Gérez votre système

Element Software

NetApp
January 15, 2024

Sommaire

Gérez votre système

Vous pouvez gérer votre système dans l'interface utilisateur Element. C'est notamment l'activation de l'authentification multifacteur, la gestion des paramètres de cluster, la prise en charge de la norme FIPS (Federal information Processing Standards) et la gestion des clés externe.

- "Activez l'authentification multifacteur"
- "Configurez les paramètres du cluster"
- "Créez un cluster prenant en charge les disques FIPS"
- "Commencez par une gestion externe des clés"

Pour en savoir plus

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

Activez l'authentification multifacteur

L'authentification multifacteur (MFA) fait appel à un fournisseur d'identités tiers via le langage SAML pour gérer les sessions utilisateur. L'authentification multifacteur permet aux administrateurs de configurer d'autres facteurs d'authentification, tels que le mot de passe et l'e-mail, ainsi que le mot de passe et l'e-mail.

Configuration de l'authentification multifacteur

Vous pouvez utiliser ces étapes de base avec l'API Element pour configurer votre cluster afin qu'il utilise l'authentification multifacteur.

Vous trouverez des détails sur chaque méthode API dans le "Référence de l'API d'élément".

1. Créez une nouvelle configuration IDP pour le cluster en appelant la méthode d'API suivante et en transmettant les métadonnées IDP au format JSON : `CreateIdpConfiguration`

   Les métadonnées IDP, au format texte brut, sont extraites du IDP tiers. Ces métadonnées doivent être validées pour être correctement formatées dans JSON. De nombreuses applications de formateur JSON sont disponibles, par exemple :https://freeformatter.com/json-escape.html.

2. Récupérez les métadonnées du cluster, via spMetadaUrl, pour les copier vers le IDP tiers en appelant la méthode d'API suivante : `ListIdpConfigurations`

   SpMetadaUrl est une URL utilisée pour récupérer les métadonnées du fournisseur de services du cluster pour le PDI afin d'établir une relation de confiance.

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

> Le nom d'utilisateur de l'administrateur de cluster IDP doit correspondre au mappage de nom/valeur de l'attribut SAML pour l'effet souhaité, comme indiqué dans les exemples suivants :

  - Email=bob@company.com — où le IDP est configuré pour publier une adresse électronique dans les attributs SAML.
  - Group=cluster-Administrator - où le IDP est configuré pour libérer une propriété de groupe dans laquelle tous les utilisateurs doivent avoir accès. Notez que le couplage nom/valeur de l'attribut SAML est sensible à la casse à des fins de sécurité.

5. Activez l'authentification multifacteur pour le cluster en appelant la méthode API suivante : `EnableIdpAuthentication`

Trouvez plus d'informations

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

Informations supplémentaires pour l'authentification multifacteur

Concernant l'authentification multifacteur, vous devez connaître les mises en garde suivantes.

- Pour actualiser les certificats IDP qui ne sont plus valides, vous devez utiliser un utilisateur non-IDP admin pour appeler la méthode API suivante : `UpdateIdpConfiguration`
- MFA est incompatible avec des certificats d'une longueur inférieure à 2048 bits. Par défaut un certificat SSL 2048 bits est créé sur le cluster. Évitez de définir un certificat de taille plus petite lors de l'appel de la méthode API : `SetSSLCertificate`

> Si le cluster utilise un certificat dont la pré-mise à niveau est inférieure à 2048 bits, le certificat du cluster doit être mis à jour avec un certificat de 2048 bits ou plus après la mise à niveau vers l'élément 12.0 ou version ultérieure.

- Les utilisateurs admin IDP ne peuvent pas être utilisés directement pour effectuer des appels d'API (par exemple, via des kits de développement logiciel ou Postman) ou pour d'autres intégrations (par exemple, OpenStack Cinder ou le plug-in vCenter). Ajoutez soit des utilisateurs d'administrateur de cluster LDAP, soit des utilisateurs d'administrateur de cluster local si vous avez besoin de créer des utilisateurs qui ont ces capacités.

Trouvez plus d'informations

- "Gestion du stockage avec l'API Element"
- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Configurez les paramètres du cluster

Vous pouvez afficher et modifier les paramètres au niveau du cluster et effectuer des tâches spécifiques au cluster à partir de l'onglet Cluster de l'interface utilisateur Element.

Vous pouvez configurer des paramètres tels que le seuil de remplissage du cluster, l'accès au support, le cryptage au repos, les volumes virtuels, SnapMirror, Et aux clients de diffusion NTP.

Options

- Utilisation des volumes virtuels
- Utilisez la réplication SnapMirror entre les clusters Element et ONTAP
- Définissez le seuil maximal du cluster
- Activez et désactivez l'accès au support
- "Comment les seuils de blocage d'espace sont-ils calculés pour l'élément"
- Activez et désactivez le cryptage pour un cluster
- Gérez la bannière Conditions d'utilisation
- Configuration des serveurs Network Time Protocol pour que le cluster puisse effectuer une requête
- Gérer SNMP
- Gérer les disques
- Gérer des nœuds
- Gérer des réseaux virtuels
- Afficher les détails des ports Fibre Channel

Trouvez plus d'informations

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

Activez et désactivez le cryptage des données 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 des lecteurs à autochiffrement (SED) au niveau du cluster à l'aide de l'une ou l'autre "chiffrement matériel ou logiciel pour les données au repos".

Vous pouvez activer le chiffrement matériel au repos à l'aide de l'interface utilisateur et de l'API d'Element. L'activation de la fonctionnalité de chiffrement matériel au repos n'a aucune incidence sur les performances ou 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. Il 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 au cours de la création du cluster et ne peut pas être désactivé une fois le cluster créé.

Ce dont vous avez besoin

- Vous disposez des privilèges d'administrateur de cluster pour activer ou modifier les paramètres de chiffrement.
- Pour le chiffrement matériel au repos, vous avez vérifié que le cluster est en état de fonctionnement avant de modifier les paramètres de chiffrement.

- Si vous désactivez le cryptage, deux nœuds doivent participer à un cluster pour accéder à la clé afin de désactiver le cryptage sur un disque.

Vérifiez le chiffrement des données au repos

Pour voir l'état actuel du chiffrement au repos et/ou logiciel au repos sur le cluster, utilisez le "GetClusterInfo" méthode. Vous pouvez utiliser le "GetSoftwareEncryptionAtRestInfo" méthode d'obtention des informations que le cluster utilise pour chiffrer les données au repos.

> Le tableau de bord de l'interface utilisateur du logiciel Element sur `https://<MVIP>/` à l'heure actuelle, le chiffrement des données au repos est uniquement affiché pour le chiffrement matériel.

Options

- Chiffrement matériel des données au repos
- Chiffrement logiciel des données au repos
- Désactivation du chiffrement matériel des données au repos

Chiffrement matériel des données au repos

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

1. Dans l'interface utilisateur de l'élément, sélectionnez **Cluster** > **Paramètres**.
2. Sélectionnez **Activer le chiffrement au repos**.

Chiffrement logiciel des données au repos

> Le chiffrement logiciel au repos ne peut pas être désactivé après son activation sur le cluster.

1. Lors de la création du cluster, exécutez la "créer une méthode de cluster" avec `enableSoftwareEncryptionAtRest` réglez sur `true`.

Désactivation du chiffrement matériel des données au repos

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

Trouvez plus d'informations

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

Définissez le seuil maximal du cluster

Vous pouvez modifier le niveau auquel le système génère un avertissement de remplissage de cluster de blocs en suivant les étapes ci-dessous. En outre, vous pouvez utiliser la méthode ModityClusterFullThreshold API pour modifier le niveau auquel le

système génère un avertissement de bloc ou de métadonnées.

Ce dont vous avez besoin

Vous devez disposer des privilèges d'administrateur de cluster.

Étapes

1. Cliquez sur **Cluster** > **Paramètres**.
2. Dans la section Paramètres complets du cluster, entrez un pourcentage dans **émettre une alerte d'avertissement lorsque la capacité de _ % reste avant que Helix n'ait pu récupérer suite à une panne du nœud**.
3. Cliquez sur **Enregistrer les modifications**.

Trouvez plus d'informations

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

Activez et désactivez l'accès au support

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

Pour modifier l'accès au support, vous devez disposer de privilèges d'administrateur du cluster.

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

Gérez la bannière Conditions d'utilisation

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

Options

Activez la bannière Conditions d'utilisation Modifiez la bannière Conditions d'utilisation Désactivez la bannière Conditions d'utilisation

Activez la bannière Conditions d'utilisation

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

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

1. Cliquez sur **utilisateurs** > **Conditions d'utilisation**.
2. Dans le formulaire **Conditions d'utilisation**, entrez le texte à afficher pour la boîte de dialogue Conditions

d'utilisation.

Ne pas dépasser 4096 caractères.

3. Cliquez sur **Activer**.

Modifiez la bannière Conditions d'utilisation

Vous pouvez modifier le texte qu'un utilisateur voit lorsqu'il sélectionne la bannière de connexion Conditions d'utilisation.

Ce dont vous avez 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**.

Désactivez la bannière Conditions d'utilisation

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

Ce dont vous avez 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**.

Définissez le protocole de temps du réseau

La configuration du protocole NTP (Network Time Protocol) peut être effectuée de deux manières : demandez à chaque nœud d'un cluster d'écouter les diffusions ou demandez à chaque nœud d'interroger un serveur NTP pour les mises à jour.

Le 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.

Configuration des serveurs Network Time Protocol pour que le cluster puisse effectuer une requête

Vous pouvez demander à chaque nœud d'un cluster d'interroger un serveur NTP (Network Time Protocol) pour les mises à jour. Le cluster contacte uniquement les

serveurs configurés et demande les informations NTP à leur place.

Configurez le protocole NTP sur le cluster afin de pointer vers un serveur NTP local. Vous pouvez utiliser l'adresse IP ou le nom d'hôte FQDN. Le serveur NTP par défaut à l'heure de 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 FQDN dépend de la mise en place et de l'exploitation des paramètres DNS de chaque nœud de stockage. 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 du port réseau.

Vous pouvez entrer jusqu'à cinq serveurs NTP différents.

Vous pouvez utiliser les adresses IPv4 et IPv6.

Ce dont vous avez 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 FQDN dans les paramètres du serveur.
2. Assurez-vous que le DNS est correctement défini sur les nœuds.
3. Cliquez sur **Cluster** > **Paramètres**.
4. Sous Paramètres du protocole d'heure du réseau, sélectionnez **non**, qui utilise la configuration NTP standard.
5. Cliquez sur **Enregistrer les modifications**.

Trouvez plus d'informations

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

Configurez le cluster pour écouter 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 NTP (Network Time Protocol) d'un serveur particulier.

Ce dont vous avez 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 qui utilisent le mode de diffusion dans la liste de serveurs.
3. Sous Paramètres du protocole d'heure du réseau, sélectionnez **Oui** pour utiliser un client de diffusion.
4. Pour définir le client de diffusion, dans le champ **Server**, saisissez le serveur NTP que vous avez configuré en mode diffusion.
5. Cliquez sur **Enregistrer les modifications**.

Trouvez plus d'informations

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

Gérer SNMP

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

Vous pouvez sélectionner un demandeur SNMP, sélectionner la version de SNMP à utiliser, identifier l'utilisateur SNMP user based Security Model (USM) et configurer les traps pour surveiller le cluster SolidFire. Vous pouvez également afficher les fichiers de la base d'informations de gestion et y accéder.

Vous pouvez utiliser les adresses IPv4 et IPv6.

Détails SNMP

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

- **MIB SNMP**

  Les fichiers MIB qui sont disponibles pour vous à visualiser ou télécharger.

- **Paramètres SNMP généraux**

  Vous pouvez activer ou désactiver SNMP. Après avoir activé SNMP, vous pouvez choisir la version à utiliser. Si vous utilisez la version 2, vous pouvez ajouter des requestors et, si vous utilisez la version 3, vous pouvez configurer des utilisateurs USM.

- **Paramètres de déroutement SNMP**

  Vous pouvez identifier les recouvrements que vous souhaitez capturer. Vous pouvez définir l'hôte, le port et la chaîne de communauté pour chaque destinataire de l'interruption.

Configurez un demandeur SNMP

Lorsque SNMP version 2 est activé, vous pouvez activer ou désactiver un demandeur et configurer les demandeurs pour qu'ils reçoivent les requêtes SNMP autorisées.

1. Cliquez sur 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 **Requetors**, saisissez les informations **Community String** et **Network**.

   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 entrez les informations **chaîne de communauté** et **réseau**.

6. Cliquez sur **Enregistrer les modifications**.

Trouvez plus d'informations

- Configurer les traps SNMP
- Affichez les données d'objet géré à l'aide des fichiers de base d'informations de gestion

Configurez un utilisateur SNMP USM

Lorsque vous activez SNMP version 3, vous devez configurer un utilisateur USM pour qu'il reçoive 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 **USM Users**, entrez le nom, le mot de passe et la phrase de passe.
5. **Facultatif:** pour ajouter un autre utilisateur USM, cliquez sur **Ajouter un utilisateur USM** et entrez le nom, le mot de passe et la phrase de passe.
6. Cliquez sur **Enregistrer les modifications**.

Configurer les traps SNMP

Les administrateurs système peuvent utiliser des traps SNMP, également appelés notifications, pour contrôler l'état de santé du cluster SolidFire.

Lorsque les traps SNMP sont activés, le cluster SolidFire génère des traps associés à des entrées du journal d'événements et à des alertes système. Pour recevoir des notifications SNMP, vous devez choisir les interruptions qui doivent être générées et identifier les destinataires des informations d'interruption. Par défaut, aucun traps n'est généré.

1. Cliquez sur **Cluster** > **SNMP**.
2. Sélectionnez un ou plusieurs types de pièges dans la section **Paramètres de déroutement SNMP** que le système doit générer :
   - Traps à la défaillance du cluster
   - Trappe à l'erreur du cluster résolue
   - N°1 : arguments concernant les événements de
3. Dans la section **Trap Recipients** , entrez les informations d'hôte, de port et de chaîne de communauté pour un destinataire.
4. **Facultatif** : pour ajouter un autre destinataire d'interruption, cliquez sur **Ajouter un destinataire d'interruption** et entrez les informations sur l'hôte, le port et la chaîne de communauté.
5. Cliquez sur **Enregistrer les modifications**.

Affichez les données d'objet géré à l'aide des fichiers de base d'informations de gestion

Vous pouvez afficher et télécharger les fichiers de la 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 SolidFire-StorageCluster-MIB.

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

- Statistiques du cluster
- Statistiques de volume
- Volumes par statistiques de compte
- Statistiques de nœud
- 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 (OID) aux produits SF-Series.

Étapes

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

Gérer les disques

Chaque nœud contient un ou plusieurs disques physiques utilisés pour stocker une partie des données pour le cluster. Le cluster utilise la capacité et les performances du disque une fois le disque ajouté au cluster. Vous pouvez gérer les disques à l'aide de l'interface utilisateur Element.

Pour en savoir plus

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

Détails sur le disque

La page lecteurs de l'onglet Cluster fournit la liste des lecteurs actifs du cluster. Vous pouvez filtrer la page en sélectionnant dans les onglets actif, disponible, Suppression, Effacement et échec.

Lorsque vous initialisez un cluster, la liste des disques actifs est vide. Vous pouvez ajouter des disques non attribués à un cluster et dans l'onglet disponible après la création d'un nouveau cluster SolidFire.

Les éléments suivants apparaissent dans la liste des lecteurs actifs.

- **ID de lecteur**

  Numéro séquentiel attribué au disque.

- **ID de nœud**

  Numéro de nœud attribué lorsque ce nœud est ajouté au cluster.

- **Nom du noeud**

  Nom du nœud qui héberge le disque.

- **Slot**

  Numéro de logement où le lecteur est physiquement situé.

- **Capacité**

  Taille du lecteur, en Go.

- **Série**

  Numéro de série du disque.

- **Usure restante**

  L'indicateur de niveau d'usure.

  Le système de stockage indique l'usure approximative disponible sur chaque disque SSD pour l'écriture et l'effacement des données. Un disque qui a consommé 5 % de ses cycles d'écriture et d'effacement prévus signale l'usure restante de 95 %. Le système n'actualise pas automatiquement les informations relatives à l'usure des disques ; vous pouvez actualiser ou fermer et recharger la page pour actualiser les informations.

- **Type**

  Type de disque. Ce type peut être un bloc ou des métadonnées.

Gérer des nœuds

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

Si un nouveau nœud ajouté augmente la capacité totale du cluster de plus de 50 %, une partie de cette capacité devient inutilisable (« bloqué »), afin de lui conformer à la règle de capacité. Cela reste le cas jusqu'à l'ajout de stockage supplémentaire. Si un nœud très volumineux est ajouté qui obéit également à la règle de capacité, le nœud précédemment bloqué ne sera plus bloqué, tandis que le nouveau nœud ajouté est bloqué. La capacité doit toujours être ajoutée par paires pour éviter ce problème. Lorsqu'un nœud est bloqué, une défaillance de cluster appropriée est déclenchée.

Trouvez plus d'informations

Ajout d'un nœud à un cluster

Ajout d'un nœud à un cluster

Vous pouvez ajouter des nœuds à un cluster lorsque plus de stockage est nécessaire ou après sa création. Les nœuds requièrent la configuration initiale lors de la 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 logicielle de chaque nœud d'un cluster doit être compatible. Lorsque vous ajoutez un nœud à un cluster, le cluster installe la version cluster du logiciel NetApp Element sur le nouveau nœud, si nécessaire.

Vous pouvez ajouter des nœuds de plus petite ou plus grande capacité à un cluster existant. Vous pouvez

ajouter de plus grandes capacités à un cluster afin d'adapter la capacité. Des nœuds plus grands ajoutés à un cluster avec des nœuds plus petits doivent être ajoutés par paires. Ainsi, l'espace nécessaire à la double Helix est suffisant pour déplacer les données en cas de panne de l'un des nœuds les plus importants. Vous pouvez ajouter des nœuds de moins grandes capacités à un cluster de nœuds afin d'améliorer les performances.

> Si un nouveau nœud ajouté augmente la capacité totale du cluster de plus de 50 %, une partie de cette capacité devient inutilisable (« bloqué »), afin de lui conformer à la règle de capacité. Cela reste le cas jusqu'à l'ajout de stockage supplémentaire. Si un nœud très volumineux est ajouté qui obéit également à la règle de capacité, le nœud précédemment bloqué ne sera plus bloqué, tandis que le nouveau nœud ajouté est bloqué. La capacité doit toujours être ajoutée par paires pour éviter ce problème. Lorsqu'un nœud est bloqué, la défaillance du cluster strandeCapacity est déclenchée.

"Vidéo NetApp : l'évolutivité à votre rythme : développement d'un cluster SolidFire"

Vous pouvez ajouter des nœuds aux appliances NetApp HCI.

Étapes

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

   Lorsque le processus d'ajout de nœuds est terminé, ils apparaissent dans la liste nœuds actifs. Les nœuds en attente apparaissent alors dans la liste en attente active.

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

3. Effectuez l'une des opérations suivantes :
   - Pour ajouter des nœuds individuels, cliquez sur l'icône **actions** du noeud que vous souhaitez ajouter.
   - Pour ajouter plusieurs nœuds, cochez la case des nœuds à ajouter, puis **actions groupées**.
     Remarque : si le nœud que vous ajoutez possède une version différente du logiciel Element que la version exécutée sur le cluster, le cluster met à jour de manière asynchrone le nœud vers la version du logiciel Element qui s'exécute sur le maître de cluster. Une fois le nœud mis à jour, il s'ajoute automatiquement au cluster. Au cours de ce processus asynchrone, le nœud sera à l'état suspendu actif.
4. Cliquez sur **Ajouter**.

   Le nœud apparaît dans la liste des nœuds actifs.

Trouvez plus d'informations

Gestion des versions de nœud et compatibilité

Gestion des versions de nœud et compatibilité

La compatibilité des nœuds repose sur la version du logiciel Element installée sur un nœud. Si le nœud et le cluster n'exécutent pas de versions compatibles, les clusters de stockage logiciel Element s'Images automatiquement d'un nœud sur la version du logiciel Element.

La liste suivante décrit les niveaux de signification de la version du logiciel qui constituent le numéro de version

du logiciel Element :

- **Majeur**

  Le premier numéro désigne une version logicielle. Un nœud avec un numéro de composant majeur ne peut pas être ajouté à un cluster contenant des nœuds d'un numéro de patch majeur différent, ni un cluster peut être créé avec des nœuds de versions majeures mixtes.

- **Mineur**

  Le deuxième nombre désigne les fonctionnalités logicielles plus petites ou les améliorations apportées aux fonctions logicielles existantes qui ont été ajoutées à une version majeure. Ce composant est incrémenté dans un composant de version majeure pour indiquer que cette version incrémentielle n'est pas compatible avec d'autres versions incrémentielles du logiciel Element avec un composant mineur différent. Par exemple, 11.0 n'est pas compatible avec 11.1 et 11.1 n'est pas compatible avec 11.2.

- **Micro**

  Le troisième nombre désigne un correctif compatible (version incrémentielle) à la version logicielle de l'élément représentée par les composants majeur.mineur. Par exemple, 11.0.1 est compatible avec 11.0.2 et 11.0.2 avec 11.0.3.

Les numéros de version majeurs et mineurs doivent correspondre à la compatibilité. Les micro-numéros ne doivent pas nécessairement correspondre pour la compatibilité.

Capacité du cluster dans un environnement de nœuds mixtes

Vous pouvez combiner plusieurs types de nœuds dans un cluster. Le SF-Series 2405, 3010, 4805, 6010, 9605 9010, 19210, 38410 et la série 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 10 GbE et 25 GbE.

Il est préférable de ne pas associer de nœuds non chiffrés et chiffrés. Dans un cluster à nœuds mixtes, aucun nœud ne peut dépasser 33 % de la capacité totale du cluster. Par exemple, dans un cluster doté de quatre nœuds SF-Series 4805, le plus grand nœud à ajouter seul est un système SF-Series 9605. Le seuil de capacité du cluster est calculé en fonction de la perte potentielle du nœud le plus grand dans ce cas.

Depuis Element 12.0, les nœuds de stockage SF-Series suivants ne sont pas pris en charge :

- SF3010
- SF6010
- SF9010

Si vous mettez à niveau l'un de ces nœuds de stockage vers Element 12.0, une erreur s'affiche, indiquant que ce nœud n'est pas pris en charge par Element 12.0.

Afficher les détails du nœud

Vous pouvez afficher les détails de chaque nœud, notamment les balises de service, les détails de disque et les graphiques de l'utilisation et des statistiques de disque. La page nœuds de l'onglet Cluster fournit la colonne version dans laquelle vous pouvez afficher la

version logicielle de chaque nœud.

Étapes

1. Cliquez sur **Cluster** > **Nodes**.
2. Pour afficher les détails d'un nœud spécifique, cliquez sur l'icône **actions** d'un nœud.
3. Cliquez sur **Afficher les détails**.
4. Vérifiez les détails du nœud :
   - **ID de nœud** : ID généré par le système pour le nœud.
   - **Nom de noeud** : nom d'hôte du noeud.
   - **4K IOPS** disponibles : le nombre d'IOPS configuré pour le nœud.
   - **Rôle de nœud** : rôle dont dispose le nœud dans le cluster. Valeurs possibles :
     - Cluster Master : nœud qui effectue des tâches administratives à l'échelle du cluster et qui contient MVIP et SVIP.
     - Nœud ensemble : nœud qui participe au cluster. Il y a 3 ou 5 nœuds d'ensemble en fonction de la taille du groupe.
     - Fibre Channel : nœud du cluster.
   - **Type de nœud** : type de modèle du nœud.
   - **Disques actifs** : nombre de disques actifs dans le nœud.
   - **IP de gestion** : adresse IP de gestion (MIP) attribuée au nœud pour les tâches d'administration réseau 1 GbE ou 10 GbE.
   - **IP du cluster** : adresse IP du cluster (CIP) attribuée au nœud utilisé pour la communication entre les nœuds du même cluster.
   - **Adresse IP de stockage** : adresse IP de stockage (SIP) attribuée au nœud utilisé pour la découverte du réseau iSCSI et tout le trafic du réseau de données.
   - **ID VLAN de gestion** : ID virtuel pour le réseau local de gestion.
   - **ID du VLAN de stockage** : ID virtuel pour le réseau local de stockage.
   - **Version** : la version du logiciel s'exécutant sur chaque nœud.
   - **Port de réplication** : port utilisé sur les nœuds pour la réplication à distance.
   - **Service Tag** : numéro de numéro de service unique attribué au nœud.

Afficher les détails des ports Fibre Channel

Vous pouvez afficher des détails sur les ports Fibre Channel, tels que son état, son nom et son adresse de port, à partir de la page des ports FC.

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

Étapes

1. Cliquez sur **Cluster** > **FC ports**.
2. Pour filtrer les informations de cette page, cliquez sur **Filter**.
3. Consultez les détails :
   - **ID de nœud** : nœud hébergeant la session pour la connexion.

- **Nom du nœud** : nom du nœud généré par le système.
- **Slot** : numéro de logement où se trouve le port Fibre Channel.
- **Port HBA** : port physique sur l'adaptateur de bus hôte Fibre Channel (HBA).
- **WWNN** : le nom de nœud mondial.
- **WWPN** : nom du port mondial cible.
- **WWN du commutateur** : nom mondial du commutateur Fibre Channel.
- **Etat du port** : état actuel du port.
- **NPort ID** : ID du port de nœud sur la structure Fibre Channel.
- **Vitesse** : vitesse Fibre Channel négociée. Les valeurs possibles sont les suivantes :
  - 4 Gbit/s
  - 8 Go/s.
  - 16 Gbits/s

Trouvez plus d'informations

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

Gérer des réseaux virtuels

La mise en réseau virtuelle dans le stockage SolidFire permet la connexion au cluster du trafic entre plusieurs clients sur des réseaux logiques distincts. Les connexions au cluster sont isolées sur la pile réseau via l'utilisation de balisage VLAN.

Trouvez 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 la connexion d'un environnement mutualisé à un cluster exécutant le logiciel Element.

Ce dont vous avez besoin

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

Vous devez tenir compte des critères suivants pour cette configuration :

- Les VLAN qui ne sont pas activés par VRF exigent que les initiateurs se trouvent dans le même sous-réseau que le SVIP.
- Les VLAN activés par VRF ne nécessitent pas que les initiateurs se trouvent sur le même sous-réseau que le SVIP, et le routage est pris en charge.
- Le SVIP par défaut ne requiert 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 pour chaque nœud est créée et chaque nœud 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 bloc et attribuées automatiquement aux nœuds individuels. Il n'est pas nécessaire d'attribuer manuellement des adresses réseau virtuelles aux nœuds du cluster.

Étapes

1. Cliquez sur **Cluster** > **Network**.
2. Cliquez sur **Create VLAN**.
3. Dans la boîte de dialogue **Créer un nouveau VLAN**, entrez les valeurs dans les champs suivants :
   - **Nom VLAN**
   - **Balise VLAN**
   - **SVIP**
   - **Masque de réseau**
   - (Facultatif) **Description**
4. Saisissez l'adresse **IP de départ** pour la plage d'adresses IP dans **blocs d'adresses IP**.
5. Saisissez **Size** de la plage IP comme nombre d'adresses IP à inclure dans le bloc.
6. Cliquez sur **Ajouter un bloc** pour ajouter un bloc non continu d'adresses IP pour ce VLAN.
7. Cliquez sur **Create VLAN**.

Afficher les détails des réseaux virtuels

Étapes

1. Cliquez sur **Cluster** > **Network**.
2. Vérifiez les détails.
   - **ID** : ID unique du réseau VLAN, qui est attribué par le système.
   - **Nom** : nom unique attribué par l'utilisateur pour le réseau VLAN.
   - **Balise VLAN** : balise VLAN attribuée lors de la création du réseau virtuel.
   - **SVIP** : adresse IP virtuelle de stockage attribuée au réseau virtuel.
   - **Masque de réseau** : masque de réseau pour ce réseau virtuel.
   - **Gateway** : adresse IP unique d'une passerelle de réseau virtuel. VRF doit être activée.
   - **VRF activée** : indication de l'activation ou non du routage et du transfert virtuels.
   - **Adresses IP utilisées** : plage d'adresses IP de réseau virtuel utilisées 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 travailler 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 une fonction non VRF, vous devez supprimer et recréer le VLAN.

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

Trouvez 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 réseau et la taille des blocs d'adresse IP. La balise VLAN et 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 d'autres sessions réseau existent, la modification peut échouer.

Lors de la gestion de la taille des plages d'adresses IP VLAN, notez les limitations suivantes :

- Vous pouvez uniquement supprimer les adresses IP de la plage d'adresses IP initiale attribuée au moment de la création du VLAN.
- Vous pouvez supprimer un bloc d'adresses IP qui a été ajouté après la plage d'adresses IP initiale, mais vous ne pouvez pas redimensionner un bloc IP en supprimant les adresses IP.
- Lorsque vous tentez de supprimer les adresses IP, depuis la plage d'adresse IP initiale ou dans un bloc IP, celles utilisées par les nœuds du cluster, l'opération peut échouer.
- Vous ne pouvez pas réaffecter d'adresses IP utilisées spécifiques à d'autres nœuds du cluster.

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

1. Sélectionnez **Cluster** > **Network**.
2. Sélectionnez l'icône actions du VLAN que vous souhaitez modifier.
3. Sélectionnez **Modifier**.
4. Dans la boîte de dialogue **Edit VLAN**, entrez les nouveaux attributs du VLAN.
5. Sélectionnez **Ajouter un bloc** pour ajouter un bloc non continu d'adresses IP pour le réseau virtuel.

6. Sélectionnez **Enregistrer les modifications**.

Lien vers les articles de la base de connaissances de dépannage

Lien vers les articles de la base de connaissances pour obtenir de l'aide pour résoudre les problèmes de gestion de vos plages d'adresses IP de VLAN.

- "Avertissement IP en double après ajout d'un nœud de stockage dans VLAN sur le cluster Element"
- "Comment déterminer les adresses IP VLAN utilisées et les nœuds auxquels ces adresses IP sont affectées dans l'élément"

Modifier les VLAN VRF

Vous pouvez modifier les attributs VLAN VRF, tels que le nom du VLAN, le masque de réseau, la passerelle et les blocs d'adresse IP.

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

Supprimer un réseau virtuel

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

1. Cliquez sur **Cluster** > **Network**.
2. Cliquez sur l'icône actions du VLAN à supprimer.
3. Cliquez sur **Supprimer**.
4. Confirmez le message.

Trouvez plus d'informations

Modifier un réseau virtuel

Créez un cluster prenant en charge les disques FIPS

La sécurité devient de plus en plus cruciale pour le déploiement de solutions dans de nombreux environnements clients. La norme FIPS (Federal information Processing Standards) est une norme en matière de sécurité et d'interopérabilité des ordinateurs. Le chiffrement certifié FIPS 140-2 pour les données au repos est un composant de la solution de sécurité globale.

- "Évitez de mélanger les nœuds pour les disques FIPS"
- "Activation du chiffrement des données au repos"
- "Identifiez si les nœuds sont prêts pour la fonctionnalité disques FIPS"

- "Activez la fonctionnalité disques FIPS"
- "Vérifiez l'état du lecteur FIPS"
- "Dépannez la fonctionnalité de lecteur FIPS"

Évitez de mélanger les nœuds pour les disques FIPS

Pour préparer l'activation de la fonctionnalité de lecteurs FIPS, évitez de combiner les nœuds où certains prennent en charge des disques FIPS et d'autres non.

Un cluster est considéré comme étant conforme à la norme FIPS dans les conditions suivantes :

- Tous les disques sont certifiés FIPS.
- Tous les nœuds sont des nœuds de disques FIPS.
- Le chiffrement au repos est activé.
- La fonctionnalité disques FIPS est activée. L'ensemble des disques et nœuds doit être compatible FIPS et le chiffrement au repos doit être activé pour que la fonctionnalité de disque FIPS soit activée.

Activation du chiffrement des données au repos

Vous pouvez activer et désactiver le chiffrement au repos au niveau 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**.

Trouvez plus d'informations

- Activez et désactivez le cryptage pour un cluster
- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Identifiez si les nœuds sont prêts pour la fonctionnalité disques FIPS

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

Le rapport obtenu affiche l'un des États suivants :

- Aucun : le nœud ne peut pas prendre en charge la fonctionnalité disques FIPS.
- Partiel : les nœuds sont compatibles 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 pas de disque.

Étapes

1. Utilisez l'API d'Element pour vérifier si les nœuds et les disques du cluster de stockage peuvent prendre en charge les disques FIPS en saisissant :

```
GetFipsReport
```

2. Examinez les résultats en notant tous les nœuds qui n'ont pas affiché l'état prêt.
3. Pour tous les nœuds n'ayant pas affiché l'état prêt, vérifiez si le disque est capable de prendre en charge la fonctionnalité disques FIPS :
   - À l'aide de l'API Element, entrez : `GetHardwareList`
   - Notez la valeur du **DriveEncryptionCapabilityType**. Si c'est le cas avec la norme fips, le matériel peut prendre en charge la fonctionnalité disques FIPS.

     Voir les détails `GetFipsReport` ou `ListDriveHardware` dans le "Référence de l'API d'élément".
4. Si le disque ne prend pas en charge la fonctionnalité disques FIPS, remplacez le matériel par du matériel FIPS (soit un nœud, soit des disques).

Trouvez plus d'informations

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

Activez la fonctionnalité disques FIPS

Vous pouvez activer la fonctionnalité 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 lecteurs doivent être compatibles FIPS, comme indiqué lorsque GetFipsReport affiche un état prêt pour tous les nœuds.

Étape

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

```
EnableFeature params: FipsDrives
```

Trouvez plus d'informations

- "Gérez le stockage avec l'API Element"
- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Vérifiez l'état du lecteur FIPS

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

1. Utilisez l'API d'Element pour vérifier la fonctionnalité disques FIPS sur le cluster en saisissant :

```
GetFeatureStatus
```

2. Examinez les résultats du `GetFeatureStatus` Appel d'API. Si la valeur des lecteurs FIPS est True, la

fonctionnalité lecteurs FIPS est activée.

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

Trouvez plus d'informations

- "Gérez le stockage avec l'API Element"
- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Dépannez la fonctionnalité de lecteur FIPS

L'interface utilisateur de NetApp Element permet d'afficher les alertes concernant les pannes de cluster ou les erreurs du système liées à la fonctionnalité disques FIPS.

1. A l'aide de l'interface utilisateur de l'élément, sélectionnez **Rapport** > **alertes**.
2. Recherchez les défauts du cluster, notamment :
   - Les disques FIPS ne correspondent pas
   - La norme FIPS est mise en conformité
3. Pour des suggestions de résolution, voir informations sur les codes de défaillance du cluster.

Trouvez plus d'informations

- Codes d'anomalie du bloc d'instruments
- "Gérez le stockage avec l'API Element"
- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Activez FIPS 140-2 pour HTTPS sur votre cluster

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

Avec le logiciel NetApp Element, vous avez le choix d'activer le mode de fonctionnement FIPS (Federal information Processing Standards) 140-2 sur votre cluster. L'activation de ce mode active NetApp Cryptographic Security module (NCSM) et exploite le chiffrement certifié FIPS 140-2 de 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, celui-ci ne peut pas être désactivé. Lorsque le mode FIPS 140-2-2 est activé, chaque nœud du cluster redémarre et s'exécute automatiquement pour assurer le bon fonctionnement de NCSM en mode certifié FIPS 140-2. Cela entraîne une interruption des connexions de stockage et de gestion du cluster. Vous devez planifier soigneusement et activer ce mode uniquement si votre environnement a besoin du mécanisme de chiffrement qu'il offre.

Pour plus d'informations, voir les informations de l'API Element.

Voici un exemple de demande d'API pour activer la norme FIPS :

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

Une fois ce mode de fonctionnement activé, toutes les communications HTTPS utilisent le chiffrement approuvé FIPS 140-2.

Trouvez plus d'informations

- Chiffrement SSL
- "Gérez le stockage avec l'API Element"
- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Chiffrement SSL

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

Les listes suivantes fournissent le chiffrement SSL (Secure Socket Layer) standard pris en charge par le logiciel Element et le 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_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

TLS_ECDHE_RSA_WITH_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_WAS_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_WITH_RC4_128_MD5 (RSA 2048) - C

TLS_RSA_WITH_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_WITH_AES_128_CBC_SHA256 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A.

TLS_ECDHE_RSA_WITH_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_WAS_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.

Trouvez plus d'informations

Activez FIPS 140-2 pour HTTPS sur votre cluster

Commencez par une gestion externe des clés

La gestion externe des clés (EKM) assure la gestion de la clé d'authentification sécurisée (AK) en association avec un serveur de clés externe hors cluster (EKS). Les clés de verrouillage sont utilisées pour verrouiller et déverrouiller les disques à autocryptage (SED) lorsque "chiffrement des données au repos" est activé sur le cluster. Le EKS fournit une génération et un stockage sécurisés des clés de sécurité. Le cluster utilise le protocole KMIP (Key Management Interoperability Protocol), un protocole standard défini PAR OASIS, pour communiquer avec le EKS.

- "Configurer la gestion externe"
- "Chiffrement logiciel de nouvelle clé pour la clé principale REST"
- "Récupérer les clés d'authentification inaccessibles ou non valides"
- "Commandes d'API de gestion externe des clés"

Trouvez plus d'informations

- "CreateCluster API pouvant être utilisée pour activer le chiffrement logiciel au repos"
- "Documentation SolidFire et Element"
- "Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"

Configurez la gestion externe des clés

Procédez comme suit et utilisez les méthodes de l'API Element répertoriées pour configurer votre fonctionnalité de gestion externe des clés.

Ce dont vous avez besoin

- Si vous configurez la gestion externe des clés en association avec le chiffrement logiciel au repos, vous avez activé le chiffrement logiciel au repos à l'aide du "CreateCluster" méthode sur un nouveau cluster qui

ne contient pas de volumes.

Étapes

1. Établissez une relation de confiance avec le serveur de clés externe (EKS).
   a. Créez une paire de clés publique/privée pour le cluster Element qui est utilisé pour établir une relation de confiance avec le serveur clé en appelant la méthode API suivante : "CreatePublicPrivateKeypair"
   b. Obtenir la demande de signature de certificat (CSR) que l'autorité de certification doit signer. La RSC permet au serveur de clés de vérifier que le cluster d'éléments qui accédera aux clés est authentifié comme cluster d'éléments. Appelez la méthode API suivante : "GetClientCertificateSignRequest"
   c. Utilisez EKS/Certificate Authority pour signer la RSC récupérée. Pour plus d'informations, consultez la documentation d'un fournisseur tiers.
2. Créez un serveur et un fournisseur sur le cluster pour communiquer avec EKS. Un fournisseur clé définit l'endroit où une clé doit être obtenue et un serveur définit les attributs spécifiques de l'EKS qui seront communiqués.
   a. Créez un fournisseur de clés où résident les détails du serveur de clés en appelant la méthode API suivante : "CreateKeyProviderKmip"
   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 : "CreateKeyServerKmip" "TestKeyServerKmip"

      Si le test échoue, vérifiez la connectivité et la configuration de votre serveur. Répétez ensuite le test.
   c. Ajoutez le serveur de clés dans le conteneur du fournisseur de clés en appelant les méthodes d'API suivantes :"AddKeyServerToProviderKmip" "TestKeyProviderKmip"

      Si le test échoue, vérifiez la connectivité et la configuration de votre serveur. Répétez ensuite le test.
3. Pour le chiffrement au repos, effectuez l'une des opérations suivantes :
   a. (Pour le chiffrement matériel des données au repos) Activer "chiffrement matériel au repos" En fournissant l'ID du fournisseur de clés qui contient le serveur de clés utilisé pour stocker les clés en appelant le "EnableEncryptionAtRest" Méthode API.

      > Vous devez activer le chiffrement au repos via le "API". L'activation du chiffrement au repos à l'aide du bouton de l'interface utilisateur d'Element entraîne la restauration de la fonctionnalité à l'aide de clés générées en interne.

   b. (Pour le chiffrement logiciel au repos) dans l'ordre de "chiffrement logiciel pour les données au repos" Pour utiliser le nouveau fournisseur de clés créé, transmettez l'ID du fournisseur de clés au "RekeySoftwareEncryptionAtResteMasterKey" Méthode API.

Trouvez plus d'informations

- "Activez et désactivez le cryptage pour un cluster"
- "Documentation SolidFire et Element"
- "Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"

Chiffrement logiciel de nouvelle clé pour la clé principale REST

Vous pouvez utiliser l'API Element pour re-saisir une clé existante. Ce processus crée une nouvelle clé principale de remplacement pour votre serveur de gestion de clés

externe. Les clés principales sont toujours remplacées par de nouvelles clés principales et ne sont jamais dupliquées ou remplacées.

Vous devrez peut-être procéder à une nouvelle clé dans le cadre de l'une des procédures suivantes :

- Créez une nouvelle clé dans le cadre d'un changement de gestion interne des clés à gestion externe des clés.
- Créez une nouvelle clé comme réaction ou comme protection contre un événement lié à la sécurité.

> Ce processus est asynchrone et renvoie une réponse avant la fin de l'opération de renouvellement de clé. Vous pouvez utiliser le "GetAsyncResult" méthode d'interrogation du système pour voir quand le processus est terminé.

Ce dont vous avez besoin

- Vous avez activé le chiffrement logiciel au repos à l'aide du "CreateCluster" D'une nouvelle méthode située 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.
- Vous avez "établissement d'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 "ListeKeyProvidersKmip" Commande et copie l'ID du fournisseur de clés (`keyProviderID`).
2. Exécutez le "RekeySoftwareEncryptionAtResteMasterKey" avec le `keyManagementType` ens. paramètre `external` et `keyProviderID` Comme numéro d'ID du fournisseur de clés de l'étape précédente :

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

3. Copiez le `asyncHandle` valeur du `RekeySoftwareEncryptionAtRestMasterKey` réponse de la commande.
4. Exécutez le "GetAsyncResult" commande avec `asyncHandle` valeur de l'étape précédente pour confirmer le changement de configuration. À partir de la réponse de commande, vous devriez voir que l'ancienne configuration de clé principale a été mise à jour avec de nouvelles informations de clé. Copiez le nouvel ID de 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 de clé, y compris le `keyProviderID`, ont été mis 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
   },
}
```

Trouvez plus d'informations

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

Récupérer les clés d'authentification inaccessibles ou non valides

Parfois, une erreur peut se produire et nécessiter l'intervention de l'utilisateur. En cas d'erreur, un défaut du bloc d'instruments (appelé code inconvénient du bloc d'instruments) est généré. Les deux cas les plus probables sont décrits ici.

Le cluster ne parvient pas à déverrouiller les lecteurs en raison d'une défaillance du cluster KmipServerFault.

Cela peut se produire lorsque le cluster démarre et que le serveur de clés est inaccessible ou que la clé requise n'est pas disponible.

1. Suivre les étapes de récupération des codes inconvénient du tableau de bord (le cas échéant).

Il est possible de définir une défaillance sliceServiceIsain, car les lecteurs de métadonnées ont été marqués comme défectueux et placés dans l'état « disponible ».

Étapes à supprimer :

1. Ajoutez à nouveau les lecteurs.
2. Au bout de 3 à 4 minutes, vérifier que le `sliceServiceUnhealthy` le défaut a disparu.

Voir "codes d'anomalie du bloc d'instruments" pour en savoir plus.

Commandes d'API de gestion externe des clés

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 appartenant à un client externe :

- CreatePublicPrivateKeypair
- GetClientCertificateSignRequest

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

- CreateKeyServerKmip
- ModityKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServoersKmip
- TestKeyServerKmip

Utilisé pour la création et la maintenance de fournisseurs clés qui gèrent des serveurs de clés externes :

- CreateKeyProviderKmip

- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListeKeyProvidersKmip
- RekeySoftwareEncryptionAtResteMasterKey
- TestKeyProviderKmip

Pour plus d’informations sur les méthodes API, voir "Informations de référence API".