commande	Dépend de la valeur spécifiée dans `-type` paramètre : • `test` envoie un message déclenché par l'utilisateur avec certaines données de base. Ce message déclenche également une réponse automatique par e-mail du support technique à toutes les adresses e-mail spécifiées, à l'aide du `-to` Pour confirmer la réception des messages AutoSupport. • `performance` envoie des données de performance. • `all` envoie un message déclenché par l'utilisateur avec un ensemble complet de données similaires au message hebdomadaire, y compris les données de dépannage de chaque sous-système. L'assistance technique demande généralement ce message.
Déclenché par le `system node autosupport invoke-core-upload` commande	Fichiers core dump d'un nœud
Déclenché par le `system node autosupport invoke-performance-archive` commande	Fichiers d'archivage des performances pendant une période donnée
Déclenché par AutoSupport OnDemand	AutoSupport OnDemand peut demander de nouveaux messages ou des messages antérieurs : • Les nouveaux messages, selon le type de collection AutoSupport, peuvent être `test`, `all`, ou `performance`. • Les messages antérieurs dépendent du type de message renvoyé. AutoSupport OnDemand peut demander la création de nouveaux messages qui chargent les fichiers suivants sur le site de support NetApp à l'adresse "mysupport.netapp.com": • « Core dump » • Archivage des performances

Nature des sous-systèmes AutoSupport

Chaque sous-système fournit des informations de base et de dépannage utilisées par AutoSupport pour ses messages. Chaque sous-système est également associé aux événements de déclenchement qui permettent à AutoSupport de collecter uniquement à partir des informations pertinentes pour l'événement de déclenchement.

AutoSupport collecte du contenu sensible au contexte. Vous pouvez afficher des informations sur les sous-systèmes et déclencher des événements à l'aide du `system node autosupport trigger show` commande.

Taille et budgets de temps des AutoSupport

AutoSupport collecte des informations, organisées par sous-système, et applique une taille et un budget consacré au contenu pour chaque sous-système. Face à la croissance des systèmes de stockage, les budgets AutoSupport assurent un contrôle de la charge utile AutoSupport, ce qui assure une livraison évolutive des données AutoSupport.

AutoSupport cesse de collecter des informations et de tronquer AutoSupport le contenu du sous-système si sa taille ou son budget. Si le contenu ne peut pas être facilement tronqué (par exemple, les fichiers binaires), AutoSupport omet le contenu.

Vous devez modifier la taille et les budgets par défaut uniquement si le support NetApp vous y invite. Vous pouvez également consulter la taille et les budgets de temps par défaut des sous-systèmes en utilisant le `autosupport manifest show` commande.

Fichiers envoyés dans des messages AutoSupport déclenchés par un événement

Les messages AutoSupport déclenchés par des événements contiennent uniquement des informations de base et de dépannage des sous-systèmes associés à l'événement qui a généré AutoSupport le message. Ses données spécifiques aident les partenaires de support et les équipes de support NetApp à résoudre le problème.

AutoSupport utilise les critères suivants pour contrôler le contenu des messages AutoSupport déclenchés par les événements :

- Quels sous-systèmes sont inclus

  Les données sont regroupées en sous-systèmes, y compris les sous-systèmes communs, tels que les fichiers journaux et certains sous-systèmes, tels que RAID. Chaque événement déclenche un message contenant uniquement les données des sous-systèmes spécifiques.

- Niveau de détail de chaque sous-système inclus

  Les données de chaque sous-système inclus sont fournies au niveau de base ou de dépannage.

Vous pouvez afficher tous les événements possibles et déterminer quels sous-systèmes sont inclus dans les messages relatifs à chaque événement à l'aide du `system node autosupport trigger show` commande avec `-instance` paramètre.

En plus des sous-systèmes inclus par défaut pour chaque événement, vous pouvez ajouter des sous-systèmes supplémentaires à un niveau de base ou de dépannage à l'aide de l' `system node autosupport`

`trigger modify` commande.

Fichiers journaux envoyés dans les messages AutoSupport

Les messages AutoSupport peuvent contenir plusieurs fichiers journaux clés qui permettent au personnel du support technique de revoir l'activité récente du système.

Tous les types de messages AutoSupport peuvent inclure les fichiers journaux suivants lorsque le sous-système fichiers journaux est activé :

Fichier journal	Quantité de données incluses dans le fichier
• Fichiers journaux à partir du `/mroot/etc/log/mlog/` répertoire • Le fichier journal DES MESSAGES	Seules les nouvelles lignes ajoutées aux journaux depuis le dernier message AutoSupport jusqu'à un maximum spécifié. Cela permet de s'assurer que les messages AutoSupport disposent de données uniques et pertinentes, sans chevauchement. (Les fichiers journaux des partenaires font exception. Pour les partenaires, le nombre maximal de données autorisé est inclus.)
• Fichiers journaux à partir du `/mroot/etc/log/shelflog/` répertoire • Fichiers journaux à partir du `/mroot/etc/log/acp/` répertoire • Données de journal du système de gestion des événements (EMS)	Les lignes de données les plus récentes jusqu'à un maximum spécifié.

Le contenu des messages AutoSupport peut changer de version d'ONTAP.

Fichiers envoyés dans des messages AutoSupport hebdomadaires

Les messages hebdomadaires AutoSupport contiennent des données supplémentaires sur la configuration et l'état, ce qui est utile pour suivre les modifications apportées à votre système au fil du temps.

Les informations suivantes sont envoyées dans des messages AutoSupport hebdomadaires :

- Informations de base sur chaque sous-système
- Contenu de sélectionné `/mroot/etc` fichiers de répertoire
- Fichiers journaux
- Résultat des commandes fournissant les informations système
- Informations supplémentaires, notamment les informations des bases de données répliquées – RDB –, les statistiques des services et bien plus encore

Comment AutoSupport OnDemand obtient des instructions de livraison auprès du support technique

AutoSupport OnDemand communique régulièrement avec le support technique pour

obtenir des instructions de livraison pour envoyer, renvoyer et refuser des messages AutoSupport, et pour télécharger des fichiers volumineux vers le site du support NetApp. AutoSupport OnDemand permet d'envoyer des messages AutoSupport à la demande au lieu d'attendre l'exécution de la tâche AutoSupport hebdomadaire.

AutoSupport OnDemand comprend les composants suivants :

- Client AutoSupport OnDemand qui s'exécute sur chaque nœud
- Service AutoSupport OnDemand qui réside dans le support technique

Le client AutoSupport OnDemand interroge régulièrement le service AutoSupport OnDemand afin d'obtenir des instructions de livraison du support technique. Par exemple, le support technique peut utiliser le service AutoSupport OnDemand pour demander la génération d'un nouveau message AutoSupport. Lorsque le client AutoSupport OnDemand interroge le service AutoSupport OnDemand, le client obtient les instructions de livraison et envoie le nouveau message AutoSupport à la demande.

AutoSupport OnDemand est activé par défaut. Cependant, AutoSupport OnDemand dépend de certains paramètres AutoSupport pour continuer à communiquer avec le support technique. AutoSupport OnDemand communique automatiquement avec le support technique lorsque les exigences suivantes sont respectées :

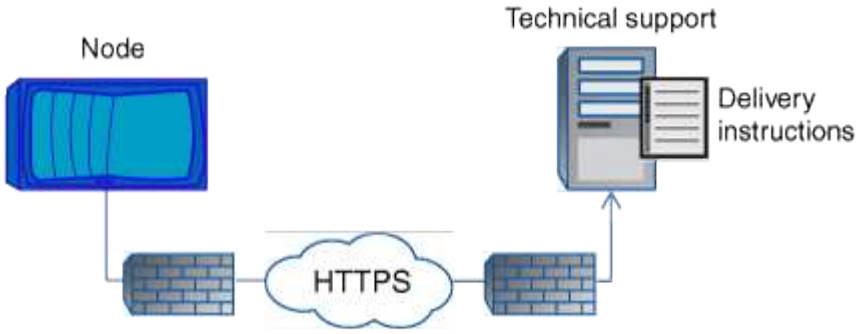
- AutoSupport est activé.
- AutoSupport est configuré pour envoyer des messages au support technique.
- AutoSupport est configuré pour utiliser le protocole de transport HTTPS.

Le client AutoSupport OnDemand envoie des demandes HTTPS au même emplacement de support technique auquel les messages AutoSupport sont envoyés. Le client AutoSupport OnDemand n'accepte pas les connexions entrantes.

AutoSupport OnDemand utilise le compte utilisateur « AutoSupport » pour communiquer avec le support technique. ONTAP vous empêche de supprimer ce compte.

Si vous souhaitez désactiver AutoSupport OnDemand mais que AutoSupport est toujours activé, utilisez la commande : LINK:https://docs.netapp.com/us-en/ontap-cli-95/system-node-autosupport-modify.html#parameters[`system node autosupport modify -ondemand-state disable`].

L'illustration suivante montre comment AutoSupport OnDemand envoie des demandes HTTPS au support technique pour obtenir des instructions de livraison.



Les instructions de livraison peuvent inclure des demandes pour que AutoSupport puisse faire ce qui suit :

- Générer de nouveaux messages AutoSupport.

Le support technique peut demander de nouveaux messages AutoSupport pour vous aider à trier les problèmes.

- Générer de nouveaux messages AutoSupport qui chargent les fichiers « core dump » ou les fichiers d'archivage des performances sur le site de support NetApp.

  Le support technique peut demander des fichiers « core dump » ou d'archivage des performances afin de gérer les problèmes urgents.

- Retransmettre les messages AutoSupport générés précédemment.

  Cette demande se produit automatiquement si aucun message n'a été reçu en raison d'un échec de livraison.

- Désactiver la distribution des messages AutoSupport pour des événements déclencheurs spécifiques.

  Le support technique peut désactiver la livraison de données non utilisées.

Structure des messages AutoSupport envoyés par e-mail

Lorsqu'un message AutoSupport est envoyé par e-mail, le message a un objet standard, un corps bref et une pièce jointe de grande taille au format de fichier 7z qui contient les données.

> Si AutoSupport est configuré pour masquer les données privées, certaines informations, telles que le nom d'hôte, sont omises ou masquées dans l'en-tête, le sujet, le corps et les pièces jointes.

Objet

La ligne d'objet des messages envoyés par le mécanisme AutoSupport contient une chaîne de texte qui identifie la raison de la notification. Le format de la ligne d'objet est le suivant :

Notification de groupe HA de *System_Name* (*message*) *Severity*

- *System_Name* est le nom d'hôte ou l'ID système, selon la configuration AutoSupport

Corps

Le corps du message AutoSupport contient les informations suivantes :

- Date et heure du message
- Version de ONTAP sur le nœud qui a généré le message
- L'ID du système, le numéro de série et le nom d'hôte du nœud qui a généré le message
- Numéro de séquence AutoSupport
- Localisation et nom du contact SNMP, si spécifiés
- ID système et nom d'hôte du nœud partenaire HA

Fichiers joints

Les informations clés d'un message AutoSupport sont contenues dans des fichiers compressés dans un fichier

7z appelé `body.7z` et joints au message.

Les fichiers contenus dans la pièce jointe sont spécifiques au type de message AutoSupport.

Types de gravité AutoSupport

Les messages AutoSupport ont des types de gravité qui vous aident à comprendre l'objet de chaque message : par exemple, pour attirer l'attention immédiate sur un problème d'urgence ou uniquement pour fournir des informations.

Les messages ont l'un des niveaux de gravité suivants :

- **Alerte** : les messages d'alerte indiquent qu'un événement de niveau supérieur peut se produire si vous ne prenez pas d'action.

  Vous devez prendre une action contre les messages d'alerte dans les 24 heures.

- **Urgence** : les messages d'urgence sont affichés lorsqu'une interruption s'est produite.

  Vous devez agir immédiatement contre les messages d'urgence.

- **Erreur** : les conditions d'erreur indiquent ce qui peut se produire si vous ignorez.
- **Avis** : condition normale mais significative.
- **Info**: Message d'information fournit des détails sur le problème, que vous pouvez ignorer.
- **Debug** : les messages au niveau du débogage fournissent des instructions que vous devez effectuer.

Si votre service de support interne reçoit des messages AutoSupport par e-mail, la gravité apparaît dans l'objet de l'e-mail.

Conditions requises pour utiliser AutoSupport

Nous vous recommandons d'utiliser HTTPS pour la distribution des messages AutoSupport afin d'assurer une sécurité optimale et de prendre en charge toutes les dernières fonctionnalités d'AutoSupport. Bien que AutoSupport prenne en charge les protocoles HTTP et SMTP pour la distribution des messages AutoSupport, HTTPS est recommandé.

Protocoles pris en charge

Tous ces protocoles s'exécutent sur IPv4 ou IPv6, en fonction de la famille d'adresses à laquelle le nom résout.

Protocole et port	Description
HTTPS sur le port 443	Il s'agit du protocole par défaut. Vous devez l'utiliser autant que possible. Ce protocole prend en charge AutoSupport OnDemand et les téléchargements de fichiers volumineux. Le certificat du serveur distant est validé par rapport au certificat racine, sauf si vous désactivez la validation. La livraison utilise une requête PUT HTTP. Avec PUT, si la demande échoue pendant la transmission, la requête redémarre là où elle s'est arrêtée. Si le serveur qui reçoit la requête ne prend pas en charge PUT, la livraison utilise une requête HTTP POST.
HTTP sur le port 80	Ce protocole est préférable à SMTP. Ce protocole prend en charge les téléchargements de fichiers volumineux, mais pas AutoSupport OnDemand. La livraison utilise une requête PUT HTTP. Avec PUT, si la demande échoue pendant la transmission, la requête redémarre là où elle s'est arrêtée. Si le serveur qui reçoit la requête ne prend pas en charge PUT, la livraison utilise une requête HTTP POST.
SMTP sur le port 25 ou un autre port	Vous devez utiliser ce protocole uniquement si la connexion réseau n'autorise pas HTTPS ou HTTP. La valeur de port par défaut est 25, mais vous pouvez configurer AutoSupport pour utiliser un autre port. Gardez à l'esprit les limitations suivantes lorsque vous utilisez SMTP : • AutoSupport OnDemand et les téléchargements de fichiers volumineux ne sont pas pris en charge. • Les données ne sont pas chiffrées. SMTP envoie des données en clair, ce qui facilite l'interception et la lecture du texte dans le message AutoSupport. • Des limites de longueur de message et de longueur de ligne peuvent être introduites.

Si vous configurez AutoSupport avec des adresses e-mail spécifiques pour votre service de support interne ou une organisation partenaire de support, ces messages sont toujours envoyés par SMTP.

Par exemple, si vous utilisez le protocole recommandé pour envoyer des messages à l'assistance technique et que vous souhaitez également envoyer des messages à votre organisation d'assistance interne, vos messages seront transportés en utilisant respectivement HTTPS et SMTP.

AutoSupport limite la taille maximale de fichier pour chaque protocole. Le paramètre par défaut pour les transferts HTTP et HTTPS est de 25 Mo. Le paramètre par défaut pour les transferts SMTP est 5 Mo. Si la taille du message AutoSupport dépasse la limite configurée, AutoSupport livre autant de messages que possible. Vous pouvez modifier la taille maximale en modifiant la configuration AutoSupport. Voir la `system node autosupport modify` page man pour plus d'informations

> AutoSupport remplace automatiquement la limite de taille maximale des fichiers pour les protocoles HTTPS et HTTP lorsque vous générez et envoyez des messages AutoSupport qui chargent les fichiers « core dump » ou d'archivage des performances vers le site de support NetApp ou un URI spécifié. Le remplacement automatique s'applique uniquement lorsque vous téléchargez des fichiers à l'aide de l' `system node autosupport invoke-core-upload` ou le `system node autosupport invoke-performance-archive` commandes.

Configuration requise

Selon la configuration de votre réseau, l'utilisation des protocoles HTTP ou HTTPS peut nécessiter une configuration supplémentaire d'URL proxy. Si vous utilisez HTTP ou HTTPS pour envoyer des messages AutoSupport au support technique et que vous disposez d'un proxy, vous devez identifier l'URL de ce proxy. Si le proxy utilise un port autre que le port par défaut, qui est 3128, vous pouvez spécifier le port pour ce proxy. Vous pouvez également spécifier un nom d'utilisateur et un mot de passe pour l'authentification par proxy.

Si vous utilisez SMTP pour envoyer des messages AutoSupport à votre organisation de support interne ou au support technique, vous devez configurer un serveur de messagerie externe. Le système de stockage ne fonctionne pas comme un serveur de messagerie ; il nécessite un serveur de messagerie externe sur votre site pour envoyer des messages. Le serveur de messagerie doit être un hôte qui écoute sur le port SMTP (25) ou sur un autre port, et il doit être configuré pour envoyer et recevoir le codage 8 bits Multipurpose Internet Mail Extensions (MIME). Les hôtes de messagerie par exemple incluent un hôte UNIX exécutant un serveur SMTP tel que le programme sendmail et un serveur Windows exécutant le serveur Microsoft Exchange. Vous pouvez avoir un ou plusieurs hôtes de messagerie.

Configurer AutoSupport

Vous pouvez contrôler si les informations de AutoSupport sont envoyées au support technique et à votre organisation de support interne, puis tester que la configuration est correcte.

Description de la tâche

Dans les versions ONTAP 9.5 et ultérieures, vous pouvez activer AutoSupport et modifier sa configuration simultanément sur tous les nœuds du cluster. Lorsqu'un nouveau nœud rejoint le cluster, le nœud hérite automatiquement de la configuration de cluster AutoSupport. Vous n'avez pas besoin de mettre à jour la configuration séparément sur chaque nœud.

Depuis ONTAP 9.5, le champ d'application du `system node autosupport modify` la commande s'effectue au niveau du cluster. La configuration AutoSupport est modifiée sur tous les nœuds du cluster, même lorsque `-node` est spécifié. L'option est ignorée, mais elle a été conservée pour la rétrocompatibilité CLI.

Dans les versions ONTAP 9.4 et précédentes, l'étendue de la commande « system node AutoSupport modify » est propre au nœud. La configuration AutoSupport doit être modifiée sur chaque nœud de votre cluster.

Par défaut, AutoSupport est activé sur chaque nœud pour envoyer des messages au support technique via le protocole de transport HTTPS.

Étapes

1. Assurez-vous que AutoSupport est activé :

```
system node autosupport modify -state enable
```

2. Si vous souhaitez que le support technique reçoive les messages AutoSupport, utilisez la commande suivante :

```
system node autosupport modify -support enable
```

   Vous devez activer cette option si vous souhaitez permettre à AutoSupport de travailler avec AutoSupport OnDemand ou si vous souhaitez télécharger des fichiers volumineux, tels que les fichiers core dump et d'archivage des performances, vers le support technique ou une URL spécifiée.

3. Si le support technique est activé pour recevoir des messages AutoSupport, spécifiez le protocole de transport à utiliser pour les messages.

   Vous pouvez choisir parmi les options suivantes :

Les fonctions que vous recherchez…	Définissez ensuite les paramètres suivants du `system node autosupport modify` commande…
Utilisez le protocole HTTPS par défaut	a. Réglez `-transport` à `https`. b. Si vous utilisez un proxy, définissez `-proxy-url` À l'URL de votre proxy. Cette configuration prend en charge la communication avec AutoSupport OnDemand et les téléchargements de fichiers volumineux.

Utilisez HTTP préféré par rapport à SMTP	a. Réglez `-transport` à `http`. b. Si vous utilisez un proxy, définissez `-proxy-url` À l'URL de votre proxy. Cette configuration prend en charge les téléchargements de fichiers volumineux, mais pas AutoSupport OnDemand.
Utiliser SMTP	Réglez `-transport` à `smtp`. Cette configuration ne prend pas en charge AutoSupport OnDemand ni les téléchargements de fichiers volumineux.

4. Si vous souhaitez que votre service de support interne ou un partenaire de support reçoive les messages AutoSupport, effectuez les opérations suivantes :
   a. Identifiez les destinataires de votre organisation en définissant les paramètres suivants de l' `system node autosupport modify` commande :

Définir ce paramètre…	À ceci…
`-to`	Jusqu'à cinq adresses e-mail ou listes de distribution individuelles séparées par des virgules dans votre service de support interne qui recevront des messages AutoSupport clés
`-noteto`	Jusqu'à cinq adresses e-mail ou listes de distribution individuelles séparées par des virgules dans votre service d'assistance interne qui recevront une version abrégée des messages clés AutoSupport conçus pour les téléphones portables et autres appareils mobiles
`-partner-address`	Jusqu'à cinq adresses e-mail ou listes de distribution séparées par des virgules dans votre organisation partenaire de support qui recevront tous les messages AutoSupport

   b. Vérifiez que les adresses sont correctement configurées en répertoriant les destinations à l'aide de l' `system node autosupport destinations show` commande.
5. Si vous envoyez des messages à votre organisation de support interne ou si vous avez choisi le transport SMTP pour les messages au support technique, configurez SMTP en définissant les paramètres suivants de l' `system node autosupport modify` commande :
   - Réglez `-mail-hosts` à un ou plusieurs hôtes de messagerie, séparés par des virgules.

     Vous pouvez définir un maximum de cinq.

   Vous pouvez configurer une valeur de port pour chaque hôte de messagerie en spécifiant un point-virgule et un numéro de port après le nom d'hôte de messagerie : par exemple,

`mymailhost.example.com:5678`, où 5678 est le port de l'hôte de messagerie.

- Réglez `-from` À l'adresse e-mail qui envoie le message AutoSupport.

6. Configurez DNS.
7. (Facultatif) Ajouter des options de commande si vous souhaitez modifier des paramètres spécifiques :

Pour cela…	Définissez ensuite les paramètres suivants du `system node autosupport modify` commande…
Masquez des données privées en supprimant, masquant ou encodant des données sensibles dans les messages	Réglez `-remove-private-data` à `true`. Si vous changez de `false` à `true`, Tous les fichiers historiques AutoSupport et tous les fichiers associés sont supprimés.
Arrêt de l'envoi des données de performance dans des messages AutoSupport périodiques	Réglez `-perf` à `false`.

8. Vérifiez la configuration globale à l'aide du `system node autosupport show` commande avec `-node` paramètre.
9. Vérifier le fonctionnement de AutoSupport à l'aide de l' `system node autosupport check show` commande.

   Si des problèmes sont signalés, utilisez le `system node autosupport check show-details` pour afficher plus d'informations.

10. Vérifiez que les messages AutoSupport sont en cours d'envoi et de réception :

    a. Utilisez le `system node autosupport invoke` commande avec `-type` paramètre défini sur `test`.

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. Vérifiez que NetApp reçoit vos messages AutoSupport :

    l'historique de AutoSupport du nœud système affiche -node local

    Le statut du dernier message AutoSupport sortant doit finalement être défini sur `sent-successful` pour toutes les destinations de protocole appropriées.

    a. (Facultatif) Confirmez que le message AutoSupport est envoyé à votre organisation de support interne ou à votre partenaire de support en consultant l'e-mail correspondant à l'adresse que vous avez configurée pour `-to`, `-noteto`, ou `-partner-address` paramètres du `system node autosupport modify` commande.

Charger les fichiers core dump

Lorsqu'un fichier « core dump » est enregistré, un message d'événement est généré. Si le service AutoSupport est activé et configuré pour envoyer des messages au support NetApp, un message AutoSupport est transmis, ainsi qu'un e-mail de confirmation

automatique vous est envoyé.

Ce dont vous avez besoin

- Vous devez avoir configuré AutoSupport avec les paramètres suivants :
  - AutoSupport est activé sur le nœud.
  - AutoSupport est configuré pour envoyer des messages au support technique.
  - AutoSupport est configuré pour utiliser le protocole de transport HTTP ou HTTPS.

    Le protocole de transport SMTP n'est pas pris en charge lors de l'envoi de messages contenant des fichiers volumineux, tels que des fichiers de vidage de mémoire.

Description de la tâche

Vous pouvez également charger le fichier « core dump » via le service AutoSupport via HTTPS en utilisant le `system node autosupport invoke-core-upload` Si le support NetApp en a besoin.

"Télécharger un fichier vers NetApp"

Étapes

1. Afficher les fichiers « core dump » d'un nœud en utilisant le `system node coredump show` commande.

   Dans l'exemple suivant, les fichiers « core dump » sont affichés pour le nœud local :

   ```
   cluster1::> system node coredump show -node local
   Node:Type Core Name Saved Panic Time
   --------- ------------------------------------------- -----
   -----------------
   node:kernel
   core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
   ```

2. Générez un message AutoSupport et téléchargez un fichier « core dump » à l'aide de `system node autosupport invoke-core-upload` commande.

   Dans l'exemple suivant, un message AutoSupport est généré et envoyé à l'emplacement par défaut, qui est le support technique, et le fichier core dump est téléchargé vers l'emplacement par défaut, qui est le site du support NetApp :

   ```
   cluster1::> system node autosupport invoke-core-upload -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

   Dans l'exemple suivant, un message AutoSupport est généré et envoyé à l'emplacement spécifié dans l'URI, et le fichier core dump est chargé dans l'URI :

   ```
   cluster1::> system node autosupport invoke-core-upload -uri
   https//files.company.com -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

Téléchargez les fichiers d'archivage des performances

Vous pouvez générer et envoyer un message AutoSupport contenant un archivage des performances. Par défaut, le support technique NetApp reçoit le message AutoSupport, et l'archivage des performances est téléchargé sur le site du support NetApp. Vous pouvez spécifier une autre destination pour le message et le téléchargement.

Ce dont vous avez besoin

- Vous devez avoir configuré AutoSupport avec les paramètres suivants :
  - AutoSupport est activé sur le nœud.
  - AutoSupport est configuré pour envoyer des messages au support technique.
  - AutoSupport est configuré pour utiliser le protocole de transport HTTP ou HTTPS.

    Le protocole de transport SMTP n'est pas pris en charge lors de l'envoi de messages contenant des fichiers volumineux, tels que des fichiers d'archivage de performance.

Description de la tâche

Vous devez spécifier une date de début pour les données d'archive de performances que vous souhaitez télécharger. La plupart des systèmes de stockage conservent des archives de performances pendant deux semaines. Vous pouvez ainsi spécifier une date de démarrage il y a deux semaines. Par exemple, si aujourd'hui est janvier 15, vous pouvez spécifier une date de début de janvier 2.

Étape

1. Générez un message AutoSupport et téléchargez le fichier d'archivage des performances à l'aide de `system node autosupport invoke-performance-archive` commande.

   Dans l'exemple suivant, 4 heures de fichiers d'archivage des performances date du 12 janvier 2015 sont ajoutés à un message AutoSupport et téléchargés sur l'emplacement par défaut, qui est le site de support NetApp :

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   Dans l'exemple suivant, 4 heures de fichiers d'archive de performances à partir du 12 janvier 2015 sont ajoutés à un message AutoSupport et chargés à l'emplacement spécifié par l'URI :

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h -uri
   https://files.company.com
   ```

Lire les descriptions de messages AutoSupport

Les descriptions des messages AutoSupport que vous recevez sont disponibles via le convertisseur Syslog ONTAP.

Étapes

1. Accédez au "Traducteur syslog".
2. Dans le champ **version**, entrez la version de ONTAP que vous utilisez. Dans le champ **Search String**, entrez « callhome ». Sélectionnez **Translate**.
3. Syslog Translator répertorie par ordre alphabétique tous les événements correspondant à la chaîne de message que vous avez saisie.

Commandes de gestion de AutoSupport

Vous utilisez le `system node autosupport` Commandes permettant de modifier ou d'afficher la configuration AutoSupport, d'afficher des informations sur les messages AutoSupport précédents et d'envoyer, de renvoyer ou d'annuler un message AutoSupport.

Configurez AutoSupport

Les fonctions que vous recherchez…	Utilisez cette commande…
Contrôlez si des messages AutoSupport sont envoyés	`system node autosupport modify` avec le `-state` paramètre
Contrôlez si les messages AutoSupport sont envoyés au support technique	`system node autosupport modify` avec le `-support` paramètre
Configurer AutoSupport ou modifier la configuration de AutoSupport	`system node autosupport modify`
Activez et désactivez les messages AutoSupport à votre organisation de support interne pour les événements de déclenchement individuels. Vous pouvez également spécifier des rapports de sous-système supplémentaires à inclure dans les messages envoyés en réponse aux événements de déclenchement individuels	`system node autosupport trigger modify`

Affiche des informations sur la configuration AutoSupport

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher la configuration AutoSupport	`system node autosupport show` avec le `-node` paramètre
Afficher un récapitulatif de toutes les adresses et URL qui reçoivent des messages AutoSupport	`system node autosupport destinations show`
Affichez les messages AutoSupport envoyés à votre organisation de support interne pour des événements déclencheurs individuels	`system node autosupport trigger show`

Les fonctions que vous recherchez…	Utilisez cette commande…
Affichage de l'état de la configuration AutoSupport ainsi que de la livraison vers différentes destinations	`system node autosupport check show`
Affiche l'état détaillé de la configuration AutoSupport ainsi que la livraison à différentes destinations	`system node autosupport check show-details`

Affiche les informations relatives aux messages AutoSupport précédents

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur un ou plusieurs des 50 messages AutoSupport les plus récents	`system node autosupport history show`
Affiche des informations sur les messages AutoSupport récents générés pour télécharger les fichiers core dump ou archive des performances vers le site de support technique ou un URI spécifié	`system node autosupport history show-upload-details`
Affichez les informations des messages AutoSupport, y compris le nom et la taille de chaque fichier collecté pour le message, ainsi que toute erreur	`system node autosupport manifest show`

Envoyer, renvoyer ou annuler des messages AutoSupport

Les fonctions que vous recherchez…	Utilisez cette commande…
Retransmettez un message AutoSupport stocké localement, identifié par son numéro de séquence AutoSupport Si vous retransmettez un message AutoSupport et que le support a déjà reçu ce message, le système de support ne crée pas de dossier en double. Si, par contre, le support ne recevait pas ce message, le système AutoSupport analysera le message et créera un dossier, si nécessaire.	`system node autosupport history retransmit`

Les fonctions que vous recherchez…	Utilisez cette commande…
Générer et envoyer un message AutoSupport, par exemple, à des fins de test	`system node autosupport invoke` Utilisez le `-force` Paramètre permettant d'envoyer un message même si AutoSupport est désactivé. Utilisez le `-uri` paramètre pour envoyer le message à la destination que vous spécifiez au lieu de la destination configurée.
Annuler un message AutoSupport	`system node autosupport history cancel`

Informations associées

"Commandes de ONTAP 9"

Informations incluses dans le manifeste AutoSupport

Le manifeste AutoSupport vous offre une vue détaillée des fichiers collectés pour chaque message AutoSupport. Le manifeste AutoSupport contient également des informations sur les erreurs de collecte lorsque AutoSupport ne peut pas collecter les fichiers dont il a besoin.

Le manifeste du AutoSupport inclut les informations suivantes :

- Numéro de séquence du message AutoSupport
- Fichiers AutoSupport inclus dans le message AutoSupport
- Taille de chaque fichier, en octets
- Statut de la collection du manifeste AutoSupport
- Description de l'erreur, si AutoSupport n'a pas pu collecter un ou plusieurs fichiers

Vous pouvez afficher le manifeste AutoSupport en utilisant le `system node autosupport manifest show` commande.

Le manifeste AutoSupport est inclus avec chaque message AutoSupport et présenté au format XML, ce qui signifie que vous pouvez soit utiliser un visualiseur XML générique pour le lire, soit l'afficher à l'aide du portail Active IQ (précédemment appelé My AutoSupport).

Suppression du boîtier AutoSupport pendant les fenêtres de maintenance planifiées

La suppression de dossier AutoSupport vous permet d'arrêter la création de dossiers inutiles provenant de messages AutoSupport déclenchés lors des fenêtres de maintenance planifiées.

Pour supprimer des cas AutoSupport, vous devez appeler manuellement un message AutoSupport avec une chaîne de texte spécialement formatée : `MAINT=xh`. `x` est la durée de la fenêtre de maintenance en unités d'heures.

Informations associées

"Comment supprimer la création automatique de dossier pendant les fenêtres de maintenance planifiées"

Résoudre les problèmes liés à AutoSupport

Dépanner AutoSupport lorsque les messages ne sont pas reçus

Si le système n'envoie pas le message AutoSupport, vous pouvez déterminer si c'est parce que AutoSupport ne peut pas générer le message ou ne peut pas le transmettre.

Étapes

1. Vérifiez l'état de transmission des messages à l'aide de `system node autosupport history show` commande.
2. Lire l'état.

Ce statut	Signifie
initialisation	Le processus de collecte démarre. Si cet état est temporaire, tout est bien. Toutefois, si cet état persiste, il y a un problème.
echec de la collecte	AutoSupport ne peut pas créer le contenu AutoSupport dans le répertoire spoule. Vous pouvez afficher ce que AutoSupport tente de collecter en entrant dans le `system node autosupport history show -detail` commande.
collecte en cours	AutoSupport collecte du contenu AutoSupport. Vous pouvez afficher les données collectées par AutoSupport en entrant `system node autosupport manifest show` commande.
en file d'attente	Les messages AutoSupport sont placés en file d'attente pour livraison, mais pas encore livrés.
transmission	AutoSupport fournit actuellement des messages.
envoi réussi	AutoSupport a envoyé le message avec succès. Pour savoir où AutoSupport a envoyé le message, entrez la `system node autosupport history show -delivery` commande.
ignorer	AutoSupport n'a aucune destination pour le message. Vous pouvez afficher les détails de livraison en entrant le `system node autosupport history show -delivery` commande.
mise en file d'attente	AutoSupport a tenté de livrer des messages, mais la tentative a échoué. Par conséquent, AutoSupport a replacé les messages dans la file d'attente de livraison pour une autre tentative. Vous pouvez afficher l'erreur en entrant le `system node autosupport history show` commande.

Ce statut	Signifie
transmission défectueuse	AutoSupport n'a pas réussi à transmettre le message le nombre spécifié de fois et a cessé d'essayer de le transmettre. Vous pouvez afficher l'erreur en entrant le `system node autosupport history show` commande.
ondemand-ignore	Le message AutoSupport a été traité avec succès, mais le service AutoSupport OnDemand a choisi de l'ignorer.

3. Effectuez l'une des opérations suivantes :

Pour ce statut	Faites ça
échec de l'initialisation ou de la collecte	Contactez le support NetApp, car AutoSupport ne peut pas générer le message. Mentionner l'article suivant de la base de connaissances : "Échec de la livraison d'AutoSupport : l'état est bloqué en cours d'initialisation"
échec de l'ignorer, de la mise en file d'attente ou de la transmission	Vérifiez que les destinations sont correctement configurées pour SMTP, HTTP ou HTTPS car AutoSupport ne peut pas transmettre le message.

Dépanner la distribution des messages AutoSupport via HTTP ou HTTPS

Si le système n'envoie pas le message AutoSupport attendu et que vous utilisez HTTP ou HTTPS ou si la fonction de mise à jour automatique ne fonctionne pas, vous pouvez vérifier un certain nombre de paramètres pour résoudre le problème.

Ce dont vous avez besoin

Vous devez avoir confirmé la connectivité réseau de base et la recherche DNS :

- Votre LIF de node-management doit être active et administrative.
- Vous devez pouvoir envoyer une requête ping à un hôte opérationnel sur le même sous-réseau à partir de la LIF de gestion du cluster (il ne s'agit pas d'une LIF sur un des nœuds).
- Vous devez pouvoir envoyer des requêtes ping à un hôte opérationnel en dehors du sous-réseau à partir de la LIF de gestion du cluster.
- Vous devez pouvoir ping un hôte opérationnel hors du sous-réseau depuis la LIF de gestion du cluster utilisant le nom de l'hôte (pas l'adresse IP).

Description de la tâche

Ces étapes sont pour les cas où vous avez déterminé que AutoSupport peut générer le message, mais que vous ne pouvez pas le transmettre via HTTP ou HTTPS.

Si vous rencontrez des erreurs ou si vous ne parvenez pas à effectuer une étape de cette procédure, déterminez et traitez le problème avant de passer à l'étape suivante.

Étapes

1. Afficher l'état détaillé du sous-système AutoSupport :

   ```
   system node autosupport check show-details
   ```

   Cela inclut la vérification de la connectivité aux destinations AutoSupport via l'envoi de messages de test et la liste des erreurs possibles dans les paramètres de configuration de AutoSupport.

2. Vérifier l'état du LIF node management :

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   Le `status-oper` et `status-admin` les champs doivent retourner « up ».

3. Enregistrer le nom du SVM, le nom de la LIF et l'adresse IP de la LIF pour une utilisation ultérieure.
4. Assurez-vous que le DNS est activé et configuré correctement :

   ```
   vserver services name-service dns show
   ```

5. Corriger toute erreur renvoyée par le message AutoSupport :

   ```
   system node autosupport history show -node * -fields node,seq-
   num,destination,last-update,status,error
   ```

   Pour obtenir de l'aide sur le dépannage des erreurs renvoyées, reportez-vous au "Guide de résolution ONTAP AutoSupport (transport HTTPS et HTTP)".

6. Vérifiez que le cluster peut accéder aux serveurs dont il a besoin et à Internet :

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

   > L'adresse `support.netapp.com` elle-même ne répond pas à la commande ping/traceroute, mais l'information par saut est utile.

   c. `system node autosupport show -fields proxy-url`

   d. `network traceroute -node node_management_LIF -destination proxy_url`

   Si l'une de ces routes ne fonctionne pas, essayez la même route à partir d'un hôte en fonctionnement sur le même sous-réseau que le cluster, en utilisant l'utilitaire « traceroute » ou « tracert » situé sur la plupart des clients réseau tiers. Cela vous aide à déterminer si le problème se situe dans votre configuration réseau ou dans votre configuration de cluster.

7. Si vous utilisez HTTPS pour votre protocole de transport AutoSupport, assurez-vous que le trafic HTTPS peut quitter le réseau :

   a. Configurez un client web sur le même sous-réseau que la LIF de gestion du cluster.

      Assurez-vous que tous les paramètres de configuration sont les mêmes que pour la configuration AutoSupport, y compris en utilisant le même serveur proxy, le même nom d'utilisateur, le même mot de passe et le même port.

   b. L'accès `https://support.netapp.com` avec le client web.

L'accès doit être réussi. Si ce n'est pas le cas, assurez-vous que tous les pare-feu sont correctement configurés pour autoriser le trafic HTTPS et DNS et que le serveur proxy est configuré correctement. Pour plus d'informations sur la configuration de la résolution statique des noms pour support.netapp.com, consultez l'article de la base de connaissances "Comment ajouter une entrée D'HÔTE dans ONTAP pour support.netapp.com?"

8. Depuis ONTAP 9.10.1, si vous avez activé la fonction mise à jour automatique, assurez-vous que vous disposez de la connectivité HTTPS aux URL supplémentaires suivantes :
   - https://support-sg-emea.netapp.com
   - https://support-sg-naeast.netapp.com
   - https://support-sg-nawest.netapp.com

Dépanner la transmission des messages AutoSupport via SMTP

Si le système ne parvient pas à transmettre les messages AutoSupport via SMTP, vous pouvez vérifier un certain nombre de paramètres pour résoudre le problème.

Ce dont vous avez besoin

Vous devez avoir confirmé la connectivité réseau de base et la recherche DNS :

- Votre LIF de node-management doit être active et administrative.
- Vous devez pouvoir envoyer une requête ping à un hôte opérationnel sur le même sous-réseau à partir de la LIF de gestion du cluster (il ne s'agit pas d'une LIF sur un des nœuds).
- Vous devez pouvoir envoyer des requêtes ping à un hôte opérationnel en dehors du sous-réseau à partir de la LIF de gestion du cluster.
- Vous devez pouvoir ping un hôte opérationnel hors du sous-réseau depuis la LIF de gestion du cluster utilisant le nom de l'hôte (pas l'adresse IP).

Description de la tâche

Ces étapes sont destinées aux cas où vous avez déterminé que AutoSupport peut générer le message, mais ne peut pas le transmettre via SMTP.

Si vous rencontrez des erreurs ou si vous ne parvenez pas à effectuer une étape de cette procédure, déterminez et traitez le problème avant de passer à l'étape suivante.

Toutes les commandes sont saisies au niveau de l'interface de ligne de commandes ONTAP, sauf indication contraire.

Étapes

1. Vérifier l'état du LIF node management :

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   Le `status-oper` et `status-admin` vous devriez y retourner `up`.

2. Enregistrer le nom du SVM, le nom de la LIF et l'adresse IP de la LIF pour une utilisation ultérieure.
3. Assurez-vous que le DNS est activé et configuré correctement :

   ```
   vserver services name-service dns show
   ```

4. Afficher tous les serveurs configurés pour être utilisés par AutoSupport :

   system node autosupport show -fields mail-hosts

   Enregistrer tous les noms de serveur affichés.

5. Pour chaque serveur affiché par l'étape précédente, et `support.netapp.com`, Assurez-vous que le serveur ou l'URL peut être atteint par le noeud :

   network traceroute -node local -destination *server_name*

   Si l'une de ces routes ne fonctionne pas, essayez la même route à partir d'un hôte en fonctionnement sur le même sous-réseau que le cluster, en utilisant l'utilitaire « traceroute » ou « tracert » situé sur la plupart des clients réseau tiers. Cela vous aide à déterminer si le problème se situe dans votre configuration réseau ou dans votre configuration de cluster.

6. Connectez-vous à l'hôte désigné comme hôte de messagerie et assurez-vous qu'il peut traiter les demandes SMTP :

   netstat -aAn|grep 25

   `25` Est le numéro de port SMTP du port d'écoute.

   Un message similaire au texte suivant s'affiche :

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

7. À partir d'un autre hôte, ouvrez une session Telnet avec le port SMTP de l'hôte de messagerie :

   telnet *mailhost* 25

   Un message similaire au texte suivant s'affiche :

   ```
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
   10:49:04 PST
   ```

8. À l'invite telnet, assurez-vous qu'un message peut être relayé depuis votre hôte de messagerie :

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   `domain_name` est le nom de domaine de votre réseau.

   Si une erreur est renvoyée indiquant que la retransmission est refusée, la retransmission n'est pas activée sur l'hôte de messagerie. Contactez votre administrateur système.

9. À l'invite telnet, envoyez un message de test :

```
DATA

SUBJECT: TESTING
THIS IS A TEST

.
```

> Assurez-vous d'entrer la dernière période (.) sur une ligne par elle-même. La période indique à l'hôte de messagerie que le message est terminé.

Si une erreur est renvoyée, votre hôte de messagerie n'est pas configuré correctement. Contactez votre administrateur système.

10. À partir de l'interface de ligne de commande ONTAP, envoyez un message de test AutoSupport à une adresse e-mail de confiance à laquelle vous avez accès :

    system node autosupport invoke -node local -type test

11. Recherchez le numéro de séquence de la tentative :

    system node autosupport history show -node local -destination smtp

    Recherchez le numéro de séquence de votre tentative en fonction de l'horodatage. C'est probablement la tentative la plus récente.

12. Afficher l'erreur de votre tentative de message de test :

    system node autosupport history show -node local -seq-num seq_num -fields error

    Si l'erreur affichée est de `Login denied`, Votre serveur SMTP n'accepte pas les requêtes d'envoi de la LIF de gestion du cluster. Si vous ne souhaitez pas passer à utiliser HTTPS comme protocole de transport, contactez votre administrateur réseau de site pour configurer les passerelles SMTP afin de résoudre ce problème.

    Si ce test réussit mais que le même message envoyé à mailto:autosupport@netapp.com ne le fait pas, assurez-vous que le relais SMTP est activé sur tous vos hôtes de messagerie SMTP ou utilisez HTTPS comme protocole de transport.

    Si même le message du compte de messagerie géré localement ne fonctionne pas, vérifiez que vos serveurs SMTP sont configurés pour transférer les pièces jointes avec les deux caractéristiques suivantes :

    - Le suffixe « 7z »
    - Le type MIME « application/x-7X-compressé ».

Dépanner le sous-système AutoSupport

Le `system node check show` Les commandes permettent de vérifier et de résoudre tous les problèmes liés à la configuration et à la livraison de AutoSupport.

Étape

1. Utiliser les commandes suivantes pour afficher l'état du sous-système AutoSupport.

Utilisez cette commande…	Pour cela…
`system node autosupport check show`	Affiche l'état général du sous-système AutoSupport, tel que l'état de la destination AutoSupport HTTP ou HTTPS, les destinations SMTP AutoSupport, le serveur AutoSupport OnDemand et la configuration AutoSupport
`system node autosupport check show-details`	Affiche l'état détaillé du sous-système AutoSupport, notamment des descriptions détaillées des erreurs et des actions correctives

Surveillez l'état de santé de votre système

Surveillez l'état de santé de votre système

Cette fonction surveille de manière proactive certaines conditions critiques du cluster et déclenche des alertes en cas de défaillance ou de risque. Si des alertes sont actives, l'état de l'état du système signale un état dégradé pour le cluster. Les alertes incluent les informations dont vous avez besoin pour répondre à la dégradation de l'état du système.

Si l'état est dégradé, vous pouvez afficher des détails sur le problème, y compris la cause probable et les actions de récupération recommandées. Une fois le problème résolu, l'état de l'état du système revient automatiquement à OK.

L'état de l'état du système reflète plusieurs moniteurs d'état distincts. Un état dégradé au sein d'un moniteur d'état entraîne un état dégradé pour l'état global du système.

Pour plus de détails sur la prise en charge des commutateurs de cluster par ONTAP pour le contrôle de l'état du système dans votre cluster, reportez-vous au *Hardware Universe*.

"Commutateurs pris en charge dans le Hardware Universe"

Pour plus d'informations sur les causes des messages AutoSupport du moniteur d'intégrité des commutateurs de cluster (CSHM) et sur les actions nécessaires pour résoudre ces alertes, consultez l'article de la base de connaissances.

"Message AutoSupport : processus de surveillance de l'état CSHM"

Fonctionnement de la surveillance de l'état

Les moniteurs de santé individuels disposent d'un ensemble de règles qui déclenchent des alertes lorsque certaines conditions se produisent. Comprendre le fonctionnement de la surveillance de l'état de santé peut vous aider à résoudre les problèmes et à contrôler les alertes futures.

La surveillance de l'état des systèmes comprend les composants suivants :

- Chaque état de santé surveille pour des sous-systèmes spécifiques, chacun ayant son propre état d'intégrité

Par exemple, le sous-système de stockage dispose d'un contrôle de l'état de la connectivité des nœuds.

- Un contrôle de l'état global du système qui consolide l'état d'intégrité des différents moniteurs de santé

  Un état dégradé dans un seul sous-système entraîne un état dégradé pour tout le système. Si aucun sous-système n'a d'alertes, l'état global du système est OK.

Chaque contrôle de l'état est constitué des éléments clés suivants :

- Alertes que le contrôle de l'état peut potentiellement générer

  Chaque alerte a une définition, qui inclut des détails tels que la gravité de l'alerte et sa cause probable.

- Règles de santé qui identifient quand chaque alerte est déclenchée

  Chaque règle de santé dispose d'une expression de règle, qui est la condition ou la modification exacte qui déclenche l'alerte.

Un contrôle de l'état surveille et valide en permanence les ressources de son sous-système à des fins de modification de l'état ou des conditions. Lorsqu'une condition ou une modification d'état correspond à une expression de règle dans une politique de santé, le contrôle de l'état génère une alerte. Une alerte provoque l'état de l'état de santé du sous-système et l'état global de l'intégrité du système.

Moyens de répondre aux alertes d'intégrité du système

Lorsqu'une alerte d'intégrité du système se produit, vous pouvez la valider, en savoir plus sur celui-ci, réparer l'état sous-jacent et éviter qu'elle ne se reproduise.

Lorsqu'un contrôle de l'état soulève une alerte, vous pouvez répondre de l'une des manières suivantes :

- Obtenez des informations sur l'alerte, qui inclut la ressource affectée, la gravité de l'alerte, la cause probable, l'effet possible et les actions correctives.
- Obtenez des informations détaillées sur l'alerte, telles que l'heure à laquelle l'alerte a été générée et si quelqu'un d'autre a déjà reconnu l'alerte.
- Consultez les informations relatives à l'état de la ressource ou du sous-système affecté, par exemple un tiroir ou un disque spécifique.
- Reconnaissez l'alerte pour indiquer qu'une personne travaille sur le problème et identifiez-vous comme « vérificateur ».
- Résolvez le problème en prenant les mesures correctives fournies dans l'alerte, telles que la résolution du câblage pour résoudre un problème de connectivité.
- Supprimez l'alerte si le système ne l'a pas supprimée automatiquement.
- Supprimez une alerte pour l'empêcher d'affecter l'état de santé d'un sous-système.

  La suppression est utile lorsque vous comprenez un problème. Après avoir supprimé une alerte, elle peut toujours se produire, mais l'état de santé du sous-système s'affiche sous la forme « ok-avec-supprimé » lorsque l'alerte supprimée se produit.

Personnalisation des alertes d'intégrité du système

Vous pouvez contrôler les alertes qu'un contrôle de l'état génère en activant et en

désactivant les politiques d'intégrité du système qui définissent lorsque les alertes sont déclenchées. Cela vous permet de personnaliser le système de surveillance de l'état de santé pour votre environnement particulier.

Pour connaître le nom d'une règle, vous pouvez afficher des informations détaillées sur une alerte générée ou afficher les définitions de règles pour un contrôle de l'état, un nœud ou un ID d'alerte spécifique.

La désactivation des politiques de santé est différente de la suppression des alertes. Lorsque vous supprimez une alerte, elle n'a pas d'impact sur l'état de santé du sous-système, mais l'alerte peut toujours se produire.

Si vous désactivez une règle, la condition ou l'état défini dans son expression de règle de gestion ne déclenche plus d'alerte.

Exemple d'alerte que vous souhaitez désactiver

Par exemple, supposons qu'une alerte ne vous soit pas utile. Vous utilisez le `system health alert show -instance` Commande pour obtenir l'ID de la règle pour l'alerte. Vous utilisez l'ID de la police dans le `system health policy definition show` commande pour afficher les informations relatives à la règle. Après avoir vérifié l'expression de règle et d'autres informations sur la stratégie, vous décidez de la désactiver. Vous utilisez le `system health policy definition modify` commande pour désactiver la règle.

Le mode d'alerte de santé déclenche des messages et des événements AutoSupport

Les alertes d'intégrité du système déclenchent des messages AutoSupport et des événements dans le système de gestion des événements (EMS), ce qui vous permet de surveiller l'état du système à l'aide des messages AutoSupport et du système EMS en plus d'utiliser directement le système de contrôle de l'état.

Votre système envoie un message AutoSupport dans les cinq minutes qui suivent une alerte. Le message AutoSupport inclut toutes les alertes générées depuis le message AutoSupport précédent, à l'exception des alertes qui dupliquent une alerte pour la même ressource et la même cause probable au cours de la semaine précédente.

Certaines alertes ne déclenchent pas de messages AutoSupport. Une alerte ne déclenche pas de message AutoSupport si sa politique d'intégrité désactive l'envoi de messages AutoSupport. Par exemple, une politique de santé peut désactiver les messages AutoSupport par défaut, car AutoSupport génère déjà un message lorsque le problème se produit. Vous pouvez configurer des règles pour ne pas déclencher de messages AutoSupport à l'aide de `system health policy definition modify` commande.

Vous pouvez afficher la liste de tous les messages AutoSupport déclenchés par les alertes envoyés au cours de la semaine précédente à l'aide du `system health autosupport trigger history show` commande.

Les alertes déclenchent également la génération d'événements au SGE. Un événement est généré chaque fois qu'une alerte est créée et chaque fois qu'une alerte est effacée.

Contrôles disponibles de l'état du cluster

Plusieurs moniteurs d'état permettent de surveiller différentes parties d'un cluster. Les contrôles d'état vous aident à corriger des erreurs au sein des systèmes ONTAP en détectant des événements, en vous envoyant des alertes et en supprimant les événements tels qu'ils sont clairs.

Nom du contrôle de l'état (identifiant)	Nom du sous-système (identifiant)	Objectif
Commutateur du cluster(commutateur du cluster)	Commutateur (commutateur - état)	Surveille les commutateurs du réseau de cluster et les commutateurs du réseau de gestion en termes de température, d'utilisation, de configuration des interfaces, de redondance (commutateurs du réseau de cluster uniquement), et de fonctionnement des ventilateurs et de l'alimentation. Le contrôle de l'état du commutateur de cluster communique avec les commutateurs via SNMP. SNMPv2c est le paramètre par défaut. Depuis ONTAP 9.2, ce moniteur peut détecter et signaler le redémarrage d'un commutateur de cluster depuis la dernière période d'interrogation.
Structure MetroCluster	Commutateur	Surveille la topologie de la configuration MetroCluster back-end de la structure et détecte les erreurs de configuration, comme le câblage et la segmentation incorrects ou les défaillances ISL.
État de santé du MetroCluster	Interconnexion, RAID et stockage	Surveille les adaptateurs FC-VI, les adaptateurs d'initiateurs FC, les agrégats et disques situés derrière le côté gauche et les ports d'intercluster
Connectivité nœud(nœud-Connect)	Continuité de l'activité CIFS	Surveille les connexions SMB afin de garantir la continuité de l'activité aux applications Hyper-V.
Stockage (SAS-Connect)	Surveille les tiroirs, les disques et les adaptateurs au niveau du nœud pour s'assurer que les chemins et les connexions sont appropriés.	Système

Nom du contrôle de l'état (identifiant)	Nom du sous-système (identifiant)	Objectif
sans objet	Rassemble les informations d'autres moniteurs de santé.	Connectivité système (system-Connect)

Recevez automatiquement les alertes d'état du système

Vous pouvez afficher manuellement les alertes d'état du système en utilisant le `system health alert show` commande. Vous devez toutefois vous abonner à des messages EMS pour recevoir automatiquement des notifications lorsqu'un contrôle de l'état génère une alerte.

Description de la tâche

La procédure suivante vous indique comment configurer les notifications pour tous les messages hm.Alert.déclenché et pour tous les messages hm.Alert.effacé.

Tous les messages hm.Alert.déclenché et tous les messages hm.Alert.décoché comprennent une interruption SNMP. Les noms des traps SNMP sont `HealthMonitorAlertRaised` et `HealthMonitorAlertCleared`. Pour plus d'informations sur les interruptions SNMP, consultez le *Network Management Guide*.

Étapes

1. Utilisez le `event destination create` Commande pour définir la destination à laquelle vous souhaitez envoyer les messages EMS.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Utilisez le `event route add-destinations` commande permettant d'acheminer le `hm.alert.raised` message et le `hm.alert.cleared` message vers une destination.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

Informations associées

"Gestion du réseau"

Répondez à la dégradation de l'état du système

Lorsque l'état de santé de votre système est dégradé, vous pouvez afficher des alertes, lire les informations sur la cause probable et les actions correctives, afficher des informations sur le sous-système dégradé et résoudre le problème. Les alertes supprimées s'affichent également pour vous permettre de les modifier et de vérifier si elles ont été acquittées.

Description de la tâche

Vous pouvez découvrir qu'une alerte a été générée en visualisant un message AutoSupport ou un événement EMS, ou en utilisant le `system health` commandes.

Étapes

1. Utilisez le `system health alert show` commande pour afficher les alertes qui compromettre l'intégrité du système
2. Lisez la cause probable, l'effet possible et les actions correctives de l'alerte pour déterminer si vous pouvez résoudre le problème ou si vous avez besoin d'informations supplémentaires.
3. Si vous avez besoin de plus d'informations, utilisez le `system health alert show -instance` pour afficher les informations supplémentaires disponibles pour l'alerte.
4. Utilisez le `system health alert modify` commande avec `-acknowledge` paramètre pour indiquer que vous travaillez sur une alerte spécifique.
5. Prendre des mesures correctives pour résoudre le problème comme décrit dans le `Corrective Actions` champ dans l'alerte.

   Les actions correctives peuvent inclure le redémarrage du système.

   Une fois le problème résolu, l'alerte est automatiquement effacée. Si le sous-système n'a pas d'autres alertes, l'intégrité du sous-système devient `OK`. Si l'intégrité de tous les sous-systèmes est correcte, l'état d'intégrité globale du système passe à `OK`.

6. Utilisez le `system health status show` commande pour vérifier que l'état de l'intégrité du système est `OK`.

   Si l'état de l'état de santé du système n'est pas `OK`, répéter cette procédure.

Exemple de réponse à une dégradation de l'état du système

En examinant un exemple spécifique de l'état du système dégradé après un tiroir qui manque deux chemins d'accès à un nœud, vous pouvez voir ce que l'interface de ligne de commandes affiche lorsque vous répondez à une alerte.

Après avoir démarré ONTAP, vous vérifiez l'état du système et vous découvrez que son état est dégradé :

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

Vous affichez les alertes pour déterminer l'emplacement du problème et vous voyez que le tiroir 2 n'a pas deux chemins d'accès au nœud 1 :

```
      cluster1::>system health alert show
                 Node: node1
             Resource: Shelf ID 2
             Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

Vous affichez des informations détaillées sur l'alerte pour obtenir plus d'informations, notamment l'ID d'alerte :

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
          Acknowledge: false
             Suppress: false
               Policy: DualPathToDiskShelf_Policy
         Acknowledger: -
           Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

Vous reconnaissez l'alerte pour indiquer que vous y travaillez.

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

Vous avez résolu le câblage entre le tiroir 2 et le nœud 1, puis redémarré le système. Ensuite, vous vérifiez de nouveau l'état du système et voyez que son état est `OK`:

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

Configurer la détection des commutateurs du réseau de gestion et du cluster

Le contrôle de l'état du switch de cluster tente automatiquement de détecter les commutateurs du réseau de gestion et de cluster à l'aide du protocole CDP (Cisco Discovery Protocol). Vous devez configurer le contrôle de l'état s'il ne peut pas détecter automatiquement un switch ou si vous ne souhaitez pas utiliser CDP pour la découverte automatique.

Description de la tâche

Le `system cluster-switch show` la commande répertorie les switchs détectés par le contrôle de l'état. Si vous ne voyez pas de commutateur que vous aviez prévu dans cette liste, le contrôle de l'état ne peut pas le détecter automatiquement.

Étapes

1. Si vous souhaitez utiliser CDP pour la découverte automatique, procédez comme suit :

   a. Assurez-vous que le Cisco Discovery Protocol (CDP) est activé sur vos commutateurs.

      Reportez-vous à la documentation de votre commutateur pour obtenir des instructions.

   b. Exécutez la commande suivante sur chaque nœud du cluster pour vérifier si CDP est activée ou désactivée :

      `run -node node_name -command options cdpd.enable`

      Si CDP est activé, passez à l'étape d. Si le CDP est désactivé, passez à l'étape c.

   c. Exécutez la commande suivante pour activer CDP :

      `run -node node_name -command options cdpd.enable on`

   Attendez cinq minutes avant de passer à l'étape suivante.

   a. Utilisez le `system cluster-switch show` Commande pour vérifier si ONTAP peut désormais détecter automatiquement les commutateurs.

2. Si le contrôle de l'état ne peut pas détecter automatiquement un commutateur, utilisez le `system cluster-switch create` commande pour configurer la découverte du commutateur :

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
   cluster-network
   ```

   Attendez cinq minutes avant de passer à l'étape suivante.

3. Utilisez le `system cluster-switch show` Commande pour vérifier que ONTAP peut détecter le switch pour lequel vous avez ajouté des informations.

Une fois que vous avez terminé

Vérifiez que le contrôle de l'état peut surveiller vos commutateurs.

Vérifier la surveillance du cluster et des commutateurs du réseau de gestion

Le contrôle de l'état du commutateur de cluster tente automatiquement de surveiller les commutateurs qu'il détecte ; toutefois, la surveillance peut ne pas se produire automatiquement si les commutateurs ne sont pas configurés correctement. Vérifiez que le contrôle de l'état est correctement configuré pour surveiller les commutateurs.

Étapes

1. Pour identifier les switchs détectés par le contrôle de l'état du commutateur de cluster, entrez la commande suivante :

   ONTAP 9.8 et versions ultérieures

   `system switch ethernet show`

   ONTAP 9.7 et versions antérieures

   `system cluster-switch show`

   Si le `Model` affiche la valeur `OTHER`, ONTAP ne peut pas surveiller le commutateur. ONTAP définit la valeur sur `OTHER` si un commutateur qu'il détecte automatiquement n'est pas pris en charge pour le contrôle de l'état de santé.

   Si un commutateur ne s'affiche pas dans la sortie de la commande, vous devez configurer la détection du commutateur.

2. Effectuez une mise à niveau vers la dernière version du logiciel de commutateur pris en charge et consultez le fichier de configuration (RCF) disponible sur le site de support NetApp.

   "Page des téléchargements du support NetApp"

   La chaîne de communauté dans le RCF du commutateur doit correspondre à la chaîne de communauté que le moniteur d'état est configuré pour utiliser. Par défaut, le contrôle de l'état utilise la chaîne de communauté `cshm1!`.

   Actuellement, le moniteur de santé ne prend en charge que SNMPv2.

   Si vous avez besoin de modifier les informations concernant un commutateur que le cluster surveille, vous pouvez modifier la chaîne de communauté utilisée par le contrôle de l'état à l'aide de la commande suivante :

ONTAP 9.8 et versions ultérieures

`system switch ethernet modify`

ONTAP 9.7 et versions antérieures

`system cluster-switch modify`

3. Vérifiez que le port de gestion du commutateur est connecté au réseau de gestion.

   Cette connexion est requise pour exécuter des requêtes SNMP.

Commandes permettant de contrôler l'état de santé de votre système

Vous pouvez utiliser le `system health` commandes permettant d'afficher des informations relatives à l'état de santé des ressources système, de répondre aux alertes et de configurer les alertes futures. L'utilisation des commandes de l'interface de ligne de commandes vous permet d'afficher des informations détaillées sur la configuration de la surveillance de l'état. Les pages de manuels des commandes contiennent plus d'informations.

Affiche l'état de l'état de santé du système

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche l'état de santé du système, qui reflète l'état global des moniteurs d'intégrité individuels	`system health status show`
Affiche l'état d'intégrité des sous-systèmes pour lesquels la surveillance de l'état est disponible	`system health subsystem show`

Affiche l'état de la connectivité du nœud

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations détaillées sur la connectivité du nœud au tiroir de stockage, notamment les informations relatives aux ports, la vitesse du port HBA, le débit d'E/S et le taux d'opérations d'E/S par seconde	`storage shelf show -connectivity` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque tiroir.
Affiche des informations sur les disques et les LUN de baie, y compris l'espace utilisable, les numéros de tiroir et de compartiment, ainsi que le nom de nœud propriétaire	`storage disk show` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque lecteur.

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations détaillées sur les ports des tiroirs de stockage, notamment le type de port, la vitesse et l'état	`storage port show` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque adaptateur.

Gérer la détection des commutateurs de cluster, de stockage et de réseau de gestion

Les fonctions que vous recherchez…	Utilisez cette commande. (ONTAP 9.8 et versions ultérieures)	Utilisez cette commande. (ONTAP 9.7 et versions antérieures)
Afficher les commutateurs surveillés par le bloc d'instruments	`system switch ethernet show`	`system cluster-switch show`
Afficher les commutateurs actuellement surveillés par le cluster, notamment les commutateurs que vous avez supprimés (indiqués dans la colonne raison de la sortie de la commande) et les informations de configuration dont vous avez besoin pour accéder au réseau au cluster et aux commutateurs du réseau de gestion. Cette commande est disponible au niveau de privilège avancé.	`system switch ethernet show-all`	`system cluster-switch show-all`
Configurer la détection d'un commutateur non découvert	`system switch ethernet create`	`system cluster-switch create`
Modifier les informations relatives à un commutateur que le cluster surveille (par exemple, nom de périphérique, adresse IP, version SNMP et chaîne de communauté)	`system switch ethernet modify`	`system cluster-switch modify`
Désactiver la surveillance d'un commutateur	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
Désactiver la détection et la surveillance d'un commutateur et supprimer les informations de configuration du commutateur	`system switch ethernet delete`	`system cluster-switch delete`

Les fonctions que vous recherchez…	Utilisez cette commande. (ONTAP 9.8 et versions ultérieures)	Utilisez cette commande. (ONTAP 9.7 et versions antérieures)
Supprimez définitivement les informations de configuration du commutateur stockées dans la base de données (ce qui permet de réactiver la détection automatique du commutateur)	`system switch ethernet delete -force`	`system cluster-switch delete -force`
Activez la journalisation automatique pour envoyer des messages AutoSupport.	`system switch ethernet log`	`system cluster-switch log`

Répondez aux alertes générées

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur les alertes générées, telles que la ressource et le nœud où l'alerte a été déclenchée, ainsi que la gravité et la cause probable de l'alerte	`system health alert show`
Affiche des informations sur chaque alerte générée	`system health alert show -instance`
Indique que quelqu'un travaille sur une alerte	`system health alert modify`
Accuser réception d'une alerte	`system health alert modify -acknowledge`
Supprimez une alerte ultérieure afin qu'elle n'affecte pas l'état de santé d'un sous-système	`system health alert modify -suppress`
Supprimez une alerte qui n'a pas été automatiquement effacée	`system health alert delete`
Affiche des informations sur les messages AutoSupport qui déclenchent les alertes la semaine dernière, par exemple pour déterminer si une alerte a déclenché un message AutoSupport	`system health autosupport trigger history show`

Configurez les alertes futures

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez ou désactivez la règle qui contrôle si un état de ressource spécifique génère une alerte spécifique	`system health policy definition modify`

Affiche des informations sur la configuration de la surveillance de l'état

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations relatives aux contrôles d'état, telles que leurs nœuds, leurs noms, leurs sous-systèmes et leur état	`system health config show` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque contrôle de l'état.
Affiche des informations sur les alertes qu'un contrôle de l'état peut générer	`system health alert definition show` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque définition d'alerte.
Affiche des informations sur les règles de contrôle de l'état, qui déterminent l'heure à laquelle les alertes sont émises	`system health policy definition show` Utilisez le `-instance` paramètre pour afficher des informations détaillées sur chaque règle. Utilisez d'autres paramètres pour filtrer la liste des alertes, par exemple en fonction de l'état (activé ou non), du contrôle de l'état, de l'alerte, etc.

Affiche des informations environnementales

Les capteurs vous aident à surveiller les composants environnementaux de votre système. Les informations que vous pouvez afficher concernant les capteurs environnementaux incluent leur type, leur nom, leur état, leur valeur et les avertissements de seuil.

Étape

1. Pour afficher des informations sur les capteurs environnementaux, utilisez le `system node environment sensors show` commande.

Gérer l'accès aux services Web

Gestion de l'accès aux services Web

Un service Web est une application que les utilisateurs peuvent accéder via HTTP ou HTTPS. L'administrateur du cluster peut configurer le moteur de protocole Web, configurer SSL, activer un service Web et permettre aux utilisateurs d'un rôle d'accéder à un service Web.

Depuis ONTAP 9.6, les services Web suivants sont pris en charge :

- Infrastructure du processeur de service (`spi`)

  Ce service met à disposition les fichiers log, core dump et MIB des nœuds pour l'accès HTTP ou HTTPS via la LIF de cluster management ou une LIF de node-management. Le paramètre par défaut est `enabled`.

  Lors d'une demande d'accès aux fichiers journaux ou aux fichiers « core dump » d'un nœud, la `spi` le service web crée automatiquement un point de montage d'un nœud vers le volume racine d'un autre nœud où les fichiers résident. Il n'est pas nécessaire de créer manuellement le point de montage. `

- Les API ONTAP (`ontapi`)

  Ce service vous permet d'exécuter des API ONTAP pour exécuter des fonctions administratives avec un programme distant. Le paramètre par défaut est `enabled`.

  Ce service peut être requis pour certains outils de gestion externes. Par exemple, si vous utilisez System Manager, vous devez laisser ce service activé.

- Détection Data ONTAP (`disco`)

  Ce service permet aux applications de gestion externes de découvrir le cluster sur le réseau. Le paramètre par défaut est `enabled`.

- Diagnostics du support (`supdiag`)

  Ce service contrôle l'accès à un environnement privilégié sur le système afin d'aider à l'analyse et à la résolution des problèmes. Le paramètre par défaut est `disabled`. Vous ne devez activer ce service que si vous y êtes invité par le support technique.

- System Manager (`sysmgr`)

  Ce service contrôle la disponibilité de System Manager, qui est inclus avec ONTAP. Le paramètre par défaut est `enabled`. Ce service est pris en charge uniquement sur le cluster.

- Mise à jour du contrôleur BMC (Baseboard Management Controller) du micrologiciel (`FW_BMC`)

  Ce service vous permet de télécharger les fichiers du micrologiciel BMC. Le paramètre par défaut est `enabled`.

- Documentation ONTAP (`docs`)

  Ce service fournit un accès à la documentation ONTAP. Le paramètre par défaut est `enabled`.

- API RESTful ONTAP (`docs_api`)

  Ce service permet d'accéder à la documentation de l'API RESTful ONTAP. Le paramètre par défaut est `enabled`.

- Téléchargement de fichiers (`fud`)

  Ce service permet le téléchargement et le téléchargement de fichiers. Le paramètre par défaut est `enabled`.

- Messagerie ONTAP (`ontapmsg`)

  Ce service prend en charge une interface de publication et d'abonnement qui vous permet de vous abonner à des événements. Le paramètre par défaut est `enabled`.

- Portail ONTAP (`portal`)

  Ce service implémente la passerelle dans un serveur virtuel. Le paramètre par défaut est `enabled`.

- Interface ONTAP RESTful (`rest`)

  Ce service prend en charge une interface RESTful qui permet de gérer à distance tous les éléments de l'infrastructure du cluster. Le paramètre par défaut est `enabled`.

- Prise en charge des fournisseurs de services SAML (`saml`)

  Ce service fournit des ressources pour prendre en charge le fournisseur de services SAML. Le paramètre par défaut est `enabled`.

- Fournisseur de services SAML (`saml-sp`)

  Ce service offre des services tels que les métadonnées SP et le service client d'assertion au fournisseur de services. Le paramètre par défaut est `enabled`.

Depuis ONTAP 9.7, les services supplémentaires suivants sont pris en charge :

- Fichiers de sauvegarde de configuration (`backups`)

  Ce service vous permet de télécharger les fichiers de sauvegarde de configuration. Le paramètre par défaut est `enabled`.

- Sécurité ONTAP (`security`)

  Ce service prend en charge la gestion des jetons CSRF pour une authentification améliorée. Le paramètre par défaut est `enabled`.

Gérer le moteur de protocole Web

Vous pouvez configurer le moteur de protocole Web sur le cluster pour contrôler si l'accès Web est autorisé et quelles versions SSL peuvent être utilisées. Vous pouvez également afficher les paramètres de configuration du moteur de protocole Web.

Vous pouvez gérer le moteur de protocole Web au niveau du cluster de plusieurs manières :

- Vous pouvez indiquer si les clients distants peuvent utiliser HTTP ou HTTPS pour accéder au contenu du service Web à l'aide de l' `system services web modify` commande avec `-external` paramètre.
- Vous pouvez spécifier si SSLv3 doit être utilisé pour un accès Web sécurisé à l'aide de l' `security config modify` commande avec `-supported-protocol` paramètre. Par défaut, SSLv3 est désactivé. La sécurité de la couche de transport 1.0 (TLSv1) est activée et elle peut être désactivée si nécessaire.
- Vous pouvez activer le mode de conformité Federal information Processing Standard (FIPS) 140-2 pour les interfaces de service Web du plan de contrôle à l'échelle du cluster.

Par défaut, le mode de conformité FIPS 140-2 est désactivé.

- **Lorsque le mode de conformité FIPS 140-2 est désactivé**, vous pouvez activer le mode de conformité FIPS 140-2 en configurant le `is-fips-enabled` paramètre à `true` pour le `security config modify` et en utilisant la commande `security config show` commande pour confirmer le statut en ligne.
- **Lorsque le mode de conformité FIPS 140-2 est activé**
  - À partir de ONTAP 9.11.1, TLSv1, TLSv1.1 et SSLv3 sont désactivés et seuls TSLv1.2 et TSLv1.3 restent activés. Elle affecte d'autres systèmes et communications internes et externes à ONTAP 9. Si vous activez le mode de conformité FIPS 140-2 puis désactivez-le, TLSv1, TLSv1.1 et SSLv3 restent désactivés. TLSv.1 ou TLSSS3.3 restent activés en fonction de la configuration précédente.
  - Pour les versions de ONTAP antérieures à 9.11.1, TLSv1 et SSLv3 sont tous deux désactivés et seuls les modèles TLSv1.1 et TLSv1.2 restent activés. ONTAP vous empêche d'activer à la fois TLSv1 et SSLv3 lorsque le mode de conformité FIPS 140-2 est activé. Si vous activez le mode de conformité FIPS 140-2 puis désactivez-le, TLSv1 et SSLv3 restent désactivés, mais TLSv1.2 ou les deux TLSv1.1 et TLSv1.2 sont activés en fonction de la configuration précédente.

- Vous pouvez afficher la configuration de la sécurité au niveau du cluster à l'aide de `system security config show` commande.

Si le pare-feu est activé, la politique de pare-feu pour l'interface logique (LIF) à utiliser pour les services Web doit être configurée de manière à autoriser l'accès HTTP ou HTTPS.

Si vous utilisez HTTPS pour l'accès aux services Web, SSL pour le cluster ou la machine virtuelle de stockage (SVM) qui offre le service Web doit également être activé, et vous devez fournir un certificat numérique pour le cluster ou la SVM.

Dans les configurations MetroCluster, les modifications de paramètre apportées au moteur de protocole Web sur un cluster ne sont pas répliquées sur le cluster partenaire.

Commandes de gestion du moteur de protocole Web

Vous utilisez le `system services web` commandes permettant de gérer le moteur de protocole web. Vous utilisez le `system services firewall policy create` et `network interface modify` commandes permettant d'autoriser les demandes d'accès web à passer par le pare-feu.

Les fonctions que vous recherchez…	Utilisez cette commande…
Configurer le moteur de protocole Web au niveau du cluster : • Activez ou désactivez le moteur de protocole Web pour le cluster • Activez ou désactivez SSLv3 pour le cluster • Activer ou désactiver la conformité FIPS 140-2 pour des services web sécurisés (HTTPS)	`system services web modify`

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher la configuration du moteur de protocole Web au niveau du cluster, déterminer si les protocoles Web sont fonctionnels dans tout le cluster et indiquer si la conformité FIPS 140-2 est activée et en ligne	`system services web show`
Afficher la configuration du moteur de protocole Web au niveau du nœud et l'activité de gestion du service Web pour les nœuds du cluster	`system services web node show`
Créez une politique de pare-feu ou ajoutez un service de protocole HTTP ou HTTPS à une politique de pare-feu existante pour permettre aux demandes d'accès Web de passer par le pare-feu	`system services firewall policy create` Réglage du `-service` paramètre à `http` ou `https` permet aux demandes d'accès web de passer par le pare-feu.
Associer une politique de pare-feu à une LIF	`network interface modify` Vous pouvez utiliser le `-firewall-policy` Paramètre pour modifier la politique de pare-feu d'une LIF.

Configurez l'authentification SAML pour les services Web

Configurez l'authentification SAML

Depuis ONTAP 9.3, vous pouvez configurer l'authentification SAML pour les services Web. Lorsque l'authentification SAML est configurée et activée, les utilisateurs sont authentifiés par un fournisseur d'identité externe (IDP) au lieu des fournisseurs de services d'annuaire tels qu'Active Directory et LDAP.

Ce dont vous avez besoin

- Vous devez avoir configuré l'IDP pour l'authentification SAML.
- Vous devez avoir l'URI IDP.

Description de la tâche

- L'authentification SAML s'applique uniquement au `http` et `ontapi` en termes de latence.

  Le `http` et `ontapi` Les applications sont utilisées par les services web suivants : infrastructure processeur de service, API ONTAP ou System Manager.

- L'authentification SAML est applicable uniquement pour l'accès au SVM d'administration.

Étapes

1. Créez une configuration SAML pour que ONTAP puisse accéder aux métadonnées IDP :

   `security saml-sp create -idp-uri` *`idp_uri`* `-sp-host` *`ontap_host_name`*

`idp_uri` Est l'adresse FTP ou HTTP de l'hôte IDP à partir de laquelle les métadonnées IDP peuvent être téléchargées.

`ontap_host_name` Est le nom d'hôte ou l'adresse IP de l'hôte du fournisseur de services SAML, qui, dans le cas présent, correspond au système ONTAP. Par défaut, l'adresse IP de la LIF de cluster-management est utilisée.

Vous pouvez éventuellement fournir les informations de certificat de serveur ONTAP. Par défaut, les informations de certificat de serveur Web ONTAP sont utilisées.

```
cluster_12::> security saml-sp create -idp-uri
https://scspr0235321001.gdl.englab.netapp.com/idp/shibboleth -verify
-metadata-server false

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.63.56.150/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server
domain to ensure that users are the same for different authentication
methods. See the "security login show" command for the Data ONTAP user
configuration.
```

L'URL permettant d'accéder aux métadonnées de l'hôte ONTAP s'affiche.

2. À partir de l'hôte IDP, configurez le IDP avec les métadonnées de l'hôte ONTAP.

   Pour plus d'informations sur la configuration du IDP, reportez-vous à la documentation IDP.

3. Activer la configuration SAML :

   security saml-sp modify -is-enabled true

   Tout utilisateur existant qui accède à l' `http` ou `ontapi` L'application est automatiquement configurée pour l'authentification SAML.

4. Si vous souhaitez créer des utilisateurs pour le `http` ou `ontapi` Application après la configuration de SAML, spécifiez SAML comme méthode d'authentification pour les nouveaux utilisateurs.

   a. Créez une méthode de connexion pour les nouveaux utilisateurs avec l'authentification SAML : **security login create -user-or-group-name *user_name* -application [http | ontapi] -authentication-method saml -vserver *svm_name***

      ```
      cluster_12::> security login create -user-or-group-name admin1
      -application http -authentication-method saml -vserver  cluster_12
      ```

b. Vérifiez que l'entrée utilisateur est créée :

security login show

```
cluster_12::> security login show

Vserver: cluster_12
                                                                  Second
User/Group                Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
admin          console     password      admin            no     none
admin          http        password      admin            no     none
admin          http        saml          admin            -      none
admin          ontapi      password      admin            no     none
admin          ontapi      saml          admin            -      none
admin          service-processor
                           password      admin            no     none
admin          ssh         password      admin            no     none
admin1         http        password      backup           no     none
**admin1         http        saml          backup           -
none**
```

Informations associées

"Commandes de ONTAP 9"

Désactivez l'authentification SAML

Vous pouvez désactiver l'authentification SAML lorsque vous souhaitez arrêter l'authentification des utilisateurs Web à l'aide d'un fournisseur d'identité externe (IDP). Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés tels qu'Active Directory et LDAP sont utilisés pour l'authentification.

Ce dont vous avez besoin

Vous devez être connecté depuis la console.

Étapes

1. Désactiver l'authentification SAML :

   security saml-sp modify -is-enabled false

2. Si vous ne souhaitez plus utiliser l'authentification SAML ou si vous souhaitez modifier l'IDP, supprimez la configuration SAML :

   security saml-sp delete

Résolution des problèmes liés à la configuration SAML

Si la configuration de l'authentification SAML échoue, vous pouvez réparer manuellement chaque nœud sur lequel la configuration SAML a échoué et effectuer une restauration suite à la défaillance. Au cours du processus de réparation, le serveur Web est redémarré et toutes les connexions HTTP ou HTTPS actives sont interrompues.

Description de la tâche

Lorsque vous configurez l'authentification SAML, ONTAP applique la configuration SAML par nœud. Lorsque vous activez l'authentification SAML, ONTAP tente automatiquement de réparer chaque nœud en cas de problèmes de configuration. Si la configuration SAML est problématique sur n'importe quel nœud, vous pouvez désactiver l'authentification SAML, puis réactiver l'authentification SAML. Lorsque la configuration SAML ne s'applique pas à un ou plusieurs nœuds, même après la réactivation de l'authentification SAML, cela peut se présenter. Vous pouvez identifier le nœud sur lequel la configuration SAML a échoué, puis réparer manuellement ce nœud.

Étapes

1. Connectez-vous au niveau de privilège avancé :

   `set -privilege advanced`

2. Identifiez le nœud sur lequel la configuration SAML a échoué :

   `security saml-sp status show -instance`

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: config-failed
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

3. Corrigez la configuration SAML sur le nœud défaillant :

   `security saml-sp repair -node *node_name*`

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

Le serveur Web est redémarré et toutes les connexions HTTP ou HTTPS actives sont interrompues.

4. Vérifiez que le langage SAML est configuré sur tous les nœuds :

   security saml-sp status show -instance

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                 Update Status: **config-success**
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

Gérer les services Web

Présentation de la gestion des services Web

Vous pouvez activer ou désactiver un service Web pour le cluster ou une machine virtuelle de stockage (SVM), afficher les paramètres des services web et contrôler si les utilisateurs d'un rôle peuvent accéder à un service web.

Vous pouvez gérer les services web du cluster ou d'un SVM des manières suivantes :

- Activation ou désactivation d'un service Web spécifique

- Spécifier si l'accès à un service Web est limité à un seul HTTP crypté (SSL)
- Affichage de la disponibilité des services Web
- Autoriser ou interdire aux utilisateurs d'un rôle d'accéder à un service Web
- Affichage des rôles autorisés à accéder à un service Web

Pour qu'un utilisateur puisse accéder à un service Web, toutes les conditions suivantes doivent être remplies :

- L'utilisateur doit être authentifié.

  Par exemple, un service Web peut demander un nom d'utilisateur et un mot de passe. La réponse de l'utilisateur doit correspondre à un compte valide.

- L'utilisateur doit être configuré avec la méthode d'accès correcte.

  L'authentification ne réussit que pour les utilisateurs disposant de la méthode d'accès correcte pour le service Web donné. Pour le service Web de l'API ONTAP `ontapi`), les utilisateurs doivent avoir le `ontapi` méthode d'accès. Pour tous les autres services Web, les utilisateurs doivent avoir le `http` méthode d'accès.

  > Vous utilisez le `security login` commandes permettant de gérer les méthodes d'accès et les méthodes d'authentification des utilisateurs.

- Le service Web doit être configuré pour permettre le rôle de contrôle d'accès de l'utilisateur.

  > Vous utilisez le `vserver services web access` commandes permettant de contrôler l'accès d'un rôle à un service web.

Si un pare-feu est activé, la politique de pare-feu de la LIF à utiliser pour les services Web doit être configurée de manière à autoriser HTTP ou HTTPS.

Si vous utilisez HTTPS pour l'accès aux services Web, SSL pour le cluster ou le SVM qui offre le service Web doit également être activé et vous devez fournir un certificat numérique pour le cluster ou SVM.

Commandes pour la gestion des services Web

Vous utilisez le `vserver services web` Commandes permettant de gérer la disponibilité des services web pour le cluster ou une machine virtuelle de stockage (SVM). Vous utilisez le `vserver services web access` commandes permettant de contrôler l'accès d'un rôle à un service web.

Les fonctions que vous recherchez…	Utilisez cette commande…
Configurer un service web pour le cluster ou anSVM : • Activer ou désactiver un service Web • Spécifiez si seul HTTPS peut être utilisé pour accéder à un service Web	`vserver services web modify`

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher la configuration et la disponibilité des services web pour le cluster ou anSVM	`vserver services web show`
Autoriser un rôle à accéder à un service web sur le cluster ou anSVM	`vserver services web access create`
Afficher les rôles autorisés pour accéder aux services web sur le cluster ou anSVM	`vserver services web access show`
Empêcher un rôle d'accéder à un service Web sur le cluster ou anSVM	`vserver services web access delete`

Informations associées

"Commandes de ONTAP 9"

Commandes permettant de gérer les points de montage sur les nœuds

Le `spi` le service web crée automatiquement un point de montage d'un nœud vers le volume racine d'un autre nœud lors d'une demande d'accès aux fichiers journaux ou fichiers « core » du nœud. Bien que vous n'ayez pas besoin de gérer manuellement les points de montage, vous pouvez le faire en utilisant le `system node root-mount` commandes.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer manuellement un point de montage d'un nœud vers le volume racine d'un autre nœud	`system node root-mount create` Un seul point de montage peut exister d'un nœud à un autre.
Affiche les points de montage existants sur les nœuds du cluster, y compris le moment où un point de montage a été créé et son état actuel	`system node root-mount show`
Supprimez un point de montage d'un nœud vers le volume racine d'un autre nœud et force les connexions vers le point de montage à fermer	`system node root-mount delete`

Informations associées

"Commandes de ONTAP 9"

Gérer SSL

Le protocole SSL améliore la sécurité de l'accès au Web en utilisant un certificat numérique pour établir une connexion chiffrée entre un serveur Web et un navigateur.

Vous pouvez gérer SSL pour le cluster ou une machine virtuelle de stockage (SVM) de la manière suivante :

- Activation de SSL
- Génération et installation d'un certificat numérique et son association au cluster ou à la SVM
- Affichage de la configuration SSL pour voir si SSL a été activé et, le cas échéant, le nom du certificat SSL
- Configuration de politiques de pare-feu pour le cluster ou SVM, de sorte que les demandes d'accès Web puissent passer par
- Définition des versions SSL pouvant être utilisées
- Limiter l'accès aux requêtes HTTPS uniquement pour un service Web

Commandes pour la gestion de SSL

Vous utilisez le `security ssl` Commandes permettant de gérer le protocole SSL pour la machine virtuelle de stockage (SVM) du cluster ora.

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez le protocole SSL pour le SVM cluster et associez un certificat numérique à celui-ci	`security ssl modify`
Afficher la configuration SSL et le nom du certificat du SVM cluster	`security ssl show`

Configurer l'accès aux services Web

La configuration de l'accès aux services Web permet aux utilisateurs autorisés d'utiliser HTTP ou HTTPS pour accéder au contenu du service sur le cluster ou sur un SVM (Storage Virtual machine).

Étapes

1. Si un pare-feu est activé, assurez-vous que l'accès HTTP ou HTTPS est configuré dans la politique de pare-feu pour la LIF qui sera utilisée pour les services Web :

   Vous pouvez vérifier si un pare-feu est activé à l'aide du `system services firewall show` commande.

   a. Pour vérifier que HTTP ou HTTPS est configuré dans la stratégie de pare-feu, utilisez le `system services firewall policy show` commande.

      Vous définissez le `-service` paramètre du `system services firewall policy create` commande à `http` ou `https` pour activer la stratégie de prise en charge de l'accès web.

   b. Pour vérifier que la politique de pare-feu prenant en charge HTTP ou HTTPS est associée au LIF qui fournit des services Web, utilisez le `network interface show` commande avec `-firewall -policy` paramètre.

      Vous utilisez le `network interface modify` commande avec `-firewall-policy` Paramètre pour mettre la politique de pare-feu en vigueur pour une LIF.

2. Pour configurer le moteur de protocole Web au niveau du cluster et rendre le contenu du service Web

accessible, utilisez le `system services web modify` commande.

3. Si vous prévoyez d'utiliser des services Web sécurisés (HTTPS), activez SSL et fournissez les informations de certificat numérique pour le cluster ou la SVM à l'aide du `security ssl modify` commande.
4. Pour activer un service Web pour le cluster ou un SVM, utilisez le `vserver services web modify` commande.

   Vous devez répéter cette étape pour chaque service que vous souhaitez activer pour le cluster ou la SVM.

5. Pour autoriser un rôle permettant d'accéder aux services web sur le cluster ou SVM, utilisez la `vserver services web access create` commande.

   Le rôle auquel vous accordez l'accès doit déjà exister. Vous pouvez afficher les rôles existants à l'aide de la `security login role show` commande ou création de nouveaux rôles à l'aide de la commande `security login role create` commande.

6. Pour un rôle autorisé à accéder à un service Web, assurez-vous que ses utilisateurs sont également configurés avec la méthode d'accès correcte en vérifiant la sortie du `security login show` commande.

   Pour accéder au service Web de l'API ONTAP `ontapi`), un utilisateur doit être configuré avec le `ontapi` méthode d'accès. Pour accéder à tous les autres services Web, un utilisateur doit être configuré avec le `http` méthode d'accès.

   > Vous utilisez le `security login create` commande permettant d'ajouter une méthode d'accès pour un utilisateur.

Résoudre les problèmes d'accès au service Web

Des erreurs de configuration provoquent des problèmes d'accès au service Web. Vous pouvez corriger les erreurs en vous assurant que la LIF, la politique de pare-feu, le moteur de protocole Web, les services Web, les certificats numériques, et l'autorisation d'accès utilisateur sont toutes correctement configurées.

Le tableau suivant vous aide à identifier et à résoudre les erreurs de configuration du service Web :

Ce problème d'accès…	Se produit en raison de cette erreur de configuration…	Pour résoudre l'erreur…
Votre navigateur Web renvoie un `unable to connect` ou `failure to establish a connection` erreur lorsque vous essayez d'accéder à un service web.	Votre LIF n'est peut-être pas configurée correctement.	Assurez-vous de pouvoir envoyer une requête ping à la LIF qui fournit le service Web. Vous utilisez le `network ping` Commande ping d'une LIF. Pour plus d'informations sur la configuration du réseau, reportez-vous au *Network Management Guide*.
Votre pare-feu est peut-être configuré de manière incorrecte.	Assurez-vous qu'une politique de pare-feu est configurée pour prendre en charge HTTP ou HTTPS et que la politique est attribuée à la LIF qui fournit le service Web. Vous utilisez le `system services firewall policy` commandes permettant de gérer les politiques de pare-feu. Vous utilisez le `network interface modify` commande avec `-firewall-policy` Paramètre pour associer une policy à une LIF.	Votre moteur de protocole Web peut être désactivé.
Assurez-vous que le moteur de protocole Web est activé pour que les services Web soient accessibles. Vous utilisez le `system services web` commandes permettant de gérer le moteur de protocole web pour le cluster.	Votre navigateur Web renvoie un `not found` erreur lorsque vous essayez d'accéder à un service web.	Le service Web est peut-être désactivé.

Ce problème d'accès…	Se produit en raison de cette erreur de configuration…	Pour résoudre l'erreur…
Assurez-vous que chaque service Web auquel vous souhaitez autoriser l'accès est activé individuellement. Vous utilisez le `vserver services web modify` commande permettant d'activer un service web pour l'accès.	Le navigateur Web ne parvient pas à se connecter à un service Web avec le nom de compte et le mot de passe d'un utilisateur.	L'utilisateur ne peut pas être authentifié, la méthode d'accès n'est pas correcte ou l'utilisateur n'est pas autorisé à accéder au service Web.
Assurez-vous que le compte utilisateur existe et est configuré avec la méthode d'accès et la méthode d'authentification appropriées. Assurez-vous également que le rôle de l'utilisateur est autorisé à accéder au service Web. Vous utilisez le `security login` commandes permettant de gérer les comptes utilisateurs, leurs méthodes d'accès et leurs méthodes d'authentification. Pour accéder au service Web de l'API ONTAP, vous devez utiliser le `ontapi` méthode d'accès. L'accès à tous les autres services Web nécessite le `http` méthode d'accès. Vous utilisez le `vserver services web access` commandes permettant de gérer l'accès d'un rôle à un service web.	Vous vous connectez à votre service Web via HTTPS et votre navigateur Web indique que votre connexion est interrompue.	Il se peut que vous n'ayez pas activé SSL sur le cluster ou la machine virtuelle de stockage (SVM) qui fournit le service Web.

Ce problème d'accès…	Se produit en raison de cette erreur de configuration…	Pour résoudre l'erreur…
S'assurer que le cluster ou le SVM a activé SSL et que le certificat numérique est valide. Vous utilisez le `security ssl` Commandes permettant de gérer la configuration SSL des serveurs HTTP et du `security certificate show` commande permettant d'afficher les informations relatives au certificat numérique.	Vous vous connectez à votre service Web via HTTPS et votre navigateur Web indique que la connexion n'est pas fiable.	Vous utilisez peut-être un certificat numérique auto-signé.

Vérifiez l'identité des serveurs distants à l'aide de certificats

Vérifiez l'identité des serveurs distants à l'aide de la présentation des certificats

ONTAP prend en charge les fonctions de certificat de sécurité pour vérifier l'identité des serveurs distants.

Le logiciel ONTAP permet des connexions sécurisées à l'aide des fonctionnalités et protocoles de certificat numérique suivants :

- Le protocole OCSP (Online Certificate Status Protocol) valide le statut des demandes de certificat numérique des services ONTAP à l'aide de connexions SSL et TLS (transport Layer Security). Cette fonction est désactivée par défaut.
- Un ensemble par défaut de certificats racine de confiance est inclus avec le logiciel ONTAP.
- Les certificats KMIP (Key Management Interoperability Protocol) permettent d'effectuer une authentification mutuelle d'un cluster et d'un serveur KMIP.

Vérifiez que les certificats numériques sont valides à l'aide du protocole OCSP

Depuis ONTAP 9.2, le protocole OCSP (Online Certificate Status Protocol) permet aux applications ONTAP qui utilisent les communications TLS (transport Layer Security) de recevoir le statut du certificat numérique lorsque le protocole OCSP est activé. Vous pouvez à tout moment activer ou désactiver les vérifications d'état des certificats OCSP pour des applications spécifiques. Par défaut, la vérification du statut du certificat OCSP est désactivée.

Ce dont vous avez besoin

Ces commandes doivent être exécutées au niveau de privilège avancé.

Description de la tâche

OCSP prend en charge les applications suivantes :

- AutoSupport
- Système de gestion des événements (EMS)
- LDAP sur TLS
- Protocole KMIP (Key Management Interoperability Protocol)
- Consignation d'audits
- FabricPool

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`.
2. Pour activer ou désactiver les vérifications du statut des certificats OCSP pour des applications ONTAP spécifiques, utilisez la commande appropriée.

Si vous souhaitez que l'état du certificat OCSP soit vérifié pour certaines applications…	Utilisez la commande…
Activé	`security config ocsp enable -app app name`
Désactivé	`security config ocsp disable -app app name`

   La commande suivante active la prise en charge OCSP pour AutoSupport et EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

   Lorsque OCSP est activé, l'application reçoit l'une des réponses suivantes :

   - Bon - le certificat est valide et la communication continue.
   - Révoqué - le certificat est considéré comme non digne de confiance par son autorité de certification émettrice et la communication ne peut pas se poursuivre.
   - Inconnu - le serveur n'a pas d'informations d'état sur le certificat et la communication ne peut pas se poursuivre.
   - Il manque des informations de serveur OCSP dans le certificat. Le serveur agit comme si OCSP est désactivé et continue avec la communication TLS, mais aucune vérification d'état n'a lieu.
   - Aucune réponse du serveur OCSP - l'application ne peut pas continuer.
3. Pour activer ou désactiver les vérifications d'état des certificats OCSP pour toutes les applications utilisant les communications TLS, utilisez la commande appropriée.

Si vous souhaitez que l'état du certificat OCSP soit vérifié pour toutes les applications…	Utilisez la commande…
Activé	`security config ocsp enable -app all`
Désactivé	`security config ocsp disable -app all`

Lorsque cette option est activée, toutes les applications reçoivent une réponse signée indiquant le statut du certificat spécifié : bon, révoqué ou inconnu. Dans le cas d'un certificat révoqué, l'application ne pourra pas continuer. Si l'application ne parvient pas à recevoir de réponse du serveur OCSP ou si le serveur est inaccessible, l'application ne pourra pas continuer.

4. Utilisez le `security config ocsp show` Commande pour afficher toutes les applications qui prennent en charge OCSP et leur état de support.

```
cluster::*> security config ocsp show
         Application                     OCSP Enabled?
         --------------------            ---------------------
         autosupport                     false
         audit_log                       false
         fabricpool                      false
         ems                             false
         kmip                            false
         ldap_ad                         true
         ldap_nis_namemap                true

         7 entries were displayed.
```

Afficher les certificats par défaut pour les applications basées sur TLS

Depuis ONTAP 9.2, ONTAP fournit un ensemble par défaut de certificats racine de confiance pour les applications ONTAP utilisant TLS (transport Layer Security).

Ce dont vous avez besoin

Les certificats par défaut ne sont installés que sur le SVM d'admin pendant sa création ou lors d'une mise à niveau vers ONTAP 9.2.

Description de la tâche

Les applications actuelles qui agissent en tant que client et qui nécessitent une validation de certificat sont AutoSupport, EMS, LDAP, Audit Logging, FabricPool, Et KMIP.

Lorsque les certificats expirent, un message EMS est appelé pour demander à l'utilisateur de supprimer les certificats. Les certificats par défaut ne peuvent être supprimés qu'au niveau de privilège avancé.

La suppression des certificats par défaut peut entraîner l'absence de fonctionnement de certaines applications ONTAP (par exemple, AutoSupport et Audit Logging).

Étape

1. Vous pouvez afficher les certificats par défaut qui sont installés sur le SVM d'admin en utilisant la commande Security Certificate show :

   security certificate show -vserver -type server-ca

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver    Serial Number   Common Name                              Type
---------- --------------- ---------------------------------------
------------
fas2552-2n-abc-3
           01              AAACertificateServices
server-ca
    Certificate Authority: AAA Certificate Services
          Expiration Date: Sun Dec 31 18:59:59 2028
```

Authentification mutuelle du cluster et d'un serveur KMIP

Authentification mutuelle du cluster et présentation d'un serveur KMIP

L'authentification mutuelle du cluster et d'un gestionnaire de clés externe, tel qu'un serveur KMIP (Key Management Interoperability Protocol), permettent au gestionnaire de clés de communiquer avec le cluster via KMIP sur SSL. Dans ce cas, une application ou certaines fonctionnalités (par exemple, la fonctionnalité Storage Encryption) nécessitent des clés sécurisées pour assurer un accès sécurisé aux données.

Générer une demande de signature de certificat pour le cluster

Vous pouvez utiliser le certificat de sécurité `generate-csr` Commande pour générer une requête de signature de certificat (CSR). Après le traitement de votre demande, l'autorité de certification vous envoie le certificat numérique signé.

Ce dont vous avez besoin

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou un administrateur SVM.

Étapes

1. Générer une RSC :

   security certificate generate-csr -common-name *FQDN_or_common_name* -size 512|1024|1536|2048 -country *country* -state *state* -locality *locality* -organization *organization* -unit *unit* -email-addr *email_of_contact* -hash -function SHA1|SHA256|MD5

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande suivante crée une RSC avec une clé privée de 2,048 bits générée par la fonction de hachage SHA256, utilisée par le groupe Software dans LE département IT d'une société dont le nom commun personnalisé est server1.companyname.com, située à Sunnyvale (Californie), aux États-Unis. L'adresse e-mail de l'administrateur du contact SVM est web@example.com. Le système affiche la RSC et la clé privée dans la sortie.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Copiez la demande de certificat à partir de la sortie CSR, puis envoyez-la sous forme électronique (par exemple, un courriel) à une autorité de certification tierce approuvée pour signature.

   Après le traitement de votre demande, l'AC vous envoie le certificat numérique signé. Vous devez conserver une copie de la clé privée et du certificat numérique signé par l'autorité de certification.

Installez un certificat de serveur signé par l'autorité de certification pour le cluster

Pour permettre à un serveur SSL d'authentifier le cluster ou la machine virtuelle de stockage (SVM) en tant que client SSL, vous installez un certificat numérique avec le type client sur le cluster ou le SVM. Ensuite, vous fournissez le certificat client-CA à l'administrateur du serveur SSL pour l'installation sur le serveur.

Ce dont vous avez besoin

Vous devez déjà avoir installé le certificat root du serveur SSL sur le cluster ou SVM avec le `server-ca` type de certificat.

Étapes

1. Pour utiliser un certificat numérique auto-signé pour l'authentification client, utilisez le `security certificate create` commande avec `type client` paramètre.
2. Pour utiliser un certificat numérique signé par une autorité de certification pour l'authentification client, procédez comme suit :

   a. Générez une demande de signature de certificat numérique (RSC) à l'aide du certificat de sécurité `generate-csr` commande.

      ONTAP affiche la sortie CSR, qui comprend une demande de certificat et une clé privée, et vous rappelle de copier la sortie dans un fichier pour référence ultérieure.

   b. Envoyez la demande de certificat de la sortie CSR sous forme électronique (par exemple, un courriel) à une autorité de certification approuvée pour signature.

      Vous devez conserver une copie de la clé privée et du certificat signé par l'AC pour référence ultérieure.

   Après le traitement de votre demande, l'AC vous envoie le certificat numérique signé.

   a. Installez le certificat signé par l'autorité de certification à l'aide du `security certificate install` commande avec `-type client` paramètre.
   b. Entrez le certificat et la clé privée lorsque vous y êtes invité, puis appuyez sur **entrée**.
   c. Entrez tout certificat racine ou intermédiaire supplémentaire lorsque vous y êtes invité, puis appuyez sur **entrée**.

      Vous installez un certificat intermédiaire sur le cluster ou le SVM si une chaîne de certificats qui commence à l'autorité de certification racine de confiance et se termine par le certificat SSL qui vous est délivré, manque les certificats intermédiaires. Un certificat intermédiaire est un certificat subordonné délivré par la racine de confiance spécifiquement pour délivrer des certificats de serveur d'entité finale. Le résultat est une chaîne de certificats qui commence au niveau de l'autorité de certification racine de confiance, passe par le certificat intermédiaire et se termine par le certificat SSL qui vous a été délivré.

3. Fournir le `client-ca` Certificat du cluster ou SVM à l'administrateur du serveur SSL pour installation sur le serveur.

   Commande du certificat de sécurité show avec `-instance` et `-type client-ca` paramètres affiche le `client-ca` informations sur le certificat.

Installez un certificat client signé par une autorité de certification pour le serveur KMIP

Le sous-type de certificat du protocole KMIP (Key Management Interoperability Protocol) (paramètre -subtype kmip-cert), ainsi que les types client et serveur-ca, spécifie que le certificat est utilisé pour authentifier mutuellement le cluster et un gestionnaire de clés externe, comme un serveur KMIP.

Description de la tâche

Installez un certificat KMIP pour authentifier un serveur KMIP en tant que serveur SSL sur le cluster.

Étapes

1. Utilisez le `security certificate install` commande avec `-type server-ca` et `-subtype kmip-cert` Paramètres pour installer un certificat KMIP pour le serveur KMIP.
2. Lorsque vous y êtes invité, entrez le certificat, puis appuyez sur entrée.

   ONTAP vous rappelle de conserver une copie du certificat à des fins de référence ultérieure.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

Informations sur le copyright

Informations sur les marques commerciales