Gérez votre système

Element Software

NetApp
November 12, 2025

Sommaire

Gérez votre système

Gérez votre système

Vous pouvez gérer votre système dans l'interface utilisateur Element. Cela inclut l'activation de l'authentification multifactorielle, la gestion des paramètres de cluster, la prise en charge des normes fédérales de traitement de l'information (FIPS) et l'utilisation de la gestion externe des clés.

- "Activer l'authentification multifacteur"
- "Configurer les paramètres du cluster"
- "Créer un cluster prenant en charge les disques FIPS"
- "Commencez la gestion des clés externes"

Pour plus d'informations

- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Activer l'authentification multifacteur

Configurer l'authentification multifacteurs

L'authentification multifactorielle (MFA) utilise un fournisseur d'identité tiers (IdP) via le langage de balisage d'assertion de sécurité (SAML) pour gérer les sessions utilisateur. L'authentification multifacteur (MFA) permet aux administrateurs de configurer des facteurs d'authentification supplémentaires selon les besoins, tels que mot de passe et SMS, ou mot de passe et e-mail.

Vous pouvez utiliser ces étapes de base via l'API Element pour configurer votre cluster afin d'utiliser l'authentification multifactorielle.

Vous trouverez des informations détaillées sur chaque méthode de l'API dans le "Référence de l'API Element".

1. Créez une nouvelle configuration de fournisseur d'identité (IdP) tiers pour le cluster en appelant la méthode API suivante et en transmettant les métadonnées IdP au format JSON : `CreateIdpConfiguration`

   Les métadonnées IdP, au format texte brut, sont récupérées auprès du fournisseur d'identité tiers. Ces métadonnées doivent être validées afin de garantir leur formatage correct en JSON. De nombreuses applications de formatage JSON sont disponibles et peuvent être utilisées, par exemple : https://freeformatter.com/json-escape.html.

2. Récupérez les métadonnées du cluster, via spMetadataUrl, pour les copier sur le fournisseur d'identité tiers en appelant la méthode API suivante : `ListIdpConfigurations`

   spMetadataUrl est une URL utilisée pour récupérer les métadonnées du fournisseur de services du cluster pour l'IdP afin d'établir une relation de confiance.

3. Configurez les assertions SAML sur le fournisseur d'identité tiers pour inclure l'attribut « `NameID` » afin d'identifier de manière unique un utilisateur pour la journalisation d'audit et pour que la déconnexion unique fonctionne correctement.
4. Créez un ou plusieurs comptes d'utilisateur d'administrateur de cluster authentifiés par un fournisseur d'identité tiers pour l'autorisation en appelant la méthode API suivante :`AddIdpClusterAdmin`

> Le nom d'utilisateur de l'administrateur du cluster IdP doit correspondre à la correspondance Nom/Valeur de l'attribut SAML pour obtenir l'effet souhaité, comme illustré dans les exemples suivants :

   - email=bob@company.com — où le fournisseur d'identité est configuré pour diffuser une adresse électronique dans les attributs SAML.
   - groupe=administrateur-cluster - où le fournisseur d'identité est configuré pour libérer une propriété de groupe à laquelle tous les utilisateurs doivent avoir accès. Notez que, pour des raisons de sécurité, la paire nom/valeur de l'attribut SAML est sensible à la casse.
5. Activez l'authentification multifacteur (MFA) pour le cluster en appelant la méthode API suivante : `EnableIdpAuthentication`

Trouver plus d'informations

- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Informations complémentaires concernant l'authentification multifactorielle

Vous devez prendre en compte les mises en garde suivantes concernant l'authentification multifacteurs.

- Pour actualiser les certificats IdP qui ne sont plus valides, vous devrez utiliser un compte utilisateur administrateur non IdP pour appeler la méthode API suivante : `UpdateIdpConfiguration`
- L'authentification multifacteur (MFA) est incompatible avec les certificats dont la longueur est inférieure à 2048 bits. Par défaut, un certificat SSL 2048 bits est créé sur le cluster. Vous devez éviter d'utiliser un certificat de taille inférieure lors de l'appel de la méthode API : `SetSSLCertificate`

> Si le cluster utilise un certificat de moins de 2048 bits avant la mise à niveau, le certificat du cluster doit être mis à jour avec un certificat de 2048 bits ou plus après la mise à niveau vers Element 12.0 ou une version ultérieure.

- Les utilisateurs administrateurs IdP ne peuvent pas être utilisés pour effectuer directement des appels API (par exemple, via des SDK ou Postman) ni pour d'autres intégrations (par exemple, OpenStack Cinder ou le plug-in vCenter). Ajoutez des utilisateurs administrateurs de cluster LDAP ou des utilisateurs administrateurs de cluster local si vous devez créer des utilisateurs disposant de ces capacités.

Trouver plus d'informations

- "Gestion du stockage avec l'API Element"
- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Configurer les paramètres du cluster

Activer et désactiver le chiffrement au repos pour un cluster

Avec les clusters SolidFire , vous pouvez chiffrer toutes les données au repos stockées sur les disques du cluster. Vous pouvez activer la protection à l'échelle du cluster des disques à chiffrement automatique (SED) en utilisant soit"chiffrement matériel ou logiciel au repos" .

Vous pouvez activer le chiffrement matériel au repos via l'interface utilisateur ou l'API d'Element. L'activation du chiffrement matériel au repos n'affecte ni les performances ni l'efficacité du cluster. Vous pouvez activer le chiffrement logiciel au repos uniquement à l'aide de l'API Element.

Le chiffrement matériel au repos n'est pas activé par défaut lors de la création du cluster et peut être activé et désactivé depuis l'interface utilisateur d'Element.

> Pour les clusters de stockage 100 % flash SolidFire , le chiffrement logiciel au repos doit être activé lors de la création du cluster et ne peut pas être désactivé après sa création.

Ce dont vous aurez besoin

- Vous disposez des privilèges d'administrateur de cluster pour activer ou modifier les paramètres de chiffrement.
- Pour le chiffrement matériel au repos, vous devez vous assurer que le cluster est en bon état avant de modifier les paramètres de chiffrement.
- Si vous désactivez le chiffrement, deux nœuds doivent participer à un cluster pour accéder à la clé permettant de désactiver le chiffrement sur un disque.

Vérifier l'état du chiffrement au repos

Pour consulter l'état actuel du chiffrement au repos et/ou du chiffrement logiciel au repos sur le cluster, utilisez"Obtenir les informations du cluster" méthode. Vous pouvez utiliser le"GetSoftwareEncryptionAtRestInfo" méthode permettant d'obtenir des informations sur la manière dont le cluster chiffre les données au repos.

> Le tableau de bord de l'interface utilisateur du logiciel Element à `https://<MVIP>/` Actuellement, seul l'état du chiffrement au repos est affiché pour le chiffrement matériel.

Options

- Activer le chiffrement matériel au repos
- Activer le chiffrement logiciel au repos
- Désactiver le chiffrement matériel au repos

Activer le chiffrement matériel au repos

> Pour activer le chiffrement au repos à l'aide d'une configuration de gestion de clés externe, vous devez activer le chiffrement au repos via le"API" . L'activation via le bouton Element UI existant rétablira l'utilisation des clés générées en interne.

1. Dans l'interface utilisateur d'Element, sélectionnez **Cluster** > **Paramètres**.

2. Sélectionnez **Activer le chiffrement au repos**.

Activer le chiffrement logiciel au repos

Le chiffrement logiciel au repos ne peut pas être désactivé après avoir été activé sur le cluster.

1. Lors de la création du cluster, exécutez la"méthode de création de cluster" avec `enableSoftwareEncryptionAtRest` défini à `true` .

Désactiver le chiffrement matériel au repos

1. Dans l'interface utilisateur d'Element, sélectionnez **Cluster** > **Paramètres**.
2. Sélectionnez **Désactiver le chiffrement au repos**.

Trouver plus d'informations

- "Documentation logicielle SolidFire et Element"
- "Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"

Définir le seuil de saturation du cluster

Vous pouvez modifier le niveau auquel le système génère un avertissement de saturation des clusters de blocs en suivant les étapes ci-dessous. De plus, vous pouvez utiliser la méthode API ModifyClusterFullThreshold pour modifier le niveau auquel le système génère un avertissement de blocage ou de métadonnées.

Ce dont vous aurez besoin

Vous devez disposer des privilèges d'administrateur de cluster.

Étapes

1. Cliquez sur **Cluster** > **Paramètres**.
2. Dans la section Paramètres complets du cluster, saisissez un pourcentage dans **Déclencher une alerte d'avertissement lorsque _% de capacité restante avant que Helix ne puisse pas se remettre d'une panne de nœud**.
3. Cliquez sur **Enregistrer les modifications**.

Trouver plus d'informations

"Comment les seuils d'espace bloc sont-ils calculés pour l'élément"

Activer et désactiver l'équilibrage de charge des volumes

À partir d'Element 12.8, vous pouvez utiliser l'équilibrage de charge des volumes pour répartir les volumes entre les nœuds en fonction des IOPS réelles de chaque volume au lieu des IOPS minimales configurées dans la politique QoS. Vous pouvez activer et désactiver l'équilibrage de charge volumétrique, désactivé par défaut, via l'interface utilisateur ou l'API d'Element.

Étapes

1. Sélectionnez **Cluster** > **Paramètres**.
2. Dans la section Spécifique au cluster, modifiez l'état de l'équilibrage de charge des volumes :

   Activer l'équilibrage de charge volumétrique

   Sélectionnez **Activer l'équilibrage de charge sur les IOPS réelles**, puis confirmez votre sélection.

   Désactiver l'équilibrage de charge volumétrique :

   Sélectionnez **Désactiver l'équilibrage de charge sur les IOPS réelles**, puis confirmez votre sélection.

3. Vous pouvez également sélectionner **Rapports** > **Aperçu** pour confirmer le changement d'état du solde des IOPS réelles. Vous devrez peut-être faire défiler vers le bas les informations sur l'état du cluster pour en consulter le statut.

Trouver plus d'informations

- "Activez l'équilibrage de charge volumétrique à l'aide de l'API"
- "Désactiver l'équilibrage de charge volumétrique via l'API"
- "Créer et gérer des politiques QoS de volume"

Activer et désactiver l'accès au support

Vous pouvez activer l'accès de support pour permettre temporairement au personnel de support NetApp d'accéder aux nœuds de stockage via SSH à des fins de dépannage.

Vous devez disposer des privilèges d'administrateur de cluster pour modifier l'accès au support.

1. Cliquez sur **Cluster** > **Paramètres**.
2. Dans la section Activer/Désactiver l'accès au support, saisissez la durée (en heures) pendant laquelle vous souhaitez autoriser le support à avoir accès.
3. Cliquez sur **Activer l'accès au support**.
4. **Facultatif :** Pour désactiver l'accès au support, cliquez sur **Désactiver l'accès au support**.

Bannière Gérer les conditions d'utilisation

Vous pouvez activer, modifier ou configurer une bannière contenant un message destiné à l'utilisateur.

Options

Activer la bannière des conditions d'utilisation Modifier la bannière des conditions d'utilisation Désactiver la bannière des conditions d'utilisation

Activer la bannière des conditions d'utilisation

Vous pouvez activer une bannière de conditions d'utilisation qui s'affiche lorsqu'un utilisateur se connecte à l'interface utilisateur d'Element. Lorsque l'utilisateur clique sur la bannière, une boîte de dialogue s'affiche contenant le message que vous avez configuré pour le cluster. La bannière peut être retirée à tout moment.

Vous devez disposer des privilèges d'administrateur de cluster pour activer la fonctionnalité des conditions d'utilisation.

1. Cliquez sur **Utilisateurs** > **Conditions d'utilisation**.
2. Dans le formulaire **Conditions d'utilisation**, saisissez le texte à afficher dans la boîte de dialogue Conditions d'utilisation.

   Ne pas dépasser 4096 caractères.

3. Cliquez sur **Activer**.

Modifier la bannière des conditions d'utilisation

Vous pouvez modifier le texte que voit un utilisateur lorsqu'il sélectionne la bannière de connexion aux conditions d'utilisation.

Ce dont vous aurez besoin

- Vous devez disposer des privilèges d'administrateur de cluster pour configurer les conditions d'utilisation.
- Assurez-vous que la fonctionnalité « Conditions d'utilisation » est activée.

Étapes

1. Cliquez sur **Utilisateurs** > **Conditions d'utilisation**.
2. Dans la boîte de dialogue **Conditions d'utilisation**, modifiez le texte que vous souhaitez afficher.

   Ne pas dépasser 4096 caractères.

3. Cliquez sur **Enregistrer les modifications**.

Désactiver la bannière des conditions d'utilisation

Vous pouvez désactiver la bannière des conditions d'utilisation. Lorsque la bannière est désactivée, l'utilisateur n'est plus tenu d'accepter les conditions d'utilisation lors de l'utilisation de l'interface utilisateur Element.

Ce dont vous aurez besoin

- Vous devez disposer des privilèges d'administrateur de cluster pour configurer les conditions d'utilisation.
- Assurez-vous que les conditions d'utilisation sont activées.

Étapes

1. Cliquez sur **Utilisateurs** > **Conditions d'utilisation**.
2. Cliquez sur **Désactiver**.

Configurer le protocole de temps réseau

Configurer les serveurs NTP (Network Time Protocol) pour que le cluster puisse interroger les serveurs.

Vous pouvez configurer chaque nœud d'un cluster pour qu'il interroge un serveur NTP (Network Time Protocol) afin d'obtenir les mises à jour. Le cluster contacte uniquement les serveurs configurés et leur demande des informations NTP.

Le protocole NTP est utilisé pour synchroniser les horloges sur un réseau. La connexion à un serveur NTP interne ou externe doit faire partie de la configuration initiale du cluster.

Configurez le protocole NTP sur le cluster pour qu'il pointe vers un serveur NTP local. Vous pouvez utiliser l'adresse IP ou le nom d'hôte FQDN. Le serveur NTP par défaut lors de la création du cluster est défini sur us.pool.ntp.org ; cependant, une connexion à ce site ne peut pas toujours être établie en fonction de l'emplacement physique du cluster SolidFire .

L'utilisation du nom de domaine pleinement qualifié (FQDN) dépend de la présence et du bon fonctionnement des paramètres DNS du nœud de stockage individuel. Pour ce faire, configurez les serveurs DNS sur chaque nœud de stockage et assurez-vous que les ports sont ouverts en consultant la page « Configuration requise pour les ports réseau ».

Vous pouvez saisir jusqu'à cinq serveurs NTP différents.

Vous pouvez utiliser les adresses IPv4 et IPv6.

Ce dont vous aurez besoin

Vous devez disposer des privilèges d'administrateur de cluster pour configurer ce paramètre.

Étapes

1. Configurez une liste d'adresses IP et/ou de noms de domaine pleinement qualifiés (FQDN) dans les paramètres du serveur.
2. Vérifiez que le DNS est correctement configuré sur les nœuds.
3. Cliquez sur **Cluster** > **Paramètres**.
4. Dans les paramètres du protocole NTP (Network Time Protocol), sélectionnez **Non**, ce qui utilise la configuration NTP standard.
5. Cliquez sur **Enregistrer les modifications**.

Trouver plus d'informations

- "Configurez le cluster pour qu'il écoute les diffusions NTP."
- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Configurez le cluster pour qu'il écoute les diffusions NTP.

En utilisant le mode de diffusion, vous pouvez demander à chaque nœud d'un cluster d'écouter sur le réseau les messages de diffusion du protocole NTP (Network Time Protocol) provenant d'un serveur particulier.

Le protocole NTP est utilisé pour synchroniser les horloges sur un réseau. La connexion à un serveur NTP interne ou externe doit faire partie de la configuration initiale du cluster.

Ce dont vous aurez besoin

- Vous devez disposer des privilèges d'administrateur de cluster pour configurer ce paramètre.
- Vous devez configurer un serveur NTP sur votre réseau en tant que serveur de diffusion.

Étapes

1. Cliquez sur **Cluster** > **Paramètres**.
2. Saisissez le ou les serveurs NTP utilisant le mode de diffusion dans la liste des serveurs.
3. Dans les paramètres du protocole de temps réseau, sélectionnez **Oui** pour utiliser un client de diffusion.
4. Pour configurer le client de diffusion, dans le champ **Serveur**, saisissez le serveur NTP que vous avez configuré en mode diffusion.
5. Cliquez sur **Enregistrer les modifications**.

Trouver plus d'informations

- "Configurer les serveurs NTP (Network Time Protocol) pour que le cluster puisse interroger les serveurs."
- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Gérer les SNMP

En savoir plus sur SNMP

Vous pouvez configurer le protocole SNMP (Simple Network Management Protocol) dans votre cluster.

Vous pouvez sélectionner un demandeur SNMP, choisir la version de SNMP à utiliser, identifier l'utilisateur du modèle de sécurité basé sur l'utilisateur (USM) SNMP et configurer les traps pour surveiller le cluster SolidFire . Vous pouvez également consulter et accéder aux fichiers de base d'informations de gestion.

Vous pouvez utiliser les adresses IPv4 et IPv6.

Détails SNMP

Sur la page SNMP de l'onglet Cluster, vous pouvez consulter les informations suivantes.

- **MIB SNMP**

  Les fichiers MIB que vous pouvez consulter ou télécharger.

- **Paramètres SNMP généraux**

  Vous pouvez activer ou désactiver le protocole SNMP. Une fois le protocole SNMP activé, vous pouvez choisir la version à utiliser. Si vous utilisez la version 2, vous pouvez ajouter des demandeurs, et si vous utilisez la version 3, vous pouvez configurer des utilisateurs USM.

- **Paramètres des pièges SNMP**

  Vous pouvez identifier les pièges que vous souhaitez capturer. Vous pouvez définir l'hôte, le port et la chaîne communautaire pour chaque destinataire de trap.

Configurer un demandeur SNMP

Lorsque la version 2 de SNMP est activée, vous pouvez activer ou désactiver un demandeur et configurer les demandeurs pour recevoir les requêtes SNMP autorisées.

1. Cliquez sur le menu : Cluster [SNMP].
2. Sous **Paramètres SNMP généraux**, cliquez sur **Oui** pour activer SNMP.
3. Dans la liste **Version**, sélectionnez **Version 2**.
4. Dans la section **Demandeurs**, saisissez la **Chaîne de communauté** et les informations du **Réseau**.

> Par défaut, la chaîne de communauté est publique et le réseau est localhost. Vous pouvez modifier ces paramètres par défaut.

5. **Facultatif :** Pour ajouter un autre demandeur, cliquez sur **Ajouter un demandeur** et saisissez les informations de la **chaîne de communauté** et du **réseau**.
6. Cliquez sur **Enregistrer les modifications**.

Trouver plus d'informations

- Configurer les traps SNMP
- Afficher les données des objets gérés à l'aide des fichiers de base d'informations de gestion

Configurer un utilisateur SNMP USM

Lorsque vous activez la version 3 de SNMP, vous devez configurer un utilisateur USM pour recevoir les requêtes SNMP autorisées.

1. Cliquez sur **Cluster** > **SNMP**.
2. Sous **Paramètres SNMP généraux**, cliquez sur **Oui** pour activer SNMP.
3. Dans la liste **Version**, sélectionnez **Version 3**.
4. Dans la section **Utilisateurs USM**, saisissez le nom, le mot de passe et la phrase secrète.
5. **Facultatif :** Pour ajouter un autre utilisateur USM, cliquez sur **Ajouter un utilisateur USM** et saisissez le nom, le mot de passe et la phrase secrète.
6. Cliquez sur **Enregistrer les modifications**.

Configurer les traps SNMP

Les administrateurs système peuvent utiliser les traps SNMP, également appelés notifications, pour surveiller l'état du cluster SolidFire .

Lorsque les traps SNMP sont activés, le cluster SolidFire génère des traps associés aux entrées du journal des événements et aux alertes système. Pour recevoir des notifications SNMP, vous devez choisir les traps à générer et identifier les destinataires des informations de trap. Par défaut, aucun piège n'est généré.

1. Cliquez sur **Cluster** > **SNMP**.
2. Dans la section **Paramètres des traps SNMP**, sélectionnez un ou plusieurs types de traps que le système doit générer :
   - Pièges à défauts de cluster
   - Pièges de défauts résolus par cluster
   - Pièges à événements de cluster
3. Dans la section **Destinataires du piège**, saisissez les informations d'hôte, de port et de chaîne

communautaire d'un destinataire.

4. **Facultatif** : Pour ajouter un autre destinataire de trap, cliquez sur **Ajouter un destinataire de trap** et saisissez les informations d'hôte, de port et de chaîne communautaire.
5. Cliquez sur **Enregistrer les modifications**.

Afficher les données des objets gérés à l'aide des fichiers de base d'informations de gestion

Vous pouvez consulter et télécharger les fichiers de base d'informations de gestion (MIB) utilisés pour définir chacun des objets gérés. La fonctionnalité SNMP prend en charge l'accès en lecture seule aux objets définis dans la MIB SolidFire-StorageCluster.

Les données statistiques fournies dans le MIB présentent l'activité du système pour les éléments suivants :

- Statistiques de cluster
- Statistiques de volume
- Statistiques des volumes par compte
- Statistiques des nœuds
- D'autres données telles que les rapports, les erreurs et les événements système

Le système prend également en charge l'accès au fichier MIB contenant les points d'accès de niveau supérieur (OIDS) aux produits de la série SF.

Étapes

1. Cliquez sur **Cluster** > **SNMP**.
2. Sous **MIB SNMP**, cliquez sur le fichier MIB que vous souhaitez télécharger.
3. Dans la fenêtre de téléchargement qui s'affiche, ouvrez ou enregistrez le fichier MIB.

Gérer les lecteurs

Chaque nœud contient un ou plusieurs disques physiques utilisés pour stocker une partie des données du cluster. Le cluster utilise la capacité et les performances du disque une fois celui-ci ajouté avec succès au cluster. Vous pouvez utiliser l'interface utilisateur Element pour gérer les lecteurs.

Détails des lecteurs

La page Lecteurs de l'onglet Cluster affiche la liste des lecteurs actifs du cluster. Vous pouvez filtrer la page en sélectionnant les onglets Actifs, Disponibles, En cours de suppression, En cours d'effacement et Échecs.

Lors de la première initialisation d'un cluster, la liste des disques actifs est vide. Vous pouvez ajouter des disques non affectés à un cluster et répertoriés dans l'onglet Disponible après la création d'un nouveau cluster SolidFire .

Les éléments suivants apparaissent dans la liste des lecteurs actifs.

- **ID du lecteur**

  Le numéro séquentiel attribué au lecteur.

- **ID du nœud**

  Le numéro de nœud attribué lors de l'ajout du nœud au cluster.

- **Nom du nœud**

  Le nom du nœud qui héberge le disque.

- **Fente**

  Le numéro d'emplacement où se trouve physiquement le lecteur.

- **Capacité**

  La taille du disque, en Go.

- **En série**

  Le numéro de série du disque.

- **Usure restante**

  Indicateur de niveau d'usure.

  Le système de stockage indique la quantité approximative d'usure disponible sur chaque disque SSD pour l'écriture et l'effacement des données. Un disque dur ayant consommé 5 % de ses cycles d'écriture et d'effacement prévus affiche une usure restante de 95 %. Le système ne met pas à jour automatiquement les informations d'usure du disque dur ; vous pouvez actualiser la page ou la fermer et la recharger pour obtenir ces informations.

- **Taper**

  Le type de lecteur. Le type peut être soit un bloc, soit des métadonnées.

Pour plus d'informations

- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Gérer les nœuds

Gérer les nœuds

Vous pouvez gérer le stockage SolidFire et les nœuds Fibre Channel depuis la page Nœuds de l'onglet Cluster.

Si un nœud nouvellement ajouté représente plus de 50 % de la capacité totale du cluster, une partie de la capacité de ce nœud est rendue inutilisable (« bloquée »), afin qu'il se conforme à la règle de capacité. Cela restera le cas jusqu'à ce que davantage d'espace de stockage soit ajouté. Si un nœud très volumineux est ajouté et qu'il enfreint également la règle de capacité, le nœud précédemment bloqué ne le sera plus, tandis que le nœud nouvellement ajouté le deviendra. Il convient toujours d'ajouter les capacités par paires pour éviter ce problème. Lorsqu'un nœud devient indisponible, une erreur de cluster appropriée est déclenchée.

Trouver plus d'informations

Ajouter un nœud à un cluster

Ajouter un nœud à un cluster

Vous pouvez ajouter des nœuds à un cluster lorsque davantage d'espace de stockage est nécessaire ou après la création du cluster. Les nœuds nécessitent une configuration initiale lors de leur première mise sous tension. Une fois le nœud configuré, il apparaît dans la liste des nœuds en attente et vous pouvez l'ajouter à un cluster.

La version du logiciel sur chaque nœud d'un cluster doit être compatible. Lorsque vous ajoutez un nœud à un cluster, celui-ci installe, si nécessaire, la version cluster du logiciel NetApp Element sur le nouveau nœud.

Vous pouvez ajouter des nœuds de capacité inférieure ou supérieure à un cluster existant. Vous pouvez ajouter des nœuds de plus grande capacité à un cluster pour permettre l'augmentation de sa capacité. Les nœuds plus volumineux ajoutés à un cluster contenant des nœuds plus petits doivent l'être par paires. Cela laisse suffisamment d'espace à Double Helix pour déplacer les données en cas de défaillance d'un des nœuds les plus importants. Vous pouvez ajouter des nœuds de plus petite capacité à un cluster de nœuds plus important pour améliorer les performances.

> Si un nœud nouvellement ajouté représente plus de 50 % de la capacité totale du cluster, une partie de la capacité de ce nœud est rendue inutilisable (« bloquée »), afin qu'il se conforme à la règle de capacité. Cela restera le cas jusqu'à ce que davantage d'espace de stockage soit ajouté. Si un nœud très volumineux est ajouté et qu'il enfreint également la règle de capacité, le nœud précédemment bloqué ne le sera plus, tandis que le nœud nouvellement ajouté le deviendra. Il convient toujours d'ajouter les capacités par paires pour éviter ce problème. Lorsqu'un nœud devient bloqué, une erreur de cluster strandedCapacity est déclenchée.

"Vidéo NetApp : Faites évoluer votre cluster SolidFire selon vos besoins : étendre un cluster SolidFire"

Vous pouvez ajouter des nœuds aux appliances NetApp HCI .

Étapes

1. Sélectionnez **Cluster** > **Nœuds**.
2. Cliquez sur **En attente** pour afficher la liste des nœuds en attente.

   Une fois le processus d'ajout des nœuds terminé, ceux-ci apparaissent dans la liste des nœuds actifs. D'ici là, les nœuds en attente apparaissent dans la liste des nœuds actifs en attente.

   SolidFire installe la version logicielle Element du cluster sur les nœuds en attente lorsque vous les ajoutez à un cluster. Cela peut prendre quelques minutes.

3. Effectuez l'une des opérations suivantes :
   - Pour ajouter des nœuds individuels, cliquez sur l'icône **Actions** du nœud que vous souhaitez ajouter.
   - Pour ajouter plusieurs nœuds, cochez la case des nœuds à ajouter, puis cliquez sur **Actions groupées**. **Remarque :** Si le nœud que vous ajoutez possède une version du logiciel Element différente de celle exécutée sur le cluster, ce dernier met à jour le nœud de manière asynchrone vers la version du logiciel Element exécutée sur le nœud maître du cluster. Une fois le nœud mis à jour, il s'ajoute automatiquement au cluster. Durant ce processus asynchrone, le nœud sera dans un état pendingActive.

4. Cliquez sur **Ajouter**.

   Le nœud apparaît dans la liste des nœuds actifs.

Trouver plus d'informations

Versionnage et compatibilité des nœuds

Versionnage et compatibilité des nœuds

La compatibilité des nœuds dépend de la version du logiciel Element installée sur un nœud. Les clusters de stockage basés sur le logiciel Element créent automatiquement une image d'un nœud avec la version du logiciel Element présente sur le cluster si le nœud et le cluster ne sont pas à des versions compatibles.

La liste suivante décrit les niveaux de signification des versions logicielles qui composent le numéro de version du logiciel Element :

- **Majeur**

  Le premier chiffre désigne une version du logiciel. Un nœud avec un numéro de composant majeur ne peut pas être ajouté à un cluster contenant des nœuds avec un numéro de correctif majeur différent, et il est impossible de créer un cluster avec des nœuds de versions majeures mixtes.

- **Mineure**

  Le deuxième chiffre désigne des fonctionnalités logicielles mineures ou des améliorations apportées à des fonctionnalités logicielles existantes et ajoutées à une version majeure. Ce composant est incrémenté au sein d'une version majeure pour indiquer que cette version incrémentale n'est compatible avec aucune autre version incrémentale du logiciel Element comportant un composant mineur différent. Par exemple, la version 11.0 n'est pas compatible avec la version 11.1, et la version 11.1 n'est pas compatible avec la version 11.2.

- **Micro**

  Le troisième chiffre désigne un correctif compatible (version incrémentale) à la version du logiciel Element représentée par les composants majeur.mineur. Par exemple, la version 11.0.1 est compatible avec la version 11.0.2, et la version 11.0.2 est compatible avec la version 11.0.3.

Pour assurer la compatibilité, les numéros de version majeure et mineure doivent correspondre. Les numéros de microcontrôleur n'ont pas besoin de correspondre pour assurer la compatibilité.

Capacité de cluster dans un environnement à nœuds mixtes

Vous pouvez mélanger différents types de nœuds dans un cluster. Les séries SF 2405, 3010, 4805, 6010, 9605, 9010, 19210, 38410 et H peuvent coexister dans un cluster.

La série H comprend les nœuds H610S-1, H610S-2, H610S-4 et H410S. Ces nœuds sont compatibles avec les technologies 10GbE et 25GbE.

Il est préférable de ne pas mélanger les nœuds non chiffrés et chiffrés. Dans un cluster à nœuds mixtes, aucun nœud ne peut être plus grand que 33 % de la capacité totale du cluster. Par exemple, dans un cluster avec quatre nœuds SF-Series 4805, le plus grand nœud qui peut être ajouté seul est un SF-Series 9605. Le

seuil de capacité du cluster est calculé en fonction de la perte potentielle du plus grand nœud dans cette situation.

Selon votre version du logiciel Element, les nœuds de stockage de la série SF suivants ne sont pas pris en charge :

Pour commencer…	Nœud de stockage non pris en charge…
Élément 12.8	• SF4805 • SF9605 • SF19210 • SF38410
Élément 12.7	• SF2405 • SF9608
Élément 12.0	• SF3010 • SF6010 • SF9010

Si vous tentez de mettre à niveau l'un de ces nœuds vers une version Element non prise en charge, vous verrez une erreur indiquant que le nœud n'est pas pris en charge par Element 12.x.

Afficher les détails du nœud

Vous pouvez consulter les détails de chaque nœud, tels que les étiquettes de service, les informations sur les disques et les graphiques d'utilisation et les statistiques des disques. La page Nœuds de l'onglet Cluster comporte la colonne Version où vous pouvez consulter la version du logiciel de chaque nœud.

Étapes

1. Cliquez sur **Cluster** > **Nœuds**.
2. Pour afficher les détails d'un nœud spécifique, cliquez sur l'icône **Actions** de ce nœud.
3. Cliquez sur **Afficher les détails**.
4. Examinez les détails du nœud :
   - **ID du nœud** : L'identifiant généré par le système pour le nœud.
   - **Nom du nœud** : Le nom d'hôte du nœud.
   - **Rôle du nœud** : Le rôle que joue le nœud dans le cluster. Valeurs possibles :
     - Maître de cluster : le nœud qui effectue les tâches administratives à l'échelle du cluster et qui contient le MVIP et le SVIP.
     - Nœud d'ensemble : un nœud participant au cluster. Il y a soit 3, soit 5 nœuds d'ensemble selon la taille du cluster.
     - Fibre Channel : un nœud du cluster.
   - **Type de nœud** : Le type de modèle du nœud.

- **Disques actifs** : Le nombre de disques actifs dans le nœud.
- **Utilisation des nœuds** : Le pourcentage d'utilisation des nœuds basé sur nodeHeat. La valeur affichée correspond à recentPrimaryTotalHeat en pourcentage. Disponible à partir d'Element 12.8.
- **Adresse IP de gestion** : L'adresse IP de gestion (MIP) attribuée au nœud pour les tâches d'administration du réseau 1 GbE ou 10 GbE.
- **Adresse IP du cluster** : L'adresse IP du cluster (CIP) attribuée au nœud utilisé pour la communication entre les nœuds du même cluster.
- **Adresse IP de stockage** : L'adresse IP de stockage (SIP) attribuée au nœud utilisée pour la découverte du réseau iSCSI et tout le trafic réseau de données.
- **ID du VLAN de gestion** : L'identifiant virtuel du réseau local de gestion.
- **ID du VLAN de stockage** : L'identifiant virtuel du réseau local de stockage.
- **Version** : La version du logiciel exécutée sur chaque nœud.
- **Port de réplication** : Le port utilisé sur les nœuds pour la réplication à distance.
- **Étiquette de service** : Numéro d'étiquette de service unique attribué au nœud.
- **Domaine de protection personnalisé** : Le domaine de protection personnalisé attribué au nœud.

Afficher les détails des ports Fibre Channel

Vous pouvez consulter les détails des ports Fibre Channel, tels que leur statut, leur nom et leur adresse, sur la page Ports FC.

Consultez les informations relatives aux ports Fibre Channel connectés au cluster.

Étapes

1. Cliquez sur **Cluster** > **Ports FC**.
2. Pour filtrer les informations de cette page, cliquez sur **Filtrer**.
3. Examinez les détails :
   - **ID du nœud** : Le nœud hébergeant la session pour la connexion.
   - **Nom du nœud** : Nom du nœud généré par le système.
   - **Emplacement** : Numéro de l'emplacement où se trouve le port Fibre Channel.
   - **Port HBA** : Port physique sur l'adaptateur de bus hôte Fibre Channel (HBA).
   - **WWNN** : Le nom du nœud mondial.
   - **WWPN** : Nom du port cible mondial.
   - **Switch WWN** : Nom mondial du commutateur Fibre Channel.
   - **État du port** : État actuel du port.
   - **nPort ID** : L'identifiant du port du nœud sur la structure Fibre Channel.
   - **Vitesse** : La vitesse négociée du canal Fibre Channel. Les valeurs possibles sont les suivantes :
     - 4Gbps
     - 8Gbps
     - 16Gbps

Trouver plus d'informations

- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Gérer les réseaux virtuels

Gérer les réseaux virtuels

La virtualisation des réseaux dans le stockage SolidFire permet de connecter le trafic entre plusieurs clients situés sur des réseaux logiques distincts à un seul cluster. Les connexions au cluster sont segmentées dans la pile réseau grâce à l'utilisation du balisage VLAN.

Trouver plus d'informations

- Ajouter un réseau virtuel
- Activer le routage et le transfert virtuels
- Modifier un réseau virtuel
- Modifier les VLAN VRF
- Supprimer un réseau virtuel

Ajouter un réseau virtuel

Vous pouvez ajouter un nouveau réseau virtuel à une configuration de cluster pour permettre une connexion à un environnement multi-locataires à un cluster exécutant le logiciel Element.

Ce dont vous aurez besoin

- Identifiez le bloc d'adresses IP qui sera attribué aux réseaux virtuels sur les nœuds du cluster.
- Identifiez une adresse IP de réseau de stockage (SVIP) qui sera utilisée comme point de terminaison pour tout le trafic de stockage NetApp Element .

Pour cette configuration, vous devez prendre en compte les critères suivants :

- Les VLAN qui ne sont pas compatibles VRF nécessitent que les initiateurs se trouvent dans le même sous-réseau que le SVIP.
- Les VLAN compatibles VRF n'exigent pas que les initiateurs se trouvent dans le même sous-réseau que le SVIP, et le routage est pris en charge.
- Le SVIP par défaut n'exige pas que les initiateurs se trouvent dans le même sous-réseau que le SVIP, et le routage est pris en charge.

Lorsqu'un réseau virtuel est ajouté, une interface est créée pour chaque nœud et chacune nécessite une adresse IP de réseau virtuel. Le nombre d'adresses IP que vous spécifiez lors de la création d'un nouveau réseau virtuel doit être égal ou supérieur au nombre de nœuds du cluster. Les adresses réseau virtuelles sont provisionnées en masse et attribuées automatiquement aux nœuds individuels. Vous n'avez pas besoin d'attribuer manuellement des adresses réseau virtuelles aux nœuds du cluster.

Étapes

1. Cliquez sur **Cluster** > **Réseau**.
2. Cliquez sur **Créer un VLAN**.
3. Dans la boîte de dialogue **Créer un nouveau VLAN**, saisissez les valeurs dans les champs suivants :
   - **Nom du VLAN**
   - **Étiquette VLAN**
   - **SVIP**
   - **Netmask**
   - (Facultatif) **Description**
4. Saisissez l'adresse IP de départ pour la plage d'adresses IP dans les blocs d'adresses IP.
5. Saisissez la **taille** de la plage d'adresses IP comme le nombre d'adresses IP à inclure dans le bloc.
6. Cliquez sur **Ajouter un bloc** pour ajouter un bloc non contigu d'adresses IP pour ce VLAN.
7. Cliquez sur **Créer un VLAN**.

Afficher les détails du réseau virtuel

Étapes

1. Cliquez sur **Cluster** > **Réseau**.
2. Passez en revue les détails.
   - **ID** : Identifiant unique du réseau VLAN, attribué par le système.
   - **Nom** : Nom unique attribué par l'utilisateur au réseau VLAN.
   - **Étiquette VLAN** : Étiquette VLAN attribuée lors de la création du réseau virtuel.
   - **SVIP** : Adresse IP virtuelle de stockage attribuée au réseau virtuel.
   - **Netmask** : Masque de sous-réseau pour ce réseau virtuel.
   - **Passerelle** : Adresse IP unique d'une passerelle de réseau virtuel. Le VRF doit être activé.
   - **VRF activé** : Indique si le routage et le transfert virtuels sont activés ou non.
   - **Adresses IP utilisées** : Plage d'adresses IP du réseau virtuel utilisée pour le réseau virtuel.

Activer le routage et le transfert virtuels

Vous pouvez activer le routage et le transfert virtuels (VRF), ce qui permet à plusieurs instances d'une table de routage d'exister dans un routeur et de fonctionner simultanément. Cette fonctionnalité est disponible uniquement pour les réseaux de stockage.

Vous ne pouvez activer VRF qu'au moment de la création d'un VLAN. Si vous souhaitez revenir à un mode non-VRF, vous devez supprimer puis recréer le VLAN.

1. Cliquez sur **Cluster** > **Réseau**.
2. Pour activer VRF sur un nouveau VLAN, sélectionnez **Créer un VLAN**.
   a. Saisissez les informations pertinentes pour le nouveau VRF/VLAN. Voir Ajout d'un réseau virtuel.
   b. Cochez la case **Activer le VRF**.
   c. **Facultatif** : Saisissez une passerelle.

3. Cliquez sur **Créer un VLAN**.

Trouver plus d'informations

Ajouter un réseau virtuel

Modifier un réseau virtuel

Vous pouvez modifier les attributs VLAN, tels que le nom du VLAN, le masque de sous-réseau et la taille des blocs d'adresses IP. L'étiquette VLAN et le SVIP ne peuvent pas être modifiés pour un VLAN. L'attribut de passerelle n'est pas un paramètre valide pour les VLAN non-VRF.

Si des sessions iSCSI, de réplication à distance ou autres sessions réseau existent, la modification risque d'échouer.

Lors de la gestion de la taille des plages d'adresses IP VLAN, il convient de tenir compte des limitations suivantes :

- Vous pouvez uniquement supprimer des adresses IP de la plage d'adresses IP initiale attribuée lors de la création du VLAN.
- Vous pouvez supprimer un bloc d'adresses IP ajouté après la plage d'adresses IP initiale, mais vous ne pouvez pas redimensionner un bloc d'adresses IP en supprimant des adresses IP.
- Lorsque vous tentez de supprimer des adresses IP, que ce soit de la plage d'adresses IP initiale ou d'un bloc d'adresses IP, qui sont utilisées par des nœuds du cluster, l'opération peut échouer.
- Vous ne pouvez pas réaffecter des adresses IP spécifiques en cours d'utilisation à d'autres nœuds du cluster.

Vous pouvez ajouter un bloc d'adresses IP en suivant la procédure suivante :

1. Sélectionnez **Cluster** > **Réseau**.
2. Sélectionnez l'icône Actions pour le VLAN que vous souhaitez modifier.
3. Sélectionnez **Modifier**.
4. Dans la boîte de dialogue **Modifier le VLAN**, saisissez les nouveaux attributs du VLAN.
5. Sélectionnez **Ajouter un bloc** pour ajouter un bloc non contigu d'adresses IP au réseau virtuel.
6. Sélectionnez **Enregistrer les modifications**.

Lien vers les articles de la base de connaissances sur le dépannage

Consultez les articles de la base de connaissances pour obtenir de l'aide sur le dépannage des problèmes liés à la gestion de vos plages d'adresses IP VLAN.

- "Avertissement d'adresse IP dupliquée après l'ajout d'un nœud de stockage dans un VLAN sur un cluster Element"
- "Comment déterminer quelles adresses IP VLAN sont utilisées et à quels nœuds elles sont attribuées dans Element ?"

Modifier les VLAN VRF

Vous pouvez modifier les attributs VLAN VRF, tels que le nom du VLAN, le masque de

sous-réseau, la passerelle et les blocs d'adresses IP.

1. Cliquez sur **Cluster** > **Réseau**.
2. Cliquez sur l'icône Actions du VLAN que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Saisissez les nouveaux attributs du VLAN VRF dans la boîte de dialogue **Modifier le VLAN**.
5. Cliquez sur **Enregistrer les modifications**.

Supprimer un réseau virtuel

Vous pouvez supprimer un objet réseau virtuel. Vous devez ajouter les blocs d'adresses à un autre réseau virtuel avant de supprimer un réseau virtuel.

1. Cliquez sur **Cluster** > **Réseau**.
2. Cliquez sur l'icône Actions correspondant au VLAN que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Confirmez le message.

Trouver plus d'informations

Modifier un réseau virtuel

Créer un cluster prenant en charge les disques FIPS

Préparer le cluster Element pour la fonction de disques FIPS

La sécurité devient un facteur de plus en plus crucial pour le déploiement de solutions dans de nombreux environnements clients. Les normes fédérales de traitement de l'information (FIPS) sont des normes relatives à la sécurité et à l'interopérabilité des ordinateurs. Le chiffrement des données au repos, certifié FIPS 140-2, est un élément de la solution de sécurité globale.

Pour préparer l'activation de la fonctionnalité des disques FIPS, vous devez éviter de mélanger des nœuds dont certains sont compatibles avec les disques FIPS et d'autres non.

Un cluster est considéré comme conforme aux normes FIPS selon les conditions suivantes :

- Tous les disques sont certifiés FIPS.
- Tous les nœuds sont des nœuds de disques FIPS.
- Le chiffrement au repos (EAR) est activé.
- La fonction de lecteur FIPS est activée. Tous les disques et nœuds doivent être compatibles FIPS et le chiffrement au repos doit être activé pour activer la fonctionnalité de disque FIPS.

Activer le chiffrement au repos

Vous pouvez activer et désactiver le chiffrement au repos à l'échelle du cluster. Cette fonctionnalité n'est pas activée par défaut. Pour prendre en charge les disques FIPS,

vous devez activer le chiffrement au repos.

1. Dans l'interface utilisateur du logiciel NetApp Element , cliquez sur **Cluster** > **Paramètres**.
2. Cliquez sur **Activer le chiffrement au repos**.

Trouver plus d'informations

- Activer et désactiver le chiffrement pour un cluster
- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Identifiez si les nœuds sont prêts pour la fonctionnalité des disques FIPS

Vous devez vérifier si tous les nœuds du cluster de stockage sont prêts à prendre en charge les disques FIPS en utilisant la méthode d'API GetFipsReport du logiciel NetApp Element .

Le rapport généré affiche l'un des statuts suivants :

- Aucun : Node n'est pas capable de prendre en charge la fonctionnalité des disques FIPS.
- Partiel : Node est compatible FIPS, mais tous les disques ne sont pas des disques FIPS.
- Prêt : le nœud est compatible FIPS et tous les disques sont des disques FIPS ou aucun disque n'est présent.

Étapes

1. À l'aide de l'API Element, vérifiez si les nœuds et les disques du cluster de stockage sont compatibles avec les disques FIPS en saisissant :

   ```
   GetFipsReport
   ```

2. Examinez les résultats et notez les nœuds qui n'ont pas affiché l'état « Prêt ».
3. Pour les nœuds n'affichant pas l'état Prêt, vérifiez si le disque est compatible avec la fonctionnalité des disques FIPS :
   - En utilisant l'API Element, saisissez : `GetHardwareList`
   - Notez la valeur de **DriveEncryptionCapabilityType**. S'il s'agit de « fips », le matériel peut prendre en charge la fonctionnalité des disques FIPS.

     Voir les détails concernant `GetFipsReport` ou `ListDriveHardware` dans le "Référence de l'API Element".

4. Si le disque ne prend pas en charge la fonctionnalité des disques FIPS, remplacez le matériel par du matériel FIPS (nœud ou disques).

Trouver plus d'informations

- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Activer la fonction des disques FIPS

Vous pouvez activer la fonction des disques FIPS à l'aide du logiciel NetApp Element . `EnableFeature` Méthode API.

Le chiffrement au repos doit être activé sur le cluster et tous les nœuds et disques doivent être compatibles FIPS, comme indiqué lorsque GetFipsReport affiche un statut Prêt pour tous les nœuds.

Étape

1. Activez FIPS sur tous les disques à l'aide de l'API Element en saisissant :

   ```
   EnableFeature params: FipsDrives
   ```

Trouver plus d'informations

- "Gérez le stockage avec l'API Element"
- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Vérifier l'état du lecteur FIPS

Vous pouvez vérifier si la fonctionnalité des disques FIPS est activée sur le cluster à l'aide du logiciel NetApp Element . `GetFeatureStatus` Méthode API indiquant si l'état d'activation des variateurs FIPS est vrai ou faux.

1. À l'aide de l'API Element, vérifiez la fonctionnalité des disques FIPS sur le cluster en saisissant :

   ```
   GetFeatureStatus
   ```

2. Examinez les résultats de `GetFeatureStatus` Appel API. Si la valeur de FIPS Drives enabled est True, la fonctionnalité des lecteurs FIPS est activée.

   ```
   {"enabled": true,
   "feature": "FipsDrives"
   }
   ```

Trouver plus d'informations

- "Gérez le stockage avec l'API Element"
- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Dépannage de la fonction de lecteur FIPS

L'interface utilisateur du logiciel NetApp Element permet de consulter les alertes relatives aux pannes de cluster ou aux erreurs système liées à la fonctionnalité des disques FIPS.

1. Dans l'interface utilisateur d'Element, sélectionnez **Rapports** > **Alertes**.
2. Recherchez les défauts de cluster, notamment :
   - Les disques FIPS sont incompatibles.
   - Les normes FIPS entraînent des écarts de conformité.
3. Pour obtenir des suggestions de résolution, consultez les informations sur les codes d'erreur du cluster.

Trouver plus d'informations

- Codes d'erreur du groupe d'outils
- "Gérez le stockage avec l'API Element"
- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Établir une communication sécurisée

Activez la norme FIPS 140-2 pour HTTPS sur votre cluster

Vous pouvez utiliser la méthode API EnableFeature pour activer le mode de fonctionnement FIPS 140-2 pour les communications HTTPS.

Avec le logiciel NetApp Element , vous pouvez choisir d'activer le mode de fonctionnement FIPS 140-2 (Federal Information Processing Standards) sur votre cluster. L'activation de ce mode active le module de sécurité cryptographique NetApp (NCSM) et exploite le chiffrement certifié FIPS 140-2 niveau 1 pour toutes les communications via HTTPS vers l'interface utilisateur et l'API de NetApp Element .

> Une fois le mode FIPS 140-2 activé, il ne peut plus être désactivé. Lorsque le mode FIPS 140-2 est activé, chaque nœud du cluster redémarre et effectue un autotest pour s'assurer que le NCSM est correctement activé et fonctionne en mode certifié FIPS 140-2. Cela provoque une interruption des connexions de gestion et de stockage sur le cluster. Vous devez planifier soigneusement et n'activer ce mode que si votre environnement a besoin du mécanisme de chiffrement qu'il propose.

Pour plus d'informations, consultez la documentation de l'API Element.

Voici un exemple de requête API pour activer FIPS :

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "fips"
    },
    "id": 1
}
```

Une fois ce mode de fonctionnement activé, toutes les communications HTTPS utilisent les chiffrements approuvés FIPS 140-2.

Trouver plus d'informations

- Chiffrements SSL
- "Gérez le stockage avec l'API Element"
- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Chiffrements SSL

Les chiffrements SSL sont des algorithmes de chiffrement utilisés par les hôtes pour établir une communication sécurisée. Le logiciel Element prend en charge des chiffrements standard et des chiffrements non standard lorsque le mode FIPS 140-2 est activé.

Les listes suivantes fournissent les algorithmes de chiffrement SSL (Secure Socket Layer) standard pris en charge par le logiciel Element et les algorithmes de chiffrement SSL pris en charge lorsque le mode FIPS 140-2 est activé :

- **FIPS 140-2 désactivé**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

  TLS_ECDHE_RSA_AVEC_AES_128_CBC_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_AVEC_AES_128_GCM_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A

  TLS_ECDHE_RSA_AVEC_AES_256_GCM_SHA384 (secp256r1) - A

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

  TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A

  TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A

TLS_RSA_AVEC_RC4_128_MD5 (rsa 2048) - C

TLS_RSA_AVEC_RC4_128_SHA (rsa 2048) - C

TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A

- **FIPS 140-2 activé**

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

TLS_ECDHE_RSA_AVEC_AES_128_CBC_SHA256 (sect571r1) - A

TLS_ECDHE_RSA_AVEC_AES_128_CBC_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_AVEC_AES_128_GCM_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_AVEC_AES_128_GCM_SHA256 (sect571r1) - A

TLS_ECDHE_RSA_AVEC_AES_256_CBC_SHA384 (sect571r1) - A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A

TLS_ECDHE_RSA_AVEC_AES_256_GCM_SHA384 (secp256r1) - A

TLS_ECDHE_RSA_AVEC_AES_256_GCM_SHA384 (sect571r1) - A

TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A

Trouver plus d'informations

Activez la norme FIPS 140-2 pour HTTPS sur votre cluster

Commencez la gestion des clés externes

Commencez la gestion des clés externes

La gestion des clés externes (EKM) assure une gestion sécurisée des clés d'authentification (AK) en conjonction avec un serveur de clés externes hors cluster (EKS). Les clés AK servent à verrouiller et déverrouiller les disques à chiffrement automatique (SED) lorsque"chiffrement au repos" est activé sur le cluster. L'EKS assure la génération et le stockage sécurisés des AK. Le cluster utilise le protocole d'interopérabilité de gestion des clés (KMIP), un protocole standard défini par OASIS, pour communiquer avec l'EKS.

- "Mettre en place une gestion externe"
- "Réinitialisation du chiffrement logiciel au repos, clé principale"
- "Récupérer les clés d'authentification inaccessibles ou invalides"
- "Commandes de l'API de gestion des clés externes"

Trouver plus d'informations

- "L'API CreateCluster permet d'activer le chiffrement logiciel au repos."
- "Documentation logicielle SolidFire et Element"
- "Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"

Configurer la gestion des clés externes

Vous pouvez suivre ces étapes et utiliser les méthodes de l'API Element répertoriées pour configurer votre fonctionnalité de gestion des clés externes.

Ce dont vous aurez besoin

- Si vous configurez la gestion des clés externes en combinaison avec le chiffrement logiciel au repos, vous avez activé le chiffrement logiciel au repos à l'aide de"Créer un cluster" méthode sur un nouveau cluster ne contenant pas de volumes.

Étapes

1. Établir une relation de confiance avec le serveur de clés externe (EKS).
   a. Créez une paire de clés publique/privée pour le cluster Element qui sera utilisée pour établir une relation de confiance avec le serveur de clés en appelant la méthode API suivante :"Créer une paire de clés publique/privée"
   b. Obtenez la demande de signature de certificat (CSR) que l'autorité de certification doit signer. Le CSR permet au serveur de clés de vérifier que le cluster Element qui accédera aux clés est authentifié en tant que cluster Element. Appelez la méthode API suivante :"Demande de signature du certificat client"
   c. Utilisez l'autorité de certification EKS pour signer la CSR récupérée. Consultez la documentation tierce pour plus d'informations.
2. Créez un serveur et un fournisseur sur le cluster pour communiquer avec EKS. Un fournisseur de clés définit où une clé doit être obtenue, et un serveur définit les attributs spécifiques de l'EKS avec lequel la communication sera établie.

a. Créez un fournisseur de clés où résideront les détails du serveur de clés en appelant la méthode API suivante :"CréerKeyProviderKmip"

b. Créez un serveur de clés fournissant le certificat signé et le certificat de clé publique de l'autorité de certification en appelant les méthodes API suivantes :"CréerKeyServerKmip" "TestKeyServerKmip"

   Si le test échoue, vérifiez la connectivité et la configuration de votre serveur. Répétez ensuite le test.

c. Ajoutez le serveur de clés au conteneur du fournisseur de clés en appelant les méthodes API suivantes :"AjouterKeyServerToProviderKmip" "TestKeyProviderKmip"

   Si le test échoue, vérifiez la connectivité et la configuration de votre serveur. Répétez ensuite le test.

3. Prochaine étape pour le chiffrement au repos :

   a. (Pour le chiffrement matériel au repos) Activer"chiffrement matériel au repos" en fournissant l'identifiant du fournisseur de clés qui contient le serveur de clés utilisé pour stocker les clés en appelant le"Activer le chiffrement au repos" Méthode API.

      Vous devez activer le chiffrement au repos via le"API" . L'activation du chiffrement au repos à l'aide du bouton existant de l'interface utilisateur Element aura pour conséquence que la fonctionnalité utilise à nouveau des clés générées en interne.

   b. (Pour le chiffrement logiciel au repos) Afin de"Cryptage logiciel au repos" Pour utiliser le fournisseur de clés nouvellement créé, transmettez l'ID du fournisseur de clés à"RekeySoftwareEncryptionAtRestMasterKey" Méthode API.

Trouver plus d'informations

- "Activer et désactiver le chiffrement pour un cluster"
- "Documentation logicielle SolidFire et Element"
- "Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"

Réinitialisation du chiffrement logiciel au repos, clé principale

Vous pouvez utiliser l'API Element pour modifier une clé existante. Ce processus crée une nouvelle clé principale de remplacement pour votre serveur de gestion de clés externe. Les clés maîtresses sont toujours remplacées par de nouvelles clés maîtresses et ne sont jamais dupliquées ni écrasées.

Vous pourriez avoir besoin de ressaisir vos identifiants dans le cadre de l'une des procédures suivantes :

- Créer une nouvelle clé dans le cadre d'une transition de la gestion des clés internes à la gestion des clés externes.
- Créer une nouvelle clé en réaction à un événement lié à la sécurité ou pour s'en protéger.

Ce processus est asynchrone et renvoie une réponse avant que l'opération de renouvellement de clé ne soit terminée. Vous pouvez utiliser le"GetAsyncResult" méthode permettant d'interroger le système pour savoir quand le processus est terminé.

Ce dont vous aurez besoin

- Vous avez activé le chiffrement logiciel au repos à l'aide de"Créer un cluster" méthode sur un nouveau

cluster qui ne contient pas de volumes et n'a pas d'E/S. Utilisez le lien :../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] pour confirmer que l'état est `enabled` avant de continuer.

- Tu as"ont établi une relation de confiance" entre le cluster SolidFire et un serveur de clés externe (EKS). Exécutez le"TestKeyProviderKmip" méthode permettant de vérifier qu'une connexion au fournisseur de clés est établie.

Étapes

1. Exécutez le"ListKeyProvidersKmip" commande et copiez l'ID du fournisseur de clés(`keyProviderID`).
2. Exécutez le"RekeySoftwareEncryptionAtRestMasterKey" avec le `keyManagementType` paramètre comme `external` et `keyProviderID` comme numéro d'identification du fournisseur de clés de l'étape précédente :

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. Copiez le `asyncHandle` la valeur de la `RekeySoftwareEncryptionAtRestMasterKey` Réponse à la commande.
4. Exécutez le"GetAsyncResult" commande avec le `asyncHandle` valeur de l'étape précédente pour confirmer la modification de la configuration. La réponse à la commande devrait indiquer que l'ancienne configuration de la clé principale a été mise à jour avec les nouvelles informations de clé. Copiez le nouvel identifiant du fournisseur de clés pour l'utiliser ultérieurement.

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. Exécutez le `GetSoftwareEncryptionatRestInfo` commande pour confirmer que les nouveaux détails clés, y compris le `keyProviderID` , ont été mises à jour.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

Trouver plus d'informations

- "Gérez le stockage avec l'API Element"
- "Documentation logicielle SolidFire et Element"
- "Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"

Récupérer les clés d'authentification inaccessibles ou invalides

Il peut arriver, de temps à autre, qu'une erreur nécessite l'intervention de l'utilisateur. En cas d'erreur, un défaut de cluster (appelé code de défaut de cluster) sera généré. Les deux cas les plus probables sont décrits ici.

Le cluster ne peut pas déverrouiller les disques en raison d'une erreur de cluster KmipServerFault.

Cela peut se produire lors du premier démarrage du cluster, lorsque le serveur de clés est inaccessible ou que la clé requise est indisponible.

1. Suivez les étapes de récupération indiquées dans les codes d'erreur du groupe (le cas échéant).

Une erreur sliceServiceUnhealthy peut être déclenchée car les disques de métadonnées ont été marqués comme défaillants et placés dans l'état « Disponible ».

Étapes à suivre pour obtenir le résultat :

1. Ajoutez à nouveau les disques.
2. Après 3 à 4 minutes, vérifiez que le `sliceServiceUnhealthy` Le problème a disparu.

Voir"codes d'erreur du groupe d'outils" pour plus d'informations.

Commandes de l'API de gestion des clés externes

Liste de toutes les API disponibles pour la gestion et la configuration d'EKM.

Utilisé pour établir une relation de confiance entre le cluster et les serveurs externes appartenant au client :

- Créer une paire de clés publique/privée
- Demande de signature du certificat client

Utilisé pour définir les détails spécifiques des serveurs externes appartenant au client :

- CréerKeyServerKmip
- ModifierKeyServerKmip
- SupprimerKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

Utilisé pour créer et maintenir des fournisseurs de clés qui gèrent des serveurs de clés externes :

- CréerKeyProviderKmip
- DeleteKeyProviderKmip

- AjouterKeyServerToProviderKmip
- SupprimerKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

Pour plus d'informations sur les méthodes de l'API, consultez "Informations de référence de l'API".

Informations sur le copyright

Informations sur les marques commerciales