Gérez le stockage avec le logiciel Element

Element Software

NetApp
November 12, 2025

Sommaire

Gérez le stockage avec le logiciel Element . . . 1
- Gérez le stockage avec le logiciel Element . . . 1
  - Trouver plus d'informations . . . 1
- Accéder à l'interface utilisateur du logiciel Element . . . 1
  - Trouver plus d'informations . . . 2
- Configurez les options système SolidFire après le déploiement. . . . 2
  - Configurez les options système SolidFire après le déploiement. . . . 2
  - Modifier les informations d'identification dans NetApp HCI et NetApp SolidFire . . . 2
  - Modifier le certificat SSL par défaut du logiciel Element . . . 6
  - Modifier le mot de passe IPMI par défaut des nœuds . . . 7
- Utilisez les options de base de l'interface utilisateur du logiciel Element. . . . 9
  - Utilisez les options de base de l'interface utilisateur du logiciel Element. . . . 9
  - Activité API . . . 9
  - Icônes dans l'interface Element . . . 10
  - Laisser des commentaires . . . 11
- Gérer les comptes . . . 11
  - Gérer les comptes . . . 11
  - Travailler avec des comptes utilisant CHAP . . . 12
  - Gérer les comptes d'utilisateurs administrateurs du cluster . . . 15
  - Gérer les LDAP . . . 18
- Gérez votre système . . . 26
  - Gérez votre système . . . 27
  - Activer l'authentification multifacteur . . . 27
  - Configurer les paramètres du cluster . . . 28
  - Créer un cluster prenant en charge les disques FIPS . . . 45
  - Établir une communication sécurisée . . . 48
  - Commencez la gestion des clés externes . . . 50
- Gérer les volumes et les volumes virtuels . . . 55
  - Découvrez comment gérer les volumes et les volumes virtuels. . . . 55
  - Travailler avec des volumes . . . 57
  - Travailler avec des volumes virtuels . . . 66
  - Collaborer avec les groupes d'accès au volume et les initiateurs . . . 74
- Protégez vos données . . . 81
  - Protégez vos données . . . 81
  - Utilisez les instantanés de volume pour la protection des données . . . 82
  - Effectuez une réplication à distance entre des clusters exécutant le logiciel NetApp Element. . . . 96
  - Utiliser la réplication SnapMirror entre les clusters Element et ONTAP (interface utilisateur Element) . . . 110
  - Réplication entre le logiciel NetApp Element et ONTAP (interface de ligne de commande ONTAP) . . . 123
  - Sauvegarder et restaurer des volumes . . . 143
  - Configurer des domaines de protection personnalisés . . . 147
- Dépannage de votre système . . . 149
  - Événements système . . . 149
  - Afficher l'état des tâches en cours . . . 153

Alertes système . . . 153
Afficher l’activité de performance du nœud . . . 171
Performances en volume . . . 172
sessions iSCSI . . . 174
sessions Fibre Channel . . . 175
Dépannage des disques . . . 176
Dépannage des nœuds . . . 180
Utilisez les utilitaires par nœud pour les nœuds de stockage . . . 181
Comprendre les niveaux de remplissage des grappes . . . 188

Gérez le stockage avec le logiciel Element

Gérez le stockage avec le logiciel Element

Utilisez le logiciel Element pour configurer le stockage SolidFire , surveiller la capacité et les performances du cluster et gérer l'activité de stockage sur une infrastructure mutualisée.

Element est le système d'exploitation de stockage au cœur d'un cluster SolidFire . Le logiciel Element s'exécute indépendamment sur tous les nœuds du cluster et permet à ces nœuds de combiner leurs ressources et de se présenter comme un système de stockage unique aux clients externes. Le logiciel Element est responsable de la coordination, de la mise à l'échelle et de la gestion de l'ensemble du système.

L'interface logicielle est construite sur l'API Element.

- "Accéder à l'interface utilisateur du logiciel Element"
- "Configurez les options système SolidFire après le déploiement."
- "Composants de mise à niveau du système de stockage"
- "Utilisez les options de base de l'interface utilisateur du logiciel Element."
- "Gérer les comptes"
- "Gérez votre système"
- "Gérer les volumes et les volumes virtuels"
- "Protégez vos données"
- "Dépannage de votre système"

Trouver plus d'informations

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

Accéder à l'interface utilisateur du logiciel Element

Vous pouvez accéder à l'interface utilisateur Element en utilisant l'adresse IP virtuelle de gestion (MVIP) du nœud principal du cluster.

Vous devez vous assurer que les bloqueurs de fenêtres contextuelles et les paramètres NoScript sont désactivés dans votre navigateur.

Vous pouvez accéder à l'interface utilisateur en utilisant une adresse IPv4 ou IPv6, selon la configuration effectuée lors de la création du cluster.

1. Choisissez l'une des options suivantes :
   - IPv6 : Saisissez https://[adresse IPv6 MVIP] Par exemple :

     ```
     https://[fd20:8b1e:b256:45a::1234]/
     ```

- IPv4 : Saisissez https://[Adresse MVIP IPv4] Par exemple :

```
https://10.123.456.789/
```

2. Pour le DNS, saisissez le nom d'hôte.
3. Cliquez sur les messages relatifs au certificat d'authentification.

Trouver plus d'informations

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

Configurez les options système SolidFire après le déploiement.

Configurez les options système SolidFire après le déploiement.

Une fois votre système SolidFire configuré, vous pouvez effectuer quelques tâches facultatives.

Si vous modifiez les identifiants du système, vous voudrez peut-être connaître l'impact sur les autres composants.

De plus, vous pouvez configurer les paramètres d'authentification multifactorielle, de gestion des clés externes et de sécurité FIPS (Federal Information Processing Standards). Il est également conseillé de mettre à jour vos mots de passe lorsque cela est nécessaire.

Trouver plus d'informations

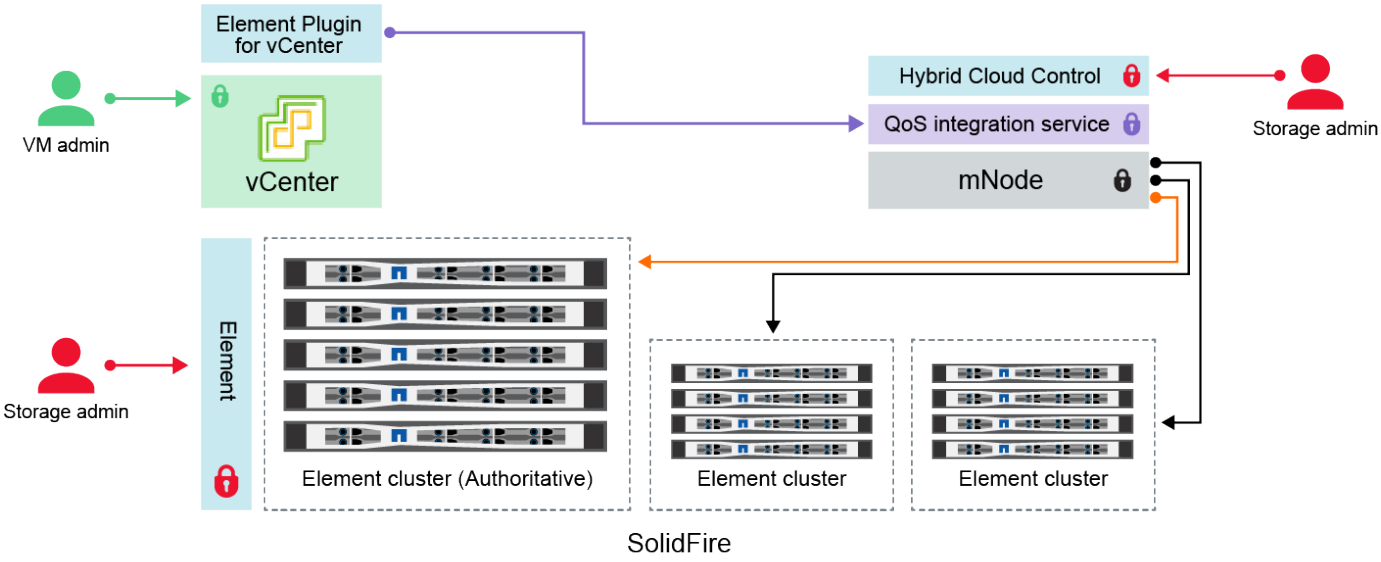
- "Modifier les informations d'identification dans NetApp HCI et NetApp SolidFire"
- "Modifier le certificat SSL par défaut du logiciel Element"
- "Modifier le mot de passe IPMI des nœuds"
- "Activer l'authentification multifacteur"
- "Commencez la gestion des clés externes"
- "Créer un cluster prenant en charge les disques FIPS"

Modifier les informations d'identification dans NetApp HCI et NetApp SolidFire

Selon les politiques de sécurité de l'organisation qui a déployé NetApp HCI ou NetApp SolidFire, la modification des identifiants ou des mots de passe fait généralement partie des pratiques de sécurité. Avant de modifier les mots de passe, vous devez prendre en compte l'impact sur les autres composants logiciels du déploiement.

Si vous modifiez les informations d'identification d'un composant d'un déploiement NetApp HCI ou NetApp SolidFire , le tableau suivant fournit des indications sur l'impact sur les autres composants.

Interactions entre les composants de NetApp SolidFire :



Type et icône d'identification	Utilisation par l'administrateur	Consultez ces instructions
Identifiants de l'élément 	**S'applique à** : NetApp HCI et SolidFire Les administrateurs utilisent ces identifiants pour se connecter à : • Interface utilisateur Element sur le cluster de stockage Element • Contrôle du cloud hybride sur le nœud de gestion (mnode) Lorsque Hybrid Cloud Control gère plusieurs clusters de stockage, il n'accepte que les informations d'identification de l'administrateur des clusters de stockage, connus sous le nom de *cluster faisant autorité* pour lesquels le mnode a été initialement configuré. Pour les clusters de stockage ajoutés ultérieurement à Hybrid Cloud Control, le mnode stocke en toute sécurité les informations d'identification de l'administrateur. Si les informations d'identification des clusters de stockage ajoutés ultérieurement sont modifiées, ces informations d'identification doivent également être mises à jour dans le mnode à l'aide de l'API mnode.	• "Mettez à jour les mots de passe d'administrateur du cluster de stockage." • Mettez à jour les informations d'identification de l'administrateur du cluster de stockage dans le mnode en utilisant le"API modifyclusteradmin" .

Type et icône d'identification	Utilisation par l'administrateur	Consultez ces instructions
Identifiants d'authentification unique vSphere 	**S'applique uniquement à** : NetApp HCI Les administrateurs utilisent ces identifiants pour se connecter au client VMware vSphere. Lorsque vCenter fait partie de l'installation NetApp HCI , les informations d'identification sont configurées dans le moteur de déploiement NetApp comme suit : • nom_utilisateur@vsphere.local avec le mot de passe spécifié, et • administrateur@vsphere.local avec le mot de passe spécifié. Lorsqu'un vCenter existant est utilisé pour déployer NetApp HCI, les informations d'identification vSphere Single Sign-on sont gérées par les administrateurs VMware du service informatique.	"Mise à jour des identifiants vCenter et ESXi".
Identifiants du contrôleur de gestion de la carte mère (BMC) 	**S'applique uniquement à** : NetApp HCI Les administrateurs utilisent ces identifiants pour se connecter au BMC des nœuds de calcul NetApp dans un déploiement NetApp HCI . Le BMC assure la surveillance matérielle de base et offre des fonctionnalités de console virtuelle. Les informations d'identification BMC (parfois appelées *IPMI*) de chaque nœud de calcul NetApp sont stockées en toute sécurité sur le mnode dans les déploiements NetApp HCI . NetApp Hybrid Cloud Control utilise les informations d'identification BMC en tant que compte de service pour communiquer avec le BMC des nœuds de calcul lors des mises à niveau du firmware des nœuds de calcul. Lorsque les identifiants BMC sont modifiés, les identifiants des nœuds de calcul respectifs doivent également être mis à jour sur le mnode afin de conserver toutes les fonctionnalités de Hybrid Cloud Control.	• "Configurez IPMI pour chaque nœud sur NetApp HCI.". • Pour les nœuds H410C, H610C et H615C,"modifier le mot de passe IPMI par défaut" . • Pour les nœuds H410S et H610S,"modifier le mot de passe IPM par défaut" . • "Modifier les informations d'identification BMC sur le nœud de gestion".

Type et icône d'identification	Utilisation par l'administrateur	Consultez ces instructions
Identifiants ESXi 	**S'applique uniquement à** : NetApp HCI Les administrateurs peuvent se connecter aux hôtes ESXi en utilisant soit SSH, soit l'interface DCUI locale avec un compte racine local. Dans les déploiements NetApp HCI , le nom d'utilisateur est « root » et le mot de passe a été spécifié lors de l'installation initiale de ce nœud de calcul dans NetApp Deployment Engine. Les informations d'identification racine ESXi de chaque nœud de calcul NetApp sont stockées en toute sécurité sur le mnode dans les déploiements NetApp HCI . NetApp Hybrid Cloud Control utilise les informations d'identification d'un compte de service pour communiquer directement avec les hôtes ESXi lors des mises à niveau du firmware et des contrôles d'intégrité des nœuds de calcul. Lorsque les informations d'identification racine ESXi sont modifiées par un administrateur VMware, les informations d'identification des nœuds de calcul respectifs doivent être mises à jour sur le mnode pour conserver la fonctionnalité de contrôle du cloud hybride.	"Mise à jour des informations d'identification pour les hôtes vCenter et ESXi".
mot de passe d'intégration QoS 	**S'applique à** : NetApp HCI et, en option , SolidFire Non utilisé pour les connexions interactives des administrateurs. L'intégration QoS entre VMware vSphere et Element Software est activée via : • Module d'extension Element pour vCenter Server, et • Service QoS sur le mnode. Pour l'authentification, le service QoS utilise un mot de passe exclusivement utilisé dans ce contexte. Le mot de passe QoS est spécifié lors de l'installation initiale du plug-in Element pour vCenter Server, ou généré automatiquement lors du déploiement de NetApp HCI . Aucun impact sur les autres composants.	"Mettez à jour les informations d'identification QoSSIOC dans le plug-in NetApp Element pour vCenter Server.". Le mot de passe SIOC du plug-in NetApp Element pour vCenter Server est également connu sous le nom de *mot de passe QoSSIOC*. Consultez l'article de la base de connaissances Element Plug-in pour vCenter Server.

Type et icône d'identification	Utilisation par l'administrateur	Consultez ces instructions
Identifiants de l'appliance vCenter Service 	**S'applique à** : NetApp HCI uniquement s'il est configuré par NetApp Deployment Engine Les administrateurs peuvent se connecter aux machines virtuelles de l'appliance vCenter Server. Dans les déploiements NetApp HCI , le nom d'utilisateur est « root » et le mot de passe a été spécifié lors de l'installation initiale de ce nœud de calcul dans le moteur de déploiement NetApp . Selon la version de VMware vSphere déployée, certains administrateurs du domaine vSphere Single Sign-on peuvent également se connecter à l'appliance. Aucun impact sur les autres composants.	Aucune modification nécessaire.
Identifiants d'administrateur du nœud de gestion NetApp 	**S'applique à** : NetApp HCI et, en option , SolidFire Les administrateurs peuvent se connecter aux machines virtuelles du nœud de gestion NetApp pour effectuer des configurations avancées et des dépannages. Selon la version du nœud de gestion déployée, la connexion via SSH n'est pas activée par défaut. Dans les déploiements NetApp HCI , le nom d'utilisateur et le mot de passe étaient spécifiés par l'utilisateur lors de l'installation initiale de ce nœud de calcul dans NetApp Deployment Engine. Aucun impact sur les autres composants.	Aucune modification nécessaire.

Trouver plus d'informations

- "Modifier le certificat SSL par défaut du logiciel Element"
- "Modifier le mot de passe IPMI des nœuds"
- "Activer l'authentification multifacteur"
- "Commencez la gestion des clés externes"
- "Créer un cluster prenant en charge les disques FIPS"

Modifier le certificat SSL par défaut du logiciel Element

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

Lors de la création d'un cluster logiciel NetApp Element , celui-ci génère un certificat SSL (Secure Sockets Layer) auto-signé unique et une clé privée utilisés pour toutes les communications HTTPS via l'interface utilisateur Element, l'interface utilisateur par nœud ou les API. Le logiciel Element prend en charge les certificats auto-signés ainsi que les certificats émis et vérifiés par une autorité de certification (AC) de confiance.

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

- **Obtenir un certificat SSL**

  Vous pouvez utiliser le"Méthode GetSSLCertificate" pour récupérer des informations sur le certificat SSL actuellement installé, y compris tous les détails du certificat.

- **Définir le certificat SSL**

  Vous pouvez utiliser le"Méthode SetSSLCertificate" pour configurer les certificats SSL du cluster et par nœud avec le certificat et la clé privée que vous fournissez. Le système valide le certificat et la clé privée afin d'empêcher l'application d'un certificat invalide.

- **Supprimer le certificat SSL**

  Le"Méthode RemoveSSLCertificate" Supprime le certificat SSL et la clé privée actuellement installés. Le cluster génère ensuite un nouveau certificat auto-signé et une nouvelle clé privée.

> Le certificat SSL du cluster est automatiquement appliqué à tous les nouveaux nœuds ajoutés au cluster. Tout nœud retiré du cluster revient à un certificat auto-signé et toutes les informations de certificat et de clé définies par l'utilisateur sont supprimées du nœud.

Trouver plus d'informations

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

Modifier le mot de passe IPMI par défaut des nœuds

Vous pouvez modifier le mot de passe administrateur par défaut de l'interface de gestion de plateforme intelligente (IPMI) dès que vous disposez d'un accès IPMI distant au nœud. Vous pourriez vouloir faire cela s'il y a des mises à jour d'installation.

Pour plus de détails sur la configuration de l'accès IPM pour les nœuds, consultez"Configurer IPMI pour chaque nœud" .

Vous pouvez modifier le mot de passe IPM pour ces nœuds :

- Nœuds H410S
- Nœuds H610S

Modifier le mot de passe IPMI par défaut des nœuds H410S

Vous devez modifier le mot de passe par défaut du compte administrateur IPMI sur chaque nœud de stockage dès que vous configurez le port réseau IPMI.

Ce dont vous aurez besoin

Vous auriez dû configurer l'adresse IP IPMI pour chaque nœud de stockage.

Étapes

1. Ouvrez un navigateur web sur un ordinateur pouvant accéder au réseau IPMI et accédez à l'adresse IP IPMI du nœud.
2. Saisissez le nom d'utilisateur `ADMIN` et mot de passe `ADMIN` dans l'invite de connexion.
3. Une fois connecté, cliquez sur l'onglet **Configuration**.
4. Cliquez sur **Utilisateurs**.
5. Sélectionnez `ADMIN` utilisateur et cliquez sur **Modifier l'utilisateur**.
6. Cochez la case **Changer le mot de passe**.
7. Saisissez un nouveau mot de passe dans les champs **Mot de passe** et **Confirmer le mot de passe**.
8. Cliquez sur **Modifier**, puis sur **OK**.
9. Répétez cette procédure pour tous les autres nœuds H410S ayant des mots de passe IPMI par défaut.

Modifier le mot de passe IPMI par défaut des nœuds H610S

Vous devez modifier le mot de passe par défaut du compte administrateur IPMI sur chaque nœud de stockage dès que vous configurez le port réseau IPMI.

Ce dont vous aurez besoin

Vous auriez dû configurer l'adresse IP IPMI pour chaque nœud de stockage.

Étapes

1. Ouvrez un navigateur web sur un ordinateur pouvant accéder au réseau IPMI et accédez à l'adresse IP IPMI du nœud.
2. Saisissez le nom d'utilisateur `root` et mot de passe `calvin` dans l'invite de connexion.
3. Une fois connecté, cliquez sur l'icône de navigation du menu en haut à gauche de la page pour ouvrir le panneau latéral.
4. Cliquez sur **Paramètres**.
5. Cliquez sur **Gestion des utilisateurs**.
6. Sélectionnez l'utilisateur **Administrateur** dans la liste.
7. Cochez la case **Changer le mot de passe**.
8. Saisissez un nouveau mot de passe fort dans les champs **Mot de passe** et **Confirmer le mot de passe**.
9. Cliquez sur **Enregistrer** en bas de la page.
10. Répétez cette procédure pour tous les autres nœuds H610S ayant des mots de passe IPMI par défaut.

Trouver plus d'informations

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

Utilisez les options de base de l'interface utilisateur du logiciel Element.

Utilisez les options de base de l'interface utilisateur du logiciel Element.

L'interface utilisateur Web du logiciel NetApp Element (Element UI) vous permet de surveiller et d'effectuer des tâches courantes sur votre système SolidFire .

Les options de base incluent la visualisation des commandes API activées par l'activité de l'interface utilisateur et la possibilité de fournir des commentaires.

- "Afficher l'activité de l'API"
- "Icônes dans l'interface Element"
- "Laisser des commentaires"

Pour plus d'informations

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

Activité API

Afficher l'activité de l'API

Le système Element utilise l'API NetApp Element comme base pour ses fonctionnalités. L'interface utilisateur Element vous permet de visualiser différents types d'activité API en temps réel sur le système pendant que vous utilisez l'interface. Le journal de l'API vous permet de consulter l'activité de l'API système initiée par l'utilisateur et en arrière-plan, ainsi que les appels d'API effectués sur la page que vous consultez actuellement.

Vous pouvez utiliser le journal de l'API pour identifier les méthodes d'API utilisées pour certaines tâches et voir comment utiliser les méthodes et les objets de l'API pour créer des applications personnalisées.

Pour plus d'informations sur chaque méthode, consultez "Référence de l'API Element Software".

1. Dans la barre de navigation de l'interface utilisateur Element, cliquez sur **Journal API**.
2. Pour modifier le type d'activité API affiché dans la fenêtre Journal API, procédez comme suit :
   a. Sélectionnez **Requêtes** pour afficher le trafic des requêtes API.
   b. Sélectionnez **Réponses** pour afficher le trafic de réponse de l'API.
   c. Filtrez les types de trafic API en sélectionnant l'une des options suivantes :
      - **Initié par l'utilisateur** : Trafic API généré par vos activités durant cette session d'interface utilisateur Web.
      - **Interrogation en arrière-plan** : Trafic API généré par l'activité système en arrière-plan.
      - **Page actuelle** : Trafic API généré par les tâches de la page que vous consultez actuellement.

Trouver plus d'informations

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

Le taux de rafraîchissement de l'interface est affecté par la charge du cluster.

En fonction des temps de réponse de l'API, le cluster peut ajuster automatiquement l'intervalle d'actualisation des données pour certaines parties de la page du logiciel NetApp Element que vous consultez.

L'intervalle d'actualisation est réinitialisé à sa valeur par défaut lorsque vous rechargez la page dans votre navigateur. Vous pouvez consulter l'intervalle d'actualisation actuel en cliquant sur le nom du cluster en haut à droite de la page. Notez que l'intervalle contrôle la fréquence des requêtes API, et non la vitesse à laquelle les données sont renvoyées par le serveur.

Lorsqu'un cluster est soumis à une charge importante, il peut mettre en file d'attente les requêtes API provenant de l'interface utilisateur Element. Dans de rares cas, lorsque la réponse du système est considérablement retardée, par exemple en cas de connexion réseau lente combinée à un cluster occupé, vous pourriez être déconnecté de l'interface utilisateur d'Element si le système ne répond pas assez rapidement aux requêtes API mises en file d'attente. Si vous êtes redirigé vers l'écran de déconnexion, vous pouvez vous reconnecter après avoir ignoré toute invite d'authentification initiale du navigateur. En revenant à la page de présentation, il se peut que l'on vous demande vos identifiants de cluster s'ils n'ont pas été enregistrés par votre navigateur.

Icônes dans l'interface Element

L'interface du logiciel NetApp Element affiche des icônes représentant les actions que vous pouvez effectuer sur les ressources système.

Le tableau suivant fournit un aperçu rapide :

Icône	Description
	Actions
	Sauvegarde de
	Cloner ou copier
	Supprimer ou purger
	Modifier

	Filtre
	Paire
	Rafraîchir
	Restaurer
	Restaurer à partir de
	Annulation
	Instantané

Laisser des commentaires

Vous pouvez contribuer à améliorer l'interface utilisateur Web du logiciel Element et signaler tout problème d'interface en utilisant le formulaire de commentaires accessible dans toute l'interface.

1. Depuis n'importe quelle page de l'interface utilisateur d'Element, cliquez sur le bouton **Commentaires**.
2. Saisissez les informations pertinentes dans les champs Résumé et Description.
3. Joignez des captures d'écran utiles.
4. Veuillez saisir un nom et une adresse électronique.
5. Cochez la case pour inclure des données sur votre environnement actuel.
6. Cliquez sur **Soumettre**.

Trouver plus d'informations

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

Gérer les comptes

Gérer les comptes

Dans les systèmes de stockage SolidFire , les locataires peuvent utiliser des comptes pour permettre aux clients de se connecter aux volumes d'un cluster. Lorsque vous créez

un volume, celui-ci est affecté à un compte spécifique. Vous pouvez également gérer les comptes d'administrateur de cluster pour un système de stockage SolidFire .

- "Travailler avec des comptes utilisant CHAP"
- "Gérer les comptes d'utilisateurs administrateurs du cluster"

Pour plus d'informations

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

Travailler avec des comptes utilisant CHAP

Dans les systèmes de stockage SolidFire , les locataires peuvent utiliser des comptes pour permettre aux clients de se connecter aux volumes d'un cluster. Un compte contient l'authentification par protocole CHAP (Challenge-Handshake Authentication Protocol) requise pour accéder aux volumes qui lui sont attribués. Lorsque vous créez un volume, celui-ci est affecté à un compte spécifique.

Un compte peut se voir attribuer jusqu'à deux mille volumes, mais un volume ne peut appartenir qu'à un seul compte.

Algorithmes CHAP

À partir de l'élément 12.7, les algorithmes CHAP sécurisés conformes à la norme FIPS SHA1, SHA-256 et SHA3-256 sont pris en charge. Lorsqu'un initiateur iSCSI hôte crée une session iSCSI avec une cible iSCSI Element, il demande une liste d'algorithmes CHAP à utiliser. La cible iSCSI Element choisit le premier algorithme qu'elle prend en charge parmi la liste demandée par l'initiateur iSCSI hôte. Pour confirmer que la cible iSCSI Element choisit l'algorithme le plus sécurisé, vous devez configurer l'initiateur iSCSI hôte pour envoyer une liste d'algorithmes classés du plus sécurisé, par exemple SHA3-256, au moins sécurisé, par exemple SHA1 ou MD5. Lorsque les algorithmes SHA ne sont pas demandés par l'initiateur iSCSI hôte, la cible iSCSI Element choisit MD5, en supposant que la liste d'algorithmes proposée par l'hôte contienne MD5. Vous devrez peut-être mettre à jour la configuration de l'initiateur iSCSI hôte pour activer la prise en charge des algorithmes sécurisés.

Lors d'une mise à niveau vers Element 12.7 ou une version ultérieure, si vous avez déjà mis à jour la configuration de l'initiateur iSCSI de l'hôte pour envoyer une requête de session avec une liste incluant les algorithmes SHA, lors du redémarrage des nœuds de stockage, les nouveaux algorithmes sécurisés sont activés et les sessions iSCSI nouvelles ou reconnectées sont établies à l'aide du protocole le plus sécurisé. Toutes les sessions iSCSI existantes passeront de MD5 à SHA lors de la mise à niveau. Si vous ne mettez pas à jour la configuration de l'initiateur iSCSI hôte pour demander SHA, les sessions iSCSI existantes continueront d'utiliser MD5. Ultérieurement, après la mise à jour des algorithmes CHAP de l'initiateur iSCSI hôte, les sessions iSCSI devraient passer progressivement de MD5 à SHA au fil du temps en fonction des activités de maintenance qui entraînent des reconnexions de session iSCSI.

Par exemple, l'initiateur iSCSI hôte par défaut dans Red Hat Enterprise Linux (RHEL) 8.3 possède le `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` Le paramètre a été commenté, ce qui a pour conséquence que l'initiateur iSCSI utilise uniquement MD5. Décommenter ce paramètre sur l'hôte et redémarrer l'initiateur iSCSI déclenche l'utilisation de SHA3-256 par les sessions iSCSI de cet hôte.

Si nécessaire, vous pouvez utiliser le "Liste des sessions ISCSI" Méthode API permettant de visualiser les algorithmes CHAP utilisés pour chaque session.

Créer un compte

Vous pouvez créer un compte pour autoriser l'accès aux volumes.

Chaque nom de compte dans le système doit être unique.

1. Sélectionnez **Gestion** > **Comptes**.
2. Cliquez sur **Créer un compte**.
3. Veuillez saisir un **nom d'utilisateur**.
4. Dans la section **Paramètres CHAP**, saisissez les informations suivantes :

   Laissez les champs d'identification vides pour générer automatiquement un mot de passe.

   - **Secret de l'initiateur** pour l'authentification de session du nœud CHAP.
   - **Secret cible** pour l'authentification de session du nœud CHAP.
5. Cliquez sur **Créer un compte**.

Afficher les détails du compte

Vous pouvez consulter les performances de chaque compte sous forme graphique.

Les informations graphiques fournissent des données sur les E/S et le débit du compte. Les niveaux d'activité moyens et de pointe sont affichés par incréments de périodes de rapport de 10 secondes. Ces statistiques incluent l'activité de tous les volumes attribués au compte.

1. Sélectionnez **Gestion** > **Comptes**.
2. Cliquez sur l'icône Actions pour un compte.
3. Cliquez sur **Afficher les détails**.

Voici quelques détails :

- **Statut** : Le statut du compte. Valeurs possibles :
  - actif : Un compte actif.
  - verrouillé : Un compte verrouillé.
  - supprimé : Un compte qui a été supprimé et purgé.
- **Volumes actifs** : Le nombre de volumes actifs attribués au compte.
- **Compression** : Score d'efficacité de la compression pour les volumes attribués au compte.
- **Déduplication** : Score d'efficacité de la déduplication pour les volumes attribués au compte.
- **Provisionnement fin** : Score d'efficacité du provisionnement fin pour les volumes affectés au compte.
- **Efficacité globale** : Score d'efficacité global pour les volumes attribués au compte.

Modifier un compte

Vous pouvez modifier un compte pour en changer le statut, les secrets CHAP ou le nom.

La modification des paramètres CHAP dans un compte ou la suppression d'initiateurs ou de volumes d'un groupe d'accès peut entraîner une perte d'accès inattendue aux volumes pour les initiateurs. Pour éviter toute perte d'accès inattendue aux volumes, déconnectez systématiquement les sessions iSCSI qui seront affectées

par une modification de compte ou de groupe d'accès, et vérifiez que les initiateurs peuvent se reconnecter aux volumes une fois les modifications apportées aux paramètres d'initiateur et aux paramètres de cluster terminées.

> Les volumes persistants associés aux services de gestion sont affectés à un nouveau compte créé lors de l'installation ou de la mise à niveau. Si vous utilisez des volumes persistants, ne modifiez ni ne supprimez le compte associé.

1. Sélectionnez **Gestion** > **Comptes**.
2. Cliquez sur l'icône Actions pour un compte.
3. Dans le menu qui s'affiche, sélectionnez **Modifier**.
4. **Facultatif :** Modifier le **nom d'utilisateur**.
5. **Facultatif :** Cliquez sur la liste déroulante **Statut** et sélectionnez un autre statut.

> Le passage au statut **verrouillé** met fin à toutes les connexions iSCSI vers le compte, et celui-ci n'est plus accessible. Les volumes associés au compte sont conservés ; cependant, ces volumes ne sont pas détectables via iSCSI.

6. **Facultatif :** Dans les **Paramètres CHAP**, modifiez les informations d'identification **Secret de l'initiateur** et **Secret cible** utilisées pour l'authentification de la session du nœud.

> Si vous ne modifiez pas les informations d'identification **Paramètres CHAP**, elles restent inchangées. Si vous laissez les champs d'identification vides, le système génère de nouveaux mots de passe.

7. Cliquez sur **Enregistrer les modifications**.

Supprimer un compte

Vous pouvez supprimer un compte lorsqu'il n'est plus nécessaire.

Supprimez et purgez tous les volumes associés au compte avant de supprimer le compte.

> Les volumes persistants associés aux services de gestion sont affectés à un nouveau compte créé lors de l'installation ou de la mise à niveau. Si vous utilisez des volumes persistants, ne modifiez ni ne supprimez le compte associé.

1. Sélectionnez **Gestion** > **Comptes**.
2. Cliquez sur l'icône Actions du compte que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, sélectionnez **Supprimer**.
4. Confirmez l'action.

Trouver plus d'informations

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

Gérer les comptes d’utilisateurs administrateurs du cluster

Vous pouvez gérer les comptes d’administrateur de cluster pour un système de stockage SolidFire en créant, supprimant et modifiant les comptes d’administrateur de cluster, en changeant le mot de passe de l’administrateur de cluster et en configurant les paramètres LDAP pour gérer l’accès au système pour les utilisateurs.

types de comptes d’administrateur de cluster de stockage

Il existe deux types de comptes d’administrateur pouvant exister dans un cluster de stockage exécutant le logiciel NetApp Element : le compte d’administrateur principal du cluster et un compte d’administrateur de cluster.

- **Compte d’administrateur principal du cluster**

  Ce compte administrateur est créé lors de la création du cluster. Ce compte est le compte d’administration principal disposant du niveau d’accès le plus élevé au cluster. Ce compte est analogue à un utilisateur root dans un système Linux. Vous pouvez modifier le mot de passe de ce compte administrateur.

- **Compte d’administrateur de cluster**

  Vous pouvez accorder à un compte d’administrateur de cluster un accès administratif limité pour effectuer des tâches spécifiques au sein d’un cluster. Les identifiants attribués à chaque compte d’administrateur de cluster sont utilisés pour authentifier les requêtes API et Element UI au sein du système de stockage.

> Un compte d’administrateur de cluster local (non-LDAP) est requis pour accéder aux nœuds actifs d’un cluster via l’interface utilisateur par nœud. Les identifiants de compte ne sont pas nécessaires pour accéder à un nœud qui ne fait pas encore partie d’un cluster.

Afficher les détails de l’administrateur du cluster

1. Pour créer un compte d’administrateur de cluster (non-LDAP) à l’échelle du cluster, procédez comme suit :
   a. Cliquez sur **Utilisateurs** > **Administrateurs du cluster**.
2. Sur la page Administrateurs du cluster de l’onglet Utilisateurs, vous pouvez consulter les informations suivantes.
   - **ID** : Numéro séquentiel attribué au compte d’administrateur du cluster.
   - **Nom d’utilisateur** : Le nom donné au compte d’administrateur du cluster lors de sa création.
   - **Accès** : Les autorisations attribuées au compte utilisateur. Valeurs possibles :
     - lire
     - reportage
     - nœuds
     - lecteurs
     - volumes
     - comptes
     - Administrateurs de cluster
     - administrateur

- supportAdmin

> Toutes les autorisations sont disponibles pour le type d'accès administrateur.
>
> Certains types d'accès disponibles via l'API ne sont pas disponibles dans l'interface utilisateur d'Element.

+

- **Type** : Le type d'administrateur de cluster. Valeurs possibles :
  - Cluster
  - LDAP
- **Attributs** : Si le compte d'administrateur du cluster a été créé à l'aide de l'API Element, cette colonne affiche toutes les paires nom-valeur définies à l'aide de cette méthode.

  Voir"Référence de l'API du logiciel NetApp Element" .

Créer un compte d'administrateur de cluster

Vous pouvez créer de nouveaux comptes d'administrateur de cluster avec des autorisations permettant d'autoriser ou de restreindre l'accès à des zones spécifiques du système de stockage. Lorsque vous définissez les autorisations du compte d'administrateur de cluster, le système accorde des droits de lecture seule pour toutes les autorisations que vous n'attribuez pas à l'administrateur de cluster.

Si vous souhaitez créer un compte d'administrateur de cluster LDAP, assurez-vous que LDAP est configuré sur le cluster avant de commencer.

"Activez l'authentification LDAP avec l'interface utilisateur Element."

Vous pourrez ultérieurement modifier les privilèges du compte d'administrateur de cluster pour la génération de rapports, les nœuds, les lecteurs, les volumes, les comptes et l'accès au niveau du cluster. Lorsque vous activez une autorisation, le système attribue un accès en écriture pour ce niveau. Le système accorde à l'utilisateur administrateur un accès en lecture seule pour les niveaux que vous ne sélectionnez pas.

Vous pouvez également supprimer ultérieurement tout compte utilisateur d'administrateur de cluster créé par un administrateur système. Vous ne pouvez pas supprimer le compte d'administrateur principal du cluster qui a été créé lors de la création du cluster.

1. Pour créer un compte d'administrateur de cluster (non-LDAP) à l'échelle du cluster, procédez comme suit :
   a. Cliquez sur **Utilisateurs** > **Administrateurs du cluster**.
   b. Cliquez sur **Créer un administrateur de cluster**.
   c. Sélectionnez le type d'utilisateur **Cluster**.
   d. Saisissez un nom d'utilisateur et un mot de passe pour le compte, puis confirmez le mot de passe.
   e. Sélectionnez les autorisations utilisateur à appliquer au compte.
   f. Cochez la case pour accepter le contrat de licence utilisateur final.
   g. Cliquez sur **Créer un administrateur de cluster**.
2. Pour créer un compte d'administrateur de cluster dans l'annuaire LDAP, procédez comme suit :
   a. Cliquez sur **Cluster** > **LDAP**.

b. Assurez-vous que l'authentification LDAP est activée.

c. Cliquez sur **Tester l'authentification de l'utilisateur** et copiez le nom distinctif qui apparaît pour l'utilisateur ou l'un des groupes dont il est membre afin de pouvoir le coller ultérieurement.

d. Cliquez sur **Utilisateurs** > **Administrateurs du cluster**.

e. Cliquez sur **Créer un administrateur de cluster**.

f. Sélectionnez le type d'utilisateur LDAP.

g. Dans le champ Nom distinctif, suivez l'exemple de la zone de texte pour saisir un nom distinctif complet pour l'utilisateur ou le groupe. Vous pouvez aussi le coller à partir du nom distinctif que vous avez copié précédemment.

   Si le nom distinctif fait partie d'un groupe, alors tout utilisateur membre de ce groupe sur le serveur LDAP disposera des autorisations de ce compte administrateur.

Pour ajouter des utilisateurs ou des groupes d'administrateurs de cluster LDAP, le format général du nom d'utilisateur est « `LDAP:<Nom distinctif complet>` ».

a. Sélectionnez les autorisations utilisateur à appliquer au compte.

b. Cochez la case pour accepter le contrat de licence utilisateur final.

c. Cliquez sur **Créer un administrateur de cluster**.

Modifier les autorisations d'administrateur du cluster

Vous pouvez modifier les privilèges du compte d'administrateur de cluster pour la génération de rapports, les nœuds, les lecteurs, les volumes, les comptes et l'accès au niveau du cluster. Lorsque vous activez une autorisation, le système attribue un accès en écriture pour ce niveau. Le système accorde à l'utilisateur administrateur un accès en lecture seule pour les niveaux que vous ne sélectionnez pas.

1. Cliquez sur **Utilisateurs** > **Administrateurs du cluster**.
2. Cliquez sur l'icône Actions correspondant à l'administrateur du cluster que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Sélectionnez les autorisations utilisateur à appliquer au compte.
5. Cliquez sur **Enregistrer les modifications**.

Modifier les mots de passe des comptes d'administrateur de cluster

Vous pouvez utiliser l'interface utilisateur Element pour modifier les mots de passe des administrateurs de cluster.

1. Cliquez sur **Utilisateurs** > **Administrateurs du cluster**.
2. Cliquez sur l'icône Actions correspondant à l'administrateur du cluster que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Dans le champ « Changer le mot de passe », saisissez un nouveau mot de passe et confirmez-le.
5. Cliquez sur **Enregistrer les modifications**.

Informations connexes

- "Découvrez les types d'accès disponibles pour les API Element."
- "Activez l'authentification LDAP avec l'interface utilisateur Element."

- "Désactiver LDAP"
- "Module d'extension NetApp Element pour vCenter Server"

Gérer les LDAP

Vous pouvez configurer le protocole LDAP (Lightweight Directory Access Protocol) pour activer une fonctionnalité de connexion sécurisée basée sur un annuaire au stockage SolidFire . Vous pouvez configurer LDAP au niveau du cluster et autoriser les utilisateurs et les groupes LDAP.

La gestion du protocole LDAP implique la configuration de l'authentification LDAP auprès d'un cluster SolidFire à l'aide d'un environnement Microsoft Active Directory existant et le test de cette configuration.

Vous pouvez utiliser les adresses IPv4 et IPv6.

L'activation de LDAP implique les étapes générales suivantes, décrites en détail :

1. **Étapes complètes de préconfiguration pour la prise en charge LDAP**. Vérifiez que vous disposez de toutes les informations nécessaires à la configuration de l'authentification LDAP.
2. **Activer l'authentification LDAP**. Utilisez soit l'interface utilisateur d'Element, soit l'API d'Element.
3. **Valider la configuration LDAP**. Vous pouvez également vérifier que le cluster est configuré avec les valeurs correctes en exécutant la méthode API GetLdapConfiguration ou en vérifiant la configuration LCAP à l'aide de l'interface utilisateur Element.
4. **Testez l'authentification LDAP** (avec le `readonly` utilisateur). Vérifiez que la configuration LDAP est correcte soit en exécutant la méthode API TestLdapAuthentication, soit en utilisant l'interface utilisateur Element. Pour ce test initial, utilisez le nom d'utilisateur « `sAMAccountName` » du `readonly` utilisateur. Cela permettra de vérifier que votre cluster est correctement configuré pour l'authentification LDAP et de valider également que le `readonly` Les identifiants et l'accès sont corrects. Si cette étape échoue, répétez les étapes 1 à 3.
5. **Testez l'authentification LDAP** (avec un compte utilisateur que vous souhaitez ajouter). Répétez l'étape 4 avec un compte utilisateur que vous souhaitez ajouter en tant qu'administrateur du cluster Element. Copiez le `distinguished` nom (DN) ou l'utilisateur (ou le groupe). Ce DN sera utilisé à l'étape 6.
6. **Ajoutez l'administrateur du cluster LDAP** (copiez et collez le DN de l'étape de test d'authentification LDAP). Créez un nouvel utilisateur administrateur de cluster avec le niveau d'accès approprié, soit via l'interface utilisateur Element, soit via la méthode API AddLdapClusterAdmin. Pour le nom d'utilisateur, collez le DN complet que vous avez copié à l'étape 5. Cela garantit que le DN est correctement formaté.
7. **Tester l'accès administrateur du cluster**. Connectez-vous au cluster en utilisant l'utilisateur administrateur du cluster LDAP nouvellement créé. Si vous avez ajouté un groupe LDAP, vous pouvez vous connecter en tant que n'importe quel utilisateur appartenant à ce groupe.

Étapes complètes de préconfiguration pour la prise en charge LDAP

Avant d'activer la prise en charge LDAP dans Element, vous devez configurer un serveur Active Directory Windows et effectuer d'autres tâches de préconfiguration.

Étapes

1. Configurer un serveur Active Directory Windows.
2. **Facultatif :** Activer la prise en charge LDAPS.

3. Créer des utilisateurs et des groupes.
4. Créez un compte de service en lecture seule (tel que « `sfreadonly` ») à utiliser pour la recherche dans l'annuaire LDAP.

Activez l'authentification LDAP avec l'interface utilisateur Element.

Vous pouvez configurer l'intégration du système de stockage avec un serveur LDAP existant. Cela permet aux administrateurs LDAP de gérer de manière centralisée l'accès des utilisateurs au système de stockage.

Vous pouvez configurer LDAP soit avec l'interface utilisateur d'Element, soit avec l'API d'Element. Cette procédure décrit comment configurer LDAP à l'aide de l'interface utilisateur Element.

Cet exemple montre comment configurer l'authentification LDAP sur SolidFire et l'utilise `SearchAndBind` comme type d'authentification. L'exemple utilise un seul serveur Active Directory Windows Server 2012 R2.

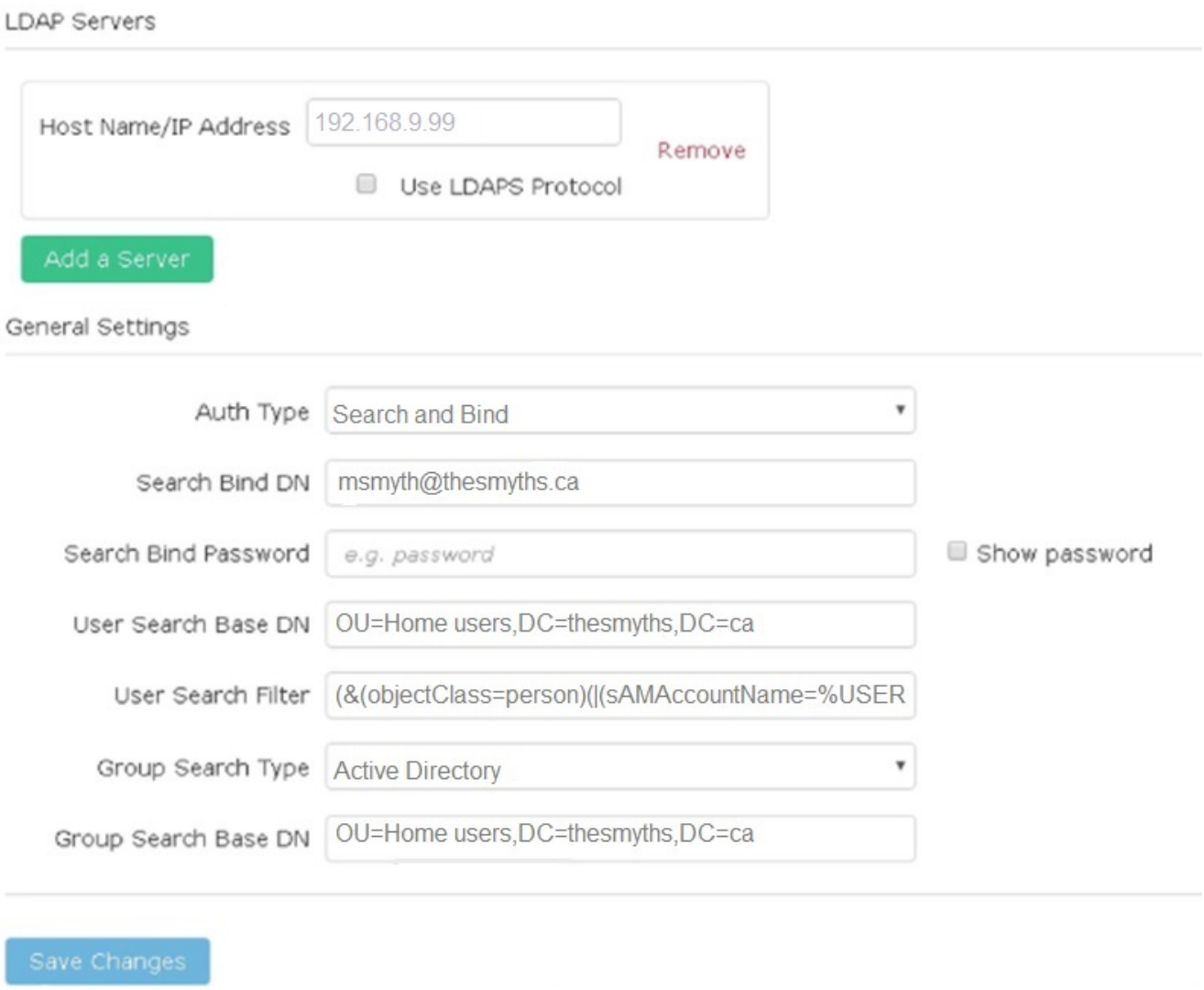
Étapes

1. Cliquez sur **Cluster** > **LDAP**.
2. Cliquez sur **Oui** pour activer l'authentification LDAP.
3. Cliquez sur **Ajouter un serveur**.
4. Saisissez le **nom d'hôte/l'adresse IP**.

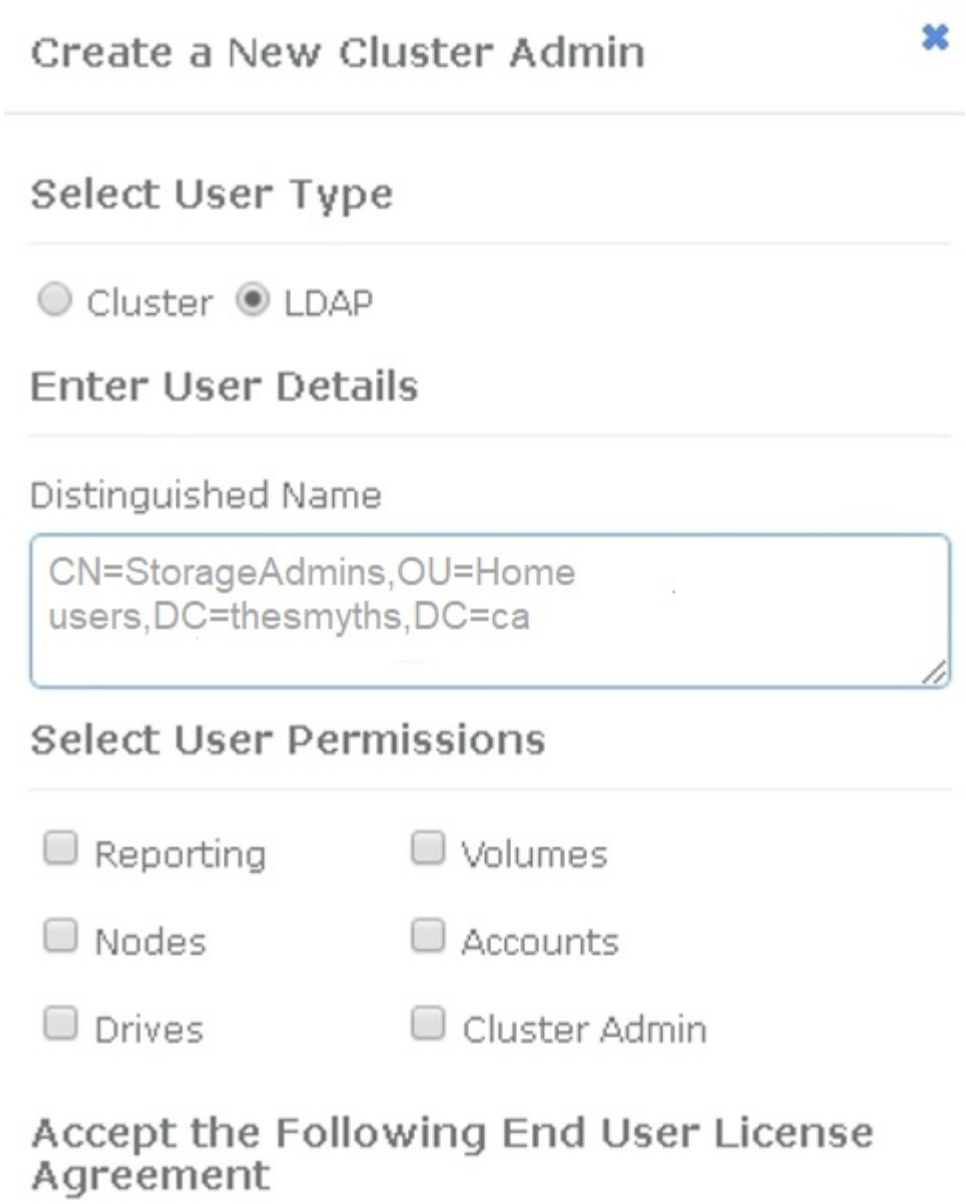
   Il est également possible de saisir un numéro de port personnalisé facultatif.

   Par exemple, pour ajouter un numéro de port personnalisé, saisissez <nom d'hôte ou adresse IP>:<numéro de port>

5. **Facultatif :** Sélectionnez **Utiliser le protocole LDAPS**.
6. Saisissez les informations requises dans **Paramètres généraux**.



7. Cliquez sur **Activer LDAP**.
8. Cliquez sur **Tester l'authentification de l'utilisateur** si vous souhaitez tester l'accès au serveur pour un utilisateur.
9. Copiez le nom distinctif et les informations du groupe d'utilisateurs qui apparaissent pour une utilisation ultérieure lors de la création d'administrateurs de cluster.
10. Cliquez sur **Enregistrer les modifications** pour enregistrer les nouveaux paramètres.
11. Pour créer un utilisateur dans ce groupe afin que n'importe qui puisse se connecter, veuillez procéder comme suit :
    a. Cliquez sur **Utilisateur** > **Afficher**.



b. Pour le nouvel utilisateur, cliquez sur **LDAP** pour le type d'utilisateur, puis collez le groupe que vous avez copié dans le champ Nom distinctif.
c. Sélectionnez les autorisations, généralement toutes les autorisations.
d. Faites défiler vers le bas jusqu'au Contrat de licence utilisateur final et cliquez sur **J'accepte**.
e. Cliquez sur **Créer un administrateur de cluster**.

   Vous disposez désormais d'un utilisateur ayant la valeur d'un groupe Active Directory.

Pour tester cela, déconnectez-vous de l'interface utilisateur d'Element et reconnectez-vous en tant qu'utilisateur de ce groupe.

Activez l'authentification LDAP avec l'API Element

Vous pouvez configurer l'intégration du système de stockage avec un serveur LDAP existant. Cela permet aux administrateurs LDAP de gérer de manière centralisée l'accès des utilisateurs au système de stockage.

Vous pouvez configurer LDAP soit avec l'interface utilisateur d'Element, soit avec l'API d'Element. Cette

procédure décrit comment configurer LDAP à l'aide de l'API Element.

Pour utiliser l'authentification LDAP sur un cluster SolidFire , vous devez d'abord activer l'authentification LDAP sur le cluster à l'aide de `EnableLdapAuthentication` Méthode API.

Étapes

1. Activez d'abord l'authentification LDAP sur le cluster à l'aide de `EnableLdapAuthentication` Méthode API.
2. Veuillez saisir les informations requises.

```
{
      "method":"EnableLdapAuthentication",
      "params":{
           "authType": "SearchAndBind",
           "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
           "groupSearchType": "ActiveDirectory",
           "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
           "searchBindPassword": "ReadOnlyPW",
           "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
           "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
           "serverURIs": [
                "ldap://172.27.1.189",
           [
      },
  "id":"1"
}
```

3. Modifiez les valeurs des paramètres suivants :

Paramètres utilisés	Description
authType: SearchAndBind	Indique que le cluster utilisera le compte de service en lecture seule pour rechercher d'abord l'utilisateur à authentifier, puis pour lier cet utilisateur s'il est trouvé et authentifié.
groupSearchBaseDN : dc=prodtest,dc=solidfire,dc=net	Spécifie l'emplacement dans l'arborescence LDAP où commencer la recherche de groupes. Pour cet exemple, nous avons utilisé la racine de notre arbre. Si votre arborescence LDAP est très volumineuse, vous pouvez envisager de définir une sous-arborescence plus fine afin de réduire les temps de recherche.

Paramètres utilisés	Description
userSearchBaseDN : dc=prodtest,dc=solidfire,dc=net	Spécifie l'emplacement dans l'arborescence LDAP où commencer la recherche des utilisateurs. Pour cet exemple, nous avons utilisé la racine de notre arbre. Si votre arborescence LDAP est très volumineuse, vous pouvez envisager de définir une sous-arborescence plus fine afin de réduire les temps de recherche.
groupSearchType : ActiveDirectory	Utilise le serveur Active Directory Windows comme serveur LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Pour utiliser l'utilisateur principal (adresse e-mail de connexion), vous pouvez modifier l'utilisateurSearchFilter comme suit :
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
Ou, pour rechercher à la fois userPrincipalName et sAMAccountName, vous pouvez utiliser le filtre userSearchFilter suivant :
 	
`"(&(objectClass=person)(`
	(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))" ----

Utilise le sAMAccountName comme nom d'utilisateur pour se connecter au cluster SolidFire . Ces paramètres indiquent à LDAP de rechercher le nom d'utilisateur spécifié lors de la connexion dans l'attribut sAMAccountName et limitent également la recherche aux entrées qui ont « personne » comme valeur dans l'attribut objectClass.	searchBindDN
Il s'agit du nom distinctif de l'utilisateur en lecture seule qui sera utilisé pour effectuer la recherche dans l'annuaire LDAP. Pour Active Directory, il est généralement plus simple d'utiliser l'identifiant utilisateur principal (format adresse e-mail) pour l'utilisateur.	rechercherLierMotDePasse

Pour tester cela, déconnectez-vous de l'interface utilisateur d'Element et reconnectez-vous en tant

qu'utilisateur de ce groupe.

Afficher les détails du LDAP

Consultez les informations LDAP sur la page LDAP, dans l'onglet Cluster.

Vous devez activer LDAP pour afficher ces paramètres de configuration LDAP.

1. Pour afficher les détails LDAP avec l'interface utilisateur Element, cliquez sur **Cluster** > **LDAP**.
   - **Nom d'hôte/Adresse IP** : Adresse d'un serveur d'annuaire LDAP ou LDAPS.
   - **Type d'authentification** : Méthode d'authentification de l'utilisateur. Valeurs possibles :
     - Liaison directe
     - Recherche et liaison
   - **DN de liaison de recherche** : DN complet permettant de se connecter pour effectuer une recherche LDAP pour l'utilisateur (nécessite un accès de niveau liaison à l'annuaire LDAP).
   - **Mot de passe de liaison de recherche** : Mot de passe utilisé pour authentifier l'accès au serveur LDAP.
   - **DN de base de la recherche utilisateur** : Le DN de base de l'arbre utilisé pour démarrer la recherche utilisateur. Le système effectue une recherche dans le sous-arbre à partir de l'emplacement spécifié.
   - **Filtre de recherche utilisateur** : Saisissez ce qui suit en utilisant votre nom de domaine :

     ```
     (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
     ```

   - **Type de recherche de groupe** : Type de recherche qui contrôle le filtre de recherche de groupe par défaut utilisé. Valeurs possibles :
     - Active Directory : Appartenance imbriquée à tous les groupes LDAP d'un utilisateur.
     - Pas de groupes : aucun soutien de groupe.
     - Membre DN : Groupes de type Membre DN (à un seul niveau).
   - **DN de base pour la recherche de groupe** : Le DN de base de l'arbre utilisé pour démarrer la recherche de groupe. Le système effectue une recherche dans le sous-arbre à partir de l'emplacement spécifié.
   - **Test d'authentification utilisateur** : Une fois LDAP configuré, utilisez cette procédure pour tester l'authentification par nom d'utilisateur et mot de passe du serveur LDAP. Saisissez un compte existant pour tester ceci. Le nom distinctif et les informations du groupe d'utilisateurs s'affichent ; vous pouvez les copier pour une utilisation ultérieure lors de la création d'administrateurs de cluster.

Tester la configuration LDAP

Après avoir configuré LDAP, vous devez le tester en utilisant soit l'interface utilisateur d'Element, soit l'API d'Element. `TestLdapAuthentication` méthode.

Étapes

1. Pour tester la configuration LDAP avec l'interface utilisateur Element, procédez comme suit :
   a. Cliquez sur **Cluster** > **LDAP**.
   b. Cliquez sur **Tester l'authentification LDAP**.

c. Résolvez tout problème en utilisant les informations du tableau ci-dessous :

Message d'erreur	Description
`xLDAPUserNotFound`	• L'utilisateur testé est introuvable dans la configuration. `userSearchBaseDN` sous-arbre. • Le `userSearchFilter` est mal configuré.
`xLDAPBindFailed (Error: Invalid credentials)`	• Le nom d'utilisateur testé est un utilisateur LDAP valide, mais le mot de passe fourni est incorrect. • Le nom d'utilisateur testé est un utilisateur LDAP valide, mais le compte est actuellement désactivé.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	L'URI du serveur LDAP est incorrect.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	Le nom d'utilisateur ou le mot de passe en lecture seule est mal configuré.
`xLDAPSearchFailed (Error: No such object)`	Le `userSearchBaseDN` n'est pas un emplacement valide dans l'arborescence LDAP.
`xLDAPSearchFailed (Error: Referral)`	• Le `userSearchBaseDN` n'est pas un emplacement valide dans l'arborescence LDAP. • Le `userSearchBaseDN` et `groupSearchBaseDN` sont dans une unité organisationnelle imbriquée. Cela peut entraîner des problèmes d'autorisation. La solution de contournement consiste à inclure l'unité organisationnelle dans les entrées DN de base de l'utilisateur et du groupe (par exemple : `ou=storage, cn=company, cn=com`)

2. Pour tester la configuration LDAP avec l'API Element, procédez comme suit :
   a. Appelez la méthode TestLdapAuthentication.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

b. Examinez les résultats. Si l'appel API réussit, les résultats incluent le nom distinctif de l'utilisateur spécifié et une liste des groupes dont l'utilisateur est membre.

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

Désactiver LDAP

Vous pouvez désactiver l'intégration LDAP via l'interface utilisateur d'Element.

Avant de commencer, vous devez noter tous les paramètres de configuration, car la désactivation de LDAP efface tous les paramètres.

Étapes

1. Cliquez sur **Cluster** > **LDAP**.
2. Cliquez sur **Non**.
3. Cliquez sur **Désactiver LDAP**.

Trouver plus d'informations

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

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".

Gérer les volumes et les volumes virtuels

Découvrez comment gérer les volumes et les volumes virtuels.

Vous pouvez gérer les données d'un cluster exécutant le logiciel Element depuis l'onglet Gestion de l'interface utilisateur d'Element. Les fonctions de gestion de cluster disponibles incluent la création et la gestion de volumes de données, de groupes d'accès aux volumes, d'initiateurs et de politiques de qualité de service (QoS).

Travailler avec des volumes

Le système SolidFire provisionne le stockage à l'aide de volumes. Les volumes sont des périphériques de stockage par blocs accessibles via le réseau par des clients iSCSI ou Fibre Channel. Depuis la page Volumes de l'onglet Gestion, vous pouvez créer, modifier, cloner et supprimer des volumes sur un nœud. Vous pouvez également consulter des statistiques sur la bande passante du volume et l'utilisation des E/S.

"Apprenez à travailler avec les volumes"

Travailler avec des volumes virtuels

Vous pouvez consulter des informations et effectuer des tâches pour les volumes virtuels et leurs conteneurs de stockage associés, les points de terminaison de protocole, les liaisons et les hôtes à l'aide de l'interface utilisateur Element.

Le système de stockage logiciel NetApp Element est livré avec la fonctionnalité Virtual Volumes (VVols) désactivée. Vous devez effectuer une tâche unique consistant à activer manuellement la fonctionnalité vSphere VVol via l'interface utilisateur Element.

Une fois la fonctionnalité VVol activée, un onglet VVols apparaît dans l'interface utilisateur, offrant des options de surveillance et de gestion limitées liées aux VVols. De plus, un composant logiciel côté stockage appelé fournisseur VASA fait office de service de sensibilisation au stockage pour vSphere. La plupart des commandes VVols, telles que la création, le clonage et la modification de VVols, sont initiées par un serveur vCenter ou un hôte ESXi et traduites par le fournisseur VASA en API Element pour le système de stockage logiciel Element. Les commandes permettant de créer, supprimer et gérer des conteneurs de stockage et de supprimer des volumes virtuels peuvent être lancées via l'interface utilisateur d'Element.

La plupart des configurations nécessaires à l'utilisation de la fonctionnalité Virtual Volumes avec les systèmes de stockage logiciels Element sont réalisées dans vSphere. Consultez le _Guide de configuration de VMware vSphere Virtual Volumes pour le stockage SolidFire pour enregistrer le fournisseur VASA dans vCenter, créer et gérer des banques de données VVol et gérer le stockage en fonction des politiques.

Pour Element 12.5 et versions antérieures, n'enregistrez pas plus d'un fournisseur NetApp Element VASA sur une seule instance vCenter. Lorsqu'un deuxième fournisseur NetApp Element VASA est ajouté, toutes les banques de données VVOL deviennent inaccessibles.

La prise en charge VASA pour plusieurs vCenters est disponible sous forme de correctif de mise à niveau si vous avez déjà enregistré un fournisseur VASA auprès de votre vCenter. Pour installer, téléchargez le fichier VASA39 .tar.gz depuis le "Téléchargements de logiciels NetApp" Rendez-vous sur le site et suivez les instructions du manifeste. Le fournisseur NetApp Element VASA utilise un certificat NetApp . Grâce à ce correctif, le certificat est utilisé sans modification par vCenter pour prendre en charge plusieurs vCenters pour l'utilisation de VASA et VVols. Ne modifiez pas le certificat. Les certificats SSL personnalisés ne sont pas pris en charge par VASA.

"Apprenez-en davantage sur le travail avec les volumes virtuels"

Collaborer avec les groupes d'accès au volume et les initiateurs

Vous pouvez utiliser des initiateurs iSCSI ou des initiateurs Fibre Channel pour accéder aux volumes définis dans les groupes d'accès aux volumes.

Vous pouvez créer des groupes d'accès en mappant les IQN d'initiateur iSCSI ou les WWPN Fibre Channel dans une collection de volumes. Chaque IQN que vous ajoutez à un groupe d'accès peut accéder à chaque volume du groupe sans nécessiter d'authentification CHAP.

Il existe deux types de méthodes d'authentification CHAP :

- Authentification CHAP au niveau du compte : vous pouvez attribuer une authentification CHAP au compte.
- Authentification CHAP au niveau de l'initiateur : vous pouvez attribuer des cibles et des secrets CHAP uniques à des initiateurs spécifiques sans être lié à un seul CHAP sur un seul compte. Cette authentification CHAP au niveau de l'initiateur remplace les informations d'identification au niveau du compte.

En option, avec CHAP par initiateur, vous pouvez imposer une autorisation de l'initiateur et une authentification CHAP par initiateur. Ces options peuvent être définies pour chaque initiateur et un groupe d'accès peut contenir un mélange d'initiateurs avec différentes options.

Chaque WWPN que vous ajoutez à un groupe d'accès active l'accès réseau Fibre Channel aux volumes du groupe d'accès.

Les groupes d'accès au volume ont les limites suivantes :

- Un maximum de 64 IQN ou WWPN est autorisé dans un groupe d'accès.
- Un groupe d'accès peut être composé d'un maximum de 2000 volumes.
- Un IQN ou un WWPN ne peut appartenir qu'à un seul groupe d'accès.
- Un même volume peut appartenir à un maximum de quatre groupes d'accès.

"Découvrez comment travailler avec les groupes d'accès en volume et les initiateurs"

Pour plus d'informations

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

Travailler avec des volumes

Politiques de gestion de la qualité de service

Une politique de qualité de service (QoS) vous permet de créer et d'enregistrer un paramètre de qualité de service standardisé qui peut être appliqué à de nombreux volumes. Vous pouvez créer, modifier et supprimer des politiques QoS à partir de la page Politiques QoS de l'onglet Gestion.

Si vous utilisez des politiques QoS, n'utilisez pas de QoS personnalisée sur un volume. La QoS personnalisée remplacera et ajustera les valeurs de stratégie QoS pour les paramètres QoS de volume.

"Vidéo NetApp : Politiques de qualité de service SolidFire"

Voir"Performance et qualité du service" .

- Créer une politique QoS
- Modifier une politique QoS
- Supprimer une politique QoS

Créer une politique QoS

Vous pouvez créer des politiques QoS et les appliquer lors de la création de volumes.

1. Sélectionnez **Gestion** > **Stratégies QoS**.
2. Cliquez sur **Créer une politique QoS**.
3. Saisissez le **Nom de la politique**.

4. Saisissez les valeurs **IOPS min**, **IOPS max** et **IOPS en rafale**.
5. Cliquez sur **Créer une politique QoS**.

Modifier une politique QoS

Vous pouvez modifier le nom d'une politique QoS existante ou modifier les valeurs associées à cette politique. La modification d'une politique QoS affecte tous les volumes associés à cette politique.

1. Sélectionnez **Gestion** > **Stratégies QoS**.
2. Cliquez sur l'icône Actions de la politique QoS que vous souhaitez modifier.
3. Dans le menu qui apparaît, sélectionnez **Modifier**.
4. Dans la boîte de dialogue **Modifier la stratégie QoS**, modifiez les propriétés suivantes selon vos besoins :
   - Nom de la politique
   - IOPS minimales
   - IOPS max
   - IOPS en rafale
5. Cliquez sur **Enregistrer les modifications**.

Supprimer une politique QoS

Vous pouvez supprimer une politique QoS si elle n'est plus nécessaire. Lorsque vous supprimez une stratégie QoS, tous les volumes associés à cette stratégie conservent leurs paramètres QoS mais ne sont plus associés à une stratégie.

> Si vous souhaitez plutôt dissocier un volume d'une stratégie QoS, vous pouvez modifier les paramètres QoS de ce volume en les personnalisant.

1. Sélectionnez **Gestion** > **Stratégies QoS**.
2. Cliquez sur l'icône Actions correspondant à la politique QoS que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, sélectionnez **Supprimer**.
4. Confirmez l'action.

Trouver plus d'informations

- "Supprimer l'association de stratégie QoS d'un volume"
- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"

Gérer les volumes

Le système SolidFire provisionne le stockage à l'aide de volumes. Les volumes sont des périphériques de stockage par blocs accessibles via le réseau par des clients iSCSI ou Fibre Channel.

Depuis la page Volumes de l'onglet Gestion, vous pouvez créer, modifier, cloner et supprimer des volumes sur un nœud.

Créer un volume

Vous pouvez créer un volume et l'associer à un compte donné. Chaque volume doit être associé à un compte. Cette association permet au compte d'accéder au volume via les initiateurs iSCSI en utilisant les identifiants CHAP.

Vous pouvez spécifier les paramètres QoS d'un volume lors de sa création.

1. Sélectionnez **Gestion** > **Volumes**.
2. Cliquez sur **Créer un volume**.
3. Dans la boîte de dialogue **Créer un nouveau volume**, saisissez le **Nom du volume**.
4. Saisissez la taille totale du volume.

   La taille de volume par défaut est exprimée en Go. Vous pouvez créer des volumes en utilisant des tailles mesurées en Go ou en Gio :

   - 1 Go = 1 000 000 000 octets
   - 1 Gio = 1 073 741 824 octets
5. Sélectionnez une **taille de bloc** pour le volume.
6. Cliquez sur la liste déroulante **Compte** et sélectionnez le compte qui doit avoir accès au volume.

   Si vous n'avez pas de compte, cliquez sur le lien **Créer un compte**, saisissez un nouveau nom de compte et cliquez sur **Créer**. Le compte est créé et associé au nouveau volume.

   S'il y a plus de 50 comptes, la liste n'apparaît pas. Commencez à saisir du texte et la fonction de saisie automatique affichera les valeurs possibles parmi lesquelles vous pourrez choisir.
7. Pour définir la **Qualité de service**, effectuez l'une des opérations suivantes :
   a. Sous **Politique**, vous pouvez sélectionner une politique QoS existante, si elle est disponible.
   b. Sous **Paramètres personnalisés**, définissez des valeurs minimales, maximales et de rafale personnalisées pour les IOPS ou utilisez les valeurs QoS par défaut.

      Les volumes dont la valeur Max ou Burst IOPS est supérieure à 20 000 IOPS peuvent nécessiter une profondeur de file d'attente élevée ou plusieurs sessions pour atteindre ce niveau d'IOPS sur un seul volume.
8. Cliquez sur **Créer un volume**.

Afficher les détails du volume

1. Sélectionnez **Gestion** > **Volumes**.
2. Passez en revue les détails.
   - **ID** : L'identifiant généré par le système pour le volume.
   - **Nom** : Le nom donné au volume lors de sa création.
   - **Compte** : Le nom du compte associé au volume.
   - **Groupes d'accès** : Nom du ou des groupes d'accès au volume auxquels appartient le volume.

- **Accès** : Le type d'accès attribué au volume lors de sa création. Valeurs possibles :
  - Lecture / Écriture : Toutes les lectures et écritures sont acceptées.
  - Lecture seule : toutes les opérations de lecture sont autorisées ; aucune écriture n'est autorisée.
  - Verrouillé : Accès réservé aux administrateurs.
  - ReplicationTarget : volume cible désigné dans une paire de volumes répliqués.
- **Utilisé** : Le pourcentage d'espace utilisé dans le volume.
- **Taille** : La taille totale (en Go) du volume.
- **ID du nœud principal** : Le nœud principal de ce volume.
- **ID du nœud secondaire** : La liste des nœuds secondaires pour ce volume. Peut prendre plusieurs valeurs lors d'états transitoires, comme le changement de nœuds secondaires, mais aura généralement une seule valeur.
- **Limitation QoS** : Indique si le volume est limité en raison d'une charge élevée sur le nœud de stockage principal.
- **Politique QoS** : Nom et lien vers la politique QoS définie par l'utilisateur.
- **IOPS min.** : Nombre minimal d'IOPS garanti pour le volume.
- **IOPS max** : Nombre maximal d'IOPS autorisé pour le volume.
- **IOPS en rafale** : Nombre maximal d'IOPS autorisé sur une courte période pour le volume. Valeur par défaut = 15 000.
- **Instantanés** : Nombre d'instantanés créés pour le volume.
- **Attributs** : Attributs qui ont été attribués au volume sous forme de paire clé/valeur via une méthode API.
- **512e** : Indique si le protocole 512e est activé sur un volume. Valeurs possibles :
  - Oui
  - Non
- **Date de création** : La date et l'heure de création du volume.

Afficher les détails de chaque volume

Vous pouvez consulter les statistiques de performance pour chaque volume.

1. Sélectionnez **Rapports** > **Performances du volume**.
2. Dans la liste des volumes, cliquez sur l'icône Actions correspondant à un volume.
3. Cliquez sur **Afficher les détails**.

   Un encadré apparaît en bas de la page, contenant des informations générales sur le volume.

4. Pour obtenir des informations plus détaillées sur le volume, cliquez sur **Voir plus de détails**.

   Le système affiche des informations détaillées ainsi que des graphiques de performance pour le volume.

Modifier les volumes actifs

Vous pouvez modifier les attributs du volume tels que les valeurs QoS, la taille du volume et l'unité de mesure dans laquelle les valeurs en octets sont calculées. Vous pouvez également modifier l'accès au compte pour une utilisation en réplication ou pour restreindre l'accès au volume.

Vous pouvez redimensionner un volume lorsqu'il y a suffisamment d'espace sur le cluster, sous les conditions suivantes :

- Conditions de fonctionnement normales.
- Des erreurs ou des pannes de volume sont signalées.
- Le volume est en cours de clonage.
- Le volume est en cours de resynchronisation.

Étapes

1. Sélectionnez **Gestion** > **Volumes**.
2. Dans la fenêtre **Actif**, cliquez sur l'icône Actions correspondant au volume que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. **Facultatif :** Modifier la taille totale du volume.
   - Vous pouvez augmenter, mais pas diminuer, la taille du volume. Vous ne pouvez redimensionner qu'un seul volume à la fois. Les opérations de nettoyage des déchets et les mises à jour logicielles n'interrompent pas l'opération de redimensionnement.
   - Si vous ajustez la taille du volume pour la réplication, vous devez d'abord augmenter la taille du volume désigné comme cible de réplication. Vous pouvez ensuite redimensionner le volume source. Le volume cible peut être supérieur ou égal au volume source, mais il ne peut pas être inférieur.

     La taille de volume par défaut est exprimée en Go. Vous pouvez créer des volumes en utilisant des tailles mesurées en Go ou en Gio :

   - 1 Go = 1 000 000 000 octets
   - 1 Gio = 1 073 741 824 octets
5. **Facultatif :** Sélectionnez un autre niveau d'accès au compte parmi les suivants :
   - Lecture seule
   - Lecture/écriture
   - Fermé
   - Cible de réplication
6. **Facultatif :** Sélectionnez le compte qui doit avoir accès au volume.

   Si le compte n'existe pas, cliquez sur le lien **Créer un compte**, saisissez un nouveau nom de compte et cliquez sur **Créer**. Le compte est créé et associé au volume.

   S'il y a plus de 50 comptes, la liste n'apparaît pas. Commencez à saisir du texte et la fonction de saisie automatique affichera les valeurs possibles parmi lesquelles vous pourrez choisir.

7. **Facultatif :** Pour modifier la sélection dans **Qualité de service**, effectuez l'une des opérations suivantes :
   a. Sous **Politique**, vous pouvez sélectionner une politique QoS existante, si elle est disponible.
   b. Sous **Paramètres personnalisés**, définissez des valeurs minimales, maximales et de rafale personnalisées pour les IOPS ou utilisez les valeurs QoS par défaut.

Si vous utilisez des politiques QoS sur un volume, vous pouvez définir une QoS personnalisée pour supprimer l'association de la politique QoS avec le volume. La QoS personnalisée remplacera et ajustera les valeurs de stratégie QoS pour les paramètres QoS de volume.

Lorsque vous modifiez les valeurs d'IOPS, vous devez les incrémenter par dizaines ou par centaines. Les valeurs saisies doivent être des nombres entiers valides.

Configurez les volumes avec une valeur de rafale extrêmement élevée. Cela permet au système de traiter plus rapidement les charges de travail séquentielles par blocs volumineux occasionnelles, tout en limitant les IOPS soutenues pour un volume.

8. Cliquez sur **Enregistrer les modifications**.

Supprimer un volume

Vous pouvez supprimer un ou plusieurs volumes d'un cluster de stockage Element.

Le système ne supprime pas immédiatement un volume supprimé ; celui-ci reste disponible pendant environ huit heures. Si vous restaurez un volume avant que le système ne le purge, le volume est remis en ligne et les connexions iSCSI sont rétablies.

Si un volume utilisé pour créer un instantané est supprimé, ses instantanés associés deviennent inactifs. Lorsque les volumes sources supprimés sont purgés, les instantanés inactifs associés sont également supprimés du système.

Les volumes persistants associés aux services de gestion sont créés et affectés à un nouveau compte lors de l'installation ou de la mise à niveau. Si vous utilisez des volumes persistants, ne modifiez ni ne supprimez les volumes ou leur compte associé.

Étapes

1. Sélectionnez **Gestion** > **Volumes**.
2. Pour supprimer un seul volume, procédez comme suit :
   a. Cliquez sur l'icône Actions correspondant au volume que vous souhaitez supprimer.
   b. Dans le menu qui s'affiche, cliquez sur **Supprimer**.
   c. Confirmez l'action.

   Le système déplace le volume vers la zone **Supprimé** de la page **Volumes**.
3. Pour supprimer plusieurs volumes, procédez comme suit :
   a. Dans la liste des volumes, cochez la case en regard des volumes que vous souhaitez supprimer.
   b. Cliquez sur **Actions groupées**.
   c. Dans le menu qui s'affiche, cliquez sur **Supprimer**.
   d. Confirmez l'action.

   Le système déplace les volumes vers la zone **Supprimés** de la page **Volumes**.

Restaurer un volume supprimé

Vous pouvez restaurer un volume du système s'il a été supprimé mais pas encore purgé. Le système purge automatiquement un volume environ huit heures après sa suppression. Si le système a purgé le volume, vous ne pouvez pas le restaurer.

1. Sélectionnez **Gestion** > **Volumes**.
2. Cliquez sur l'onglet **Supprimés** pour afficher la liste des volumes supprimés.
3. Cliquez sur l'icône Actions correspondant au volume que vous souhaitez restaurer.
4. Dans le menu qui s'affiche, cliquez sur **Restaurer**.
5. Confirmez l'action.

   Le volume est placé dans la liste des volumes **actifs** et les connexions iSCSI au volume sont rétablies.

Purger un volume

Lorsqu'un volume est purgé, il est définitivement supprimé du système. Toutes les données du volume sont perdues.

Le système purge automatiquement les volumes supprimés huit heures après leur suppression. Toutefois, si vous souhaitez purger un volume avant l'heure prévue, vous pouvez le faire.

1. Sélectionnez **Gestion** > **Volumes**.
2. Cliquez sur le bouton **Supprimé**.
3. Suivez les étapes pour purger un seul volume ou plusieurs volumes.

Option	Étapes
Purger un seul volume	a. Cliquez sur l'icône Actions correspondant au volume que vous souhaitez purger. b. Cliquez sur **Purge**. c. Confirmez l'action.
Purger plusieurs volumes	a. Sélectionnez les volumes que vous souhaitez purger. b. Cliquez sur **Actions groupées**. c. Dans le menu qui s'affiche, sélectionnez **Purge**. d. Confirmez l'action.

Cloner un volume

Vous pouvez créer un clone d'un seul volume ou de plusieurs volumes pour réaliser une copie des données à un instant précis. Lorsque vous clonez un volume, le système crée un instantané du volume, puis une copie des données référencées par cet instantané. Il s'agit d'un processus asynchrone, et sa durée dépend de la taille du volume à cloner et de la charge actuelle du cluster.

Le cluster prend en charge jusqu'à deux demandes de clonage en cours par volume simultanément et jusqu'à huit opérations de clonage de volume actives simultanément. Les requêtes dépassant ces limites sont mises en file d'attente pour un traitement ultérieur.

Les systèmes d'exploitation diffèrent dans leur manière de traiter les volumes clonés. VMware ESXi traitera un volume cloné comme une copie de volume ou un volume instantané. Ce volume constituera un périphérique disponible pour créer un nouveau datastore. Pour plus d'informations sur le montage des volumes clonés et la gestion des LUN de snapshot, consultez la documentation VMware. "montage d'une copie de banque de données VMFS" et "gestion des datastores VMFS dupliqués" .

Avant de tronquer un volume cloné en le clonant à une taille plus petite, assurez-vous de préparer les partitions de manière à ce qu'elles s'adaptent au volume plus petit.

Étapes

1. Sélectionnez **Gestion** > **Volumes**.
2. Pour cloner un seul volume, procédez comme suit :
   a. Dans la liste des volumes de la page **Actif**, cliquez sur l'icône Actions du volume que vous souhaitez cloner.
   b. Dans le menu qui s'affiche, cliquez sur **Cloner**.
   c. Dans la fenêtre **Cloner le volume**, saisissez un nom pour le volume nouvellement cloné.
   d. Sélectionnez une taille et une mesure pour le volume à l'aide de la zone de saisie et de la liste **Taille du volume**.

      La taille de volume par défaut est exprimée en Go. Vous pouvez créer des volumes en utilisant des tailles mesurées en Go ou en Gio :

      - 1 Go = 1 000 000 000 octets
      - 1 Gio = 1 073 741 824 octets

   e. Sélectionnez le type d'accès pour le volume nouvellement cloné.
   f. Sélectionnez un compte à associer au volume nouvellement cloné dans la liste **Compte**.

      Vous pouvez créer un compte lors de cette étape si vous cliquez sur le lien **Créer un compte**, saisissez un nom de compte et cliquez sur **Créer**. Le système ajoute automatiquement le compte à la liste **Comptes** après sa création.

3. Pour cloner plusieurs volumes, procédez comme suit :
   a. Dans la liste des volumes de la page **Actifs**, cochez la case en regard des volumes que vous souhaitez cloner.
   b. Cliquez sur **Actions groupées**.
   c. Dans le menu qui s'affiche, sélectionnez **Cloner**.
   d. Dans la boîte de dialogue **Cloner plusieurs volumes**, saisissez un préfixe pour les volumes clonés dans le champ **Préfixe du nouveau nom de volume**.
   e. Sélectionnez un compte à associer aux volumes clonés dans la liste **Compte**.
   f. Sélectionnez le type d'accès pour les volumes clonés.
4. Cliquez sur **Démarrer le clonage**.

Augmenter le volume d'un clone crée un nouveau volume avec de l'espace libre supplémentaire à la fin de celui-ci. Selon l'utilisation que vous faites du volume, vous devrez peut-être étendre les partitions ou créer de nouvelles partitions dans l'espace libre pour pouvoir l'utiliser.

Pour plus d'informations

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

Attribuer des LUN à des volumes Fibre Channel

Vous pouvez modifier l'affectation LUN d'un volume Fibre Channel dans un groupe d'accès aux volumes. Vous pouvez également effectuer des affectations de LUN de volume Fibre Channel lors de la création d'un groupe d'accès aux volumes.

L'attribution de nouveaux LUN Fibre Channel est une fonction avancée qui peut avoir des conséquences inconnues sur l'hôte connecté. Par exemple, le nouvel ID LUN peut ne pas être automatiquement détecté sur l'hôte, et ce dernier peut nécessiter une nouvelle analyse pour le découvrir.

1. Sélectionnez **Gestion** > **Groupes d'accès**.
2. Cliquez sur l'icône Actions du groupe d'accès que vous souhaitez modifier.
3. Dans le menu qui apparaît, sélectionnez **Modifier**.
4. Sous **Attribuer des ID LUN** dans la boîte de dialogue **Modifier le groupe d'accès au volume**, cliquez sur la flèche de la liste **Attributions LUN**.
5. Pour chaque volume de la liste auquel vous souhaitez attribuer un LUN, saisissez une nouvelle valeur dans le champ **LUN** correspondant.
6. Cliquez sur **Enregistrer les modifications**.

Appliquer une politique QoS aux volumes

Vous pouvez appliquer en masse une politique QoS existante à un ou plusieurs volumes.

La politique QoS que vous souhaitez appliquer en masse doit exister.

1. Sélectionnez **Gestion** > **Volumes**.
2. Dans la liste des volumes, cochez la case en regard des volumes auxquels vous souhaitez appliquer la politique QoS.
3. Cliquez sur **Actions groupées**.
4. Dans le menu qui s'affiche, cliquez sur **Appliquer la politique QoS**.
5. Sélectionnez la politique QoS dans la liste déroulante.
6. Cliquez sur **Appliquer**.

Trouver plus d'informations

Politiques de qualité de service

Supprimer l'association de stratégie QoS d'un volume

Vous pouvez supprimer une association de stratégie QoS d'un volume en sélectionnant des paramètres QoS personnalisés.

Le volume que vous souhaitez modifier doit être associé à une politique QoS.

1. Sélectionnez **Gestion** > **Volumes**.
2. Cliquez sur l'icône Actions pour un volume contenant une stratégie QoS que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Dans le menu qui s'affiche, sous **Qualité de service**, cliquez sur **Paramètres personnalisés**.
5. Modifiez **Min IOPS**, **Max IOPS** et **Burst IOPS**, ou conservez les paramètres par défaut.
6. Cliquez sur **Enregistrer les modifications**.

Trouver plus d'informations

Supprimer une politique QoS

Travailler avec des volumes virtuels

Activer les volumes virtuels

Vous devez activer manuellement la fonctionnalité vSphere Virtual Volumes (VVols) via le logiciel NetApp Element . Le système logiciel Element est livré avec la fonctionnalité VVols désactivée par défaut, et celle-ci n'est pas activée automatiquement lors d'une nouvelle installation ou d'une mise à niveau. L'activation de la fonctionnalité VVols est une tâche de configuration ponctuelle.

Ce dont vous aurez besoin

- Le cluster doit exécuter Element 9.0 ou une version ultérieure.
- Le cluster doit être connecté à un environnement ESXi 6.0 ou ultérieur compatible avec VVols.
- Si vous utilisez Element 11.3 ou une version ultérieure, le cluster doit être connecté à un environnement ESXi 6.0 update 3 ou une version ultérieure.

> L'activation de la fonctionnalité vSphere Virtual Volumes modifie de façon permanente la configuration du logiciel Element. Vous ne devez activer la fonctionnalité VVols que si votre cluster est connecté à un environnement VMware ESXi compatible VVols. Vous pouvez désactiver la fonction VVols et restaurer les paramètres par défaut uniquement en restaurant le cluster à son image d'usine, ce qui supprime toutes les données du système.

Étapes

1. Sélectionnez **Clusters** > **Paramètres**.
2. Trouvez les paramètres spécifiques au cluster pour les volumes virtuels.
3. Cliquez sur **Activer les volumes virtuels**.
4. Cliquez sur **Oui** pour confirmer la modification de la configuration des volumes virtuels.

   L'onglet **VVols** apparaît dans l'interface utilisateur d'Element.

Lorsque la fonctionnalité VVols est activée, le cluster SolidFire démarre le fournisseur VASA, ouvre le port 8444 pour le trafic VASA et crée des points de terminaison de protocole qui peuvent être découverts par vCenter et tous les hôtes ESXi.

5. Copiez l'URL du fournisseur VASA à partir des paramètres des volumes virtuels (VVols) dans **Clusters** > **Paramètres**. Vous utiliserez cette URL pour enregistrer le fournisseur VASA dans vCenter.
6. Créez un conteneur de stockage dans **VVols** > **Conteneurs de stockage**.

Vous devez créer au moins un conteneur de stockage pour que les machines virtuelles puissent être provisionnées sur un datastore VVol.

7. Sélectionnez **VVols** > **Points de terminaison de protocole**.
8. Vérifiez qu'un point de terminaison de protocole a été créé pour chaque nœud du cluster.

Des tâches de configuration supplémentaires sont nécessaires dans vSphere. Consultez le _Guide de configuration de VMware vSphere Virtual Volumes pour le stockage SolidFire pour enregistrer le fournisseur VASA dans vCenter, créer et gérer des banques de données VVol et gérer le stockage en fonction des politiques.

Trouver plus d'informations

"Guide de configuration des volumes virtuels VMware vSphere pour le stockage SolidFire"

Afficher les détails du volume virtuel

Vous pouvez consulter les informations sur les volumes virtuels pour tous les volumes virtuels actifs sur le cluster dans l'interface utilisateur d'Element. Vous pouvez également consulter l'activité de performance de chaque volume virtuel, notamment les entrées, les sorties, le débit, la latence, la profondeur de la file d'attente et les informations sur le volume.

Ce dont vous aurez besoin

- Vous auriez dû activer la fonctionnalité VVols dans l'interface utilisateur Element pour le cluster.
- Vous auriez dû créer un conteneur de stockage associé.
- Vous auriez dû configurer votre cluster vSphere pour utiliser la fonctionnalité VVols du logiciel Element.
- Vous auriez dû créer au moins une machine virtuelle dans vSphere.

Étapes

1. Cliquez sur **VVols** > **Volumes virtuels**.

   Les informations relatives à tous les volumes virtuels actifs sont affichées.

2. Cliquez sur l'icône **Actions** correspondant au volume virtuel que vous souhaitez consulter.
3. Dans le menu qui s'affiche, sélectionnez **Afficher les détails**.

Détails

La page Volumes virtuels de l'onglet VVols fournit des informations sur chaque volume virtuel actif du cluster,

telles que l'ID du volume, l'ID de l'instantané, l'ID du volume virtuel parent et l'ID du volume virtuel.

- **ID du volume** : L'identifiant du volume sous-jacent.
- **ID de l'instantané** : L'identifiant de l'instantané du volume sous-jacent. La valeur est 0 si le volume virtuel ne représente pas un instantané SolidFire .
- **ID du volume virtuel parent** : L'ID du volume virtuel parent. Si l'identifiant est composé uniquement de zéros, le volume virtuel est indépendant et n'est lié à aucun volume parent.
- **ID du volume virtuel** : L'UUID du volume virtuel.
- **Nom** : Le nom attribué au volume virtuel.
- **Conteneur de stockage** : Le conteneur de stockage qui possède le volume virtuel.
- **Type de système d'exploitation invité** : Système d'exploitation associé au volume virtuel.
- **Type de volume virtuel** : Le type de volume virtuel : Config, Données, Mémoire, Swap ou Autre.
- **Accès** : Les autorisations de lecture et d'écriture attribuées au volume virtuel.
- **Taille** : La taille du volume virtuel en Go ou GiB.
- **Instantanés** : Le nombre d'instantanés associés. Cliquez sur le numéro pour accéder aux détails de l'instantané.
- **IOPS min** : Paramètre QoS IOPS minimal du volume virtuel.
- **IOPS max** : Paramètre QoS IOPS maximal du volume virtuel.
- **IOPS en rafale** : Paramètre QoS en rafale maximal du volume virtuel.
- **VMW_VmID** : Les informations contenues dans les champs précédés de « VMW_ » sont définies par VMware.
- **Heure de création** : Heure à laquelle la tâche de création du volume virtuel a été terminée.

Détails individuels du volume virtuel

La page Volumes virtuels de l'onglet VVols fournit les informations suivantes sur le volume virtuel lorsque vous sélectionnez un volume virtuel individuel et que vous consultez ses détails.

- **VMW_XXX** : Les informations contenues dans les champs précédés de « VMW_ » sont définies par VMware.
- **ID du volume virtuel parent** : L'ID du volume virtuel parent. Si l'identifiant est composé uniquement de zéros, le volume virtuel est indépendant et n'est lié à aucun volume parent.
- **ID du volume virtuel** : L'UUID du volume virtuel.
- **Type de volume virtuel** : Le type de volume virtuel : Config, Données, Mémoire, Swap ou Autre.
- **ID du volume** : L'identifiant du volume sous-jacent.
- **Accès** : Les autorisations de lecture et d'écriture attribuées au volume virtuel.
- **Nom du compte** : Nom du compte contenant le volume.
- **Groupes d'accès** : Groupes d'accès aux volumes associés.
- **Taille totale du volume** : Capacité totale provisionnée en octets.
- **Blocs non nuls** : Nombre total de blocs de 4 Kio contenant des données après la dernière opération de nettoyage de la mémoire.
- **Zéro bloc** : Nombre total de blocs de 4 Kio sans données après la dernière opération de nettoyage de la mémoire.

- **Instantanés** : Le nombre d'instantanés associés. Cliquez sur le numéro pour accéder aux détails de l'instantané.
- **IOPS min** : Paramètre QoS IOPS minimal du volume virtuel.
- **IOPS max** : Paramètre QoS IOPS maximal du volume virtuel.
- **IOPS en rafale** : Paramètre QoS en rafale maximal du volume virtuel.
- **Activer 512** : Étant donné que les volumes virtuels utilisent toujours une émulation de taille de bloc de 512 octets, la valeur est toujours oui.
- **Volumes appariés** : Indique si un volume est apparié.
- **Heure de création** : Heure à laquelle la tâche de création du volume virtuel a été terminée.
- **Taille des blocs** : Taille des blocs dans le volume.
- **Écritures non alignées** : Pour les volumes 512e, le nombre d'opérations d'écriture qui n'étaient pas sur une limite de secteur de 4 k. Un nombre élevé d'écritures non alignées peut indiquer un alignement incorrect des partitions.
- **Lectures non alignées** : Pour les volumes 512e, le nombre d'opérations de lecture qui n'étaient pas sur une limite de secteur de 4 k. Un nombre élevé de lectures non alignées peut indiquer un alignement incorrect des partitions.
- **scsiEUIDeviceID** : Identifiant unique global du périphérique SCSI pour le volume au format 16 octets basé sur EUI-64.
- **scsiNAADeviceID** : Identifiant unique global du périphérique SCSI pour le volume au format NAA IEEE Registered Extended.
- **Attributs** : Liste de paires nom-valeur au format objet JSON.

Supprimer un volume virtuel

Bien que les volumes virtuels doivent toujours être supprimés de la couche de gestion VMware, la fonctionnalité permettant de supprimer les volumes virtuels est activée depuis l'interface utilisateur d'Element. Vous ne devez supprimer un volume virtuel de l'interface utilisateur d'Element qu'en cas d'absolue nécessité, par exemple lorsque vSphere ne parvient pas à nettoyer les volumes virtuels sur le stockage SolidFire .

1. Sélectionnez **VVols** > **Volumes virtuels**.
2. Cliquez sur l'icône Actions correspondant au volume virtuel que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, sélectionnez **Supprimer**.

> Vous devez supprimer un volume virtuel de la couche de gestion VMware pour vous assurer que le volume virtuel est correctement délié avant sa suppression. Vous ne devez supprimer un volume virtuel de l'interface utilisateur d'Element qu'en cas d'absolue nécessité, par exemple lorsque vSphere ne parvient pas à nettoyer les volumes virtuels sur le stockage SolidFire . Si vous supprimez un volume virtuel depuis l'interface utilisateur d'Element, le volume sera immédiatement purgé.

4. Confirmez l'action.
5. Actualisez la liste des volumes virtuels pour confirmer que le volume virtuel a bien été supprimé.
6. **Facultatif** : Sélectionnez **Rapports** > **Journal des événements** pour confirmer que la purge a réussi.

Gérer les conteneurs de stockage

Un conteneur de stockage est une représentation de datastore vSphere créée sur un cluster exécutant le logiciel Element.

Des conteneurs de stockage sont créés et associés à des comptes NetApp Element . Un conteneur de stockage créé sur un stockage Element apparaît comme un datastore vSphere dans vCenter et ESXi. Les conteneurs de stockage n'allouent aucun espace sur le stockage Element. Ils servent simplement à associer logiquement des volumes virtuels.

Un maximum de quatre conteneurs de stockage par cluster est pris en charge. Un conteneur de stockage minimum est requis pour activer la fonctionnalité VVols.

Créer un conteneur de stockage

Vous pouvez créer des conteneurs de stockage dans l'interface utilisateur d'Element et les découvrir dans vCenter. Vous devez créer au moins un conteneur de stockage pour commencer à provisionner des machines virtuelles basées sur VVol.

Avant de commencer, activez la fonctionnalité VVols dans l'interface utilisateur Element pour le cluster.

Étapes

1. Sélectionnez **VVols** > **Conteneurs de stockage**.
2. Cliquez sur le bouton **Créer des conteneurs de stockage**.
3. Saisissez les informations du conteneur de stockage dans la boîte de dialogue **Créer un nouveau conteneur de stockage** :
   a. Saisissez un nom pour le conteneur de stockage.
   b. Configurez les secrets de l'initiateur et de la cible pour CHAP.

      Laissez les champs Paramètres CHAP vides pour générer automatiquement les secrets.

   c. Cliquez sur le bouton **Créer un conteneur de stockage**.
4. Vérifiez que le nouveau conteneur de stockage apparaît bien dans la liste de l'onglet **Conteneurs de stockage**.

   Comme un ID de compte NetApp Element est créé automatiquement et attribué au conteneur de stockage, il n'est pas nécessaire de créer un compte manuellement.

Afficher les détails du conteneur de stockage

Sur la page « Conteneurs de stockage » de l'onglet VVols, vous pouvez consulter les informations relatives à tous les conteneurs de stockage actifs sur le cluster.

- **ID du compte** : L'identifiant du compte NetApp Element associé au conteneur de stockage.
- **Nom** : Le nom du conteneur de stockage.
- **Statut** : L'état du conteneur de stockage. Valeurs possibles :
  - Actif : Le conteneur de stockage est en cours d'utilisation.
  - Verrouillé : Le conteneur de stockage est verrouillé.

- **Type PE** : Le type de point de terminaison du protocole (SCSI est le seul protocole disponible pour le logiciel Element).
- **ID du conteneur de stockage** : L'UUID du conteneur de stockage du volume virtuel.
- **Volumes virtuels actifs** : Nombre de volumes virtuels actifs associés au conteneur de stockage.

Afficher les détails de chaque conteneur de stockage

Vous pouvez consulter les informations relatives à un conteneur de stockage individuel en le sélectionnant sur la page « Conteneurs de stockage » de l'onglet VVols.

- **ID du compte** : L'identifiant du compte NetApp Element associé au conteneur de stockage.
- **Nom** : Le nom du conteneur de stockage.
- **Statut** : L'état du conteneur de stockage. Valeurs possibles :
  - Actif : Le conteneur de stockage est en cours d'utilisation.
  - Verrouillé : Le conteneur de stockage est verrouillé.
- **Secret de l'initiateur CHAP** : Le secret unique du CHAP pour l'initiateur.
- **Secret cible CHAP** : Le secret CHAP unique pour la cible.
- **ID du conteneur de stockage** : L'UUID du conteneur de stockage du volume virtuel.
- **Type de point de terminaison de protocole** : Indique le type de point de terminaison de protocole (SCSI est le seul protocole disponible).

Modifier un conteneur de stockage

Vous pouvez modifier l'authentification CHAP du conteneur de stockage dans l'interface utilisateur Element.

1. Sélectionnez **VVols** > **Conteneurs de stockage**.
2. Cliquez sur l'icône **Actions** du conteneur de stockage que vous souhaitez modifier.
3. Dans le menu qui s'affiche, sélectionnez **Modifier**.
4. Dans les paramètres CHAP, modifiez les informations d'identification secrètes de l'initiateur et de la cible utilisées pour l'authentification.

   Si vous ne modifiez pas les informations d'identification des paramètres CHAP, elles restent inchangées. Si vous laissez les champs d'identification vides, le système génère automatiquement de nouveaux secrets.

5. Cliquez sur **Enregistrer les modifications**.

Supprimer un conteneur de stockage

Vous pouvez supprimer les conteneurs de stockage depuis l'interface utilisateur d'Element.

Ce dont vous aurez besoin

Assurez-vous que toutes les machines virtuelles ont été supprimées du datastore VVol.

Étapes

1. Sélectionnez **VVols** > **Conteneurs de stockage**.
2. Cliquez sur l'icône **Actions** correspondant au conteneur de stockage que vous souhaitez supprimer.

3. Dans le menu qui s'affiche, sélectionnez **Supprimer**.
4. Confirmez l'action.
5. Actualisez la liste des conteneurs de stockage dans l'onglet **Conteneurs de stockage** pour confirmer que le conteneur de stockage a bien été supprimé.

Points de terminaison du protocole

Découvrez les points de terminaison du protocole

Les points de terminaison de protocole sont des points d'accès utilisés par un hôte pour adresser le stockage sur un cluster exécutant le logiciel NetApp Element . Les points de terminaison de protocole ne peuvent être ni supprimés ni modifiés par un utilisateur, ne sont pas associés à un compte et ne peuvent pas être ajoutés à un groupe d'accès aux volumes.

Un cluster exécutant le logiciel Element crée automatiquement un point de terminaison de protocole par nœud de stockage dans le cluster. Par exemple, un cluster de stockage à six nœuds possède six points de terminaison de protocole qui sont mappés sur chaque hôte ESXi. Les points de terminaison du protocole sont gérés dynamiquement par le logiciel Element et sont créés, déplacés ou supprimés selon les besoins, sans aucune intervention. Les points de terminaison de protocole sont la cible du multipathing et servent de proxy d'E/S pour les LUN subsidiaires. Chaque point de terminaison du protocole consomme une adresse SCSI disponible, tout comme une cible iSCSI standard. Les points de terminaison du protocole apparaissent comme un périphérique de stockage à bloc unique (512 octets) dans le client vSphere, mais ce périphérique de stockage n'est pas disponible pour être formaté ou utilisé comme stockage.

iSCSI est le seul protocole pris en charge. Le protocole Fibre Channel n'est pas pris en charge.

Détails des points de terminaison du protocole

La page Points de terminaison du protocole de l'onglet VVols fournit des informations sur les points de terminaison du protocole.

- **Identifiant du fournisseur principal**

  L'identifiant du fournisseur de point de terminaison du protocole principal.

- **Identifiant du fournisseur secondaire**

  L'identifiant du fournisseur de point de terminaison du protocole secondaire.

- **ID du point de terminaison du protocole**

  L'UUID du point de terminaison du protocole.

- **État du point de terminaison du protocole**

  État du point de terminaison du protocole. Les valeurs possibles sont les suivantes :

  - Actif : Le point de terminaison du protocole est en cours d'utilisation.
  - Démarrage : Le point de terminaison du protocole démarre.
  - Basculement : Le point de terminaison du protocole a basculé.

- Réservé : le point de terminaison du protocole est réservé.

- **Type de fournisseur**

  Le type de fournisseur du point de terminaison du protocole. Les valeurs possibles sont les suivantes :

  - Primaire
  - Secondaire

- **Identifiant du périphérique SCSI NAA**

  L'identifiant unique au niveau mondial du périphérique SCSI pour le point de terminaison du protocole au format étendu enregistré NAA IEEE.

Reliures

Découvrez les reliures

Pour effectuer des opérations d'E/S avec un volume virtuel, un hôte ESXi doit d'abord lier le volume virtuel.

Le cluster SolidFire choisit un point de terminaison de protocole optimal, crée une liaison qui associe l'hôte ESXi et le volume virtuel à ce point de terminaison, et renvoie cette liaison à l'hôte ESXi. Une fois lié, l'hôte ESXi peut effectuer des opérations d'E/S avec le volume virtuel lié.

Détails des reliures

La page Liaisons de l'onglet VVols fournit des informations de liaison pour chaque volume virtuel.

Les informations suivantes sont affichées :

- **ID de l'hôte**

  L'UUID de l'hôte ESXi qui héberge les volumes virtuels et qui est connu du cluster.

- **ID du point de terminaison du protocole**

  Identifiants des points de terminaison de protocole correspondant à chaque nœud du cluster SolidFire .

- **Point de terminaison du protocole dans l'identifiant de bande**

  L'identifiant du périphérique SCSI NAA du point de terminaison du protocole.

- **Type de point de terminaison de protocole**

  Le type de point de terminaison du protocole.

- **ID de liaison VVol**

  L'UUID de liaison du volume virtuel.

- **ID VVol**

  L'identifiant unique universel (UUID) du volume virtuel.

- **Identifiant secondaire VVol**

  L'identifiant secondaire du volume virtuel qui est un identifiant LUN de deuxième niveau SCSI.

Détails de l'hôte

La page Hôtes de l'onglet VVols fournit des informations sur les hôtes VMware ESXi qui hébergent des volumes virtuels.

Les informations suivantes sont affichées :

- **ID de l'hôte**

  L'UUID de l'hôte ESXi qui héberge les volumes virtuels et qui est connu du cluster.

- **Adresse de l'hôte**

  L'adresse IP ou le nom DNS de l'hôte ESXi.

- **Reliures**

  Identifiants de liaison pour tous les volumes virtuels liés par l'hôte ESXi.

- **ID du cluster ESX**

  L'ID du cluster hôte vSphere ou le GUID vCenter.

- **IQN initiateurs**

  IQN d'initiateur pour l'hôte de volume virtuel.

- * Identifiants des points de terminaison du protocole SolidFire *

  Les points de terminaison du protocole actuellement visibles par l'hôte ESXi.

Collaborer avec les groupes d'accès au volume et les initiateurs

Créer un groupe d'accès aux volumes

Vous pouvez créer des groupes d'accès aux volumes en associant des initiateurs à une collection de volumes pour un accès sécurisé. Vous pouvez ensuite accorder l'accès aux volumes du groupe avec un secret d'initiateur CHAP et un secret cible.

Si vous utilisez CHAP basé sur l'initiateur, vous pouvez ajouter des informations d'identification CHAP pour un seul initiateur dans un groupe d'accès aux volumes, ce qui renforce la sécurité. Cela vous permet d'appliquer cette option aux groupes d'accès aux volumes qui existent déjà.

Étapes

1. Cliquez sur **Gestion** > **Groupes d'accès**.
2. Cliquez sur **Créer un groupe d'accès**.
3. Saisissez un nom pour le groupe d'accès au volume dans le champ **Nom**.

4. Ajoutez un initiateur au groupe d'accès au volume de l'une des manières suivantes :

Option	Description
Ajout d'un initiateur Fibre Channel	a. Sous Ajouter des initiateurs, sélectionnez un initiateur Fibre Channel existant dans la liste Initiateurs Fibre Channel non liés. b. Cliquez sur **Ajouter un initiateur FC**. Vous pouvez créer un initiateur au cours de cette étape si vous cliquez sur le lien **Créer un initiateur**, saisissez un nom d'initiateur et cliquez sur **Créer**. Le système ajoute automatiquement l'initiateur à la liste des initiateurs après sa création. Voici un exemple de format : `5f:47:ac:c0:5c:74:d4:02`
Ajout d'un initiateur iSCSI	Sous « Ajouter des initiateurs », sélectionnez un initiateur existant dans la liste des initiateurs. **Remarque :** Vous pouvez créer un initiateur au cours de cette étape si vous cliquez sur le lien **Créer un initiateur**, saisissez un nom d'initiateur et cliquez sur **Créer**. Le système ajoute automatiquement l'initiateur à la liste des initiateurs après sa création. Voici un exemple de format : `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` Vous pouvez trouver l'IQN de l'initiateur pour chaque volume en sélectionnant **Afficher les détails** dans le menu Actions du volume sur la liste **Gestion** > **Volumes** > **Actifs**. Lorsque vous modifiez un initiateur, vous pouvez activer l'attribut requiredCHAP, ce qui vous permet de définir le secret de l'initiateur cible. Pour plus de détails, consultez les informations de l'API concernant la méthode ModifyInitiator. "Gérez le stockage avec l'API Element"

5. **Facultatif :** Ajoutez d'autres initiateurs au besoin.
6. Sous Ajouter des volumes, sélectionnez un volume dans la liste **Volumes**.

   Le volume figure dans la liste des **volumes joints**.
7. **Facultatif :** Ajoutez des volumes supplémentaires au besoin.
8. Cliquez sur **Créer un groupe d'accès**.

Trouver plus d'informations

Ajouter des volumes à un groupe d'accès

Afficher les détails du groupe d'accès individuel

Vous pouvez consulter les détails d'un groupe d'accès individuel, tels que les volumes et les initiateurs associés, sous forme graphique.

1. Cliquez sur **Gestion** > **Groupes d'accès**.
2. Cliquez sur l'icône Actions pour un groupe d'accès.
3. Cliquez sur **Afficher les détails**.

Détails du groupe d'accès au volume

La page Groupes d'accès de l'onglet Gestion fournit des informations sur les groupes d'accès aux volumes.

Les informations suivantes sont affichées :

- **ID** : L'identifiant généré par le système pour le groupe d'accès.
- **Nom** : Le nom donné au groupe d'accès lors de sa création.
- **Volumes actifs** : Le nombre de volumes actifs dans le groupe d'accès.
- **Compression** : Score d'efficacité de compression pour le groupe d'accès.
- **Déduplication** : Score d'efficacité de la déduplication pour le groupe d'accès.
- **Provisionnement fin** : Score d'efficacité du provisionnement fin pour le groupe d'accès.
- **Efficacité globale** : Score d'efficacité globale du groupe d'accès.
- **Initiateurs** : Le nombre d'initiateurs connectés au groupe d'accès.

Ajouter des volumes à un groupe d'accès

Vous pouvez ajouter des volumes à un groupe d'accès aux volumes. Chaque volume peut appartenir à plusieurs groupes d'accès aux volumes ; vous pouvez consulter les groupes auxquels chaque volume appartient sur la page **Volumes actifs**.

Vous pouvez également utiliser cette procédure pour ajouter des volumes à un groupe d'accès aux volumes Fibre Channel.

1. Cliquez sur **Gestion** > **Groupes d'accès**.
2. Cliquez sur l'icône Actions du groupe d'accès auquel vous souhaitez ajouter des volumes.
3. Cliquez sur le bouton **Modifier**.
4. Sous Ajouter des volumes, sélectionnez un volume dans la liste **Volumes**.

   Vous pouvez ajouter d'autres volumes en répétant cette étape.

5. Cliquez sur **Enregistrer les modifications**.

Supprimer des volumes d'un groupe d'accès

Lorsque vous retirez un volume d'un groupe d'accès, ce groupe n'a plus accès à ce volume.

La modification des paramètres CHAP dans un compte ou la suppression d'initiateurs ou de volumes d'un groupe d'accès peut entraîner une perte d'accès inattendue aux volumes pour les initiateurs. Pour éviter toute perte d'accès inattendue aux volumes, déconnectez systématiquement les sessions iSCSI qui seront affectées par une modification de compte ou de groupe d'accès, et vérifiez que les initiateurs peuvent se reconnecter aux volumes une fois les modifications apportées aux paramètres d'initiateur et aux paramètres de cluster terminées.

1. Cliquez sur **Gestion** > **Groupes d'accès**.
2. Cliquez sur l'icône Actions du groupe d'accès dont vous souhaitez supprimer des volumes.
3. Cliquez sur **Modifier**.
4. Sous Ajouter des volumes dans la boîte de dialogue **Modifier le groupe d'accès aux volumes**, cliquez sur la flèche de la liste **Volumes attachés**.
5. Sélectionnez le volume que vous souhaitez supprimer de la liste et cliquez sur l'icône **x** pour le supprimer.

   Vous pouvez supprimer davantage de volumes en répétant cette étape.

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

Créer un initiateur

Vous pouvez créer des initiateurs iSCSI ou Fibre Channel et, si vous le souhaitez, leur attribuer des alias.

Vous pouvez également attribuer des attributs CHAP basés sur l'initiateur en utilisant un appel API. Pour ajouter un nom de compte CHAP et des identifiants par initiateur, vous devez utiliser le `CreateInitiator` Appel API pour supprimer et ajouter des accès et des attributs CHAP. L'accès de l'initiateur peut être limité à un ou plusieurs VLAN en spécifiant un ou plusieurs ID de réseau virtuel via le `CreateInitiators` et `ModifyInitiators` Appels API. Si aucun réseau virtuel n'est spécifié, l'initiateur peut accéder à tous les réseaux.

Pour plus de détails, consultez la documentation de référence de l'API. "Gérez le stockage avec l'API Element"

Étapes

1. Cliquez sur **Gestion** > **Initiateurs**.
2. Cliquez sur **Créer un initiateur**.
3. Suivez les étapes pour créer un seul initiateur ou plusieurs initiateurs :

Option	Étapes
Créer un initiateur unique	a. Cliquez sur **Créer un initiateur unique**. b. Saisissez l'IQN ou le WWPN de l'initiateur dans le champ **IQN/WWPN**. c. Saisissez un nom convivial pour l'initiateur dans le champ **Alias**. d. Cliquez sur **Créer un initiateur**.

Option	Étapes
Créer plusieurs initiateurs	a. Cliquez sur **Créer des initiateurs en masse**. b. Saisissez une liste d'IQN ou de WWPN dans la zone de texte. c. Cliquez sur **Ajouter des initiateurs**. d. Choisissez un initiateur dans la liste qui s'affiche et cliquez sur l'icône Ajouter correspondante dans la colonne **Alias** pour ajouter un alias à l'initiateur. e. Cliquez sur la coche pour confirmer le nouvel alias. f. Cliquez sur **Créer des initiateurs**.

Modifier un initiateur

Vous pouvez modifier l'alias d'un initiateur existant ou ajouter un alias s'il n'en existe pas déjà un.

Pour ajouter un nom de compte CHAP et des identifiants par initiateur, vous devez utiliser le `ModifyInitiator` Appel API pour supprimer et ajouter des accès et des attributs CHAP.

Voir"Gérez le stockage avec l'API Element" .

Étapes

1. Cliquez sur **Gestion** > **Initiateurs**.
2. Cliquez sur l'icône Actions de l'initiateur que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Saisissez un nouvel alias pour l'initiateur dans le champ **Alias**.
5. Cliquez sur **Enregistrer les modifications**.

Ajouter un seul initiateur à un groupe d'accès aux volumes

Vous pouvez ajouter un initiateur à un groupe d'accès aux volumes existant.

Lorsque vous ajoutez un initiateur à un groupe d'accès aux volumes, cet initiateur a accès à tous les volumes de ce groupe.

Vous pouvez trouver l'initiateur de chaque volume en cliquant sur l'icône Actions, puis en sélectionnant **Afficher les détails** pour le volume dans la liste des volumes actifs.

Si vous utilisez CHAP basé sur l'initiateur, vous pouvez ajouter des informations d'identification CHAP pour un seul initiateur dans un groupe d'accès aux volumes, ce qui renforce la sécurité. Cela vous permet d'appliquer cette option aux groupes d'accès aux volumes qui existent déjà.

Étapes

1. Cliquez sur **Gestion** > **Groupes d'accès**.
2. Cliquez sur l'icône **Actions** du groupe d'accès que vous souhaitez modifier.
3. Cliquez sur **Modifier**.

4. Pour ajouter un initiateur Fibre Channel au groupe d'accès au volume, procédez comme suit :

   a. Sous Ajouter des initiateurs, sélectionnez un initiateur Fibre Channel existant dans la liste **Initiateurs Fibre Channel non liés**.

   b. Cliquez sur **Ajouter un initiateur FC**.

   Vous pouvez créer un initiateur au cours de cette étape si vous cliquez sur le lien **Créer un initiateur**, saisissez un nom d'initiateur et cliquez sur **Créer**. Le système ajoute automatiquement l'initiateur à la liste **Initiateurs** après sa création.

   Voici un exemple de format :

```
5f:47:ac:c0:5c:74:d4:02
```

5. Pour ajouter un initiateur iSCSI au groupe d'accès au volume, sous Ajouter des initiateurs, sélectionnez un initiateur existant dans la liste **Initiateurs**.

   Vous pouvez créer un initiateur au cours de cette étape si vous cliquez sur le lien **Créer un initiateur**, saisissez un nom d'initiateur et cliquez sur **Créer**. Le système ajoute automatiquement l'initiateur à la liste **Initiateurs** après sa création.

   Le format accepté d'un IQN d'initiateur est le suivant : iqn.yyyy-mm, dans lequel y et m sont des chiffres, suivis d'un texte qui ne doit contenir que des chiffres, des caractères alphabétiques minuscules, un point (.), deux-points (:) ou un tiret (-).

   Voici un exemple de format :

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

   Vous pouvez trouver l'IQN de l'initiateur pour chaque volume sur la page **Gestion** > **Volumes** Volumes actifs en cliquant sur l'icône Actions puis en sélectionnant **Afficher les détails** pour le volume.

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

Ajouter plusieurs initiateurs à un groupe d'accès au volume

Vous pouvez ajouter plusieurs initiateurs à un groupe d'accès aux volumes existant pour autoriser l'accès aux volumes du groupe d'accès aux volumes avec ou sans authentification CHAP.

Lorsque vous ajoutez des initiateurs à un groupe d'accès aux volumes, ces initiateurs ont accès à tous les volumes de ce groupe.

Vous pouvez trouver l'initiateur de chaque volume en cliquant sur l'icône Actions, puis sur **Afficher les détails** du volume dans la liste des volumes actifs.

Vous pouvez ajouter plusieurs initiateurs à un groupe d'accès aux volumes existant pour activer l'accès aux

volumes et attribuer des informations d'identification CHAP uniques à chaque initiateur au sein de ce groupe d'accès aux volumes. Cela vous permet d'appliquer cette option aux groupes d'accès aux volumes qui existent déjà.

Vous pouvez attribuer des attributs CHAP basés sur l'initiateur en utilisant un appel API. Pour ajouter un nom de compte CHAP et des informations d'identification par initiateur, vous devez utiliser l'appel d'API ModifyInitiator pour supprimer et ajouter l'accès et les attributs CHAP.

Pour plus de détails, voir"Gérez le stockage avec l'API Element" .

Étapes

1. Cliquez sur **Gestion** > **Initiateurs**.
2. Sélectionnez les initiateurs que vous souhaitez ajouter à un groupe d'accès.
3. Cliquez sur le bouton **Actions groupées**.
4. Cliquez sur **Ajouter au groupe d'accès au volume**.
5. Dans la boîte de dialogue Ajouter au groupe d'accès aux volumes, sélectionnez un groupe d'accès dans la liste **Groupe d'accès aux volumes**.
6. Cliquez sur **Ajouter**.

Supprimer les initiateurs d'un groupe d'accès

Lorsque vous retirez un initiateur d'un groupe d'accès, celui-ci ne peut plus accéder aux volumes de ce groupe d'accès. L'accès normal au volume via le compte n'est pas interrompu.

La modification des paramètres CHAP dans un compte ou la suppression d'initiateurs ou de volumes d'un groupe d'accès peut entraîner une perte d'accès inattendue aux volumes pour les initiateurs. Pour éviter toute perte d'accès inattendue aux volumes, déconnectez systématiquement les sessions iSCSI qui seront affectées par une modification de compte ou de groupe d'accès, et vérifiez que les initiateurs peuvent se reconnecter aux volumes une fois les modifications apportées aux paramètres d'initiateur et aux paramètres de cluster terminées.

Étapes

1. Cliquez sur **Gestion** > **Groupes d'accès**.
2. Cliquez sur l'icône **Actions** du groupe d'accès que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, sélectionnez **Modifier**.
4. Sous Ajouter des initiateurs dans la boîte de dialogue **Modifier le groupe d'accès aux volumes**, cliquez sur la flèche de la liste **Initiateurs**.
5. Sélectionnez l'icône x pour chaque initiateur que vous souhaitez retirer du groupe d'accès.
6. Cliquez sur **Enregistrer les modifications**.

Supprimer un groupe d'accès

Vous pouvez supprimer un groupe d'accès lorsqu'il n'est plus nécessaire. Il n'est pas nécessaire de supprimer les ID d'initiateur et les ID de volume du groupe d'accès au volume avant de supprimer le groupe. Une fois le groupe d'accès supprimé, l'accès du groupe aux volumes est interrompu.

1. Cliquez sur **Gestion** > **Groupes d'accès**.
2. Cliquez sur l'icône **Actions** du groupe d'accès que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, cliquez sur **Supprimer**.
4. Pour supprimer également les initiateurs associés à ce groupe d'accès, cochez la case **Supprimer les initiateurs de ce groupe d'accès**.
5. Confirmez l'action.

Supprimer un initiateur

Vous pouvez supprimer un initiateur lorsqu'il n'est plus nécessaire. Lorsque vous supprimez un initiateur, le système le retire de tout groupe d'accès aux volumes associé. Toute connexion utilisant l'initiateur reste valide jusqu'à sa réinitialisation.

Étapes

1. Cliquez sur **Gestion** > **Initiateurs**.
2. Suivez les étapes pour supprimer un ou plusieurs initiateurs :

Option	Étapes
Supprimer l'initiateur unique	a. Cliquez sur l'icône **Actions** correspondant à l'initiateur que vous souhaitez supprimer. b. Cliquez sur **Supprimer**. c. Confirmez l'action.
Supprimer plusieurs initiateurs	a. Cochez les cases correspondant aux initiateurs que vous souhaitez supprimer. b. Cliquez sur le bouton **Actions groupées**. c. Dans le menu qui s'affiche, sélectionnez **Supprimer**. d. Confirmez l'action.

Protégez vos données

Protégez vos données

Le logiciel NetApp Element vous permet de protéger vos données de différentes manières grâce à des fonctionnalités telles que les instantanés pour des volumes individuels ou des groupes de volumes, la réplication entre les clusters et les volumes exécutés sur Element, et la réplication vers les systèmes ONTAP .

- **Instantanés**

  La protection des données par instantané réplique les données modifiées à des moments précis sur un cluster distant. Seuls les instantanés créés sur le cluster source sont répliqués. Les écritures actives à partir du volume source ne le sont pas.

Utilisez les instantanés de volume pour la protection des données

- **Réplication à distance entre les clusters et les volumes exécutés sur Element**

  Vous pouvez répliquer les données de volume de manière synchrone ou asynchrone à partir de l'un ou l'autre cluster d'une paire de clusters s'exécutant tous deux sur Element pour les scénarios de basculement et de restauration.

  Effectuez une réplication à distance entre des clusters exécutant le logiciel NetApp Element.

- *Réplication entre les clusters Element et ONTAP à l'aide de la technologie SnapMirror *

  Grâce à la technologie NetApp SnapMirror , vous pouvez répliquer les instantanés pris avec Element vers ONTAP à des fins de reprise après sinistre. Dans une relation SnapMirror , Element est un point de terminaison et ONTAP est l'autre.

  Utilisez la réplication SnapMirror entre les clusters Element et ONTAP.

- **Sauvegarde et restauration de volumes à partir de stockages d'objets SolidFire, S3 ou Swift**

  Vous pouvez sauvegarder et restaurer des volumes sur d'autres systèmes de stockage SolidFire , ainsi que sur des systèmes de stockage d'objets secondaires compatibles avec Amazon S3 ou OpenStack Swift.

  Sauvegardez et restaurez des volumes sur SolidFire, S3 ou des stockages d'objets Swift.

Pour plus d'informations

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

Utilisez les instantanés de volume pour la protection des données

Utilisez les instantanés de volume pour la protection des données

Un instantané de volume est une copie d'un volume à un instant précis. Vous pouvez prendre un instantané d'un volume et l'utiliser ultérieurement si vous devez restaurer un volume à l'état dans lequel il se trouvait au moment de la création de l'instantané.

Les instantanés sont similaires aux clones de volume. Cependant, les instantanés ne sont que des répliques des métadonnées du volume ; vous ne pouvez donc ni les monter ni y écrire. La création d'un instantané de volume ne nécessite qu'une petite quantité de ressources système et d'espace, ce qui rend la création d'un instantané plus rapide que le clonage.

Vous pouvez prendre un instantané d'un volume individuel ou d'un ensemble de volumes.

Vous pouvez également répliquer les instantanés sur un cluster distant et les utiliser comme copie de sauvegarde du volume. Cela vous permet de restaurer un volume à un point précis dans le temps en utilisant l'instantané répliqué. Vous pouvez également créer un clone d'un volume à partir d'un instantané répliqué.

Trouver plus d'informations

- Utilisez des instantanés de volumes individuels pour la protection des données

- Utilisation des instantanés de groupe pour la tâche de protection des données
- Planification d'un instantané

Utilisez des instantanés de volumes individuels pour la protection des données

Utilisez des instantanés de volumes individuels pour la protection des données

Un instantané de volume est une copie d'un volume à un instant précis. Vous pouvez utiliser un volume individuel plutôt qu'un groupe de volumes pour l'instantané.

Trouver plus d'informations

- Créer un instantané de volume
- Conservation des instantanés de modification
- Suppression d'un instantané
- Clonage d'un volume à partir d'un instantané
- Restauration d'un volume à un instantané
- Sauvegarde d'un instantané de volume sur un stockage d'objets Amazon S3
- Sauvegarde d'un instantané de volume sur un magasin d'objets OpenStack Swift
- Sauvegarde d'un instantané de volume sur un cluster SolidFire

Créer un instantané de volume

Vous pouvez créer un instantané d'un volume actif afin de préserver l'image du volume à tout moment. Vous pouvez créer jusqu'à 32 instantanés pour un seul volume.

1. Cliquez sur **Gestion** > **Volumes**.
2. Cliquez sur l'icône **Actions** du volume que vous souhaitez utiliser pour la capture d'écran.
3. Dans le menu qui s'affiche, sélectionnez **Capture d'écran**.
4. Dans la boîte de dialogue **Créer un instantané de volume**, saisissez le nom du nouvel instantané.
5. **Facultatif :** Cochez la case **Inclure l'instantané dans la réplication lors du couplage** pour vous assurer que l'instantané est capturé lors de la réplication lorsque le volume parent est couplé.
6. Pour définir la durée de conservation de l'instantané, sélectionnez l'une des options suivantes :
   - Cliquez sur **Conserver indéfiniment** pour conserver l'instantané sur le système de façon permanente.
   - Cliquez sur **Définir la période de conservation** et utilisez les champs de date pour choisir la durée pendant laquelle le système conservera l'instantané.
7. Pour prendre une photo instantanée, procédez comme suit :
   a. Cliquez sur **Prendre un instantané maintenant**.
   b. Cliquez sur **Créer un instantané**.
8. Pour programmer l'exécution de la capture instantanée à une date ultérieure, procédez comme suit :
   a. Cliquez sur **Créer un calendrier d'instantanés**.
   b. Saisissez un **Nom pour le nouvel horaire**.
   c. Choisissez un **type de planification** dans la liste.

d. **Facultatif :** Cochez la case **Planification récurrente** pour répéter périodiquement la capture d'écran planifiée.

e. Cliquez sur **Créer un planning**.

Trouver plus d'informations

Planifiez une prise de vue

Conservation des instantanés de modification

Vous pouvez modifier la période de conservation d'un instantané pour contrôler quand, et si, le système supprime les instantanés. La période de conservation que vous spécifiez commence lorsque vous entrez dans le nouvel intervalle. Lorsque vous définissez une période de conservation, vous pouvez sélectionner une période qui commence à l'heure actuelle (la conservation n'est pas calculée à partir de la date de création de l'instantané). Vous pouvez spécifier les intervalles en minutes, en heures et en jours.

Étapes

1. Cliquez sur **Protection des données** > **Instantanés**.
2. Cliquez sur l'icône **Actions** de la capture d'écran que vous souhaitez modifier.
3. Dans le menu qui apparaît, cliquez sur **Modifier**.
4. **Facultatif :** Cochez la case **Inclure l'instantané dans la réplication lors du couplage** pour vous assurer que l'instantané est capturé dans la réplication lorsque le volume parent est couplé.
5. **Facultatif :** Sélectionnez une option de conservation pour l'instantané :
   - Cliquez sur **Conserver indéfiniment** pour conserver l'instantané sur le système de façon permanente.
   - Cliquez sur **Définir la période de conservation** et utilisez les champs de date pour sélectionner la durée pendant laquelle le système conservera l'instantané.
6. Cliquez sur **Enregistrer les modifications**.

Supprimer un instantané

Vous pouvez supprimer un instantané de volume d'un cluster de stockage exécutant le logiciel Element. Lorsque vous supprimez un instantané, le système le supprime immédiatement.

Vous pouvez supprimer les instantanés en cours de réplication à partir du cluster source. Si un instantané est en cours de synchronisation avec le cluster cible lorsque vous le supprimez, la réplication de synchronisation se termine et l'instantané est supprimé du cluster source. L'instantané n'est pas supprimé du cluster cible.

Vous pouvez également supprimer les instantanés qui ont été répliqués sur la cible depuis le cluster cible. L'instantané supprimé est conservé dans une liste d'instantanés supprimés sur la cible jusqu'à ce que le système détecte que vous avez supprimé l'instantané sur le cluster source. Lorsque la cible détecte que vous avez supprimé l'instantané source, elle interrompt la réplication de cet instantané.

Lorsque vous supprimez un instantané du cluster source, l'instantané du cluster cible n'est pas affecté (et inversement).

1. Cliquez sur **Protection des données** > **Instantanés**.

2. Cliquez sur l'icône **Actions** correspondant à l'instantané que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, sélectionnez **Supprimer**.
4. Confirmez l'action.

Cloner un volume à partir d'un instantané

Vous pouvez créer un nouveau volume à partir d'un instantané d'un volume. Lorsque vous effectuez cette opération, le système utilise les informations de l'instantané pour cloner un nouveau volume en utilisant les données contenues sur le volume au moment de la création de l'instantané. Ce processus stocke dans le volume nouvellement créé des informations relatives à d'autres instantanés du volume.

1. Cliquez sur **Protection des données** > **Instantanés**.
2. Cliquez sur l'icône **Actions** correspondant à l'instantané que vous souhaitez utiliser pour le clonage du volume.
3. Dans le menu qui s'affiche, cliquez sur **Cloner le volume à partir d'un instantané**.
4. Saisissez un **nom de volume** dans la boîte de dialogue **Cloner le volume à partir d'un instantané**.
5. Sélectionnez une **taille totale** et des unités de mesure pour le nouveau volume.
6. Sélectionnez un type d'**accès** pour le volume.
7. Sélectionnez un **compte** dans la liste à associer au nouveau volume.
8. Cliquez sur **Démarrer le clonage**.

Restaurer un volume à un instantané

Vous pouvez restaurer un volume à un instantané précédent à tout moment. Cette opération annule toutes les modifications apportées au volume depuis la création de l'instantané.

Étapes

1. Cliquez sur **Protection des données** > **Instantanés**.
2. Cliquez sur l'icône **Actions** correspondant à l'instantané que vous souhaitez utiliser pour la restauration du volume.
3. Dans le menu qui s'affiche, sélectionnez **Restaurer le volume à l'instantané**.
4. **Facultatif :** Pour enregistrer l'état actuel du volume avant de revenir à l'instantané :
   a. Dans la boîte de dialogue **Restaurer à partir d'un instantané**, sélectionnez **Enregistrer l'état actuel du volume sous forme d'instantané**.
   b. Saisissez un nom pour le nouveau snapshot.
5. Cliquez sur **Restaurer l'instantané**.

Sauvegarder un instantané de volume

Sauvegarder un instantané de volume

Vous pouvez utiliser la fonction de sauvegarde intégrée pour sauvegarder un instantané de volume. Vous pouvez sauvegarder des instantanés d'un cluster SolidFire sur un

stockage d'objets externe ou sur un autre cluster SolidFire . Lorsque vous sauvegardez un instantané sur un stockage d'objets externe, vous devez disposer d'une connexion à ce stockage d'objets autorisant les opérations de lecture/écriture.

- "Sauvegardez un instantané de volume sur un stockage d'objets Amazon S3"
- "Sauvegardez un instantané de volume sur un stockage d'objets OpenStack Swift"
- "Sauvegardez un instantané de volume sur un cluster SolidFire"

Sauvegardez un instantané de volume sur un stockage d'objets Amazon S3

Vous pouvez sauvegarder les instantanés SolidFire sur des supports de stockage d'objets externes compatibles avec Amazon S3.

1. Cliquez sur **Protection des données** > **Instantanés**.
2. Cliquez sur l'icône **Actions** correspondant à l'instantané que vous souhaitez sauvegarder.
3. Dans le menu qui apparaît, cliquez sur **Sauvegarder vers**.
4. Dans la boîte de dialogue **Sauvegarde intégrée**, sous **Sauvegarder vers**, sélectionnez **S3**.
5. Sélectionnez une option sous **Format des données** :
   - **Natif** : Un format compressé lisible uniquement par les systèmes de stockage SolidFire .
   - **Non compressé** : Un format non compressé compatible avec d'autres systèmes.
6. Saisissez un nom d'hôte à utiliser pour accéder au stockage d'objets dans le champ **Nom d'hôte**.
7. Saisissez un identifiant de clé d'accès pour le compte dans le champ **Identifiant de clé d'accès**.
8. Saisissez la clé d'accès secrète du compte dans le champ **Clé d'accès secrète**.
9. Saisissez le compartiment S3 dans lequel stocker la sauvegarde dans le champ **Compartiment S3**.
10. **Facultatif** : Saisissez un nom à ajouter au préfixe dans le champ **Nom**.
11. Cliquez sur **Commencer la lecture**.

Sauvegardez un instantané de volume sur un stockage d'objets OpenStack Swift

Vous pouvez sauvegarder les instantanés SolidFire sur des supports de stockage d'objets secondaires compatibles avec OpenStack Swift.

1. Cliquez sur **Protection des données** > **Instantanés**.
2. Cliquez sur l'icône **Actions** correspondant à l'instantané que vous souhaitez sauvegarder.
3. Dans le menu qui apparaît, cliquez sur **Sauvegarder vers**.
4. Dans la boîte de dialogue **Sauvegarde intégrée**, sous **Sauvegarder vers**, sélectionnez **Swift**.
5. Sélectionnez une option sous **Format des données** :
   - **Natif** : Un format compressé lisible uniquement par les systèmes de stockage SolidFire .
   - **Non compressé** : Un format non compressé compatible avec d'autres systèmes.
6. Saisissez une **URL** pour accéder au magasin d'objets.
7. Veuillez saisir un **nom d'utilisateur** pour le compte.
8. Saisissez la **clé d'authentification** du compte.

9. Saisissez le **conteneur** dans lequel stocker la sauvegarde.
10. **Facultatif** : Saisissez un **nom**.
11. Cliquez sur **Commencer la lecture**.

Sauvegardez un instantané de volume sur un cluster SolidFire

Vous pouvez sauvegarder des instantanés de volumes résidant sur un cluster SolidFire vers un cluster SolidFire distant.

Assurez-vous que les clusters source et cible sont appariés.

Lors de la sauvegarde ou de la restauration d'un cluster à un autre, le système génère une clé qui servira d'authentification entre les clusters. Cette clé d'écriture en masse permet au cluster source de s'authentifier auprès du cluster de destination, assurant ainsi un niveau de sécurité lors de l'écriture sur le volume de destination. Dans le cadre du processus de sauvegarde ou de restauration, vous devez générer une clé d'écriture de volume en masse à partir du volume de destination avant de démarrer l'opération.

1. Sur le cluster de destination, cliquez sur **Gestion** > **Volumes**.
2. Cliquez sur l'icône **Actions** du volume de destination.
3. Dans le menu qui s'affiche, cliquez sur **Restaurer à partir de**.
4. Dans la boîte de dialogue **Restauration intégrée**, sous **Restaurer à partir de**, sélectionnez * SolidFire*.
5. Sélectionnez un format de données sous **Format des données** :
   - **Natif** : Un format compressé lisible uniquement par les systèmes de stockage SolidFire .
   - **Non compressé** : Un format non compressé compatible avec d'autres systèmes.
6. Cliquez sur **Générer la clé**.
7. Copiez la clé contenue dans la zone **Clé d'écriture en masse** dans votre presse-papiers.
8. Sur le cluster source, cliquez sur **Protection des données** > **Instantanés**.
9. Cliquez sur l'icône Actions correspondant à l'instantané que vous souhaitez utiliser pour la sauvegarde.
10. Dans le menu qui apparaît, cliquez sur **Sauvegarder vers**.
11. Dans la boîte de dialogue **Sauvegarde intégrée**, sous **Sauvegarder vers**, sélectionnez * SolidFire*.
12. Sélectionnez le même format de données que celui que vous avez sélectionné précédemment dans le champ **Format des données**.
13. Saisissez l'adresse IP virtuelle de gestion du cluster du volume de destination dans le champ **Adresse IP virtuelle du cluster distant**.
14. Saisissez le nom d'utilisateur du cluster distant dans le champ **Nom d'utilisateur du cluster distant**.
15. Saisissez le mot de passe du cluster distant dans le champ **Mot de passe du cluster distant**.
16. Dans le champ **Clé d'écriture en masse**, collez la clé que vous avez générée précédemment sur le cluster de destination.
17. Cliquez sur **Commencer la lecture**.

Utilisez les instantanés de groupe pour la protection des données

Utilisation des instantanés de groupe pour la tâche de protection des données

Vous pouvez créer un instantané de groupe d'un ensemble de volumes liés afin de préserver une copie à un instant donné des métadonnées de chaque volume. Vous pourrez utiliser ultérieurement l'instantané de groupe comme sauvegarde ou restauration pour rétablir l'état du groupe de volumes à un état antérieur.

Trouver plus d'informations

- Créer un instantané de groupe
- Modifier les instantanés de groupe
- Modifier les membres du groupe (instantané)
- Supprimer un instantané de groupe
- Restaurez les volumes à partir d'un instantané de groupe
- Cloner plusieurs volumes
- Cloner plusieurs volumes à partir d'un snapshot de groupe

Détails de l'instantané de groupe

La page « Instantanés de groupe » de l'onglet « Protection des données » fournit des informations sur les instantanés de groupe.

- **IDENTIFIANT**

  L'identifiant généré par le système pour l'instantané du groupe.

- **UUID**

  L'identifiant unique de l'instantané du groupe.

- **Nom**

  Nom défini par l'utilisateur pour l'instantané du groupe.

- **Créer du temps**

  L'heure à laquelle l'instantané de groupe a été créé.

- **Statut**

  État actuel de l'instantané. Valeurs possibles :

  - Préparation : L'instantané est en cours de préparation et n'est pas encore modifiable.
  - Terminé : cette capture d'écran a terminé sa préparation et est maintenant utilisable.
  - Actif : L'instantané correspond à la branche active.

- **# Volumes**

  Le nombre de volumes dans le groupe.

- **À conserver jusqu'au**

Le jour et l'heure de suppression de l'instantané.

- **Réplication à distance**

  Indication indiquant si la réplication de l'instantané vers un cluster SolidFire distant est activée ou non. Valeurs possibles :

  - Activé : La réplication à distance de l'instantané est activée.
  - Désactivé : la réplication à distance de l'instantané n'est pas activée.

Création d'un instantané de groupe

Vous pouvez créer un instantané d'un groupe de volumes, et vous pouvez également créer une planification d'instantanés de groupe pour automatiser les instantanés de groupe. Une seule capture instantanée de groupe peut capturer simultanément jusqu'à 32 volumes.

Étapes

1. Cliquez sur **Gestion** > **Volumes**.
2. Utilisez les cases à cocher pour sélectionner plusieurs volumes pour un groupe de volumes.
3. Cliquez sur **Actions groupées**.
4. Cliquez sur **Aperçu du groupe**.
5. Saisissez un nouveau nom pour l'instantané de groupe dans la boîte de dialogue Créer un instantané de groupe de volumes.
6. **Facultatif :** Cochez la case **Inclure chaque membre du snapshot de groupe dans la réplication lors de l'appairage** pour vous assurer que chaque snapshot est capturé dans la réplication lorsque le volume parent est apparié.
7. Sélectionnez une option de conservation pour l'instantané de groupe :
   - Cliquez sur **Conserver indéfiniment** pour conserver l'instantané sur le système de façon permanente.
   - Cliquez sur **Définir la période de conservation** et utilisez les champs de date pour choisir la durée pendant laquelle le système conservera l'instantané.
8. Pour prendre une photo instantanée, procédez comme suit :
   a. Cliquez sur **Prendre une photo de groupe maintenant**.
   b. Cliquez sur **Créer un instantané de groupe**.
9. Pour programmer l'exécution de la capture instantanée à une date ultérieure, procédez comme suit :
   a. Cliquez sur **Créer un calendrier de clichés de groupe**.
   b. Saisissez un **Nom pour le nouvel horaire**.
   c. Sélectionnez un **type de planification** dans la liste.
   d. **Facultatif :** Cochez la case **Planification récurrente** pour répéter périodiquement la capture d'écran planifiée.
   e. Cliquez sur **Créer un planning**.

Modification des instantanés de groupe

Vous pouvez modifier les paramètres de réplication et de conservation des instantanés

de groupe existants.

1. Cliquez sur **Protection des données** > **Instantanés de groupe**.
2. Cliquez sur l'icône Actions de l'instantané de groupe que vous souhaitez modifier.
3. Dans le menu qui s'affiche, sélectionnez **Modifier**.
4. **Facultatif :** Pour modifier le paramètre de réplication de l'instantané de groupe :
   a. Cliquez sur **Modifier** à côté de **Réplication actuelle**.
   b. Cochez la case **Inclure chaque membre du snapshot de groupe dans la réplication lors de l'appairage** pour garantir que chaque snapshot est capturé dans la réplication lorsque le volume parent est apparié.
5. **Facultatif :** Pour modifier le paramètre de conservation de l'instantané de groupe, sélectionnez parmi les options suivantes :
   a. Cliquez sur **Modifier** à côté de **Rétention actuelle**.
   b. Sélectionnez une option de conservation pour l'instantané de groupe :
      - Cliquez sur **Conserver indéfiniment** pour conserver l'instantané sur le système de façon permanente.
      - Cliquez sur **Définir la période de conservation** et utilisez les champs de date pour choisir la durée pendant laquelle le système conservera l'instantané.
6. Cliquez sur **Enregistrer les modifications**.

Suppression d'un instantané de groupe

Vous pouvez supprimer un instantané de groupe du système. Lorsque vous supprimez l'instantané de groupe, vous pouvez choisir si tous les instantanés associés au groupe sont supprimés ou conservés individuellement.

Si vous supprimez un volume ou un instantané qui fait partie d'un instantané de groupe, vous ne pourrez plus revenir à cet instantané de groupe. Vous pouvez toutefois annuler chaque volume individuellement.

1. Cliquez sur **Protection des données** > **Instantanés de groupe**.
2. Cliquez sur l'icône Actions correspondant à l'instantané que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, cliquez sur **Supprimer**.
4. Dans la boîte de dialogue de confirmation, sélectionnez l'une des options suivantes :
   - Cliquez sur **Supprimer l'instantané du groupe ET tous les membres de l'instantané du groupe** pour supprimer l'instantané du groupe et tous les instantanés de ses membres.
   - Cliquez sur **Conserver les membres du groupe en tant qu'instantanés individuels** pour supprimer l'instantané du groupe tout en conservant tous les instantanés des membres.
5. Confirmez l'action.

Restaurez les volumes à partir d'un instantané de groupe

Vous pouvez à tout moment restaurer un groupe de volumes à partir d'un instantané de groupe.

Lorsque vous restaurez un groupe de volumes, tous les volumes du groupe sont rétablis dans l'état où ils se trouvaient au moment de la création de l'instantané du groupe. La restauration de la version précédente

rétablit également les tailles de volume à la taille enregistrée dans l'instantané d'origine. Si le système a purgé un volume, tous les instantanés de ce volume ont également été supprimés au moment de la purge ; le système ne restaure aucun instantané de volume supprimé.

1. Cliquez sur **Protection des données** > **Instantanés de groupe**.
2. Cliquez sur l'icône Actions correspondant à l'instantané de groupe que vous souhaitez utiliser pour la restauration du volume.
3. Dans le menu qui s'affiche, sélectionnez **Restaurer les volumes à partir de l'instantané de groupe**.
4. **Facultatif** : Pour enregistrer l'état actuel des volumes avant de revenir à l'instantané :
   a. Dans la boîte de dialogue **Restaurer à partir d'un instantané**, sélectionnez **Enregistrer l'état actuel des volumes sous forme d'instantané de groupe**.
   b. Saisissez un nom pour le nouveau snapshot.
5. Cliquez sur **Rétablir l'instantané du groupe**.

Modification des membres de la capture d'écran du groupe

Vous pouvez modifier les paramètres de conservation des données pour les membres d'un instantané de groupe existant.

1. Cliquez sur **Protection des données** > **Instantanés**.
2. Cliquez sur l'onglet **Membres**.
3. Cliquez sur l'icône Actions du membre du groupe que vous souhaitez modifier.
4. Dans le menu qui s'affiche, sélectionnez **Modifier**.
5. Pour modifier les paramètres de réplication de l'instantané, sélectionnez parmi les options suivantes :
   - Cliquez sur **Conserver indéfiniment** pour conserver l'instantané sur le système de façon permanente.
   - Cliquez sur **Définir la période de conservation** et utilisez les champs de date pour choisir la durée pendant laquelle le système conservera l'instantané.
6. Cliquez sur **Enregistrer les modifications**.

Cloner plusieurs volumes

Vous pouvez créer plusieurs clones de volume en une seule opération afin de créer une copie à un instant donné des données sur un groupe de volumes.

Lorsque vous clonez un volume, le système crée un instantané du volume, puis crée un nouveau volume à partir des données contenues dans cet instantané. Vous pouvez monter le nouveau clone de volume et y écrire. Le clonage de plusieurs volumes est un processus asynchrone et prend un temps variable en fonction de la taille et du nombre de volumes clonés.

La taille du volume et la charge actuelle du cluster influent sur le temps nécessaire pour effectuer une opération de clonage.

Étapes

1. Cliquez sur **Gestion** > **Volumes**.
2. Cliquez sur l'onglet **Actif**.
3. Utilisez les cases à cocher pour sélectionner plusieurs volumes et créer un groupe de volumes.

4. Cliquez sur **Actions groupées**.
5. Cliquez sur **Cloner** dans le menu qui s'affiche.
6. Saisissez un **préfixe de nom de nouveau volume** dans la boîte de dialogue **Cloner plusieurs volumes**.

   Le préfixe est appliqué à tous les volumes du groupe.

7. **Facultatif :** Sélectionnez un autre compte auquel le clone appartiendra.

   Si vous ne sélectionnez pas de compte, le système attribue les nouveaux volumes au compte de volumes actuel.

8. **Facultatif :** Sélectionnez une autre méthode d'accès pour les volumes du clone.

   Si vous ne sélectionnez pas de méthode d'accès, le système utilise l'accès au volume actuel.

9. Cliquez sur **Démarrer le clonage**.

Clonage de plusieurs volumes à partir d'un instantané de groupe

Vous pouvez cloner un groupe de volumes à partir d'un instantané de groupe à un instant donné. Cette opération nécessite qu'un instantané de groupe des volumes existe déjà, car cet instantané de groupe sert de base à la création des volumes. Une fois les volumes créés, vous pouvez les utiliser comme n'importe quel autre volume du système.

La taille du volume et la charge actuelle du cluster influent sur le temps nécessaire pour effectuer une opération de clonage.

1. Cliquez sur **Protection des données** > **Instantanés de groupe**.
2. Cliquez sur l'icône Actions correspondant à l'instantané de groupe que vous souhaitez utiliser pour les clones de volume.
3. Dans le menu qui s'affiche, sélectionnez **Cloner les volumes à partir d'un instantané de groupe**.
4. Saisissez un **préfixe de nom de nouveau volume** dans la boîte de dialogue **Cloner les volumes à partir d'un instantané de groupe**.

   Le préfixe est appliqué à tous les volumes créés à partir de l'instantané de groupe.

5. **Facultatif :** Sélectionnez un autre compte auquel le clone appartiendra.

   Si vous ne sélectionnez pas de compte, le système attribue les nouveaux volumes au compte de volumes actuel.

6. **Facultatif :** Sélectionnez une autre méthode d'accès pour les volumes du clone.

   Si vous ne sélectionnez pas de méthode d'accès, le système utilise l'accès au volume actuel.

7. Cliquez sur **Démarrer le clonage**.

Planifiez une prise de vue

Planifiez une prise de vue

Vous pouvez protéger les données d'un volume ou d'un groupe de volumes en

programmant des instantanés de volume à intervalles spécifiés. Vous pouvez programmer l'exécution automatique de snapshots de volumes individuels ou de snapshots de groupes.

Lorsque vous configurez une planification de capture instantanée, vous pouvez choisir des intervalles de temps basés sur les jours de la semaine ou les jours du mois. Vous pouvez également spécifier les jours, les heures et les minutes avant la prochaine capture d'écran. Vous pouvez stocker les instantanés obtenus sur un système de stockage distant si le volume est répliqué.

Trouver plus d'informations

- Créer un planning instantané
- Modifier un calendrier instantané
- Supprimer une planification d'instantané
- Copier un planning instantané

Aperçu du calendrier

Sur la page Protection des données > Planifications, vous pouvez consulter les informations suivantes dans la liste des planifications d'instantanés.

- **IDENTIFIANT**

  L'identifiant généré par le système pour l'instantané.

- **Taper**

  Le type d'horaire. Seul le type « snapshot » est actuellement pris en charge.

- **Nom**

  Le nom donné au planning lors de sa création. Les noms des calendriers instantanés peuvent comporter jusqu'à 223 caractères et contenir les caractères az, 0-9 et le tiret (-).

- **Fréquence**

  La fréquence d'exécution du programme. La fréquence peut être réglée en heures et minutes, en semaines ou en mois.

- **Récurrent**

  Indication précisant si l'exécution doit être ponctuelle ou régulière.

- **Pause manuelle**

  Indication précisant si la planification a été suspendue manuellement ou non.

- **Identifiants de volume**

  L'identifiant du volume que la planification utilisera lors de son exécution.

- **Dernière course**

La dernière fois que le programme a été exécuté.

- **Statut de la dernière exécution**

  Résultat de la dernière exécution du planning. Valeurs possibles :

  - Succès
  - Échec

Créer un planning instantané

Vous pouvez programmer la prise d'un instantané d'un ou plusieurs volumes à intervalles spécifiés.

Lorsque vous configurez une planification de capture instantanée, vous pouvez choisir des intervalles de temps basés sur les jours de la semaine ou les jours du mois. Vous pouvez également créer une planification récurrente et spécifier les jours, les heures et les minutes avant la prochaine prise de cliché.

Si vous programmez une capture instantanée à un intervalle de temps qui n'est pas divisible par 5 minutes, la capture instantanée s'exécutera à la prochaine période de temps divisible par 5 minutes. Par exemple, si vous programmez une capture instantanée pour qu'elle s'exécute à 12:42:00 UTC, elle s'exécutera à 12:45:00 UTC. Vous ne pouvez pas programmer l'exécution d'un instantané à des intervalles inférieurs à 5 minutes.

À partir d'Element 12.5, vous pouvez activer la création en série et choisir de conserver les instantanés selon le principe du premier entré, premier sorti (FIFO) depuis l'interface utilisateur.

- L'option **Activer la création en série** spécifie qu'un seul instantané est répliqué à la fois. La création d'un nouvel instantané échoue lorsqu'une réplication d'instantané précédente est toujours en cours. Si la case n'est pas cochée, la création d'un instantané est autorisée même si une autre réplication d'instantané est en cours.
- L'option **FIFO** permet de conserver un nombre constant des derniers instantanés. Lorsque la case est cochée, les instantanés sont conservés selon le principe du premier entré, premier sorti (FIFO). Une fois que la file d'attente des instantanés FIFO atteint sa profondeur maximale, l'instantané FIFO le plus ancien est supprimé lorsqu'un nouvel instantané FIFO est inséré.

Étapes

1. Sélectionnez **Protection des données** > **Planifications**.
2. Sélectionnez **Créer un planning**.
3. Dans le champ **ID de volume CSV**, saisissez un seul ID de volume ou une liste d'ID de volume séparés par des virgules à inclure dans l'opération de snapshot.
4. Saisissez un nouveau nom pour le planning.
5. Sélectionnez un type de planification et définissez-la à partir des options proposées.
6. **Facultatif :** Sélectionnez **Planification récurrente** pour répéter indéfiniment la planification de la capture instantanée.
7. **Facultatif :** Saisissez un nom pour le nouvel instantané dans le champ **Nom du nouvel instantané**.

   Si vous laissez ce champ vide, le système utilisera la date et l'heure de création de l'instantané comme nom.

8. **Facultatif :** Cochez la case **Inclure les instantanés dans la réplication lors du couplage** pour vous assurer que les instantanés sont capturés dans la réplication lorsque le volume parent est couplé.

9. **Facultatif :** Cochez la case **Activer la création en série** pour vous assurer qu'un seul instantané est répliqué à la fois.
10. Pour définir la durée de conservation de l'instantané, sélectionnez parmi les options suivantes :
    - **Facultatif :** Cochez la case **FIFO (Premier entré, premier sorti)** pour conserver un nombre constant des derniers instantanés.
    - Sélectionnez **Conserver indéfiniment** pour conserver l'instantané sur le système de manière permanente.
    - Sélectionnez **Définir la période de conservation** et utilisez les champs de date pour choisir la durée pendant laquelle le système conservera l'instantané.
11. Sélectionnez **Créer un planning**.

Modifier un calendrier instantané

Vous pouvez modifier les planifications d'instantanés existantes. Après modification, lors de sa prochaine exécution, la planification utilisera les attributs mis à jour. Toutes les captures d'écran créées par la planification d'origine restent sur le système de stockage.

Étapes

1. Cliquez sur **Protection des données** > **Plannings**.
2. Cliquez sur l'icône **Actions** correspondant à la planification que vous souhaitez modifier.
3. Dans le menu qui apparaît, cliquez sur **Modifier**.
4. Dans le champ **ID de volume CSV**, modifiez l'ID de volume unique ou la liste d'ID de volume séparés par des virgules actuellement inclus dans l'opération d'instantané.
5. Pour suspendre ou reprendre la programmation, sélectionnez parmi les options suivantes :
    - Pour suspendre une planification active, sélectionnez **Oui** dans la liste **Suspendre manuellement la planification**.
    - Pour reprendre une programmation suspendue, sélectionnez **Non** dans la liste **Suspendre manuellement la programmation**.
6. Saisissez un autre nom pour le planning dans le champ **Nouveau nom du planning** si vous le souhaitez.
7. Pour modifier la planification et la faire s'exécuter à différents jours de la semaine ou du mois, sélectionnez **Type de planification** et modifiez la planification à partir des options proposées.
8. **Facultatif :** Sélectionnez **Planification récurrente** pour répéter indéfiniment la planification de la capture instantanée.
9. **Facultatif :** Saisissez ou modifiez le nom du nouvel instantané dans le champ **Nom du nouvel instantané**.

   Si vous laissez ce champ vide, le système utilisera la date et l'heure de création de l'instantané comme nom.

10. **Facultatif :** Cochez la case **Inclure les instantanés dans la réplication lors du couplage** pour vous assurer que les instantanés sont capturés dans la réplication lorsque le volume parent est couplé.
11. Pour modifier le paramètre de rétention, sélectionnez parmi les options suivantes :
    - Cliquez sur **Conserver indéfiniment** pour conserver l'instantané sur le système de façon permanente.
    - Cliquez sur **Définir la période de conservation** et utilisez les champs de date pour sélectionner la durée pendant laquelle le système conservera l'instantané.

12. Cliquez sur **Enregistrer les modifications**.

Copier un planning instantané

Vous pouvez copier un planning et conserver ses attributs actuels.

1. Cliquez sur **Protection des données** > **Plannings**.
2. Cliquez sur l'icône Actions correspondant à la planification que vous souhaitez copier.
3. Dans le menu qui s'affiche, cliquez sur **Créer une copie**.

   La boîte de dialogue **Créer une planification** s'affiche, préremplie avec les attributs actuels de la planification.

4. **Facultatif :** Saisissez un nom et les attributs mis à jour pour le nouveau planning.
5. Cliquez sur **Créer un planning**.

Supprimer une planification d'instantané

Vous pouvez supprimer une planification d'instantané. Une fois la planification supprimée, elle n'exécutera plus aucune capture instantanée planifiée. Les instantanés créés par la planification restent sur le système de stockage.

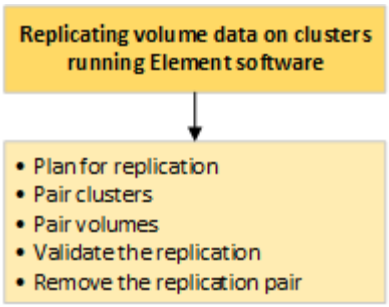
1. Cliquez sur **Protection des données** > **Plannings**.
2. Cliquez sur l'icône **Actions** correspondant à la planification que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, cliquez sur **Supprimer**.
4. Confirmez l'action.

Effectuez une réplication à distance entre des clusters exécutant le logiciel NetApp Element.

Effectuez une réplication à distance entre des clusters exécutant le logiciel NetApp Element.

Pour les clusters exécutant le logiciel Element, la réplication en temps réel permet la création rapide de copies distantes des données de volume. Vous pouvez associer un cluster de stockage à un maximum de quatre autres clusters de stockage. Vous pouvez répliquer les données de volume de manière synchrone ou asynchrone à partir de l'un ou l'autre cluster d'une paire de clusters pour les scénarios de basculement et de restauration.

Le processus de réplication comprend les étapes suivantes :



- "Planifier l'association des clusters et des volumes pour la réplication en temps réel"
- "Apparier les clusters pour la réplication"
- "Volumes de paires"
- "Valider la réplication du volume"
- "Supprimer une relation de volume après la réplication"
- "Gérer les relations de volume"

Planifier l'association des clusters et des volumes pour la réplication en temps réel

La réplication à distance en temps réel nécessite que vous appariiez deux clusters de stockage exécutant le logiciel Element, appariiez les volumes sur chaque cluster et validiez la réplication. Une fois la réplication terminée, vous devez supprimer la relation de volume.

Ce dont vous aurez besoin

- Vous devez disposer des privilèges d'administrateur de cluster pour l'un ou les deux clusters appariés.
- Toutes les adresses IP des nœuds des réseaux de gestion et de stockage des clusters appariés sont routées entre elles.
- L'unité de transmission maximale (MTU) de tous les nœuds appariés doit être identique et prise en charge de bout en bout entre les clusters.
- Chaque cluster de stockage doit avoir un nom de cluster unique, des adresses IP virtuelles multiples (MVIP), des adresses IP virtuelles de second niveau (SVIP) et des adresses IP de nœud uniques.
- La différence entre les versions du logiciel Element sur les clusters ne dépasse pas une version majeure. Si la différence est plus importante, l'un des clusters doit être mis à niveau pour effectuer la réplication des données.

> Les appliances WAN Accelerator n'ont pas été homologuées par NetApp pour une utilisation lors de la réplication de données. Ces dispositifs peuvent interférer avec la compression et la déduplication s'ils sont déployés entre deux clusters qui répliquent des données. Veillez à bien évaluer les effets de tout dispositif d'accélération WAN avant de le déployer dans un environnement de production.

Trouver plus d'informations

- Apparier les clusters pour la réplication
- Volumes de paires

- Attribuer une source et une cible de réplication aux volumes appariés

Apparier les clusters pour la réplication

Apparier les clusters pour la réplication

Vous devez d'abord coupler deux clusters pour pouvoir utiliser la fonctionnalité de réplication en temps réel. Après avoir jumelé et connecté deux clusters, vous pouvez configurer les volumes actifs d'un cluster pour qu'ils soient répliqués en continu sur un deuxième cluster, assurant ainsi une protection continue des données (CDP).

Ce dont vous aurez besoin

- Vous devez disposer des privilèges d'administrateur de cluster pour l'un ou les deux clusters appariés.
- Tous les MIP et SIP des nœuds sont acheminés les uns vers les autres.
- Latence aller-retour entre les clusters inférieure à 2000 ms.
- Chaque cluster de stockage doit avoir un nom de cluster unique, une adresse IP virtuelle principale (MVIP), une adresse IP virtuelle secondaire (SVIP) et une adresse IP pour chaque nœud.
- La différence entre les versions du logiciel Element sur les clusters ne dépasse pas une version majeure. Si la différence est plus importante, l'un des clusters doit être mis à niveau pour effectuer la réplication des données.

> Le jumelage en cluster nécessite une connectivité complète entre les nœuds du réseau de gestion. La réplication nécessite une connectivité entre les différents nœuds du réseau du cluster de stockage.

Vous pouvez associer un cluster à un maximum de quatre autres clusters pour la réplication de volumes. Vous pouvez également apparier des clusters au sein d'un même groupe de clusters.

Apparier les clusters à l'aide de MVIP ou d'une clé d'appariement

Vous pouvez associer un cluster source et un cluster cible en utilisant l'adresse MVIP du cluster cible si les deux clusters disposent d'un accès administrateur. Si l'accès administrateur de cluster n'est disponible que sur un seul cluster d'une paire de clusters, une clé d'appairage peut être utilisée sur le cluster cible pour finaliser l'appairage des clusters.

1. Sélectionnez l'une des méthodes suivantes pour apparier les clusters :
   - "Clusters appariés utilisant MVIP"Utilisez cette méthode si l'administrateur du cluster a accès aux deux clusters. Cette méthode utilise le MVIP du cluster distant pour apparier deux clusters.
   - "Apparier les clusters à l'aide d'une clé d'appariement"Utilisez cette méthode si l'administrateur du cluster n'a accès qu'à un seul des clusters. Cette méthode génère une clé d'appariement qui peut être utilisée sur le cluster cible pour finaliser l'appariement des clusters.

Trouver plus d'informations

Exigences relatives aux ports réseau

Clusters appariés utilisant MVIP

Vous pouvez coupler deux clusters pour une réplication en temps réel en utilisant le MVIP d'un cluster pour établir une connexion avec l'autre cluster. L'accès administrateur

de cluster sur les deux clusters est requis pour utiliser cette méthode. Le nom d'utilisateur et le mot de passe de l'administrateur du cluster sont utilisés pour authentifier l'accès au cluster avant que les clusters puissent être appariés.

1. Sur le cluster local, sélectionnez **Protection des données** > **Paires de clusters**.
2. Cliquez sur **Pair Cluster**.
3. Cliquez sur **Démarrer l'appairage** et sur **Oui** pour indiquer que vous avez accès au cluster distant.
4. Saisissez l'adresse MVIP du cluster distant.
5. Cliquez sur **Terminer l'appairage sur le cluster distant**.

   Dans la fenêtre **Authentification requise**, saisissez le nom d'utilisateur et le mot de passe de l'administrateur du cluster distant.

6. Sur le cluster distant, sélectionnez **Protection des données** > **Paires de clusters**.
7. Cliquez sur **Pair Cluster**.
8. Cliquez sur **Terminer l'appairage**.
9. Cliquez sur le bouton **Terminer l'appairage**.

Trouver plus d'informations

- Apparier les clusters à l'aide d'une clé d'appariement
- "Appariement de clusters à l'aide de MVIP (vidéo)"

Apparier les clusters à l'aide d'une clé d'appariement

Si vous disposez d'un accès d'administrateur de cluster à un cluster local mais pas au cluster distant, vous pouvez apparier les clusters à l'aide d'une clé d'appariement. Une clé d'appairage est générée sur un cluster local, puis envoyée de manière sécurisée à un administrateur de cluster sur un site distant afin d'établir une connexion et de finaliser l'appairage du cluster pour la réplication en temps réel.

1. Sur le cluster local, sélectionnez **Protection des données** > **Paires de clusters**.
2. Cliquez sur **Pair Cluster**.
3. Cliquez sur **Démarrer l'appairage** et sur **Non** pour indiquer que vous n'avez pas accès au cluster distant.
4. Cliquez sur **Générer la clé**.

   Cette action génère une clé de texte pour l'appariement et crée une paire de clusters non configurée sur le cluster local. Si vous ne terminez pas la procédure, vous devrez supprimer manuellement la paire de clusters.

5. Copiez la clé d'appairage du cluster dans votre presse-papiers.
6. Rendez la clé d'appairage accessible à l'administrateur du cluster sur le site distant.

La clé d'appairage du cluster contient une version du MVIP, le nom d'utilisateur, le mot de passe et les informations de la base de données pour permettre les connexions de volume pour la réplication à distance. Cette clé doit être traitée de manière sécurisée et ne doit pas être stockée d'une façon qui permettrait un accès accidentel ou non sécurisé au nom d'utilisateur ou au mot de passe.

Ne modifiez aucun des caractères de la clé d'appariement. La clé devient invalide si elle est modifiée.

7. Sur le cluster distant, sélectionnez **Protection des données** > **Paires de clusters**.
8. Cliquez sur **Pair Cluster**.
9. Cliquez sur **Terminer l'appairage** et saisissez la clé d'appairage dans le champ **Clé d'appairage** (le collage est la méthode recommandée).
10. Cliquez sur **Terminer l'appairage**.

Trouver plus d'informations

- Clusters appariés utilisant MVIP
- "Appariement de clusters à l'aide d'une clé d'appariement de clusters (vidéo)"

Valider la connexion de la paire de clusters

Une fois l'appairage des clusters terminé, vous pouvez vérifier la connexion entre les clusters pour garantir le succès de la réplication.

1. Sur le cluster local, sélectionnez **Protection des données** > **Paires de clusters**.
2. Dans la fenêtre **Paires de clusters**, vérifiez que la paire de clusters est connectée.
3. **Facultatif :** Retournez au cluster local et à la fenêtre **Paires de clusters** et vérifiez que la paire de clusters est connectée.

Volumes de paires

Volumes de paires

Une fois la connexion établie entre les clusters d'une paire de clusters, vous pouvez associer un volume d'un cluster à un volume de l'autre cluster de la paire. Lorsqu'une relation d'appariement de volumes est établie, vous devez identifier quel volume est la cible de réplication.

Vous pouvez associer deux volumes pour la réplication en temps réel qui sont stockés sur des clusters de stockage différents dans une paire de clusters connectés. Après avoir associé deux clusters, vous pouvez configurer les volumes actifs d'un cluster pour qu'ils soient répliqués en continu sur un deuxième cluster, assurant ainsi une protection continue des données (CDP). Vous pouvez également désigner l'un ou l'autre volume comme source ou cible de la réplication.

Les correspondances de volume sont toujours de un à un. Une fois qu'un volume a été associé à un volume situé sur un autre cluster, vous ne pouvez plus l'associer à un autre volume.

Ce dont vous aurez besoin

- Vous avez établi une connexion entre les clusters d'une paire de clusters.
- Vous disposez des privilèges d'administrateur de cluster pour l'un ou les deux clusters appariés.

Étapes

1. Créez un volume cible avec accès en lecture ou en écriture
2. Associer les volumes à l'aide d'un identifiant de volume ou d'une clé d'association
3. Attribuer une source et une cible de réplication aux volumes appariés

Créez un volume cible avec accès en lecture ou en écriture

Le processus de réplication comprend deux points d'extrémité : le volume source et le volume cible. Lorsque vous créez le volume cible, celui-ci est automatiquement configuré en mode lecture/écriture pour accepter les données lors de la réplication.

1. Sélectionnez **Gestion** > **Volumes**.
2. Cliquez sur **Créer un volume**.
3. Dans la boîte de dialogue Créer un nouveau volume, saisissez le nom du volume.
4. Saisissez la taille totale du volume, sélectionnez une taille de bloc pour le volume et sélectionnez le compte qui doit avoir accès au volume.
5. Cliquez sur **Créer un volume**.
6. Dans la fenêtre active, cliquez sur l'icône Actions du volume.
7. Cliquez sur **Modifier**.
8. Modifiez le niveau d'accès du compte en Cible de réplication.
9. Cliquez sur **Enregistrer les modifications**.

Associer les volumes à l'aide d'un identifiant de volume ou d'une clé d'association

Associer les volumes à l'aide d'un ID de volume

Vous pouvez associer un volume à un autre volume sur un cluster distant si vous disposez d'un accès d'administrateur de cluster aux deux clusters sur lesquels les volumes doivent être associés. Cette méthode utilise l'identifiant du volume sur le cluster distant pour établir une connexion.

Ce dont vous aurez besoin

- Assurez-vous que les clusters contenant les volumes soient appariés.
- Créez un nouveau volume sur le cluster distant.

> Vous pouvez attribuer une source et une cible de réplication après le processus d'appairage. Une source ou une cible de réplication peut être l'un ou l'autre volume d'une paire de volumes. Vous devez créer un volume cible ne contenant aucune donnée et possédant les caractéristiques exactes du volume source, telles que la taille, le paramètre de taille de bloc pour les volumes (soit 512e, soit 4k) et la configuration QoS. Si vous désignez un volume existant comme cible de réplication, les données de ce volume seront écrasées. Le volume cible peut être supérieur ou égal au volume source, mais il ne peut pas être inférieur.

- Connaître l'ID du volume cible.

Étapes

1. Sélectionnez **Gestion** > **Volumes**.
2. Cliquez sur l'icône **Actions** correspondant au volume que vous souhaitez appairer.
3. Cliquez sur **Associer**.
4. Dans la boîte de dialogue **Appairer le volume**, sélectionnez **Démarrer l'appairage**.
5. Sélectionnez **Oui** pour indiquer que vous avez accès au cluster distant.
6. Sélectionnez un **mode de réplication** dans la liste :
   - **Temps réel (asynchrone)** : Les écritures sont confirmées auprès du client après leur validation sur le cluster source.
   - **Temps réel (synchrone)** : Les écritures sont confirmées au client après leur validation sur les clusters source et cible.
   - **Instantanés uniquement** : Seuls les instantanés créés sur le cluster source sont répliqués. Les écritures actives provenant du volume source ne sont pas répliquées.
7. Sélectionnez un cluster distant dans la liste.
8. Choisissez un ID de volume distant.
9. Cliquez sur **Démarrer l'appairage**.

   Le système ouvre un onglet de navigateur Web qui se connecte à l'interface utilisateur Element du cluster distant. Il se peut que vous deviez vous connecter au cluster distant avec des identifiants d'administrateur de cluster.

10. Dans l'interface utilisateur Element du cluster distant, sélectionnez **Finaliser l'appairage**.
11. Veuillez confirmer les détails dans **Confirmer le couplage du volume**.
12. Cliquez sur **Terminer l'appairage**.

    Une fois l'appairage confirmé, les deux clusters entament le processus de connexion des volumes pour l'appairage. Pendant le processus d'appairage, vous pouvez voir des messages dans la colonne **État du volume** de la fenêtre **Paires de volumes**. La paire de volumes affiche `PausedMisconfigured` jusqu'à ce que la paire de volumes source et cible soit attribuée.

    Une fois l'appairage terminé avec succès, il est recommandé d'actualiser le tableau Volumes pour supprimer l'option **Apparier** de la liste **Actions** du volume apparié. Si vous ne rafraîchissez pas le tableau, l'option **Paire** reste disponible pour la sélection. Si vous sélectionnez à nouveau l'option **Associer**, un nouvel onglet s'ouvre et, comme le volume est déjà associé, le système signale un `StartVolumePairing Failed: xVolumeAlreadyPaired` Message d'erreur dans la fenêtre **Volume de la paire** de la page Element UI.

Trouver plus d'informations

- Messages de couplage de volume
- Avertissements de couplage de volume
- Attribuer une source et une cible de réplication aux volumes appariés

Appairer les volumes à l'aide d'une clé d'appairage

Si vous disposez d'un accès d'administrateur de cluster uniquement au cluster source (vous ne disposez pas d'identifiants d'administrateur de cluster pour un cluster distant), vous pouvez associer un volume à un autre volume sur un cluster distant à l'aide d'une clé d'association.

Ce dont vous aurez besoin

- Assurez-vous que les clusters contenant les volumes soient appariés.
- Assurez-vous qu'un volume est disponible sur le cluster distant pour l'appairage.

> Vous pouvez attribuer une source et une cible de réplication après le processus d'appairage. Une source ou une cible de réplication peut être l'un ou l'autre volume d'une paire de volumes. Vous devez créer un volume cible ne contenant aucune donnée et possédant les caractéristiques exactes du volume source, telles que la taille, le paramètre de taille de bloc pour les volumes (soit 512e, soit 4k) et la configuration QoS. Si vous désignez un volume existant comme cible de réplication, les données de ce volume seront écrasées. Le volume cible peut être supérieur ou égal au volume source, mais il ne peut pas être inférieur.

Étapes

1. Sélectionnez **Gestion** > **Volumes**.
2. Cliquez sur l'icône **Actions** pour le volume que vous souhaitez appairer.
3. Cliquez sur **Associer**.
4. Dans la boîte de dialogue **Appairer le volume**, sélectionnez **Démarrer l'appairage**.
5. Sélectionnez **Je ne** pour indiquer que vous n'avez pas accès au cluster distant.
6. Sélectionnez un **mode de réplication** dans la liste :
   - **Temps réel (asynchrone)** : Les écritures sont confirmées auprès du client après leur validation sur le cluster source.
   - **Temps réel (synchrone)** : Les écritures sont confirmées au client après leur validation sur les clusters source et cible.
   - **Instantanés uniquement** : Seuls les instantanés créés sur le cluster source sont répliqués. Les écritures actives provenant du volume source ne sont pas répliquées.
7. Cliquez sur **Générer la clé**.

> Cette action génère une clé de texte pour l'appariement et crée une paire de volumes non configurée sur le cluster local. Si vous ne terminez pas la procédure, vous devrez supprimer manuellement la paire de volumes.

8. Copiez la clé d'appairage dans le presse-papiers de votre ordinateur.
9. Rendez la clé d'appairage accessible à l'administrateur du cluster sur le site distant.

> La clé d'appairage du volume doit être traitée de manière sécurisée et ne doit pas être utilisée d'une façon qui permettrait un accès accidentel ou non sécurisé.

Ne modifiez aucun des caractères de la clé d'appariement. La clé devient invalide si elle est modifiée.

10. Dans l'interface utilisateur Element du cluster distant, sélectionnez **Gestion** > **Volumes**.
11. Cliquez sur l'icône Actions correspondant au volume que vous souhaitez appairer.
12. Cliquez sur **Associer**.
13. Dans la boîte de dialogue **Appairer le volume**, sélectionnez **Terminer l'appairage**.
14. Collez la clé d'appairage de l'autre cluster dans la case **Clé d'appairage**.
15. Cliquez sur **Terminer l'appairage**.

    Une fois l'appairage confirmé, les deux clusters entament le processus de connexion des volumes pour l'appairage. Pendant le processus d'appairage, vous pouvez voir des messages dans la colonne **État du volume** de la fenêtre **Paires de volumes**. La paire de volumes affiche `PausedMisconfigured` jusqu'à ce que la paire de volumes source et cible soit attribuée.

    Une fois l'appairage terminé avec succès, il est recommandé d'actualiser le tableau Volumes pour supprimer l'option **Apparier** de la liste **Actions** du volume apparié. Si vous ne rafraîchissez pas le tableau, l'option **Paire** reste disponible pour la sélection. Si vous sélectionnez à nouveau l'option **Associer**, un nouvel onglet s'ouvre et, comme le volume est déjà associé, le système signale un `StartVolumePairing Failed: xVolumeAlreadyPaired` Message d'erreur dans la fenêtre **Volume de la paire** de la page Element UI.

Trouver plus d'informations

- Messages de couplage de volume
- Avertissements de couplage de volume
- Attribuer une source et une cible de réplication aux volumes appariés

Attribuer une source et une cible de réplication aux volumes appariés

Une fois les volumes appariés, vous devez leur attribuer un volume source et son volume cible de réplication. Une source ou une cible de réplication peut être l'un ou l'autre volume d'une paire de volumes. Vous pouvez également utiliser cette procédure pour rediriger les données envoyées à un volume source vers un volume cible distant si le volume source devient indisponible.

Ce dont vous aurez besoin

Vous avez accès aux clusters contenant les volumes source et cible.

Étapes

1. Préparer le volume source :

    a. À partir du cluster contenant le volume que vous souhaitez désigner comme source, sélectionnez **Gestion** > **Volumes**.

    b. Cliquez sur l'icône **Actions** du volume que vous souhaitez désigner comme source, puis cliquez sur **Modifier**.

    c. Dans la liste déroulante **Accès**, sélectionnez **Lecture/Écriture**.

> Si vous inversez l'affectation de la source et de la cible, cette action affichera le message suivant pour la paire de volumes jusqu'à ce qu'une nouvelle cible de réplication soit affectée : `PausedMisconfigured`

La modification des droits d'accès interrompt la réplication du volume et provoque l'arrêt de la transmission des données. Assurez-vous d'avoir coordonné ces changements sur les deux sites.

a. Cliquez sur **Enregistrer les modifications**.

2. Préparer le volume cible :
   a. À partir du cluster contenant le volume que vous souhaitez assigner comme cible, sélectionnez **Gestion** > **Volumes**.
   b. Cliquez sur l'icône Actions du volume que vous souhaitez désigner comme cible, puis cliquez sur **Modifier**.
   c. Dans la liste déroulante **Accès**, sélectionnez **Cible de réplication**.

> Si vous désignez un volume existant comme cible de réplication, les données de ce volume seront écrasées. Vous devez utiliser un nouveau volume cible ne contenant aucune donnée et présentant les mêmes caractéristiques que le volume source, telles que la taille, le paramètre 512e et la configuration QoS. Le volume cible peut être supérieur ou égal au volume source, mais il ne peut pas être inférieur.

   d. Cliquez sur **Enregistrer les modifications**.

Trouver plus d'informations

- Associer les volumes à l'aide d'un ID de volume
- Appairer les volumes à l'aide d'une clé d'appairage

Valider la réplication du volume

Une fois un volume répliqué, vous devez vous assurer que les volumes source et cible sont actifs. En mode actif, les volumes sont appariés, les données sont envoyées de la source au volume cible et les données sont synchronisées.

1. Dans les deux clusters, sélectionnez **Protection des données** > **Paires de volumes**.
2. Vérifiez que l'état du volume est Actif.

Trouver plus d'informations

Avertissements de couplage de volume

Supprimer une relation de volume après la réplication

Une fois la réplication terminée et si vous n'avez plus besoin de la relation entre les paires de volumes, vous pouvez supprimer cette relation.

1. Sélectionnez **Protection des données** > **Paires de volumes**.
2. Cliquez sur l'icône **Actions** correspondant à la paire de volumes que vous souhaitez supprimer.

3. Cliquez sur **Supprimer**.
4. Confirmez le message.

Gérer les relations de volume

Pause réplication

Vous pouvez suspendre manuellement la réplication si vous devez interrompre le traitement des E/S pendant une courte période. Vous pourriez souhaiter suspendre la réplication en cas de forte augmentation du traitement des E/S et si vous souhaitez réduire la charge de traitement.

1. Sélectionnez **Protection des données** > **Paires de volumes**.
2. Cliquez sur l'icône Actions pour la paire de volumes.
3. Cliquez sur **Modifier**.
4. Dans le volet **Modifier la paire de volumes**, suspendez manuellement le processus de réplication.

> La mise en pause ou la reprise manuelle de la réplication de volume entraîne l'arrêt ou la reprise de la transmission des données. Assurez-vous d'avoir coordonné ces changements sur les deux sites.

5. Cliquez sur **Enregistrer les modifications**.

Modifier le mode de réplication

Vous pouvez modifier les propriétés de la paire de volumes pour changer le mode de réplication de la relation entre les paires de volumes.

1. Sélectionnez **Protection des données** > **Paires de volumes**.
2. Cliquez sur l'icône Actions pour la paire de volumes.
3. Cliquez sur **Modifier**.
4. Dans le volet **Modifier la paire de volumes**, sélectionnez un nouveau mode de réplication :
   - **Temps réel (asynchrone)** : Les écritures sont confirmées auprès du client après leur validation sur le cluster source.
   - **Temps réel (synchrone)** : Les écritures sont confirmées au client après leur validation sur les clusters source et cible.
   - **Instantanés uniquement** : Seuls les instantanés créés sur le cluster source sont répliqués. Les écritures actives provenant du volume source ne sont pas répliquées. **Attention :** Modifier le mode de réplication modifie immédiatement le mode. Assurez-vous d'avoir coordonné ces changements sur les deux sites.
5. Cliquez sur **Enregistrer les modifications**.

Supprimer les paires de volumes

Vous pouvez supprimer une paire de volumes si vous souhaitez supprimer une association entre deux volumes.

1. Sélectionnez **Protection des données** > **Paires de volumes**.
2. Cliquez sur l'icône Actions correspondant à la paire de volumes que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Confirmez le message.

Supprimer une paire de clusters

Vous pouvez supprimer une paire de clusters depuis l'interface utilisateur Element de l'un ou l'autre des clusters de la paire.

1. Cliquez sur **Protection des données** > **Paires de clusters**.
2. Cliquez sur l'icône Actions pour une paire de clusters.
3. Dans le menu qui s'affiche, cliquez sur **Supprimer**.
4. Confirmez l'action.
5. Répétez les étapes à partir du deuxième groupe dans l'appariement des groupes.

Détails de la paire de clusters

La page « Paires de clusters » de l'onglet « Protection des données » fournit des informations sur les clusters qui ont été appariés ou qui sont en cours d'appariement. Le système affiche les messages d'appairage et de progression dans la colonne État.

- **IDENTIFIANT**

  Un identifiant généré par le système est attribué à chaque paire de clusters.

- **Nom du cluster distant**

  Le nom de l'autre groupe de la paire.

- **MVIP à distance**

  L'adresse IP virtuelle de gestion de l'autre cluster de la paire.

- **Statut**

  État de réplication du cluster distant

- **Réplication des volumes**

  Le nombre de volumes contenus dans le cluster qui sont appariés pour la réplication.

- **UUID**

  Un identifiant unique est attribué à chaque cluster de la paire.

paires de volumes

Détails de la paire de volumes

La page « Paires de volumes » de l'onglet « Protection des données » fournit des informations sur les volumes qui ont été appariés ou qui sont en cours d'appariement. Le système affiche les messages d'appairage et de progression dans la colonne État du volume.

- **IDENTIFIANT**

  Identifiant généré par le système pour le volume.

- **Nom**

  Le nom donné au volume lors de sa création. Les noms de volumes peuvent comporter jusqu'à 223 caractères et contenir az, 0-9 et un tiret (-).

- **Compte**

  Nom du compte associé au volume.

- **État du volume**

  État de réplication du volume

- **État de l'instantané**

  État du volume de snapshot.

- **Mode**

  La méthode de réplication d'écriture du client. Les valeurs possibles sont les suivantes :

  - Asynchrone
  - Instantané uniquement
  - Synchroniser

- **Direction**

  Sens des données de volume :

  - icône du volume source (→) indique que des données sont écrites sur une cible située en dehors du cluster.
  - icône du volume cible (←) indique que des données sont écrites sur le volume local à partir d'une source externe.

- **Délai asynchrone**

  Durée écoulée depuis la dernière synchronisation du volume avec le cluster distant. Si le volume n'est pas apparié, la valeur est nulle.

- **Cluster distant**

  Nom du cluster distant sur lequel réside le volume.

- **ID du volume distant**

  Identifiant du volume sur le cluster distant.

- **Nom du volume distant**

  Nom donné au volume distant lors de sa création.

Messages de couplage de volume

Vous pouvez consulter les messages de jumelage de volumes pendant le processus de jumelage initial depuis la page « Paires de volumes » sous l'onglet « Protection des données ». Ces messages peuvent s'afficher à la fois sur la source et sur la cible de la paire dans la vue de liste des volumes répliqués.

- **PauseDéconnecté**

  Les appels de procédure distante (RPC) de réplication ou de synchronisation de la source ont expiré. La connexion au cluster distant a été perdue. Vérifiez les connexions réseau au cluster.

- **Reprise de la connexion**

  La synchronisation de la réplication distante est maintenant active. Début du processus de synchronisation et attente des données.

- **Reprise de la synchronisation RR**

  Une copie unique des métadonnées du volume est effectuée sur le cluster apparié.

- **Reprise de la synchronisation locale**

  Une copie en double hélice des métadonnées du volume est en cours de création pour le cluster apparié.

- **Reprise du transfert de données**

  Le transfert de données a repris.

- **Actif**

  Les volumes sont appariés et les données sont envoyées de la source au volume cible, et les données sont synchronisées.

- **Inactif**

  Aucune activité de réplication n'est en cours.

Avertissements de couplage de volume

La page « Paires de volumes » de l'onglet « Protection des données » affiche ces messages après l'appairage des volumes. Ces messages peuvent s'afficher à la fois sur la source et sur la cible de la paire (sauf indication contraire) dans la vue de liste des volumes répliqués.

- **PausedClusterFull**

  Le cluster cible étant plein, la réplication source et le transfert de données en masse ne peuvent pas avoir lieu. Le message s'affiche uniquement sur le périphérique source de la paire.

- **PausedExceededMaxSnapshotCount**

  Le volume cible possède déjà le nombre maximal d'instantanés et ne peut pas répliquer d'instantanés supplémentaires.

- **Manuel en pause**

  Le volume local a été mis en pause manuellement. Il faut la réactiver avant que la réplication ne reprenne.

- **Télécommande manuelle en pause**

  Le volume de la télécommande est en mode pause manuelle. Une intervention manuelle est nécessaire pour réactiver le volume distant avant que la réplication ne reprenne.

- **Pause - Configuration incorrecte**

  En attente d'une source et d'une cible actives. Intervention manuelle requise pour reprendre la réplication.

- **QoS en pause**

  La qualité de service cible n'a pas pu supporter les E/S entrantes. La réplication reprend automatiquement. Le message s'affiche uniquement sur le périphérique source de la paire.

- **Lien lent en pause**

  Lien lent détecté, réplication arrêtée. La réplication reprend automatiquement. Le message s'affiche uniquement sur le périphérique source de la paire.

- **Incompatibilité de taille de volume en pause**

  Le volume cible n'est pas de la même taille que le volume source.

- **CopieX en pause**

  Une commande SCSI XCOPY est émise vers un volume source. La commande doit s'exécuter complètement avant que la réplication puisse reprendre. Le message s'affiche uniquement sur le périphérique source de la paire.

- **Arrêt dû à une mauvaise configuration**

  Une erreur de configuration permanente a été détectée. Le volume distant a été purgé ou dissocié. Aucune mesure corrective n'est possible ; un nouveau jumelage doit être établi.

Utiliser la réplication SnapMirror entre les clusters Element et ONTAP (interface utilisateur Element)

Utiliser la réplication SnapMirror entre les clusters Element et ONTAP (interface utilisateur Element)

Vous pouvez créer des relations SnapMirror à partir de l'onglet Protection des données

de l’interface utilisateur NetApp Element . La fonctionnalité SnapMirror doit être activée pour que cela s’affiche dans l’interface utilisateur.

Le protocole IPv6 n’est pas pris en charge pour la réplication SnapMirror entre le logiciel NetApp Element et les clusters ONTAP .

"Vidéo NetApp : SnapMirror pour NetApp HCI et Element Software"

Les systèmes exécutant le logiciel NetApp Element prennent en charge la fonctionnalité SnapMirror pour copier et restaurer des copies Snapshot avec les systèmes NetApp ONTAP . La principale raison d’utiliser cette technologie est la reprise après sinistre de NetApp HCI vers ONTAP. Les points de terminaison incluent ONTAP, ONTAP Select et Cloud Volumes ONTAP. Voir TR-4641 Protection des données NetApp HCI .

"Rapport technique NetApp 4641 : Protection des données NetApp HCI"

Trouver plus d’informations

- "Construisez votre infrastructure de données avec NetApp HCI, ONTAP et l’infrastructure convergée"
- "Réplication entre NetApp Element Software et ONTAP (interface de ligne de commande ONTAP)"

Présentation de SnapMirror

Les systèmes exécutant le logiciel NetApp Element prennent en charge la fonctionnalité SnapMirror pour copier et restaurer les instantanés avec les systèmes NetApp ONTAP .

Les systèmes exécutant Element peuvent communiquer directement avec SnapMirror sur les systèmes ONTAP 9.3 ou supérieurs. L’API NetApp Element fournit des méthodes permettant d’activer la fonctionnalité SnapMirror sur les clusters, les volumes et les snapshots. De plus, l’interface utilisateur d’Element inclut toutes les fonctionnalités nécessaires pour gérer les relations SnapMirror entre le logiciel Element et les systèmes ONTAP .

Vous pouvez répliquer des volumes d’origine ONTAP vers des volumes Element dans des cas d’utilisation spécifiques, mais avec des fonctionnalités limitées. Pour plus d’informations, voir "Réplication entre le logiciel Element et ONTAP (interface de ligne de commande ONTAP)".

Activez SnapMirror sur le cluster

Vous devez activer manuellement la fonctionnalité SnapMirror au niveau du cluster via l’interface utilisateur de NetApp Element . La fonctionnalité SnapMirror est désactivée par défaut sur le système et n’est pas activée automatiquement lors d’une nouvelle installation ou d’une mise à niveau. L’activation de la fonctionnalité SnapMirror est une tâche de configuration ponctuelle.

SnapMirror ne peut être activé que pour les clusters exécutant le logiciel Element utilisé conjointement avec des volumes sur un système NetApp ONTAP . Vous ne devez activer la fonctionnalité SnapMirror que si votre cluster est connecté pour être utilisé avec des volumes NetApp ONTAP .

Ce dont vous aurez besoin

Le cluster de stockage doit exécuter le logiciel NetApp Element .

Étapes

1. Cliquez sur **Clusters** > **Paramètres**.

2. Trouvez les paramètres spécifiques au cluster pour SnapMirror.
3. Cliquez sur **Activer SnapMirror**.

> L'activation de la fonctionnalité SnapMirror modifie de façon permanente la configuration du logiciel Element. Vous pouvez désactiver la fonction SnapMirror et restaurer les paramètres par défaut uniquement en restaurant le cluster à son image d'usine.

4. Cliquez sur **Oui** pour confirmer la modification de la configuration de SnapMirror .

Activez SnapMirror sur le volume

Vous devez activer SnapMirror sur le volume dans l'interface utilisateur Element. Cela permet la réplication des données vers des volumes ONTAP spécifiés. Il s'agit de l'autorisation de l'administrateur du cluster exécutant le logiciel NetApp Element pour que SnapMirror puisse contrôler un volume.

Ce dont vous aurez besoin

- Vous avez activé SnapMirror dans l'interface utilisateur Element pour le cluster.
- Un point de terminaison SnapMirror est disponible.
- Le volume doit avoir une taille de bloc de 512 e.
- Le volume ne participe pas à la réplication à distance.
- Le type d'accès au volume n'est pas une cible de réplication.

> Vous pouvez également définir cette propriété lors de la création ou du clonage d'un volume.

Étapes

1. Cliquez sur **Gestion** > **Volumes**.
2. Cliquez sur l'icône **Actions** correspondant au volume pour lequel vous souhaitez activer SnapMirror .
3. Dans le menu qui s'affiche, sélectionnez **Modifier**.
4. Dans la boîte de dialogue **Modifier le volume**, cochez la case **Activer SnapMirror**.
5. Cliquez sur **Enregistrer les modifications**.

Créer un point de terminaison SnapMirror

Vous devez créer un point de terminaison SnapMirror dans l'interface utilisateur de NetApp Element avant de pouvoir créer une relation.

Un point de terminaison SnapMirror est un cluster ONTAP qui sert de cible de réplication pour un cluster exécutant le logiciel Element. Avant de créer une relation SnapMirror , vous devez d'abord créer un point de terminaison SnapMirror .

Vous pouvez créer et gérer jusqu'à quatre points de terminaison SnapMirror sur un cluster de stockage exécutant le logiciel Element.

Si un point de terminaison existant a été créé à l'origine à l'aide de l'API et que les informations d'identification n'ont pas été enregistrées, vous pouvez voir le point de terminaison dans l'interface utilisateur d'Element et vérifier son existence, mais il ne peut pas être géré à l'aide de l'interface utilisateur d'Element. Ce point de terminaison ne peut alors être géré qu'à l'aide de l'API Element.

Pour plus de détails sur les méthodes API, consultez "Gérez le stockage avec l'API Element".

Ce dont vous aurez besoin

- Vous auriez dû activer SnapMirror dans l'interface utilisateur Element pour le cluster de stockage.
- Vous connaissez les identifiants ONTAP pour le point de terminaison.

Étapes

1. Cliquez sur **Protection des données** > *Points de terminaison SnapMirror *.
2. Cliquez sur **Créer un point de terminaison**.
3. Dans la boîte de dialogue **Créer un nouveau point de terminaison**, saisissez l'adresse IP de gestion du cluster du système ONTAP .
4. Saisissez les identifiants de l'administrateur ONTAP associés au point de terminaison.
5. Consultez les détails supplémentaires :
   - LIF : Liste les interfaces logiques inter-clusters ONTAP utilisées pour communiquer avec Element.
   - Statut : Affiche l'état actuel du point de terminaison SnapMirror . Les valeurs possibles sont : connecté, déconnecté et non géré.
6. Cliquez sur **Créer un point de terminaison**.

Créer une relation SnapMirror

Vous devez créer une relation SnapMirror dans l'interface utilisateur de NetApp Element .

Lorsqu'un volume n'est pas encore activé pour SnapMirror et que vous choisissez de créer une relation à partir de l'interface utilisateur Element, SnapMirror est automatiquement activé sur ce volume.

Ce dont vous aurez besoin

SnapMirror est activé sur le volume.

Étapes

1. Cliquez sur **Gestion** > **Volumes**.
2. Cliquez sur l'icône **Actions** pour le volume qui doit faire partie de la relation.
3. Cliquez sur *Créer une relation SnapMirror *.
4. Dans la boîte de dialogue **Créer une relation SnapMirror *, sélectionnez un point de terminaison dans la liste *Point de terminaison**.
5. Indiquez si la relation sera créée à l'aide d'un nouveau volume ONTAP ou d'un volume ONTAP existant.
6. Pour créer un nouveau volume ONTAP dans l'interface utilisateur d'Element, cliquez sur **Créer un nouveau volume**.
   a. Sélectionnez la **machine virtuelle de stockage** pour cette relation.

b. Sélectionnez **Agrégat** dans la liste déroulante.

c. Dans le champ **Suffixe du nom du volume**, saisissez un suffixe.

> Le système détecte le nom du volume source et le copie dans le champ **Nom du volume**. Le suffixe que vous saisissez s'ajoute au nom.

d. Cliquez sur **Créer un volume de destination**.

7. Pour utiliser un volume ONTAP existant, cliquez sur **Utiliser un volume existant**.
   a. Sélectionnez la **machine virtuelle de stockage** pour cette relation.
   b. Sélectionnez le volume qui sera la destination de cette nouvelle relation.
8. Dans la section **Détails de la relation**, sélectionnez une police d'assurance. Si la politique sélectionnée comporte des règles de conservation, le tableau des règles affiche les règles et les étiquettes associées.
9. **Facultatif** : Sélectionnez un horaire.

   Cela détermine la fréquence à laquelle la relation crée des copies.

10. **Facultatif** : Dans le champ **Limiter la bande passante à**, saisissez la quantité maximale de bande passante pouvant être consommée par les transferts de données associés à cette relation.
11. Consultez les détails supplémentaires :
    - **État** : État actuel de la relation du volume de destination. Les valeurs possibles sont :
      - non initialisé : le volume de destination n'a pas été initialisé.
      - snapmirrored : Le volume de destination a été initialisé et est prêt à recevoir les mises à jour SnapMirror .
      - interrompu : Le volume de destination est en lecture/écriture et des instantanés sont présents.
    - **Statut** : État actuel de la relation. Les valeurs possibles sont : inactif, transfert, vérification, mise en veille, mise en veille, en file d'attente, préparation, finalisation, abandon et rupture.
    - **Délai de latence** : Le temps, en secondes, pendant lequel le système de destination est en retard par rapport au système source. Le délai de latence ne doit pas dépasser l'intervalle de planification des transferts.
    - **Limite de bande passante** : Quantité maximale de bande passante pouvant être consommée par les transferts de données associés à cette relation.
    - **Dernier transfert** : Horodatage du dernier instantané transféré. Cliquez ici pour plus d'informations.
    - **Nom de la stratégie** : Le nom de la stratégie ONTAP SnapMirror pour la relation.
    - **Type de stratégie** : Type de stratégie ONTAP SnapMirror sélectionnée pour la relation. Les valeurs possibles sont :
      - miroir asynchrone
      - coffre-fort miroir
    - **Nom de la planification** : Nom de la planification préexistante sur le système ONTAP sélectionné pour cette relation.
12. Pour ne pas initialiser à ce stade, assurez-vous que la case **Initialiser** n'est pas cochée.

L'initialisation peut prendre du temps. Vous pourriez envisager de lancer cela pendant les heures creuses. L'initialisation effectue un transfert de base ; elle crée une copie instantanée du volume source, puis transfère cette copie et tous les blocs de données auxquels elle fait référence vers le volume de destination. Vous pouvez initialiser manuellement ou utiliser une planification pour démarrer le processus d'initialisation (et les mises à jour ultérieures) selon la planification.

13. Cliquez sur **Créer une relation**.
14. Cliquez sur **Protection des données** > *Relations SnapMirror * pour afficher cette nouvelle relation SnapMirror .

Actions relationnelles SnapMirror

Vous pouvez configurer une relation depuis la page Relations SnapMirror de l'onglet Protection des données. Les options accessibles via l'icône Actions sont décrites ici.

- **Modifier** : Modifie la politique ou le calendrier utilisé pour la relation.
- **Supprimer** : Supprime la relation SnapMirror . Cette fonction ne supprime pas le volume de destination.
- **Initialisation** : Effectue le premier transfert initial de données de référence pour établir une nouvelle relation.
- **Mise à jour** : Effectue une mise à jour à la demande de la relation, en répliquant vers la destination toutes les nouvelles données et les copies Snapshot incluses depuis la dernière mise à jour.
- **Quiesce** : Empêche toute mise à jour ultérieure d'une relation.
- **Reprendre** : Reprend une relation qui était en sommeil.
- **Pause** : Permet de lire et d'écrire sur le volume de destination et interrompt tous les transferts en cours et futurs. Vérifiez que les clients n'utilisent pas le volume source d'origine, car l'opération de resynchronisation inverse rend le volume source d'origine en lecture seule.
- **Resynchronisation** : Rétablit une relation interrompue dans la même direction qu'avant la rupture.
- **Resynchronisation inverse** : Automatise les étapes nécessaires pour créer et initialiser une nouvelle relation dans le sens inverse. Cela n'est possible que si la relation existante est rompue. Cette opération ne supprimera pas la relation actuelle. Le volume source d'origine revient à la copie Snapshot commune la plus récente et se resynchronise avec la destination. Toutes les modifications apportées au volume source d'origine depuis la dernière mise à jour réussie de SnapMirror sont perdues. Toute modification apportée au volume de destination actuel, ou toute nouvelle donnée écrite dans celui-ci, est renvoyée au volume source d'origine.
- **Annuler** : Annule un transfert en cours. Si une mise à jour SnapMirror est émise pour une relation interrompue, la relation reprend avec le dernier transfert à partir du dernier point de contrôle de redémarrage créé avant l'interruption.

Étiquettes SnapMirror

Étiquettes SnapMirror

Une étiquette SnapMirror sert de marqueur pour le transfert d'un instantané spécifique selon les règles de conservation de la relation.

L'attribution d'une étiquette à un instantané le désigne comme cible pour la réplication SnapMirror . Le rôle de cette relation est de faire respecter les règles de transfert de données en sélectionnant l'instantané étiqueté

correspondant, en le copiant sur le volume de destination et en veillant à conserver le nombre correct de copies. Il s'agit de la politique visant à déterminer le nombre de documents à conserver et la durée de conservation. La politique peut comporter un nombre quelconque de règles et chaque règle possède une étiquette unique. Cette étiquette sert de lien entre l'instantané et la règle de conservation.

C'est l'étiquette SnapMirror qui indique quelle règle est appliquée à l'instantané, à l'instantané de groupe ou à la planification sélectionnés.

Ajouter des étiquettes SnapMirror aux instantanés

Les étiquettes SnapMirror spécifient la politique de conservation des instantanés sur le point de terminaison SnapMirror . Vous pouvez ajouter des étiquettes aux instantanés et regrouper les instantanés.

Vous pouvez consulter les étiquettes disponibles à partir d'une boîte de dialogue de relation SnapMirror existante ou du gestionnaire système NetApp ONTAP .

> Lorsque vous ajoutez une étiquette à un instantané de groupe, toutes les étiquettes existantes sur les instantanés individuels sont écrasées.

Ce dont vous aurez besoin

- SnapMirror est activé sur le cluster.
- L'étiquette que vous souhaitez ajouter existe déjà dans ONTAP.

Étapes

1. Cliquez sur **Protection des données** > **Instantanés** ou **Instantanés de groupe**.
2. Cliquez sur l'icône **Actions** de l'instantané ou de l'instantané de groupe auquel vous souhaitez ajouter une étiquette SnapMirror .
3. Dans la boîte de dialogue **Modifier l'instantané**, saisissez du texte dans le champ *Étiquette SnapMirror *. L'étiquette doit correspondre à une étiquette de règle dans la politique appliquée à la relation SnapMirror .
4. Cliquez sur **Enregistrer les modifications**.

Ajouter des étiquettes SnapMirror aux planifications de snapshots

Vous pouvez ajouter des étiquettes SnapMirror aux planifications de snapshots pour garantir l'application d'une stratégie SnapMirror . Vous pouvez consulter les étiquettes disponibles à partir d'une boîte de dialogue de relation SnapMirror existante ou du gestionnaire système NetAppONTAP.

Ce dont vous aurez besoin

- SnapMirror doit être activé au niveau du cluster.
- L'étiquette que vous souhaitez ajouter existe déjà dans ONTAP.

Étapes

1. Cliquez sur **Protection des données** > **Plannings**.
2. Ajoutez une étiquette SnapMirror à une planification de l'une des manières suivantes :

Option	Étapes
Création d'un nouvel horaire	a. Sélectionnez **Créer un planning**. b. Veuillez saisir tous les autres détails pertinents. c. Sélectionnez **Créer un planning**.
Modification du calendrier existant	a. Cliquez sur l'icône **Actions** de la planification à laquelle vous souhaitez ajouter une étiquette et sélectionnez **Modifier**. b. Dans la boîte de dialogue qui s'affiche, saisissez du texte dans le champ * Étiquette SnapMirror *. c. Sélectionnez **Enregistrer les modifications**.

Trouver plus d'informations

Créer un planning instantané

Reprise après sinistre à l'aide de SnapMirror

Reprise après sinistre à l'aide de SnapMirror

En cas de problème avec un volume ou un cluster exécutant le logiciel NetApp Element , utilisez la fonctionnalité SnapMirror pour rompre la relation et basculer vers le volume de destination.

Si le cluster d'origine est complètement défaillant ou n'existe plus, contactez le support NetApp pour obtenir de l'aide.

Effectuez un basculement à partir d'un cluster Element

Vous pouvez effectuer un basculement à partir du cluster Element pour rendre le volume de destination accessible en lecture/écriture aux hôtes du côté destination. Avant d'effectuer un basculement à partir du cluster Element, vous devez rompre la relation SnapMirror .

Utilisez l'interface utilisateur de NetApp Element pour effectuer le basculement. Si l'interface utilisateur Element n'est pas disponible, vous pouvez également utiliser ONTAP System Manager ou ONTAP CLI pour exécuter la commande de rupture de relation.

Ce dont vous aurez besoin

- Une relation SnapMirror existe et possède au moins un instantané valide sur le volume de destination.
- Vous devez basculer vers le volume de destination en raison d'une panne imprévue ou d'un événement planifié sur le site principal.

Étapes

1. Dans l'interface utilisateur d'Element, cliquez sur **Protection des données** > *Relations SnapMirror *.
2. Trouvez la relation avec le volume source que vous souhaitez basculer.
3. Cliquez sur l'icône **Actions**.

4. Cliquez sur **Pause**.
5. Confirmez l'action.

   Le volume sur le cluster de destination dispose désormais d'un accès en lecture-écriture et peut être monté sur les hôtes d'application pour reprendre les charges de travail de production. Toute réplication SnapMirror est interrompue suite à cette action. La relation est rompue.

Effectuer un retour à l'élément

Découvrez comment effectuer un retour à Element

Une fois le problème du côté principal résolu, vous devez resynchroniser le volume source d'origine et revenir au logiciel NetApp Element . Les étapes à suivre varient selon que le volume source d'origine existe toujours ou que vous deviez revenir à un volume nouvellement créé.

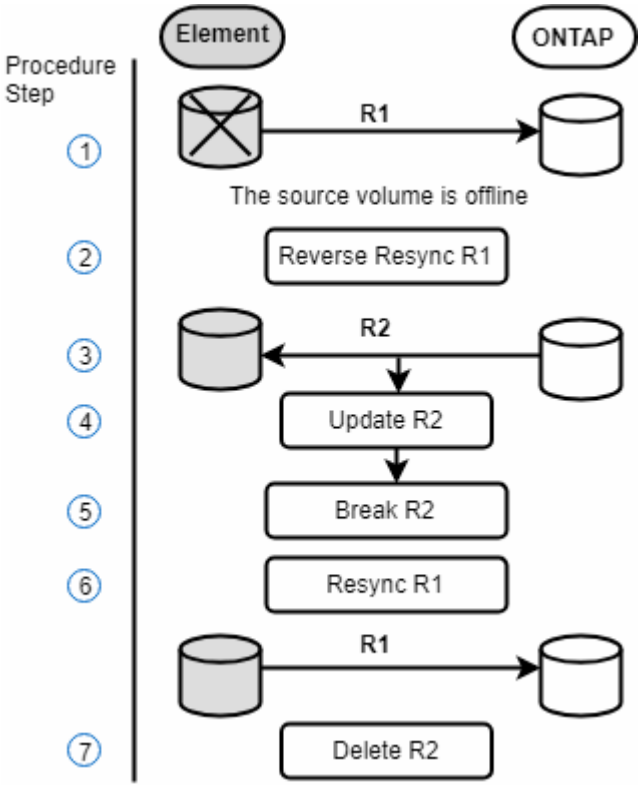
Scénarios de restauration SnapMirror

La fonctionnalité de reprise après sinistre de SnapMirror est illustrée par deux scénarios de restauration. Ces hypothèses supposent que la relation initiale a été rompue (rupture).

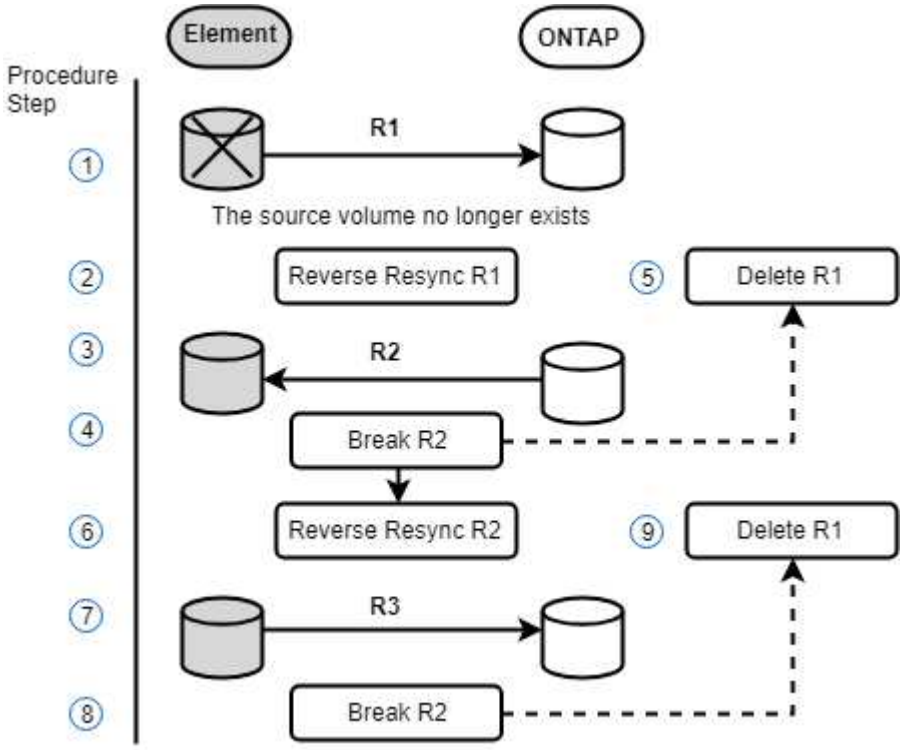
Les étapes des procédures correspondantes sont ajoutées à titre de référence.

> Dans les exemples présentés ici, R1 = la relation d'origine dans laquelle le cluster exécutant le logiciel NetApp Element est le volume source d'origine (Element) et ONTAP est le volume de destination d'origine (ONTAP). R2 et R3 représentent les relations inverses créées par l'opération de resynchronisation inverse.

L'image suivante illustre le scénario de retour en arrière lorsque le volume source existe toujours :



L’image suivante illustre le scénario de retour en arrière lorsque le volume source n’existe plus :



Trouver plus d’informations

- Effectuer une restauration lorsque le volume source existe toujours.
- Effectuer une restauration lorsque le volume source n’existe plus.
- Scénarios de restauration SnapMirror

Effectuer une restauration lorsque le volume source existe toujours.

Vous pouvez resynchroniser le volume source d’origine et revenir en arrière à l’aide de l’interface utilisateur de NetApp Element . Cette procédure s’applique aux scénarios où le volume source d’origine existe toujours.

1. Dans l’interface utilisateur de l’élément, recherchez la relation que vous avez interrompue pour effectuer le basculement.
2. Cliquez sur l’icône Actions, puis sur **Resynchronisation inversée**.
3. Confirmez l’action.

> L’opération de resynchronisation inversée crée une nouvelle relation dans laquelle les rôles des volumes source et de destination d’origine sont inversés (cela crée deux relations, la relation d’origine persistant). Toutes les nouvelles données provenant du volume de destination d’origine sont transférées vers le volume source d’origine dans le cadre de l’opération de resynchronisation inverse. Vous pouvez continuer à accéder aux données et à y écrire sur le volume actif côté destination, mais vous devrez déconnecter tous les hôtes du volume source et effectuer une mise à jour SnapMirror avant de rediriger vers le volume principal d’origine.

4. Cliquez sur l'icône Actions de la relation inverse que vous venez de créer, puis cliquez sur **Mettre à jour**.

   Maintenant que vous avez terminé la resynchronisation inverse et vérifié qu'aucune session active n'est connectée au volume de destination et que les données les plus récentes se trouvent sur le volume principal d'origine, vous pouvez effectuer les étapes suivantes pour terminer le retour en arrière et réactiver le volume principal d'origine :

5. Cliquez sur l'icône Actions de la relation inverse et cliquez sur **Interrompre**.
6. Cliquez sur l'icône Actions de la relation d'origine, puis sur **Resynchroniser**.

   Le volume principal d'origine peut désormais être monté pour reprendre les charges de travail de production sur ce volume. La réplication SnapMirror d'origine reprend selon la politique et la planification configurées pour la relation.

7. Après avoir confirmé que le statut de la relation d'origine est « `snapmirrored` », cliquez sur l'icône Actions de la relation inverse et cliquez sur **Supprimer**.

Trouver plus d'informations

Scénarios de restauration SnapMirror

Effectuer une restauration lorsque le volume source n'existe plus.

Vous pouvez resynchroniser le volume source d'origine et revenir en arrière à l'aide de l'interface utilisateur de NetApp Element . Cette section s'applique aux scénarios dans lesquels le volume source d'origine a été perdu, mais où le cluster d'origine est toujours intact. Pour obtenir des instructions sur la procédure de restauration vers un nouveau cluster, consultez la documentation sur le site d'assistance NetApp .

Ce dont vous aurez besoin

- Vous avez une relation de réplication interrompue entre les volumes Element et ONTAP .
- Le volume de données Element est irrémédiablement perdu.
- Le nom du volume d'origine apparaît comme INTROUVABLE.

Étapes

1. Dans l'interface utilisateur de l'élément, recherchez la relation que vous avez interrompue pour effectuer le basculement.

   Meilleure pratique : Prenez note de la politique de SnapMirror et des détails du calendrier de la relation initiale interrompue. Ces informations seront nécessaires lors de la recréation de la relation.

2. Cliquez sur l'icône **Actions** puis sur **Resynchronisation inversée**.
3. Confirmez l'action.

L'opération de resynchronisation inversée crée une nouvelle relation dans laquelle les rôles du volume source d'origine et du volume de destination sont inversés (cela crée deux relations, la relation d'origine persistant). Comme le volume d'origine n'existe plus, le système crée un nouveau volume Element portant le même nom et la même taille que le volume source d'origine. Le nouveau volume se voit attribuer une stratégie QoS par défaut appelée sm-recovery et est associé à un compte par défaut appelé sm-recovery. Vous devrez modifier manuellement le compte et la politique QoS pour tous les volumes créés par SnapMirror afin de remplacer les volumes sources d'origine qui ont été détruits.

Les données de la dernière capture instantanée sont transférées vers le nouveau volume dans le cadre de l'opération de resynchronisation inverse. Vous pouvez continuer à accéder aux données et à y écrire sur le volume actif côté destination, mais vous devrez déconnecter tous les hôtes du volume actif et effectuer une mise à jour SnapMirror avant de rétablir la relation principale d'origine ultérieurement. Une fois la resynchronisation inverse terminée et après avoir vérifié qu'aucune session active n'est connectée au volume de destination et que les données les plus récentes se trouvent sur le volume principal d'origine, poursuivez avec les étapes suivantes pour terminer le retour en arrière et réactiver le volume principal d'origine :

4. Cliquez sur l'icône **Actions** de la relation inverse créée lors de l'opération de resynchronisation inverse, puis cliquez sur **Interrompre**.
5. Cliquez sur l'icône **Actions** de la relation d'origine, dans laquelle le volume source n'existe pas, puis cliquez sur **Supprimer**.
6. Cliquez sur l'icône **Actions** de la relation inverse que vous avez rompue à l'étape 4, puis cliquez sur **Resynchronisation inverse**.
7. Cela inverse la source et la destination et aboutit à une relation avec la même source de volume et la même destination de volume que la relation d'origine.
8. Cliquez sur l'icône **Actions** puis sur **Modifier** pour mettre à jour cette relation avec la politique QoS et les paramètres de planification d'origine que vous avez notés.
9. Vous pouvez maintenant supprimer en toute sécurité la relation inverse que vous avez inversée et resynchronisée à l'étape 6.

Trouver plus d'informations

Scénarios de restauration SnapMirror

Effectuez un transfert ou une migration ponctuelle d' ONTAP vers Element.

En règle générale, lorsque vous utilisez SnapMirror pour la reprise après sinistre d'un cluster de stockage SolidFire exécutant le logiciel NetApp Element vers le logiciel ONTAP , Element est la source et ONTAP la destination. Cependant, dans certains cas, le système de stockage ONTAP peut servir de source et Element de destination.

- Deux scénarios sont possibles :
  - Il n'existe aucune relation antérieure en matière de reprise après sinistre. Suivez toutes les étapes de cette procédure.
  - Il existe bien une relation de reprise après sinistre antérieure, mais pas entre les volumes utilisés pour cette atténuation. Dans ce cas, suivez uniquement les étapes 3 et 4 ci-dessous.

Ce dont vous aurez besoin

- Le nœud de destination de l'élément doit avoir été rendu accessible à ONTAP.
- Le volume Element doit avoir été activé pour la réplication SnapMirror .

Vous devez spécifier le chemin de destination de l'élément sous la forme hostip:/lun/<id_number>, où lun est la chaîne de caractères "lun" et id_number est l'ID du volume de l'élément.

Étapes

1. À l'aide d' ONTAP, créez la relation avec le cluster Element :

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume
-destination-path hostip:/lun/name -type XDP -schedule schedule -policy
    policy
```

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

2. Vérifiez que la relation SnapMirror a été créée à l'aide de la commande ONTAP snapmirror show.

   Consultez la documentation ONTAP pour obtenir des informations sur la création d'une relation de réplication et la page de manuel ONTAP pour connaître la syntaxe complète des commandes.

3. En utilisant le `ElementCreateVolume` API, créez le volume cible et définissez le mode d'accès au volume cible sur SnapMirror:

   Créez un volume Element à l'aide de l'API Element.

```
{
   "method": "CreateVolume",
   "params": {
        "name": "SMTargetVolumeTest2",
        "accountID": 1,
        "totalSize": 100000000000,
        "enable512e": true,
        "attributes": {},
        "qosPolicyID": 1,
        "enableSnapMirrorReplication": true,
        "access": "snapMirrorTarget"
    },
    "id": 1
}
```

4. Initialisez la relation de réplication à l'aide d' ONTAP `snapmirror initialize` commande:

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

Réplication entre le logiciel NetApp Element et ONTAP (interface de ligne de commande ONTAP)

Vue d'ensemble de la réplication entre le logiciel NetApp Element et ONTAP (interface de ligne de commande ONTAP)

Vous pouvez garantir la continuité des activités sur un système Element en utilisant SnapMirror pour répliquer des copies instantanées d'un volume Element vers une destination ONTAP . En cas de sinistre sur le site Element, vous pouvez fournir des données aux clients à partir du système ONTAP , puis réactiver le système Element une fois le service rétabli.

À partir d' ONTAP 9.4, vous pouvez répliquer des copies instantanées d'un LUN créé sur un nœud ONTAP vers un système Element. Vous avez peut-être créé un LUN lors d'une panne sur le site Element, ou vous utilisez peut-être un LUN pour migrer des données d' ONTAP vers le logiciel Element.

Vous devriez utiliser la sauvegarde Element to ONTAP si les conditions suivantes s'appliquent :

- Vous souhaitez utiliser les meilleures pratiques, et non explorer toutes les options disponibles.
- Vous souhaitez utiliser l'interface de ligne de commande (CLI) ONTAP , et non System Manager ou un outil de script automatisé.
- Vous utilisez iSCSI pour fournir des données aux clients.

Si vous avez besoin d'informations supplémentaires sur la configuration ou le concept de SnapMirror , consultez"Aperçu de la protection des données" .

À propos de la réplication entre Element et ONTAP

À partir d' ONTAP 9.3, vous pouvez utiliser SnapMirror pour répliquer des copies instantanées d'un volume Element vers une destination ONTAP . En cas de sinistre sur le site Element, vous pouvez fournir des données aux clients à partir du système ONTAP , puis réactiver le volume source Element une fois le service rétabli.

À partir d' ONTAP 9.4, vous pouvez répliquer des copies instantanées d'un LUN créé sur un nœud ONTAP vers un système Element. Vous avez peut-être créé un LUN lors d'une panne sur le site Element, ou vous utilisez peut-être un LUN pour migrer des données d' ONTAP vers le logiciel Element.

Types de relations de protection des données

SnapMirror propose deux types de relations de protection des données. Pour chaque type, SnapMirror crée une copie instantanée du volume source Element avant d'initialiser ou de mettre à jour la relation :

- Dans une relation de protection des données de *reprise après sinistre (DR)*, le volume de destination contient uniquement la copie instantanée créée par SnapMirror, à partir de laquelle vous pouvez continuer à diffuser des données en cas de catastrophe sur le site principal.
- Dans une relation de protection des données à *conservation à long terme*, le volume de destination contient des copies instantanées à un instant donné créées par le logiciel Element, ainsi que la copie

instantanée créée par SnapMirror. Vous pourriez par exemple souhaiter conserver des copies mensuelles instantanées créées sur une période de 20 ans.

Politiques par défaut

Lors de la première utilisation de SnapMirror, un transfert de base est effectué du volume source vers le volume de destination. La politique *SnapMirror* définit le contenu de la configuration de base et toutes les mises à jour.

Vous pouvez utiliser une politique par défaut ou personnalisée lorsque vous créez une relation de protection des données. Le *type de politique* détermine quelles copies d'instantané inclure et combien de copies conserver.

Le tableau ci-dessous présente les politiques par défaut. Utilisez le `MirrorLatest` politique visant à créer une relation de gestion de sinistres traditionnelle. Utilisez le `MirrorAndVault` ou `Unified7year` politique visant à créer une relation de réplication unifiée, dans laquelle la reprise après sinistre et la conservation à long terme sont configurées sur le même volume de destination.

Politique	Type de police	Comportement de mise à jour
MirrorLatest	miroir asynchrone	Transférez la copie instantanée créée par SnapMirror.
Miroir et coffre-fort	coffre-miroir	Transférez la copie instantanée créée par SnapMirror et toutes les copies instantanées moins récentes effectuées depuis la dernière mise à jour, à condition qu'elles portent les étiquettes SnapMirror « `daily` » ou « `weekly` ».
Unified7year	coffre-miroir	Transférez la copie instantanée créée par SnapMirror et toutes les copies instantanées moins récentes effectuées depuis la dernière mise à jour, à condition qu'elles portent les étiquettes SnapMirror « `daily` », « `weekly` » ou « `monthly` ».

Pour obtenir des informations complètes sur les politiques SnapMirror , y compris des conseils sur la politique à utiliser, consultez"Aperçu de la protection des données" .

Comprendre les étiquettes SnapMirror

Chaque politique de type « mirror-vault » doit comporter une règle spécifiant quelles copies d'instantané répliquer. La règle « `daily` », par exemple, indique que seules les copies instantanées auxquelles est attribuée l'étiquette SnapMirror « `daily` » doivent être répliquées. Vous attribuez l'étiquette SnapMirror lors de la configuration des copies d'instantanés Element.

Réplication d'un cluster source Element vers un cluster de destination ONTAP

Vous pouvez utiliser SnapMirror pour répliquer des copies instantanées d'un volume Element vers un système de destination ONTAP . En cas de sinistre sur le site Element, vous pouvez fournir des données aux clients à partir du système ONTAP , puis réactiver le volume source Element une fois le service rétabli.

Un volume Element est à peu près équivalent à un LUN ONTAP . SnapMirror crée un LUN portant le nom du volume Element lorsqu'une relation de protection des données entre le logiciel Element et ONTAP est

initialisée. SnapMirror réplique les données sur un LUN existant si celui-ci répond aux exigences de réplication Element vers ONTAP .

Les règles de réplication sont les suivantes :

- Un volume ONTAP ne peut contenir que des données provenant d'un seul volume Element.
- Vous ne pouvez pas répliquer les données d'un volume ONTAP vers plusieurs volumes Element.

Réplication d'un cluster source ONTAP vers un cluster de destination Element

À partir d' ONTAP 9.4, vous pouvez répliquer des copies instantanées d'un LUN créé sur un système ONTAP vers un volume Element :

- Si une relation SnapMirror existe déjà entre une source Element et une destination ONTAP , un LUN créé pendant que vous servez des données à partir de la destination est automatiquement répliqué lorsque la source est réactivée.
- Sinon, vous devez créer et initialiser une relation SnapMirror entre le cluster source ONTAP et le cluster de destination Element.

Les règles de réplication sont les suivantes :

- La relation de réplication doit avoir une politique de type « `async-mirror` ».

  Les politiques de type « `mirror-vault` » ne sont pas prises en charge.

- Seuls les LUN iSCSI sont pris en charge.
- Vous ne pouvez pas répliquer plus d'un LUN d'un volume ONTAP vers un volume Element.
- Vous ne pouvez pas répliquer un LUN d'un volume ONTAP vers plusieurs volumes Element.

Prérequis

Vous devez avoir effectué les tâches suivantes avant de configurer une relation de protection des données entre Element et ONTAP:

- Le cluster Element doit exécuter la version 10.1 ou ultérieure du logiciel NetApp Element .
- Le cluster ONTAP doit exécuter ONTAP 9.3 ou une version ultérieure.
- SnapMirror doit avoir été autorisé sur le cluster ONTAP .
- Vous devez avoir configuré sur les clusters Element et ONTAP des volumes suffisamment grands pour gérer les transferts de données prévus.
- Si vous utilisez le type de stratégie « `mirror-vault` », une étiquette SnapMirror doit avoir été configurée pour que les copies d'instantané Element soient répliquées.

  Vous ne pouvez effectuer cette tâche que dans le"Interface utilisateur Web du logiciel Element" ou en utilisant le"Méthodes API" .

- Vous devez vous être assuré que le port 5010 est disponible.
- Si vous prévoyez de devoir déplacer un volume de destination, vous devez vous assurer qu'une connectivité maillée complète existe entre la source et la destination. Chaque nœud du cluster source Element doit pouvoir communiquer avec chaque nœud du cluster de destination ONTAP .

Détails de l’assistance

Le tableau suivant présente les détails de prise en charge de la sauvegarde Element vers ONTAP .

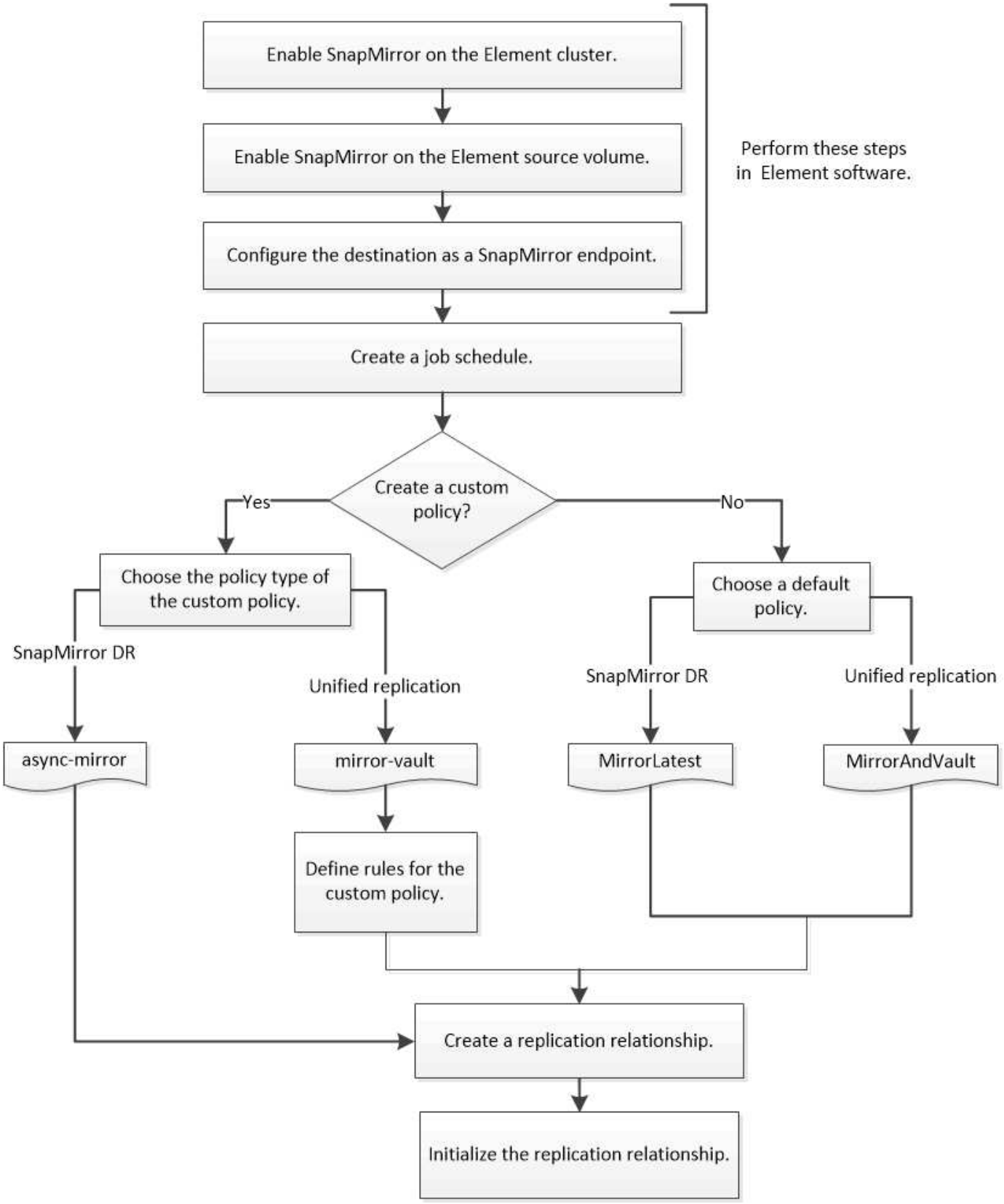
Ressource ou fonctionnalité	Détails de l’assistance
SnapMirror	• La fonction de restauration SnapMirror n’est pas prise en charge. • Le `MirrorAllSnapshots` et `XDPDefault` Les politiques ne sont pas prises en charge. • Le type de stratégie « `vault` » n’est pas pris en charge. • La règle système « `all_source_snapshots` » n’est pas prise en charge. • Le type de stratégie « `mirror-vault` » est pris en charge uniquement pour la réplication du logiciel Element vers ONTAP. Utilisez « `async-mirror` » pour la réplication d' ONTAP vers le logiciel Element. • Le `-schedule` et `-prefix` options pour `snapmirror policy add-rule` ne sont pas pris en charge. • Le `-preserve` et `-quick-resync` options pour `snapmirror resync` ne sont pas pris en charge. • L’efficacité du stockage n’est pas préservée. • Les déploiements de protection des données en mode Fan-out et en cascade ne sont pas pris en charge.
ONTAP	• ONTAP Select est pris en charge à partir d' ONTAP 9.4 et Element 10.3. • Cloud Volumes ONTAP est pris en charge à partir d' ONTAP 9.5 et Element 11.0.
Élément	• La limite de taille du volume est de 8 Tio. • La taille des blocs de volume doit être de 512 octets. La taille de bloc de 4 Ko n’est pas prise en charge. • La taille du volume doit être un multiple de 1 Mio. • Les attributs de volume ne sont pas conservés. • Le nombre maximal de copies d’instantané à répliquer est de 30.
Réseau	• Une seule connexion TCP est autorisée par transfert. • Le nœud Element doit être spécifié sous forme d’adresse IP. La résolution de noms d’hôtes DNS n’est pas prise en charge. • Les espaces IP ne sont pas pris en charge.
SnapLock	Les volumes SnapLock ne sont pas pris en charge.
FlexGroup	Les volumes FlexGroup ne sont pas pris en charge.
SVM DR	Les volumes ONTAP dans une configuration SVM DR ne sont pas pris en charge.

MetroCluster	Les volumes ONTAP dans une configuration MetroCluster ne sont pas pris en charge.

Flux de travail pour la réplication entre Element et ONTAP

Que vous répliquiez des données d'Element vers ONTAP ou d' ONTAP vers Element, vous devez configurer une planification de tâches, spécifier une stratégie, puis créer et initialiser la relation. Vous pouvez utiliser une stratégie par défaut ou personnalisée.

Le flux de travail suppose que vous avez effectué les tâches préalables énumérées dans"Prérequis" . Pour obtenir des informations complètes sur les politiques SnapMirror , y compris des conseils sur la politique à utiliser, consultez"Aperçu de la protection des données" .



Activer SnapMirror dans le logiciel Element

Activez SnapMirror sur le cluster Element.

Vous devez activer SnapMirror sur le cluster Element avant de pouvoir créer une relation

de réplication. Vous pouvez uniquement effectuer cette tâche dans l'interface utilisateur Web du logiciel Element ou en utilisant le "Méthode API".

Avant de commencer

- Le cluster Element doit exécuter la version 10.1 ou ultérieure du logiciel NetApp Element .
- SnapMirror ne peut être activé que pour les clusters Element utilisés avec des volumes NetApp ONTAP .

À propos de cette tâche

Le système Element est livré avec SnapMirror désactivé par défaut. SnapMirror n'est pas activé automatiquement lors d'une nouvelle installation ou d'une mise à niveau.

Une fois activé, SnapMirror ne peut pas être désactivé. Vous ne pouvez désactiver la fonction SnapMirror et restaurer les paramètres par défaut qu'en rétablissant l'image d'usine du cluster.

Étapes

1. Cliquez sur **Clusters** > **Paramètres**.
2. Trouvez les paramètres spécifiques au cluster pour SnapMirror.
3. Cliquez sur **Activer SnapMirror**.

Activez SnapMirror sur le volume source Element.

Vous devez activer SnapMirror sur le volume source Element avant de pouvoir créer une relation de réplication. Vous pouvez uniquement effectuer cette tâche dans l'interface utilisateur Web du logiciel Element ou en utilisant le"Modifier le volume" et"Modifier les volumes" Méthodes API.

Avant de commencer

- Vous devez avoir activé SnapMirror sur le cluster Element.
- La taille des blocs de volume doit être de 512 octets.
- Le volume ne doit pas participer à la réplication à distance d'Element.
- Le type d'accès au volume ne doit pas être « `Cible de réplication` ».

À propos de cette tâche

La procédure ci-dessous suppose que le volume existe déjà. Vous pouvez également activer SnapMirror lors de la création ou du clonage d'un volume.

Étapes

1. Sélectionnez **Gestion** > **Volumes**.
2. Sélectionnez le bouton pour le volume.
3. Dans le menu déroulant, sélectionnez **Modifier**.
4. Dans la boîte de dialogue **Modifier le volume**, sélectionnez **Activer SnapMirror**.
5. Sélectionnez **Enregistrer les modifications**.

Créer un point de terminaison SnapMirror

Vous devez créer un point de terminaison SnapMirror avant de pouvoir créer une relation

de réplication. Vous pouvez uniquement effectuer cette tâche dans l'interface utilisateur Web du logiciel Element ou en utilisant le "Méthodes de l'API SnapMirror".

Avant de commencer

Vous devez avoir activé SnapMirror sur le cluster Element.

Étapes

1. Cliquez sur **Protection des données** > *Points de terminaison SnapMirror *.
2. Cliquez sur **Créer un point de terminaison**.
3. Dans la boîte de dialogue **Créer un nouveau point de terminaison**, saisissez l'adresse IP de gestion du cluster ONTAP .
4. Saisissez l'identifiant et le mot de passe de l'administrateur du cluster ONTAP .
5. Cliquez sur **Créer un point de terminaison**.

Configurer une relation de réplication

Créer une planification de tâche de réplication

Que vous répliquiez des données d'Element vers ONTAP ou d' ONTAP vers Element, vous devez configurer une planification de tâches, spécifier une stratégie, puis créer et initialiser la relation. Vous pouvez utiliser une stratégie par défaut ou personnalisée.

Vous pouvez utiliser le `job schedule cron create` commande permettant de créer une planification de tâche de réplication. La planification des tâches détermine à quel moment SnapMirror met automatiquement à jour la relation de protection des données à laquelle cette planification est associée.

À propos de cette tâche

Vous définissez un planning de travail lorsque vous créez une relation de protection des données. Si vous n'attribuez pas de calendrier de travail, vous devez mettre à jour la relation manuellement.

Étape

1. Créer un planning de travail :

   ```
   job schedule cron create -name job_name -month month -dayofweek day_of_week
   -day day_of_month -hour hour -minute minute
   ```

   Pour `-month` , `-dayofweek` , et `-hour` , vous pouvez spécifier `all` pour exécuter la tâche respectivement chaque mois, chaque jour de la semaine et chaque heure.

   À partir d' ONTAP 9.10.1, vous pouvez inclure le serveur virtuel dans votre planification des tâches :

   ```
   job schedule cron create -name job_name -vserver Vserver_name -month month
   -dayofweek day_of_week -day day_of_month -hour hour -minute minute
   ```

   L'exemple suivant crée une planification de tâches nommée `my_weekly` qui a lieu le samedi à 3h00 du matin :

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

Créer une politique de réplication personnalisée

Vous pouvez utiliser une stratégie par défaut ou personnalisée lors de la création d'une relation de réplication. Pour une politique de réplication unifiée personnalisée, vous devez définir une ou plusieurs *règles* qui déterminent quelles copies d'instantané sont transférées lors de l'initialisation et de la mise à jour.

Vous pouvez créer une stratégie de réplication personnalisée si la stratégie par défaut d'une relation ne convient pas. Vous pourriez par exemple vouloir compresser les données lors d'un transfert réseau, ou modifier le nombre de tentatives effectuées par SnapMirror pour transférer les copies d'instantané.

À propos de cette tâche

Le *type de politique* de la politique de réplication détermine le type de relation qu'elle prend en charge. Le tableau ci-dessous présente les types de polices disponibles.

Type de politique	Type de relation
miroir asynchrone	SnapMirror DR
coffre-miroir	Réplication unifiée

Étape

1. Créer une stratégie de réplication personnalisée :

   ```
   snapmirror policy create -vserver SVM -policy policy -type async-
   mirror|mirror-vault -comment comment -tries transfer_tries -transfer-priority
   low|normal -is-network-compression-enabled true|false
   ```

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   À partir d' ONTAP 9.5, vous pouvez spécifier la planification de création d'une planification de copie d'instantané commune pour les relations synchrones SnapMirror en utilisant `-common-snapshot -schedule` paramètre. Par défaut, la fréquence de copie des instantanés pour les relations synchrones SnapMirror est d'une heure. Vous pouvez spécifier une valeur comprise entre 30 minutes et deux heures pour la planification de la copie d'instantané pour les relations synchrones SnapMirror .

   L'exemple suivant crée une stratégie de réplication personnalisée pour SnapMirror DR qui active la compression réseau pour les transferts de données :

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_compressed -type async-mirror -comment "DR with network compression
   enabled" -is-network-compression-enabled true
   ```

   L'exemple suivant crée une stratégie de réplication personnalisée pour la réplication unifiée :

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy my_unified
-type mirror-vault
```

Après avoir terminé

Pour les types de politiques « `mirror-vault` », vous devez définir des règles qui déterminent quelles copies d'instantané sont transférées lors de l'initialisation et de la mise à jour.

Utilisez le `snapmirror policy show` commande permettant de vérifier que la politique SnapMirror a été créée. Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

Définir une règle pour une politique

Pour les politiques personnalisées de type « mirror-vault », vous devez définir au moins une règle qui détermine quelles copies d'instantané sont transférées lors de l'initialisation et de la mise à jour. Vous pouvez également définir des règles pour les politiques par défaut avec le type de politique « `mirror-vault` ».

À propos de cette tâche

Chaque politique de type « mirror-vault » doit comporter une règle spécifiant quelles copies d'instantané répliquer. La règle « bi-mensuelle », par exemple, indique que seules les copies instantanées auxquelles est attribuée l'étiquette SnapMirror « bi-mensuelle » doivent être répliquées. Vous attribuez l'étiquette SnapMirror lors de la configuration des copies d'instantanés Element.

Chaque type de politique est associé à une ou plusieurs règles définies par le système. Ces règles sont automatiquement attribuées à une politique lorsque vous spécifiez son type de politique. Le tableau ci-dessous présente les règles définies par le système.

Règle définie par le système	Utilisé dans les types de polices	Résultat
sm_créé	miroir asynchrone, coffre-fort miroir	Une copie instantanée créée par SnapMirror est transférée lors de l'initialisation et de la mise à jour.
tous les jours	coffre-miroir	De nouvelles copies instantanées de la source portant l'étiquette SnapMirror « `daily` » sont transférées lors de l'initialisation et de la mise à jour.
hebdomadaire	coffre-miroir	De nouvelles copies instantanées de la source portant l'étiquette SnapMirror « hebdomadaire » sont transférées lors de l'initialisation et de la mise à jour.

mensuel	coffre-miroir	De nouvelles copies instantanées de la source portant l'étiquette SnapMirror « mensuelle » sont transférées lors de l'initialisation et de la mise à jour.

Vous pouvez spécifier des règles supplémentaires selon vos besoins, pour les politiques par défaut ou personnalisées. Par exemple:

- Pour la valeur par défaut `MirrorAndVault` Dans le cadre de cette politique, vous pouvez créer une règle appelée « `bi-monthly` » pour faire correspondre les copies instantanées sur la source avec l'étiquette SnapMirror « `bi-monthly` ».
- Pour une politique personnalisée avec le type de politique « `mirror-vault` », vous pouvez créer une règle appelée « `bi-weekly` » pour faire correspondre les copies instantanées sur la source avec l'étiquette SnapMirror « `bi-weekly` ».

Étape

1. Définir une règle pour une politique :

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `bi-monthly` par défaut `MirrorAndVault` politique:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `bi-weekly` à la douane `my_snapvault` politique:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   L'exemple suivant ajoute une règle avec l'étiquette SnapMirror `app_consistent` à la douane `Sync` politique:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
   -snapmirror-label app_consistent -keep 1
   ```

   Vous pouvez ensuite répliquer des copies d'instantanés du cluster source qui correspondent à cette étiquette SnapMirror :

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Créer une relation de réplication

Créez une relation entre une source Element et une destination ONTAP .

La relation entre le volume source dans le stockage principal et le volume de destination dans le stockage secondaire est appelée *relation de protection des données*. Vous pouvez utiliser le `snapmirror create` commande permettant de créer une relation de protection des données d'une source Element vers une destination ONTAP , ou d'une source ONTAP vers une destination Element.

Vous pouvez utiliser SnapMirror pour répliquer des copies instantanées d'un volume Element vers un système de destination ONTAP . En cas de sinistre sur le site Element, vous pouvez fournir des données aux clients à partir du système ONTAP , puis réactiver le volume source Element une fois le service rétabli.

Avant de commencer

- Le nœud Element contenant le volume à répliquer doit avoir été rendu accessible à ONTAP.
- Le volume Element doit avoir été activé pour la réplication SnapMirror .
- Si vous utilisez le type de stratégie « `mirror-vault` », une étiquette SnapMirror doit avoir été configurée pour que les copies d'instantané Element soient répliquées.

> Vous ne pouvez effectuer cette tâche que dans le"Interface utilisateur Web du logiciel Element" ou en utilisant le"Méthodes API" .

À propos de cette tâche

Vous devez spécifier le chemin source de l'élément dans le formulaire `<hostip:>/lun/<name>` , où "lun" est la chaîne de caractères réelle "lun" et `name` est le nom du volume Element.

Un volume Element est à peu près équivalent à un LUN ONTAP . SnapMirror crée un LUN portant le nom du volume Element lorsqu'une relation de protection des données entre le logiciel Element et ONTAP est initialisée. SnapMirror réplique les données sur un LUN existant si celui-ci répond aux exigences de réplication du logiciel Element vers ONTAP.

Les règles de réplication sont les suivantes :

- Un volume ONTAP ne peut contenir que des données provenant d'un seul volume Element.
- Vous ne pouvez pas répliquer les données d'un volume ONTAP vers plusieurs volumes Element.

Dans ONTAP 9.3 et versions antérieures, un volume de destination peut contenir jusqu'à 251 copies d'instantané. Dans ONTAP 9.4 et versions ultérieures, un volume de destination peut contenir jusqu'à 1019 copies d'instantané.

Étape

1. À partir du cluster de destination, créez une relation de réplication d'une source Element vers une destination ONTAP :

```
snapmirror create -source-path <hostip:>/lun/<name> -destination-path
<SVM:volume>|<cluster://SVM/volume> -type XDP -schedule schedule -policy
<policy>
```

Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

L'exemple suivant crée une relation SnapMirror DR en utilisant la configuration par défaut. `MirrorLatest` politique:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorLatest
```

L'exemple suivant crée une relation de réplication unifiée à l'aide de la configuration par défaut. `MirrorAndVault` politique:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorAndVault
```

L'exemple suivant crée une relation de réplication unifiée à l'aide de `Unified7year` politique:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy Unified7year
```

L'exemple suivant crée une relation de réplication unifiée à l'aide de la configuration personnalisée `my_unified` politique:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy my_unified
```

Après avoir terminé

Utilisez le `snapmirror show` commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

Créez une relation entre une source ONTAP et une destination Element.

À partir d' ONTAP 9.4, vous pouvez utiliser SnapMirror pour répliquer des copies instantanées d'un LUN créé sur une source ONTAP vers une destination Element. Vous pourriez utiliser le LUN pour migrer des données d' ONTAP vers le logiciel Element.

Avant de commencer

- Le nœud de destination de l'élément doit avoir été rendu accessible à ONTAP.
- Le volume Element doit avoir été activé pour la réplication SnapMirror .

À propos de cette tâche

Vous devez spécifier le chemin de destination de l'élément dans le formulaire `<hostip:>/lun/<name>` , où "lun" est la chaîne de caractères réelle "lun" et `name` est le nom du volume Element.

Les règles de réplication sont les suivantes :

- La relation de réplication doit avoir une politique de type « `async-mirror` ».

  Vous pouvez utiliser une stratégie par défaut ou personnalisée.

- Seuls les LUN iSCSI sont pris en charge.
- Vous ne pouvez pas répliquer plus d'un LUN d'un volume ONTAP vers un volume Element.
- Vous ne pouvez pas répliquer un LUN d'un volume ONTAP vers plusieurs volumes Element.

Étape

1. Créez une relation de réplication d'une source ONTAP vers une destination Element :

   ```
   snapmirror create -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -type XDP -schedule schedule -policy
   <policy>
   ```

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   L'exemple suivant crée une relation SnapMirror DR en utilisant la configuration par défaut. `MirrorLatest` politique:

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy MirrorLatest
   ```

   L'exemple suivant crée une relation SnapMirror DR à l'aide de la configuration personnalisée. `my_mirror` politique:

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy my_mirror
   ```

Après avoir terminé

Utilisez le `snapmirror show` commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

Initialiser une relation de réplication

Pour tous les types de relations, l'initialisation effectue un *transfert de base* : elle crée une

copie instantanée du volume source, puis transfère cette copie et tous les blocs de données auxquels elle fait référence vers le volume de destination.

Avant de commencer

- Le nœud Element contenant le volume à répliquer doit avoir été rendu accessible à ONTAP.
- Le volume Element doit avoir été activé pour la réplication SnapMirror .
- Si vous utilisez le type de stratégie « `mirror-vault` », une étiquette SnapMirror doit avoir été configurée pour que les copies d'instantané Element soient répliquées.

Vous ne pouvez effectuer cette tâche que dans le"Interface utilisateur Web du logiciel Element" ou en utilisant le"Méthodes API" .

À propos de cette tâche

Vous devez spécifier le chemin source de l'élément dans le formulaire `<hostip:>/lun/<name>` , où "lun" est la chaîne de caractères réelle "lun" et *`name`* est le nom du volume Element.

L'initialisation peut prendre du temps. Il serait peut-être judicieux d'effectuer le transfert de base en dehors des heures de pointe.

Si l'initialisation d'une relation entre une source ONTAP et une destination Element échoue pour une raison quelconque, elle continuera d'échouer même après que vous ayez corrigé le problème (un nom de LUN invalide, par exemple). La solution de contournement est la suivante :

1. Supprimez la relation.
2. Supprimez le volume de destination Element.
3. Créez un nouveau volume de destination Element.
4. Créez et initialisez une nouvelle relation entre la source ONTAP et le volume de destination Element.

Étape

1. Initialiser une relation de réplication :

   ```
   snapmirror initialize -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume|cluster://SVM/volume>
   ```

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   L'exemple suivant initialise la relation entre le volume source `0005` à l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` sur `svm_backup` :

   ```
   cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Diffuser des données à partir d'un volume de destination SnapMirror DR

Rendre le volume de destination inscriptible

Lorsqu'un sinistre met hors service le site principal d'une relation de reprise après sinistre SnapMirror , vous pouvez diffuser des données à partir du volume de destination avec une interruption minimale. Vous pouvez réactiver le volume source une fois le service rétabli sur le site principal.

Vous devez rendre le volume de destination accessible en écriture avant de pouvoir diffuser des données de ce volume aux clients. Vous pouvez utiliser le `snapmirror quiesce` l'ordre d'arrêter les transferts programmés vers la destination, le `snapmirror abort` l'ordre d'arrêter les transferts en cours, et le `snapmirror break` commande permettant de rendre la destination accessible en écriture.

À propos de cette tâche

Vous devez spécifier le chemin source de l'élément dans le formulaire `<hostip:>/lun/<name>` , où "lun" est la chaîne de caractères réelle "lun" et `name` est le nom du volume Element.

Étapes

1. Arrêter les transferts programmés vers la destination :

   ```
   snapmirror quiesce -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   L'exemple suivant interrompt les transferts planifiés entre le volume source `0005` à l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` sur `svm_backup` :

   ```
   cluster_dst::> snapmirror quiesce -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

2. Interrompre les transferts en cours vers la destination :

   ```
   snapmirror abort -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   L'exemple suivant interrompt les transferts en cours entre le volume source et le volume source. `0005` à l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` sur `svm_backup` :

   ```
   cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

3. Rompre la relation avec SnapMirror DR :

   ```
   snapmirror break -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

L'exemple suivant rompt la relation entre le volume source `0005` à l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` sur `svm_backup` et le volume de destination `volA_dst` sur `svm_backup` :

```
cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

Configurez le volume de destination pour l'accès aux données

Après avoir rendu le volume de destination accessible en écriture, vous devez configurer le volume pour l'accès aux données. Les hôtes SAN peuvent accéder aux données du volume de destination jusqu'à ce que le volume source soit réactivé.

1. Associez l'élément LUN au groupe d'initiateurs approprié.
2. Créer des sessions iSCSI depuis les initiateurs hôtes SAN vers les LIF SAN.
3. Sur le client SAN, effectuez une nouvelle analyse du stockage pour détecter le LUN connecté.

Réactiver le volume source d'origine

Vous pouvez rétablir la relation de protection des données d'origine entre les volumes source et de destination lorsque vous n'avez plus besoin de diffuser de données depuis la destination.

À propos de cette tâche

La procédure ci-dessous suppose que la ligne de base du volume source d'origine est intacte. Si la ligne de base n'est pas intacte, vous devez créer et initialiser la relation entre le volume à partir duquel vous servez les données et le volume source d'origine avant d'effectuer la procédure.

Vous devez spécifier le chemin source de l'élément dans le formulaire `<hostip:>/lun/<name>` , où "lun" est la chaîne de caractères réelle "lun" et `name` est le nom du volume Element.

À partir d' ONTAP 9.4, les copies instantanées d'un LUN créées pendant que vous servez des données à partir de la destination ONTAP sont automatiquement répliquées lorsque la source Element est réactivée.

Les règles de réplication sont les suivantes :

- Seuls les LUN iSCSI sont pris en charge.
- Vous ne pouvez pas répliquer plus d'un LUN d'un volume ONTAP vers un volume Element.
- Vous ne pouvez pas répliquer un LUN d'un volume ONTAP vers plusieurs volumes Element.

Étapes

1. Supprimer la relation de protection des données d'origine :

   ```
   snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -policy <policy>
   ```

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

L'exemple suivant supprime la relation entre le volume source d'origine, `0005` à l'adresse IP 10.0.0.11 et le volume à partir duquel vous servez des données, `volA_dst` sur `svm_backup` :

```
cluster_dst::> snapmirror delete -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

2. Inverser la relation initiale de protection des données :

   ```
   snapmirror resync -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -policy <policy>
   ```

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Il serait peut-être préférable d'effectuer la resynchronisation en dehors des heures de pointe.

   L'exemple suivant inverse la relation entre le volume source d'origine, `0005` à l'adresse IP 10.0.0.11 et le volume à partir duquel vous servez des données, `volA_dst` sur `svm_backup` :

   ```
   cluster_dst::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
   ```

3. Mettre à jour la relation inversée :

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name>
   ```

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   > La commande échoue si une copie instantanée commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

   L'exemple suivant met à jour la relation entre le volume à partir duquel vous servez des données, `volA_dst` sur `svm_backup` , et le volume source original, `0005` à l'adresse IP 10.0.0.11 :

   ```
   cluster_dst::> snapmirror update -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005
   ```

4. Interrompre les virements programmés pour la relation inversée :

   ```
   snapmirror quiesce -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name>
   ```

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   L'exemple suivant interrompt les transferts planifiés entre le volume à partir duquel vous servez des données, `volA_dst` sur `svm_backup` , et le volume source original, `0005` à l'adresse IP 10.0.0.11 :

```
cluster_dst::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

5. Arrêter les transferts en cours pour la relation inversée :

   `snapmirror abort -source-path <SVM:volume>|<cluster://SVM/volume> -destination -path <hostip:>/lun/<name>`

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   L'exemple suivant interrompt les transferts en cours entre le volume à partir duquel vous servez les données, `volA_dst` sur `svm_backup` , et le volume source original, `0005` à l'adresse IP 10.0.0.11 :

```
cluster_dst::> snapmirror abort -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

6. Rompre la relation inversée :

   `snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume> -destination -path <hostip:>/lun/<name>`

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   L'exemple suivant rompt la relation entre le volume à partir duquel vous servez des données, `volA_dst` sur `svm_backup` , et le volume source original, `0005` à l'adresse IP 10.0.0.11 :

```
cluster_dst::> snapmirror break -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

7. Supprimer la relation de protection des données inversée :

   `snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume> -destination-path <hostip:>/lun/<name> -policy <policy>`

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   L'exemple suivant supprime la relation inversée entre le volume source d'origine, `0005` à l'adresse IP 10.0.0.11 et le volume à partir duquel vous servez des données, `volA_dst` sur `svm_backup` :

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

8. Rétablir la relation initiale de protection des données :

   `snapmirror resync -source-path <hostip:>/lun/<name> -destination-path <SVM:volume>|<cluster://SVM/volume>`

Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

L'exemple suivant rétablit la relation entre le volume source original, `0005` à l'adresse IP 10.0.0.11 et au volume de destination d'origine, `volA_dst` sur `svm_backup` :

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

Après avoir terminé

Utilisez le `snapmirror show` commande permettant de vérifier que la relation SnapMirror a été créée. Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

Mettre à jour manuellement une relation de réplication

Vous devrez peut-être mettre à jour manuellement une relation de réplication si une mise à jour échoue en raison d'une erreur réseau.

À propos de cette tâche

Vous devez spécifier le chemin source de l'élément dans le formulaire `<hostip:>/lun/<name>` , où "lun" est la chaîne de caractères réelle "lun" et `name` est le nom du volume Element.

Étapes

1. Mettre à jour manuellement une relation de réplication :

   ```
   snapmirror update -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   > La commande échoue si une copie instantanée commune n'existe pas sur la source et la destination. Utiliser `snapmirror initialize` pour réinitialiser la relation.

   L'exemple suivant met à jour la relation entre le volume source `0005` à l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` sur `svm_backup` :

   ```
   cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Resynchroniser une relation de réplication

Vous devez resynchroniser une relation de réplication après avoir rendu un volume de destination accessible en écriture, après l'échec d'une mise à jour parce qu'une copie Snapshot commune n'existe pas sur les volumes source et de destination, ou si vous souhaitez modifier la stratégie de réplication de la relation.

À propos de cette tâche

Bien que la resynchronisation ne nécessite pas de transfert de base, elle peut prendre du temps. Il serait peut-être préférable d'effectuer la resynchronisation en dehors des heures de pointe.

Vous devez spécifier le chemin source de l'élément dans le formulaire `<hostip:>/lun/<name>` , où "lun" est la chaîne de caractères réelle "lun" et `name` est le nom du volume Element.

Étape

1. Resynchronisez les volumes source et de destination :

   ```
   snapmirror resync -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume> -type XDP -policy <policy>
   ```

   Pour connaître la syntaxe complète des commandes, consultez la page de manuel.

   L'exemple suivant resynchronise la relation entre le volume source `0005` à l'adresse IP 10.0.0.11 et au volume de destination `volA_dst` sur `svm_backup` :

   ```
   cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
   -policy MirrorLatest -destination-path svm_backup:volA_dst
   ```

Sauvegarder et restaurer des volumes

Sauvegarder et restaurer des volumes

Vous pouvez sauvegarder et restaurer des volumes sur d'autres systèmes de stockage SolidFire , ainsi que sur des systèmes de stockage d'objets secondaires compatibles avec Amazon S3 ou OpenStack Swift.

Lorsque vous restaurez des volumes à partir d'OpenStack Swift ou d'Amazon S3, vous avez besoin des informations du manifeste issues du processus de sauvegarde d'origine. Si vous restaurez un volume sauvegardé sur un système de stockage SolidFire , aucune information de manifeste n'est requise.

Trouver plus d'informations

- Sauvegardez un volume sur un stockage d'objets Amazon S3
- Sauvegarder un volume sur un stockage d'objets OpenStack Swift
- Sauvegardez un volume sur un cluster de stockage SolidFire
- Restaurez un volume à partir d'une sauvegarde sur un stockage d'objets Amazon S3.
- Restaurez un volume à partir d'une sauvegarde sur un magasin d'objets OpenStack Swift
- Restaurez un volume à partir d'une sauvegarde sur un cluster de stockage SolidFire .

Sauvegardez un volume sur un stockage d'objets Amazon S3

Vous pouvez sauvegarder des volumes sur des supports de stockage d'objets externes compatibles avec Amazon S3.

1. Cliquez sur **Gestion** > **Volumes**.

2. Cliquez sur l'icône Actions correspondant au volume que vous souhaitez sauvegarder.
3. Dans le menu qui apparaît, cliquez sur **Sauvegarder vers**.
4. Dans la boîte de dialogue **Sauvegarde intégrée**, sous **Sauvegarder vers**, sélectionnez **S3**.
5. Sélectionnez une option sous **Format des données** :
   - **Natif** : Un format compressé lisible uniquement par les systèmes de stockage SolidFire .
   - **Non compressé** : Un format non compressé compatible avec d'autres systèmes.
6. Saisissez un nom d'hôte à utiliser pour accéder au stockage d'objets dans le champ **Nom d'hôte**.
7. Saisissez un identifiant de clé d'accès pour le compte dans le champ **Identifiant de clé d'accès**.
8. Saisissez la clé d'accès secrète du compte dans le champ **Clé d'accès secrète**.
9. Saisissez le compartiment S3 dans lequel stocker la sauvegarde dans le champ **Compartiment S3**.
10. Saisissez un nom à ajouter au préfixe dans le champ **Nom**.
11. Cliquez sur **Commencer la lecture**.

Sauvegarder un volume sur un stockage d'objets OpenStack Swift

Vous pouvez sauvegarder des volumes sur des supports de stockage d'objets externes compatibles avec OpenStack Swift.

1. Cliquez sur **Gestion** > **Volumes**.
2. Cliquez sur l'icône Actions pour rétablir le volume.
3. Dans le menu qui apparaît, cliquez sur **Sauvegarder vers**.
4. Dans la boîte de dialogue **Sauvegarde intégrée**, sous **Sauvegarder vers**, sélectionnez **Swift**.
5. Sélectionnez un format de données sous **Format des données** :
   - **Natif** : Un format compressé lisible uniquement par les systèmes de stockage SolidFire .
   - **Non compressé** : Un format non compressé compatible avec d'autres systèmes.
6. Saisissez une URL dans le champ **URL** pour accéder au magasin d'objets.
7. Veuillez saisir un nom d'utilisateur pour le compte dans le champ **Nom d'utilisateur**.
8. Saisissez la clé d'authentification du compte dans le champ **Clé d'authentification**.
9. Saisissez le conteneur dans lequel stocker la sauvegarde dans le champ **Conteneur**.
10. **Facultatif** : Saisissez un nom à ajouter au préfixe dans le champ **Nom**.
11. Cliquez sur **Commencer la lecture**.

Sauvegardez un volume sur un cluster de stockage SolidFire

Pour les clusters de stockage exécutant le logiciel Element, vous pouvez sauvegarder les volumes résidant sur un cluster vers un cluster distant.

Assurez-vous que les clusters source et cible sont appariés.

Voir"Apparier les clusters pour la réplication" .

Lors de la sauvegarde ou de la restauration d'un cluster à un autre, le système génère une clé qui servira d'authentification entre les clusters. Cette clé d'écriture en masse permet au cluster source de s'authentifier

auprès du cluster de destination, assurant ainsi un niveau de sécurité lors de l'écriture sur le volume de destination. Dans le cadre du processus de sauvegarde ou de restauration, vous devez générer une clé d'écriture de volume en masse à partir du volume de destination avant de démarrer l'opération.

1. Sur le cluster de destination, **Gestion** > **Volumes**.
2. Cliquez sur l'icône Actions du volume de destination.
3. Dans le menu qui s'affiche, cliquez sur **Restaurer à partir de**.
4. Dans la boîte de dialogue **Restauration intégrée**, sous **Restaurer à partir de**, sélectionnez * SolidFire*.
5. Sélectionnez une option sous **Format des données** :
   - **Natif** : Un format compressé lisible uniquement par les systèmes de stockage SolidFire .
   - **Non compressé** : Un format non compressé compatible avec d'autres systèmes.
6. Cliquez sur **Générer la clé**.
7. Copiez la clé contenue dans la zone **Clé d'écriture en masse** dans votre presse-papiers.
8. Sur le cluster source, accédez à **Gestion** > **Volumes**.
9. Cliquez sur l'icône Actions pour rétablir le volume.
10. Dans le menu qui apparaît, cliquez sur **Sauvegarder vers**.
11. Dans la boîte de dialogue **Sauvegarde intégrée**, sous **Sauvegarder vers**, sélectionnez * SolidFire*.
12. Sélectionnez la même option que celle que vous avez sélectionnée précédemment dans le champ **Format des données**.
13. Saisissez l'adresse IP virtuelle de gestion du cluster du volume de destination dans le champ **Adresse IP virtuelle du cluster distant**.
14. Saisissez le nom d'utilisateur du cluster distant dans le champ **Nom d'utilisateur du cluster distant**.
15. Saisissez le mot de passe du cluster distant dans le champ **Mot de passe du cluster distant**.
16. Dans le champ **Clé d'écriture en masse**, collez la clé que vous avez générée précédemment sur le cluster de destination.
17. Cliquez sur **Commencer la lecture**.

Restaurez un volume à partir d'une sauvegarde sur un stockage d'objets Amazon S3.

Vous pouvez restaurer un volume à partir d'une sauvegarde sur un stockage d'objets Amazon S3.

1. Cliquez sur **Rapports** > **Journal des événements**.
2. Localisez l'événement de sauvegarde qui a créé la sauvegarde que vous devez restaurer.
3. Dans la colonne **Détails** de l'événement, cliquez sur **Afficher les détails**.
4. Copiez les informations du manifeste dans votre presse-papiers.
5. Cliquez sur **Gestion** > **Volumes**.
6. Cliquez sur l'icône Actions correspondant au volume que vous souhaitez restaurer.
7. Dans le menu qui s'affiche, cliquez sur **Restaurer à partir de**.
8. Dans la boîte de dialogue **Restauration intégrée**, sous **Restaurer à partir de**, sélectionnez **S3**.
9. Sélectionnez l'option correspondant à la sauvegarde sous **Format des données** :

- **Natif** : Un format compressé lisible uniquement par les systèmes de stockage SolidFire .
- **Non compressé** : Un format non compressé compatible avec d'autres systèmes.

10. Saisissez un nom d'hôte à utiliser pour accéder au stockage d'objets dans le champ **Nom d'hôte**.
11. Saisissez un identifiant de clé d'accès pour le compte dans le champ **Identifiant de clé d'accès**.
12. Saisissez la clé d'accès secrète du compte dans le champ **Clé d'accès secrète**.
13. Saisissez le compartiment S3 dans lequel stocker la sauvegarde dans le champ **Compartiment S3**.
14. Collez les informations du manifeste dans le champ **Manifeste**.
15. Cliquez sur **Commencer à écrire**.

Restaurez un volume à partir d'une sauvegarde sur un magasin d'objets OpenStack Swift

Vous pouvez restaurer un volume à partir d'une sauvegarde sur un stockage d'objets OpenStack Swift.

1. Cliquez sur **Rapports** > **Journal des événements**.
2. Localisez l'événement de sauvegarde qui a créé la sauvegarde que vous devez restaurer.
3. Dans la colonne **Détails** de l'événement, cliquez sur **Afficher les détails**.
4. Copiez les informations du manifeste dans votre presse-papiers.
5. Cliquez sur **Gestion** > **Volumes**.
6. Cliquez sur l'icône Actions correspondant au volume que vous souhaitez restaurer.
7. Dans le menu qui s'affiche, cliquez sur **Restaurer à partir de**.
8. Dans la boîte de dialogue **Restauration intégrée**, sous **Restaurer à partir de**, sélectionnez **Swift**.
9. Sélectionnez l'option correspondant à la sauvegarde sous **Format des données** :
   - **Natif** : Un format compressé lisible uniquement par les systèmes de stockage SolidFire .
   - **Non compressé** : Un format non compressé compatible avec d'autres systèmes.
10. Saisissez une URL dans le champ **URL** pour accéder au magasin d'objets.
11. Veuillez saisir un nom d'utilisateur pour le compte dans le champ **Nom d'utilisateur**.
12. Saisissez la clé d'authentification du compte dans le champ **Clé d'authentification**.
13. Saisissez le nom du conteneur dans lequel la sauvegarde est stockée dans le champ **Conteneur**.
14. Collez les informations du manifeste dans le champ **Manifeste**.
15. Cliquez sur **Commencer à écrire**.

Restaurez un volume à partir d'une sauvegarde sur un cluster de stockage SolidFire .

Vous pouvez restaurer un volume à partir d'une sauvegarde sur un cluster de stockage SolidFire .

Lors de la sauvegarde ou de la restauration d'un cluster à un autre, le système génère une clé qui servira d'authentification entre les clusters. Cette clé d'écriture en masse permet au cluster source de s'authentifier auprès du cluster de destination, assurant ainsi un niveau de sécurité lors de l'écriture sur le volume de destination. Dans le cadre du processus de sauvegarde ou de restauration, vous devez générer une clé d'écriture de volume en masse à partir du volume de destination avant de démarrer l'opération.

1. Sur le cluster de destination, cliquez sur **Gestion** > **Volumes**.
2. Cliquez sur l'icône Actions correspondant au volume que vous souhaitez restaurer.
3. Dans le menu qui s'affiche, cliquez sur **Restaurer à partir de**.
4. Dans la boîte de dialogue **Restauration intégrée**, sous **Restaurer à partir de**, sélectionnez * SolidFire*.
5. Sélectionnez l'option correspondant à la sauvegarde sous **Format des données** :
   - **Natif** : Un format compressé lisible uniquement par les systèmes de stockage SolidFire .
   - **Non compressé** : Un format non compressé compatible avec d'autres systèmes.
6. Cliquez sur **Générer la clé**.
7. Copiez les informations de la **clé d'écriture en masse** dans le presse-papiers.
8. Sur le cluster source, cliquez sur **Gestion** > **Volumes**.
9. Cliquez sur l'icône Actions correspondant au volume que vous souhaitez utiliser pour la restauration.
10. Dans le menu qui apparaît, cliquez sur **Sauvegarder vers**.
11. Dans la boîte de dialogue **Sauvegarde intégrée**, sélectionnez * SolidFire* sous **Sauvegarder vers**.
12. Sélectionnez l'option correspondant à la sauvegarde sous **Format des données**.
13. Saisissez l'adresse IP virtuelle de gestion du cluster du volume de destination dans le champ **Adresse IP virtuelle du cluster distant**.
14. Saisissez le nom d'utilisateur du cluster distant dans le champ **Nom d'utilisateur du cluster distant**.
15. Saisissez le mot de passe du cluster distant dans le champ **Mot de passe du cluster distant**.
16. Collez la clé depuis votre presse-papiers dans le champ **Clé d'écriture en masse**.
17. Cliquez sur **Commencer la lecture**.

Configurer des domaines de protection personnalisés

Pour les clusters Element contenant plus de deux nœuds de stockage, vous pouvez configurer des domaines de protection personnalisés pour chaque nœud. Lorsque vous configurez des domaines de protection personnalisés, vous devez affecter tous les nœuds du cluster à un domaine.

Lorsque vous attribuez des domaines de protection, une synchronisation des données entre les nœuds démarre et certaines opérations du cluster sont indisponibles jusqu'à ce que la synchronisation des données soit terminée. Une fois un domaine de protection personnalisé configuré pour un cluster, lorsque vous ajoutez un nouveau nœud de stockage, vous ne pouvez pas ajouter de disques à ce nouveau nœud tant que vous n'avez pas attribué un domaine de protection à ce nœud et laissé la synchronisation des données se terminer. Visitez le"Documentation sur les domaines de protection" pour en savoir plus sur les domaines de protection.

Pour qu'un schéma de domaine de protection personnalisé soit utile à un cluster, tous les nœuds de stockage de chaque châssis doivent être affectés au même domaine de protection personnalisé. Vous devez créer autant de domaines de protection personnalisés que nécessaire pour que cela soit le cas (le plus petit schéma de domaine de protection personnalisé possible est de trois domaines). Il est recommandé de configurer un nombre égal de nœuds par domaine et de veiller à ce que chaque nœud affecté à un domaine particulier soit du même type.

Étapes

1. Cliquez sur **Cluster** > **Nœuds**.
2. Cliquez sur **Configurer les domaines de protection**.

   Dans la fenêtre **Configurer les domaines de protection personnalisés**, vous pouvez voir les domaines de protection actuellement configurés (le cas échéant) ainsi que les affectations de domaines de protection pour chaque nœud.

3. Saisissez un nom pour le nouveau domaine de protection personnalisé, puis cliquez sur **Créer**.

   Répétez cette étape pour tous les nouveaux domaines de protection que vous devez créer.

4. Pour chaque nœud de la liste **Assigner les nœuds**, cliquez sur la liste déroulante de la colonne **Domaine de protection** et sélectionnez un domaine de protection à attribuer à ce nœud.

   Avant d'appliquer les modifications, assurez-vous de bien comprendre la configuration de vos nœuds et de votre châssis, le schéma de domaine de protection personnalisé que vous avez configuré et les effets de ce schéma sur la protection des données. Si vous appliquez un schéma de domaine de protection et que vous devez immédiatement apporter des modifications, il se peut que vous ne puissiez pas le faire pendant un certain temps en raison de la synchronisation des données qui a lieu une fois la configuration appliquée.

5. Cliquez sur **Configurer les domaines de protection**.

Résultat

En fonction de la taille de votre cluster, la synchronisation des données entre les domaines peut prendre un certain temps. Une fois la synchronisation des données terminée, vous pouvez consulter les affectations de domaine de protection personnalisées sur la page **Cluster** > **Nœuds**, et le tableau de bord de l'interface utilisateur Web d'Element affiche l'état de protection du cluster dans le volet **État du domaine de protection personnalisé**.

Erreurs possibles

Voici quelques erreurs que vous pourriez rencontrer après l'application d'une configuration de domaine de protection personnalisée :

Erreur	Description	Résolution
Échec de SetProtectionDomainLayout : ProtectionDomainLayout rendrait le NodeID {9} inutilisable. Les noms par défaut et les noms non par défaut ne peuvent pas être utilisés simultanément.	Aucun domaine de protection n'est attribué à ce nœud.	Attribuer un domaine de protection au nœud.
Échec de SetProtectionDomainLayout : le type de domaine de protection « custom » divise le type de domaine de protection « chassis ».	Dans un châssis multi-nœuds, un nœud se voit attribuer un domaine de protection différent de celui des autres nœuds du châssis.	Assurez-vous que tous les nœuds du châssis se voient attribuer le même domaine de protection.

Trouver plus d'informations

- "Domaines de protection personnalisés"
- "Gérez le stockage avec l'API Element"

Dépannage de votre système

Événements système

Afficher les informations relatives aux événements système

Vous pouvez consulter des informations sur différents événements détectés dans le système. Le système actualise les messages d'événements toutes les 30 secondes. Le journal des événements affiche les événements clés du cluster.

1. Dans l'interface utilisateur d'Element, sélectionnez **Rapports** > **Journal des événements**.

   Pour chaque événement, vous trouverez les informations suivantes :

Article	Description
ID	Un identifiant unique est associé à chaque événement.
Type d'événement	Le type d'événement enregistré, par exemple, les événements d'API ou les événements de clonage.
Message	Message associé à l'événement.
Détails	Informations permettant d'identifier les causes de l'événement.
ID de service	Le service qui a signalé l'événement (le cas échéant).
Nœud	Le nœud qui a signalé l'événement (le cas échéant).
ID du lecteur	Le lecteur qui a signalé l'événement (le cas échéant).
Heure de l'événement	L'heure à laquelle l'événement s'est produit.

Trouver plus d'informations

Types d'événements

Types d’événements

Le système signale plusieurs types d’événements ; chaque événement correspond à une opération effectuée par le système. Les événements peuvent être des événements de routine et normaux, ou des événements nécessitant l’attention d’un administrateur. La colonne « Types d’événements » de la page « Journal des événements » indique dans quelle partie du système l’événement s’est produit.

> Le système n’enregistre pas les commandes API en lecture seule dans le journal des événements.

La liste suivante décrit les types d’événements qui apparaissent dans le journal des événements :

- **événement API**

  Événements déclenchés par un utilisateur via une API ou une interface utilisateur web qui modifient les paramètres.

- **binAssignmentsEvent**

  Événements liés à l’attribution des compartiments de données. Les bins sont essentiellement des conteneurs qui stockent des données et sont répartis sur l’ensemble du cluster.

- **binSyncEvent**

  Événements système liés à une réaffectation de données entre services de blocs.

- **bsCheckEvent**

  Événements système liés aux contrôles de service de blocage.

- **bsKillEvent**

  Événements système liés aux arrêts de service par blocs.

- **événement d’opération en masse**

  Événements liés aux opérations effectuées sur un volume entier, telles qu’une sauvegarde, une restauration, un instantané ou un clonage.

- **événement clone**

  Événements liés au clonage de volumes.

- **événement maître de cluster**

  Événements survenant lors de l’initialisation du cluster ou lors de modifications de sa configuration, telles que l’ajout ou la suppression de nœuds.

- **cSumEvent**

  Événements liés à la détection d’une incohérence de somme de contrôle lors de la validation de bout en bout de la somme de contrôle.

Les services qui détectent une erreur de somme de contrôle sont automatiquement arrêtés et ne sont pas redémarrés après la génération de cet événement.

- **dataEvent**

  Événements liés à la lecture et à l'écriture de données.

- **dbEvent**

  Événements liés à la base de données globale gérée par les nœuds de l'ensemble dans le cluster.

- **driveEvent**

  Événements liés aux opérations de conduite.

- **événement de chiffrement au repos**

  Événements liés au processus de chiffrement sur un cluster.

- **ensembleEvent**

  Événements liés à l'augmentation ou à la diminution du nombre de nœuds dans un ensemble.

- **événement fibreChannel**

  Événements liés à la configuration et aux connexions des nœuds.

- **gcEvent**

  Des événements liés aux processus s'exécutent toutes les 60 minutes afin de récupérer de l'espace de stockage sur les disques durs par blocs. Ce processus est également connu sous le nom de collecte des ordures.

- **ieEvent**

  Erreur système interne.

- **événement d'installation**

  Événements d'installation automatique de logiciels. Le logiciel est en cours d'installation automatique sur un nœud en attente.

- **Événement iSCS**

  Événements liés à des problèmes iSCSI dans le système.

- **limitEvent**

  Événements liés au nombre de volumes ou de volumes virtuels dans un compte ou dans le cluster qui approche du maximum autorisé.

- **événement de mode maintenance**

  Événements liés au mode de maintenance du nœud, tels que la désactivation du nœud.

- **networkEvent**

Événements liés au signalement des erreurs réseau pour chaque interface de carte réseau physique (NIC).

Ces événements sont déclenchés lorsque le nombre d'erreurs pour une interface dépasse un seuil par défaut de 1000 au cours d'un intervalle de surveillance de 10 minutes. Ces événements s'appliquent aux erreurs de réseau telles que les défauts de réception, les erreurs de contrôle de redondance cyclique (CRC), les erreurs de longueur, les erreurs de dépassement et les erreurs de trame.

- **platformHardwareEvent**

  Événements liés à des problèmes détectés sur les périphériques matériels.

- **événement de cluster distant**

  Événements liés au jumelage de clusters distants.

- **événement de planification**

  Événements liés aux instantanés planifiés.

- **événement de service**

  Événements liés à l'état du service système.

- **sliceEvent**

  Événements liés au serveur Slice, tels que la suppression d'un lecteur ou d'un volume de métadonnées.

  Il existe trois types d'événements de réaffectation de tranches, qui incluent des informations sur le service auquel un volume est affecté :

  - basculement : changement du service principal vers un nouveau service principal

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

  - Déplacement : changement du service secondaire vers un nouveau service secondaire

    ```
    sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
    ```

  - élagage : suppression d'un volume d'un ensemble de services

    ```
    sliceID {oldSecondaryServiceID(s)}
    ```

- **snmpTrapEvent**

  Événements liés aux traps SNMP.

- **événement d'état**

  Événements liés aux statistiques système.

- **tsEvent**

  Événements liés au service de transport du système.

- **exception inattendue**

  Événements liés à des exceptions système inattendues.

- **ureEvent**

  Événements liés aux erreurs de lecture irrécupérables qui surviennent lors de la lecture à partir du périphérique de stockage.

- **vasaProviderEvent**

  Événements liés à un fournisseur VASA (vSphere APIs for Storage Awareness).

Afficher l'état des tâches en cours

Vous pouvez consulter l'état d'avancement et d'achèvement des tâches en cours dans l'interface utilisateur Web, tel que rapporté par les méthodes API ListSyncJobs et ListBulkVolumeJobs. Vous pouvez accéder à la page « Tâches en cours » depuis l'onglet « Rapports » de l'interface utilisateur d'Element.

S'il y a un grand nombre de tâches, le système peut les mettre en file d'attente et les exécuter par lots. La page « Tâches en cours » affiche les services actuellement synchronisés. Lorsqu'une tâche est terminée, elle est remplacée par la tâche de synchronisation suivante mise en file d'attente. Les tâches de synchronisation peuvent continuer d'apparaître sur la page Tâches en cours jusqu'à ce qu'il n'y ait plus de tâches à terminer.

Vous pouvez consulter les données de synchronisation de réplication pour les volumes en cours de réplication sur la page Tâches en cours d'exécution du cluster contenant le volume cible.

Alertes système

Afficher les alertes système

Vous pouvez consulter les alertes pour obtenir des informations sur les pannes de cluster ou les erreurs du système. Les alertes peuvent être des informations, des avertissements ou des erreurs et constituent un bon indicateur du bon fonctionnement du cluster. La plupart des erreurs se résolvent automatiquement.

Vous pouvez utiliser la méthode API ListClusterFaults pour automatiser la surveillance des alertes. Cela vous permet d'être informé de toutes les alertes qui se produisent.

1. Dans l'interface utilisateur d'Element, sélectionnez **Rapports** > **Alertes**.

   Le système actualise les alertes sur la page toutes les 30 secondes.

   Pour chaque événement, vous trouverez les informations suivantes :

Article	Description

ID	Identifiant unique associé à une alerte de cluster.
Gravité	Le degré d'importance de l'alerte. Valeurs possibles : • Avertissement : Un problème mineur qui pourrait bientôt nécessiter une attention particulière. Les mises à niveau du système sont toujours autorisées. • erreur : Une défaillance pouvant entraîner une dégradation des performances ou une perte de haute disponibilité (HA). Les erreurs ne devraient généralement pas affecter le service. • Critique : Une défaillance grave qui affecte le service. Le système est incapable de traiter les requêtes d'E/S API ou client. Le fonctionnement dans cet état pourrait entraîner une perte potentielle de données. • Meilleure pratique : Une bonne pratique de configuration système recommandée n'est pas appliquée.
Type	Le composant affecté par la panne. Peut être un nœud, un lecteur, un cluster, un service ou un volume.
Nœud	Identifiant du nœud auquel cette erreur fait référence. Inclus pour les défauts de nœud et de lecteur, sinon réglé sur - (tiret).
ID du lecteur	Identifiant du lecteur auquel ce défaut fait référence. Inclus pour les défauts de transmission, sinon réglé sur - (tiret).
Code d'erreur	Un code descriptif indiquant la cause de la panne.
Détails	Description du défaut avec des détails supplémentaires.
Date	Date et heure d'enregistrement du défaut.

2. Cliquez sur **Afficher les détails** pour une alerte individuelle afin de consulter les informations la concernant.
3. Pour afficher le détail de toutes les alertes sur la page, cliquez sur la colonne Détails.

   Une fois qu'une alerte est résolue par le système, toutes les informations la concernant, y compris la date de résolution, sont déplacées vers la zone « Résolu ».

Trouver plus d'informations

- Codes d'erreur du groupe d'outils
- "Gérez le stockage avec l'API Element"

Codes d'erreur du groupe d'outils

Le système signale une erreur ou un état susceptible de présenter un intérêt en générant un code d'erreur, qui est répertorié sur la page Alertes. Ces codes vous aident à déterminer quel composant du système a déclenché l'alerte et pourquoi celle-ci a été générée.

La liste suivante présente les différents types de codes :

- **erreur de service d'authentification**

  Le service d'authentification sur un ou plusieurs nœuds du cluster ne fonctionne pas comme prévu.

  Contactez le support NetApp pour obtenir de l'aide.

- **AdressesIPRéseauVirtuelDisponiblesFaibles**

  Le nombre d'adresses de réseau virtuel dans le bloc d'adresses IP est faible.

  Pour résoudre ce problème, ajoutez des adresses IP supplémentaires au bloc d'adresses réseau virtuelles.

- **blockClusterFull**

  L'espace de stockage libre par blocs est insuffisant pour supporter la perte d'un seul nœud. Consultez la méthode API GetClusterFullThreshold pour plus de détails sur les niveaux de remplissage du cluster. Ce défaut de cluster indique l'une des conditions suivantes :

  - stage3Low (Avertissement) : Le seuil défini par l'utilisateur a été franchi. Ajustez les paramètres du cluster complet ou ajoutez des nœuds.
  - stage4Critique (Erreur) : Il n'y a pas assez d'espace pour récupérer après la défaillance d'un nœud. La création de volumes, d'instantanés et de clones n'est pas autorisée.
  - étape5CompletelyConsumed (Critique)1; Aucune écriture ni nouvelle connexion iSCSI n'est autorisée. Les connexions iSCSI actuelles seront maintenues. Les opérations d'écriture échoueront jusqu'à ce que davantage de capacité soit ajoutée au cluster.

  Pour résoudre ce problème, purgez ou supprimez les volumes ou ajoutez un autre nœud de stockage au cluster de stockage.

- **blocs dégradés**

  Les données par blocs ne sont plus entièrement répliquées en raison d'une panne.

Gravité	Description
Avertissement	Seules deux copies complètes des données du bloc sont accessibles.

Erreur	Seule une copie complète des données du bloc est accessible.
Primordial	Aucune copie complète des données du bloc n'est accessible.

Remarque : Ce statut d'avertissement ne peut apparaître que sur un système Triple Helix.

Pour résoudre ce problème, restaurez les nœuds hors ligne ou bloquez les services, ou contactez le support NetApp pour obtenir de l'aide.

- **blockServiceTooFull**

  Un service de bloc utilise trop d'espace.

  Pour résoudre ce problème, ajoutez de la capacité provisionnée.

- **blockServiceUnhealthy**

  Un service de bloc a été détecté comme étant défaillant :

  - Gravité = Avertissement : Aucune mesure n'est prise. Cette période d'avertissement expirera dans cTimeUntilBSIsKilledMSec=330000 millisecondes.
  - Gravité = Erreur : Le système désactive automatiquement les données et les réplique sur d'autres disques sains.
  - Gravité = Critique : Des services de blocs ont échoué sur plusieurs nœuds, un nombre supérieur ou égal au nombre de réplications (2 pour la double hélice). Les données sont indisponibles et la synchronisation des fichiers ne pourra pas se terminer.

    Vérifiez la connectivité réseau et les erreurs matérielles. D'autres pannes surviendront si certains composants matériels tombent en panne. Le problème disparaîtra lorsque le service sera accessible ou lorsque le service aura été mis hors service.

- **Échec du test BmcSelfTest**

  Le contrôleur de gestion de la carte mère (BMC) a échoué à un autotest.

  Contactez le support NetApp pour obtenir de l'aide.

  Lors d'une mise à niveau vers Element 12.5 ou une version ultérieure, `BmcSelfTestFailed` Aucune erreur n'est générée pour un nœud dont le BMC est déjà défaillant, ou lorsque le BMC d'un nœud tombe en panne pendant la mise à niveau. Les BMC qui échouent aux autotests lors de la mise à niveau émettront un `BmcSelfTestFailed` Un défaut d'avertissement s'est produit après la mise à niveau complète du cluster.

- **Le décalage d'horloge dépasse le seuil de défaut**

  Le décalage temporel entre le maître du cluster et le nœud qui présente un jeton dépasse le seuil recommandé. Le cluster de stockage ne peut pas corriger automatiquement le décalage horaire entre les nœuds.

  Pour résoudre ce problème, utilisez des serveurs NTP internes à votre réseau plutôt que les serveurs par défaut de l'installation. Si vous utilisez un serveur NTP interne, contactez le support NetApp pour obtenir

de l’aide.

- **clusterCannotSync**

  L’espace disque est insuffisant et les données des disques de stockage bloc hors ligne ne peuvent pas être synchronisées avec les disques encore actifs.

  Pour résoudre ce problème, ajoutez du stockage.

- **clusterFull**

  Il n’y a plus d’espace de stockage libre dans le cluster de stockage.

  Pour résoudre ce problème, ajoutez du stockage.

- **clusterIOPSAreOverProvisioned**

  Les IOPS du cluster sont surdimensionnées. La somme de toutes les IOPS minimales de QoS est supérieure aux IOPS attendues du cluster. Il est impossible de maintenir un niveau de qualité de service (QoS) minimal pour tous les volumes simultanément.

  Pour résoudre ce problème, abaissez les paramètres IOPS QoS minimaux pour les volumes.

- **Seuil d’événement thermique du processeur**

  Le nombre d’événements thermiques du processeur sur un ou plusieurs processeurs dépasse le seuil configuré.

  Si aucun nouvel événement thermique du processeur n’est détecté dans les dix minutes qui suivent, l’avertissement disparaîtra automatiquement.

- **disableDriveSecurityFailed**

  Le cluster n’est pas configuré pour activer la sécurité des disques (chiffrement au repos), mais au moins un disque a la sécurité des disques activée, ce qui signifie que la désactivation de la sécurité des disques sur ces disques a échoué. Ce défaut est enregistré avec le niveau de gravité « Avertissement ».

  Pour résoudre ce problème, consultez les détails de l’erreur pour connaître la raison pour laquelle la sécurité du lecteur n’a pas pu être désactivée. Les raisons possibles sont :

  - Impossible d’obtenir la clé de chiffrement. Veuillez vérifier le problème d’accès à la clé ou au serveur de clés externe.
  - L’opération de désactivation a échoué sur le lecteur ; veuillez déterminer si une clé incorrecte a pu être saisie.

    Si aucune de ces causes n’est à l’origine du problème, il faudra peut-être remplacer le disque dur.

  Vous pouvez tenter de récupérer un disque dont la sécurité n’est pas désactivée même lorsque la clé d’authentification correcte est fournie. Pour effectuer cette opération, retirez le ou les disques du système en les déplaçant vers l’état Disponible, effectuez un effacement sécurisé du disque et replacez-le dans l’état Actif.

- **paire de cluster déconnectée**

  Une paire de clusters est déconnectée ou mal configurée.

Vérifiez la connectivité réseau entre les clusters.

- **nœud distant déconnecté**

  Un nœud distant est soit déconnecté, soit mal configuré.

  Vérifiez la connectivité réseau entre les nœuds.

- **point de terminaison SnapMirror déconnecté**

  Un point de terminaison SnapMirror distant est déconnecté ou mal configuré.

  Vérifiez la connectivité réseau entre le cluster et le point de terminaison SnapMirror distant.

- **driveDisponible**

  Un ou plusieurs disques sont disponibles dans le cluster. En règle générale, tous les clusters doivent avoir tous les disques ajoutés et aucun à l'état disponible. Si ce problème survient de manière inattendue, contactez l'assistance NetApp .

  Pour résoudre ce problème, ajoutez les disques disponibles au cluster de stockage.

- **Lecteur défaillant**

  Le cluster renvoie cette erreur lorsqu'un ou plusieurs disques sont défaillants, indiquant l'une des conditions suivantes :

  - Le gestionnaire de lecteur ne peut pas accéder au lecteur.
  - Le service de découpage ou de bloc a échoué trop de fois, probablement en raison d'échecs de lecture ou d'écriture sur le disque, et ne peut pas redémarrer.
  - Le disque dur est manquant.
  - Le service principal du nœud est inaccessible (tous les disques du nœud sont considérés comme manquants/défaillants).
  - Le disque est verrouillé et la clé d'authentification du disque ne peut être obtenue.
  - Le lecteur est verrouillé et l'opération de déverrouillage a échoué.

    Pour résoudre ce problème :

  - Vérifiez la connectivité réseau du nœud.
  - Remplacez le disque dur.
  - Assurez-vous que la clé d'authentification est disponible.

- **driveHealthFault**

  Un disque dur a échoué au contrôle d'intégrité SMART et, par conséquent, ses fonctions sont réduites. Ce défaut présente un niveau de gravité critique :

  - Le disque portant le numéro de série : <numéro de série> dans l'emplacement : <emplacement du nœud><emplacement du disque> a échoué au contrôle d'intégrité global SMART.

  Pour résoudre ce problème, remplacez le disque dur.

- **défaut d'usure du disque dur**

La durée de vie restante d'un disque dur est passée sous les seuils critiques, mais il fonctionne toujours. Ce défaut peut avoir deux niveaux de gravité : critique et avertissement.

- Le disque avec le numéro de série : <numéro de série> dans l'emplacement : <emplacement du nœud><emplacement du disque> présente des niveaux d'usure critiques.
- Le disque avec le numéro de série : <numéro de série> dans l'emplacement : <emplacement du nœud><emplacement du disque> a de faibles réserves d'usure.

  Pour résoudre ce problème, remplacez le disque dur rapidement.

- **candidats ClusterMaster en double**

  Plusieurs candidats maîtres de cluster de stockage ont été détectés.

  Contactez le support NetApp pour obtenir de l'aide.

- **Échec de l'activation de la sécurité du lecteur**

  Le cluster est configuré pour exiger la sécurité des disques (chiffrement au repos), mais la sécurité des disques n'a pas pu être activée sur au moins un disque. Ce défaut est enregistré avec le niveau de gravité « Avertissement ».

  Pour résoudre ce problème, consultez les détails de l'erreur pour connaître la raison pour laquelle la sécurité du lecteur n'a pas pu être activée. Les raisons possibles sont :

  - Impossible d'obtenir la clé de chiffrement. Veuillez vérifier le problème d'accès à la clé ou au serveur de clés externe.
  - L'opération d'activation a échoué sur le lecteur ; veuillez déterminer si une clé incorrecte a pu être saisie. Si aucune de ces causes n'est à l'origine du problème, il faudra peut-être remplacer le disque dur.

  Vous pouvez tenter de récupérer un disque dont la sécurité ne s'active pas correctement, même lorsque la clé d'authentification correcte est fournie. Pour effectuer cette opération, retirez le ou les disques du système en les déplaçant vers l'état Disponible, effectuez un effacement sécurisé du disque et replacez-le dans l'état Actif.

- **ensembleDegraded**

  La connectivité réseau ou l'alimentation électrique a été perdue pour un ou plusieurs nœuds de l'ensemble.

  Pour résoudre ce problème, rétablissez la connectivité réseau ou l'alimentation électrique.

- **exception**

  Un défaut signalé qui n'est pas un défaut de routine. Ces défauts ne sont pas automatiquement supprimés de la file d'attente des défauts.

  Contactez le support NetApp pour obtenir de l'aide.

- **échecEspaceTropPlein**

  Un service de bloc ne répond pas aux requêtes d'écriture de données. Cela provoque une saturation de l'espace du service de découpage pour stocker les écritures ayant échoué.

Pour résoudre ce problème, rétablissez la fonctionnalité des services de blocs afin de permettre aux écritures de se poursuivre normalement et à l'espace défaillant d'être vidé par le service de tranches.

- **FanSensor**

  Un capteur de ventilateur est défectueux ou manquant.

  Pour résoudre ce problème, remplacez tout matériel défectueux.

- **Accès fibre Channel dégradé**

  Un nœud Fibre Channel ne répond pas aux autres nœuds du cluster de stockage via son adresse IP de stockage pendant un certain temps. Dans cet état, le nœud sera alors considéré comme non réactif et générera une erreur de cluster.

  Vérifiez la connectivité réseau.

- **Accès fibre indisponible**

  Tous les nœuds Fibre Channel ne répondent pas. Les identifiants des nœuds sont affichés.

  Vérifiez la connectivité réseau.

- **fibreChannelActiveIxL**

  Le nombre de Nexus IxL approche la limite prise en charge de 8000 sessions actives par nœud Fibre Channel.

  - La limite recommandée est de 5500.
  - La limite d'alerte est de 7500.
  - La limite maximale (non appliquée) est de 8192.

  Pour résoudre ce problème, réduisez le nombre de Nexus IxL en dessous de la limite recommandée de 5500.

- **fibreChannelConfig**

  Ce défaut de cluster indique l'une des conditions suivantes :

  - Il y a un port Fibre Channel inattendu sur un emplacement PCI.
  - Il existe un modèle HBA Fibre Channel inattendu.
  - Il y a un problème avec le firmware d'un contrôleur HBA Fibre Channel.
  - Un port Fibre Channel n'est pas en ligne.
  - Il existe un problème persistant lors de la configuration du transfert Fibre Channel.

  Contactez le support NetApp pour obtenir de l'aide.

- **fibreChannelIOPS**

  Le nombre total d'IOPS approche la limite d'IOPS pour les nœuds Fibre Channel du cluster. Les limites sont :

  - FC0025 : Limite de 450 000 IOPS à une taille de bloc de 4 Ko par nœud Fibre Channel.

- FCN001 : Limite de 625 000 OPS à une taille de bloc de 4 Ko par nœud Fibre Channel.

Pour résoudre ce problème, répartissez la charge sur tous les nœuds Fibre Channel disponibles.

- **fibreChannelStaticIxL**

  Le nombre de Nexus IxL approche la limite prise en charge de 16 000 sessions statiques par nœud Fibre Channel.

  - La limite recommandée est de 11 000.
  - La limite d'alerte est de 15 000.
  - La limite maximale (appliquée) est de 16384.

  Pour résoudre ce problème, réduisez le nombre de Nexus IxL en dessous de la limite recommandée de 11 000.

- **Capacité du système de fichiers faible**

  L'espace disponible sur l'un des systèmes de fichiers est insuffisant.

  Pour résoudre ce problème, augmentez la capacité du système de fichiers.

- **Le système de fichiers est en lecture seule**

  Le système de fichiers est passé en mode lecture seule.

  Contactez le support NetApp pour obtenir de l'aide.

- **fipsDrivesMismatch**

  Un disque non conforme à la norme FIPS a été physiquement inséré dans un nœud de stockage compatible FIPS ou un disque conforme à la norme FIPS a été physiquement inséré dans un nœud de stockage non conforme à la norme FIPS. Un seul défaut est généré par nœud et répertorie tous les disques affectés.

  Pour résoudre ce problème, retirez ou remplacez le ou les disques incompatibles.

- **fipsDrivesOutOfCompliance**

  Le système a détecté que le chiffrement au repos a été désactivé après l'activation de la fonctionnalité des lecteurs FIPS. Ce défaut est également généré lorsque la fonctionnalité FIPS Drives est activée et qu'un disque ou un nœud non-FIPS est présent dans le cluster de stockage.

  Pour résoudre ce problème, activez le chiffrement au repos ou retirez le matériel non conforme à la norme FIPS du cluster de stockage.

- **fipsSelfTestFailure**

  Le sous-système FIPS a détecté une défaillance lors de l'autotest.

  Contactez le support NetApp pour obtenir de l'aide.

- **Configuration matérielle incompatible**

  Ce défaut de cluster indique l'une des conditions suivantes :

- La configuration ne correspond pas à la définition du nœud.
- La taille du disque est incorrecte pour ce type de nœud.
- Un disque non pris en charge a été détecté. Une des raisons possibles est que la version d'Element installée ne reconnaît pas ce lecteur. Il est recommandé de mettre à jour le logiciel Element sur ce nœud.
- Il y a une incompatibilité au niveau du firmware du disque dur.
- L'état de chiffrement du disque ne correspond pas au nœud.

Contactez le support NetApp pour obtenir de l'aide.

- **Expiration du certificat d'identité**

  Le certificat SSL du fournisseur de services du cluster, destiné à être utilisé avec un fournisseur d'identité tiers (IdP), arrive à expiration ou a déjà expiré. Ce défaut utilise les niveaux de gravité suivants en fonction de l'urgence :

Gravité	Description
Avertissement	Le certificat expire dans 30 jours.
Erreur	Le certificat expire dans 7 jours.
Primordial	Le certificat expire dans 3 jours ou a déjà expiré.

  Pour résoudre ce problème, mettez à jour le certificat SSL avant son expiration. Utilisez la méthode d'API UpdateIdpConfiguration avec `refreshCertificateExpirationTime=true` fournir le certificat SSL mis à jour.

- **Modes de liaison incohérents**

  Les modes de liaison sur le périphérique VLAN sont manquants. Ce code d'erreur affichera le mode de liaison attendu et le mode de liaison actuellement utilisé.

- **incohérentMtus**

  Ce défaut de cluster indique l'une des conditions suivantes :

  - Incompatibilité Bond1G : des MTU incohérentes ont été détectées sur les interfaces Bond1G.
  - Incompatibilité Bond10G : des MTU incohérentes ont été détectées sur les interfaces Bond10G.

  Ce code d'erreur affiche le ou les nœuds concernés ainsi que la valeur MTU associée.

- **règles de routage incohérentes**

  Les règles de routage pour cette interface sont incohérentes.

- **Masques de sous-réseau incohérents**

  Le masque de réseau sur le périphérique VLAN ne correspond pas au masque de réseau enregistré en interne pour le VLAN. Ce message d'erreur affiche le masque de réseau attendu et le masque de réseau actuellement utilisé.

- **incorrectBondPortCount**

  Le nombre de ports de liaison est incorrect.

- **invalidConfigureFibreChannelNodeCount**

  L'une des deux connexions de nœud Fibre Channel attendues est dégradée. Ce défaut apparaît lorsqu'un seul nœud Fibre Channel est connecté.

  Pour résoudre ce problème, vérifiez la connectivité du réseau du cluster et le câblage réseau, et recherchez les services défaillants. S'il n'y a aucun problème de réseau ou de service, contactez le support NetApp pour le remplacement d'un nœud Fibre Channel.

- **irqBalanceFailed**

  Une exception s'est produite lors de la tentative d'équilibrage des interruptions.

  Contactez le support NetApp pour obtenir de l'aide.

- **kmipCertificateFault**
  - Le certificat de l'autorité de certification racine (CA) arrive bientôt à expiration.

    Pour résoudre ce problème, obtenez un nouveau certificat auprès de l'autorité de certification racine avec une date d'expiration d'au moins 30 jours et utilisez ModifyKeyServerKmip pour fournir le certificat de l'autorité de certification racine mis à jour.

  - Le certificat client arrive bientôt à expiration.

    Pour résoudre ce problème, créez une nouvelle CSR à l'aide de GetClientCertificateSigningRequest, faites-la signer en veillant à ce que la nouvelle date d'expiration soit d'au moins 30 jours, et utilisez ModifyKeyServerKmip pour remplacer le certificat client KMIP expirant par le nouveau certificat.

  - Le certificat de l'autorité de certification racine (CA) a expiré.

    Pour résoudre ce problème, obtenez un nouveau certificat auprès de l'autorité de certification racine avec une date d'expiration d'au moins 30 jours et utilisez ModifyKeyServerKmip pour fournir le certificat de l'autorité de certification racine mis à jour.

  - Le certificat client a expiré.

    Pour résoudre ce problème, créez une nouvelle CSR à l'aide de GetClientCertificateSigningRequest, faites-la signer en veillant à ce que la nouvelle date d'expiration soit d'au moins 30 jours, et utilisez ModifyKeyServerKmip pour remplacer le certificat client KMIP expiré par le nouveau certificat.

  - Erreur de certificat de l'autorité de certification racine (CA).

    Pour résoudre ce problème, vérifiez que le certificat correct a été fourni et, si nécessaire, récupérez-le auprès de l'autorité de certification racine. Utilisez ModifyKeyServerKmip pour installer le certificat client KMIP correct.

  - Erreur de certificat client.

    Pour résoudre ce problème, vérifiez que le certificat client KMIP correct est installé. L'autorité de certification racine du certificat client doit être installée sur EKS. Utilisez ModifyKeyServerKmip pour installer le certificat client KMIP correct.

- **kmipServerFault**
  - Échec de la connexion

    Pour résoudre ce problème, vérifiez que le serveur de clés externe est opérationnel et accessible via le réseau. Utilisez TestKeyServerKimp et TestKeyProviderKmip pour tester votre connexion.

  - Échec de l'authentification

    Pour résoudre ce problème, vérifiez que les certificats d'autorité de certification racine et les certificats clients KMIP corrects sont utilisés, et que la clé privée et le certificat client KMIP correspondent.

  - Erreur serveur

    Pour résoudre ce problème, consultez les détails de l'erreur. Un dépannage sur le serveur de clés externe pourrait être nécessaire en fonction de l'erreur renvoyée.

- **seuil d'Ecc de mémoire**

  Un grand nombre d'erreurs ECC, corrigibles ou non, ont été détectées. Ce défaut utilise les niveaux de gravité suivants en fonction de l'urgence :

Événement	Gravité	Description
Un seul DIMM cErrorCount atteint le seuil cDimmCorrectableErrWarnThreshold.	Avertissement	Erreurs de mémoire ECC corrigibles supérieures au seuil sur la barrette DIMM : <Processeur> <Emplacement DIMM>
Un seul DIMM cErrorCount reste au-dessus de cDimmCorrectableErrWarnThreshold jusqu'à ce que cErrorFaultTimer expire pour le DIMM.	Erreur	Erreurs de mémoire ECC corrigibles supérieures au seuil sur la barrette DIMM : <Processeur> <DIMM>
Un contrôleur de mémoire signale un cErrorCount supérieur à cMemCtlrCorrectableErrWarnThreshold, et cMemCtlrCorrectableErrWarnDuration est spécifié.	Avertissement	Erreurs de mémoire ECC corrigibles supérieures au seuil sur le contrôleur de mémoire : <Processeur> <Contrôleur de mémoire>
Un contrôleur de mémoire signale un cErrorCount supérieur à cMemCtlrCorrectableErrWarnThreshold jusqu'à ce que cErrorFaultTimer expire pour le contrôleur de mémoire.	Erreur	Erreurs de mémoire ECC corrigibles supérieures au seuil sur la barrette DIMM : <Processeur> <DIMM>

Une seule barrette DIMM signale un uErrorCount supérieur à zéro, mais inférieur à cDimmUncorrectableErrFaultThreshold.	Avertissement	Erreur(s) de mémoire ECC non corrigible(s) détectée(s) sur la barrette DIMM : <Processeur> <Emplacement DIMM>
Une seule barrette DIMM signale un uErrorCount d'au moins cDimmUncorrectableErrFaultThreshold.	Erreur	Erreur(s) de mémoire ECC non corrigible(s) détectée(s) sur la barrette DIMM : <Processeur> <Emplacement DIMM>
Un contrôleur de mémoire signale un uErrorCount supérieur à zéro, mais inférieur à cMemCtlrUncorrectableErrFaultThreshold.	Avertissement	Erreur(s) de mémoire ECC non corrigible(s) détectée(s) sur le contrôleur de mémoire : <Processeur> <Contrôleur de mémoire>
Un contrôleur de mémoire signale un uErrorCount d'au moins cMemCtlrUncorrectableErrFaultThreshold.	Erreur	Erreur(s) de mémoire ECC non corrigible(s) détectée(s) sur le contrôleur de mémoire : <Processeur> <Contrôleur de mémoire>

Pour résoudre ce problème, contactez le support NetApp .

- **seuil d'utilisation de la mémoire**

  L'utilisation de la mémoire est supérieure à la normale. Ce défaut utilise les niveaux de gravité suivants en fonction de l'urgence :

  Consultez la rubrique **Détails** du code d'erreur pour obtenir des informations plus détaillées sur le type de panne.

Gravité	Description
Avertissement	La mémoire système est faible.
Erreur	La mémoire système est très faible.
Primordial	La mémoire système est entièrement consommée.

  Pour résoudre ce problème, contactez le support NetApp .

- **metadataClusterFull**

  L'espace de stockage libre des métadonnées est insuffisant pour supporter la perte d'un seul nœud. Consultez la méthode API GetClusterFullThreshold pour plus de détails sur les niveaux de remplissage du cluster. Ce défaut de cluster indique l'une des conditions suivantes :

  - stage3Low (Avertissement) : Le seuil défini par l'utilisateur a été franchi. Ajustez les paramètres du

cluster complet ou ajoutez des nœuds.

- stage4Critique (Erreur) : Il n'y a pas assez d'espace pour récupérer après la défaillance d'un nœud. La création de volumes, d'instantanés et de clones n'est pas autorisée.
- étape5CompletelyConsumed (Critique)1; Aucune écriture ni nouvelle connexion iSCSI n'est autorisée. Les connexions iSCSI actuelles seront maintenues. Les opérations d'écriture échoueront jusqu'à ce que davantage de capacité soit ajoutée au cluster. Purgez ou supprimez des données ou ajoutez des nœuds.

Pour résoudre ce problème, purgez ou supprimez les volumes ou ajoutez un autre nœud de stockage au cluster de stockage.

- **Échec de la vérification mtu**

  Le périphérique réseau n'est pas configuré pour la taille MTU appropriée.

  Pour résoudre ce problème, assurez-vous que toutes les interfaces réseau et les ports du commutateur sont configurés pour les trames jumbo (MTU jusqu'à 9000 octets).

- **configuration réseau**

  Ce défaut de cluster indique l'une des conditions suivantes :

  - L'interface attendue est absente.
  - Une interface dupliquée est présente.
  - Une interface configurée est hors service.
  - Un redémarrage du réseau est nécessaire.

  Contactez le support NetApp pour obtenir de l'aide.

- **Aucune adresse IP de réseau virtuel disponible**

  Aucune adresse réseau virtuelle n'est disponible dans le bloc d'adresses IP.

  - virtualNetworkID # TAG(###) ne dispose d'aucune adresse IP de stockage disponible. Il est impossible d'ajouter des nœuds supplémentaires au cluster.

  Pour résoudre ce problème, ajoutez des adresses IP supplémentaires au bloc d'adresses réseau virtuelles.

- **nodeHardwareFault (L'interface réseau <nom> est hors service ou le câble est débranché)**

  L'interface réseau est soit hors service, soit le câble est débranché.

  Pour résoudre ce problème, vérifiez la connectivité réseau du ou des nœuds.

- **nodeHardwareFault (L'état de capacité de chiffrement du disque ne correspond pas à l'état de capacité de chiffrement du nœud pour le disque dans l'emplacement <emplacement du nœud><emplacement du disque>)**

  Les capacités de chiffrement d'un disque ne correspondent pas à celles du nœud de stockage dans lequel il est installé.

- **nodeHardwareFault (Taille du disque <type de disque> incorrecte <taille réelle> pour le disque dans l'emplacement <emplacement du nœud><emplacement du disque> pour ce type de nœud - taille attendue <taille attendue>)**

Un nœud de stockage contient un disque dur dont la taille est incorrecte pour ce nœud.

- **nodeHardwareFault (Disque non pris en charge détecté dans l'emplacement <emplacement du nœud><emplacement du disque> ; les statistiques et les informations sur l'état du disque ne seront pas disponibles)**

  Un nœud de stockage contient un lecteur qu'il ne prend pas en charge.

- **nodeHardwareFault (Le disque dans l'emplacement <node slot><drive slot> devrait utiliser la version de firmware <expected version>, mais utilise une version non prise en charge <actual version>)**

  Un nœud de stockage contient un disque exécutant une version de firmware non prise en charge.

- **nodeMaintenanceMode**

  Un nœud a été placé en mode maintenance. Ce défaut utilise les niveaux de gravité suivants en fonction de l'urgence :

Gravité	Description
Avertissement	Indique que le nœud est toujours en mode maintenance.
Erreur	Indique que le mode maintenance n'a pas pu être désactivé, probablement en raison de pannes ou d'activations de systèmes de secours.

  Pour résoudre ce problème, désactivez le mode maintenance une fois la maintenance terminée. Si l'erreur persiste, contactez le support NetApp pour obtenir de l'aide.

- **nœudHorsLigne**

  Le logiciel Element ne peut pas communiquer avec le nœud spécifié. Vérifiez la connectivité réseau.

- **notUsingLACPBondMode**

  Le mode de liaison LACP n'est pas configuré.

  Pour résoudre ce problème, utilisez l'agrégation de liens LACP lors du déploiement des nœuds de stockage ; les clients peuvent rencontrer des problèmes de performances si LACP n'est pas activé et correctement configuré.

- **Serveur NTP inaccessible**

  Le cluster de stockage ne peut pas communiquer avec le ou les serveurs NTP spécifiés.

  Pour résoudre ce problème, vérifiez la configuration du serveur NTP, du réseau et du pare-feu.

- **ntpTimeNotInSync**

  La différence entre l'heure du cluster de stockage et l'heure du serveur NTP spécifié est trop importante. Le cluster de stockage ne peut pas corriger automatiquement la différence.

Pour résoudre ce problème, utilisez des serveurs NTP internes à votre réseau plutôt que les serveurs par défaut de l'installation. Si vous utilisez des serveurs NTP internes et que le problème persiste, contactez le support NetApp pour obtenir de l'aide.

- **nvramDeviceStatus**

  Un périphérique NVRAM présente une erreur, est en panne ou est tombé en panne. Ce défaut présente les degrés de gravité suivants :

Gravité	Description
Avertissement	Un avertissement a été détecté par le matériel. Cette situation peut être transitoire, comme par exemple une alerte de température. • nvmLifetimeError • nvmLifetimeStatus • Durée de vie de la source d'énergie • état de la source d'énergie • Seuil d'avertissement dépassé
Erreur	Un état d'erreur ou critique a été détecté par le matériel. Le maître du cluster tente de retirer le disque de partition du fonctionnement (ceci génère un événement de retrait de disque). Si les services de tranche secondaire ne sont pas disponibles, le disque ne sera pas retiré. Erreurs renvoyées en plus des erreurs de niveau Avertissement : • Le point de montage du périphérique NVRAM n'existe pas. • La partition du périphérique NVRAM n'existe pas. • La partition du périphérique NVRAM existe, mais elle n'est pas montée.
Primordial	Un état d'erreur ou critique a été détecté par le matériel. Le maître du cluster tente de retirer le disque de partition du fonctionnement (ceci génère un événement de retrait de disque). Si les services de tranche secondaire ne sont pas disponibles, le disque ne sera pas retiré. • persistancePerdue • armStatusSaveNArmé • Erreur csaveStatusError

  Remplacez tout matériel défectueux dans le nœud. Si le problème persiste, contactez le support NetApp pour obtenir de l'aide.

- **Erreur d’alimentation**

  Ce défaut de cluster indique l’une des conditions suivantes :

  - L’alimentation électrique est absente.
  - Une alimentation électrique est défaillante.
  - L’alimentation électrique est absente ou hors de portée.

  Pour résoudre ce problème, vérifiez que tous les nœuds sont alimentés par une alimentation redondante. Contactez le support NetApp pour obtenir de l’aide.

- **Espace réservé Trop plein**

  La capacité totale allouée au cluster est trop élevée.

  Pour résoudre ce problème, ajoutez de l’espace provisionné ou supprimez et purgez les volumes.

- **remoteRepAsyncDelayExceeded**

  Le délai asynchrone configuré pour la réplication a été dépassé. Vérifier la connectivité réseau entre les clusters.

- **remoteRepClusterFull**

  La réplication à distance des volumes a été suspendue car le cluster de stockage cible est trop plein.

  Pour résoudre ce problème, libérez de l’espace sur le cluster de stockage cible.

- **remoteRepSnapshotClusterFull**

  La réplication à distance des instantanés a été suspendue car le cluster de stockage cible est saturé.

  Pour résoudre ce problème, libérez de l’espace sur le cluster de stockage cible.

- **remoteRepSnapshotsExceededLimit**

  La réplication à distance des instantanés a été suspendue car le volume du cluster de stockage cible a dépassé sa limite d’instantanés.

  Pour résoudre ce problème, augmentez la limite de snapshots sur le cluster de stockage cible.

- **erreur de planification d’action**

  Une ou plusieurs des activités planifiées ont été exécutées, mais ont échoué.

  Le problème disparaît si l’activité planifiée s’exécute à nouveau et réussit, si l’activité planifiée est supprimée ou si l’activité est mise en pause puis reprise.

- **Échec de la lecture du capteur**

  Un capteur n’a pas pu communiquer avec le contrôleur de gestion de la carte mère (BMC).

  Contactez le support NetApp pour obtenir de l’aide.

- **serviceNotRunning**

Un service requis n’est pas en cours d’exécution.

Contactez le support NetApp pour obtenir de l’aide.

- **ServiceDeTrancheTropPlein**

  La capacité allouée à un service de tranche est insuffisante.

  Pour résoudre ce problème, ajoutez de la capacité provisionnée.

- **sliceServiceUnhealthy**

  Le système a détecté qu’un service de tranche est défaillant et le désactive automatiquement.

  - Gravité = Avertissement : Aucune mesure n’est prise. Ce délai d’avertissement expirera dans 6 minutes.
  - Gravité = Erreur : Le système désactive automatiquement les données et les réplique sur d’autres disques sains.

  Vérifiez la connectivité réseau et les erreurs matérielles. D’autres pannes surviendront si certains composants matériels tombent en panne. Le problème disparaîtra lorsque le service de tranche sera accessible ou lorsque le service aura été mis hors service.

- **sshEnabled**

  Le service SSH est activé sur un ou plusieurs nœuds du cluster de stockage.

  Pour résoudre ce problème, désactivez le service SSH sur le ou les nœuds concernés ou contactez le support NetApp pour obtenir de l’aide.

- **Expiration du certificat SSL**

  Le certificat SSL associé à ce nœud arrive bientôt à expiration ou a expiré. Ce défaut utilise les niveaux de gravité suivants en fonction de l’urgence :

Gravité	Description
Avertissement	Le certificat expire dans 30 jours.
Erreur	Le certificat expire dans 7 jours.
Primordial	Le certificat expire dans 3 jours ou a déjà expiré.

  Pour résoudre ce problème, renouvelez le certificat SSL. En cas de besoin, contactez le support NetApp pour obtenir de l’aide.

- **capacité bloquée**

  Un seul nœud représente plus de la moitié de la capacité du cluster de stockage.

  Afin de maintenir la redondance des données, le système réduit la capacité du plus grand nœud de sorte qu’une partie de sa capacité de bloc soit inutilisée.

  Pour résoudre ce problème, ajoutez des disques supplémentaires aux nœuds de stockage existants ou

ajoutez des nœuds de stockage au cluster.

- **capteur de température**

  Un capteur de température signale des températures supérieures à la normale. Ce défaut peut être déclenché conjointement à une erreur d'alimentation ou à un défaut du capteur de ventilateur.

  Pour résoudre ce problème, vérifiez la présence d'obstructions au flux d'air à proximité du bloc de stockage. En cas de besoin, contactez le support NetApp pour obtenir de l'aide.

- **mise à niveau**

  Une mise à jour est en cours depuis plus de 24 heures.

  Pour résoudre ce problème, reprenez la mise à niveau ou contactez le support NetApp pour obtenir de l'aide.

- **Service non réactif**

  Un service ne répond plus.

  Contactez le support NetApp pour obtenir de l'aide.

- **virtualNetworkConfig**

  Ce défaut de cluster indique l'une des conditions suivantes :

  - Aucune interface n'est présente.
  - L'espace de noms d'une interface est incorrect.
  - Le masque de sous-réseau est incorrect.
  - L'adresse IP est incorrecte.
  - L'interface n'est pas opérationnelle.
  - Il existe une interface superflue sur un nœud.

  Contactez le support NetApp pour obtenir de l'aide.

- **volumesDegraded**

  La réplication et la synchronisation des volumes secondaires ne sont pas terminées. Le message disparaît une fois la synchronisation terminée.

- **volumesOffline**

  Un ou plusieurs volumes du cluster de stockage sont hors ligne. Le défaut **volumeDegraded** sera également présent.

  Contactez le support NetApp pour obtenir de l'aide.

Afficher l'activité de performance du nœud

Vous pouvez visualiser l'activité de performance de chaque nœud sous forme graphique. Ces informations fournissent des statistiques en temps réel sur les opérations d'E/S de lecture/écriture du processeur par seconde (IOPS) pour chaque disque du nœud. Le

graphique d'utilisation est mis à jour toutes les cinq secondes, et le graphique des statistiques du disque dur est mis à jour toutes les dix secondes.

1. Cliquez sur **Cluster** > **Nœuds**.
2. Cliquez sur **Actions** pour le nœud que vous souhaitez afficher.
3. Cliquez sur **Afficher les détails**.

> Vous pouvez visualiser des points précis dans le temps sur les graphiques linéaires et à barres en positionnant votre curseur sur la ligne ou la barre.

Performances en volume

Afficher les performances en volume

Vous pouvez consulter des informations détaillées sur les performances de tous les volumes du cluster. Vous pouvez trier les informations par ID de volume ou par n'importe quelle colonne de performance. Vous pouvez également filtrer les informations selon certains critères.

Vous pouvez modifier la fréquence d'actualisation des informations de performance sur la page en cliquant sur la liste **Actualiser toutes les** et en choisissant une valeur différente. L'intervalle d'actualisation par défaut est de 10 secondes si le cluster comporte moins de 1000 volumes ; sinon, la valeur par défaut est de 60 secondes. Si vous choisissez la valeur « Jamais », l'actualisation automatique de la page est désactivée.

Vous pouvez réactiver l'actualisation automatique en cliquant sur **Activer l'actualisation automatique**.

1. Dans l'interface utilisateur d'Element, sélectionnez **Rapports** > **Performances du volume**.
2. Dans la liste des volumes, cliquez sur l'icône Actions correspondant à un volume.
3. Cliquez sur **Afficher les détails**.

   Un encadré contenant des informations générales sur le volume est affiché en bas de la page.
4. Pour obtenir des informations plus détaillées sur le volume, cliquez sur **Voir plus de détails**.

   Le système affiche des informations détaillées ainsi que des graphiques de performance pour le volume.

Trouver plus d'informations

Détails des performances du volume

Détails des performances du volume

Vous pouvez consulter les statistiques de performance des volumes depuis la page Performances des volumes de l'onglet Rapports dans l'interface utilisateur d'Element.

La liste suivante décrit les détails dont vous disposez :

- **IDENTIFIANT**

  L'identifiant généré par le système pour le volume.

- **Nom**

  Le nom donné au volume lors de sa création.

- **Compte**

  Le nom du compte associé au volume.

- **Groupes d'accès**

  Le nom du ou des groupes d'accès au volume auxquels appartient le volume.

- **Utilisation du volume**

  Un pourcentage qui décrit le niveau d'utilisation du volume par le client.

  Valeurs possibles :

  - 0 = Le client n'utilise pas le volume
  - 100 = Le client utilise le maximum
  - >100 = Le client utilise la rafale

- **Total des IOPS**

  Le nombre total d'IOPS (lecture et écriture) actuellement exécutés sur le volume.

- **Lire IOPS**

  Le nombre total d'IOPS de lecture actuellement exécutées sur le volume.

- **Écrire les IOPS**

  Le nombre total d'IOPS d'écriture actuellement en cours d'exécution sur le volume.

- **Débit total**

  Le débit total (lecture et écriture) actuellement exécuté sur le volume.

- **Débit de lecture**

  Le débit total de lecture actuellement exécuté sur le volume.

- **Débit d'écriture**

  Le débit total d'écriture actuellement exécuté sur le volume.

- **Latence totale**

  Le temps moyen, en microsecondes, pour effectuer des opérations de lecture et d'écriture sur un volume.

- **Latence de lecture**

  Le temps moyen, en microsecondes, pour effectuer les opérations de lecture sur le volume au cours des 500 dernières millisecondes.

- **Latence d'écriture**

  Le temps moyen, en microsecondes, pour effectuer des opérations d'écriture sur un volume au cours des 500 dernières millisecondes.

- **Profondeur de la file d'attente**

  Le nombre d'opérations de lecture et d'écriture en attente sur le volume.

- **Taille moyenne des E/S**

  Taille moyenne en octets des E/S récentes sur le volume au cours des 500 dernières millisecondes.

sessions iSCSI

Afficher les sessions iSCSI

Vous pouvez visualiser les sessions iSCSI connectées au cluster. Vous pouvez filtrer les informations pour n'inclure que les sessions souhaitées.

1. Dans l'interface utilisateur d'Element, sélectionnez **Rapports** > **Sessions iSCSI**.
2. Pour afficher les champs de critères de filtrage, cliquez sur **Filtrer**.

Trouver plus d'informations

Détails de la session iSCSI

Détails de la session iSCSI

Vous pouvez consulter les informations relatives aux sessions iSCSI connectées au cluster.

La liste suivante décrit les informations que vous pouvez trouver sur les sessions iSCSI :

- **Nœud**

  Le nœud hébergeant la partition de métadonnées principale du volume.

- **Compte**

  Le nom du compte propriétaire du volume. Si la valeur est vide, un tiret (-) est affiché.

- **Volume**

  Le nom du volume identifié sur le nœud.

- **ID du volume**

  Identifiant du volume associé à l'IQN cible.

- **ID de l'initiateur**

  Un identifiant généré par le système pour l'initiateur.

- **Alias de l'initiateur**

  Un nom facultatif pour l'initiateur, qui facilite sa recherche dans une longue liste.

- **Adresse IP de l'initiateur**

  L'adresse IP du point de terminaison qui initie la session.

- **Initiateur IQN**

  L'IQN du point de terminaison qui initie la session.

- **Adresse IP cible**

  L'adresse IP du nœud hébergeant le volume.

- **IQN cible**

  L'IQN du volume.

- **TYPE**

  L'algorithme CHAP pour une session iSCSI. Si aucun algorithme CHAP n'est utilisé, un tiret (-) est affiché. Disponible à partir d'Element 12.8.

- **Créé le**

  Date de création de la session.

sessions Fibre Channel

Visionnez les sessions Fibre Channel

Vous pouvez visualiser les sessions Fibre Channel (FC) connectées au cluster. Vous pouvez filtrer les informations pour n'afficher que les connexions que vous souhaitez dans la fenêtre.

1. Dans l'interface utilisateur d'Element, sélectionnez **Rapports** > **Sessions FC**.
2. Pour afficher les champs de critères de filtrage, cliquez sur **Filtrer**.

Trouver plus d'informations

Détails de la session Fibre Channel

Détails de la session Fibre Channel

Vous pouvez trouver des informations sur les sessions Fibre Channel (FC) actives connectées au cluster.

La liste suivante décrit les informations que vous pouvez trouver sur les sessions FC connectées au cluster :

- **ID du nœud**

Le nœud hébergeant la session pour la connexion.

- **Nom du nœud**

  Nom du nœud généré par le système.

- **ID de l'initiateur**

  Un identifiant généré par le système pour l'initiateur.

- **Initiateur WWPN**

  Le nom du port d'origine à l'échelle mondiale.

- **Alias de l'initiateur**

  Un nom facultatif pour l'initiateur, qui facilite sa recherche dans une longue liste.

- **Cible WWPN**

  Nom du port cible mondial.

- **Groupe d'accès aux volumes**

  Nom du groupe d'accès au volume auquel appartient la session.

- **ID du groupe d'accès au volume**

  Identifiant généré par le système pour le groupe d'accès.

Dépannage des disques

Dépannage des disques

Vous pouvez remplacer un disque SSD défectueux par un disque de remplacement. Les disques SSD pour les nœuds de stockage SolidFire sont remplaçables à chaud. Si vous soupçonnez une défaillance d'un disque SSD, contactez le support NetApp pour vérifier la panne et obtenir de l'aide concernant la procédure de résolution appropriée. L'assistance NetApp travaille également avec vous pour obtenir un disque de remplacement conformément à votre contrat de niveau de service.

Dans ce cas, « remplaçable » signifie que vous pouvez retirer un disque défaillant d'un nœud actif et le remplacer par un nouveau disque SSD de NetApp. Il est déconseillé de retirer les disques non défaillants d'un cluster actif.

Vous devez conserver sur site les pièces de rechange recommandées par le support NetApp afin de permettre le remplacement immédiat du disque en cas de panne.

> À des fins de test, si vous simulez une panne de disque en retirant un disque d'un nœud, vous devez attendre 30 secondes avant de réinsérer le disque dans son emplacement.

En cas de panne d'un disque, Double Helix redistribue les données qu'il contient sur les nœuds restants du cluster. Les pannes de plusieurs disques sur le même nœud ne posent pas de problème, car le logiciel

Element protège contre la présence de deux copies de données sur le même nœud. Une panne de disque entraîne les événements suivants :

- Les données sont transférées hors du disque.
- La capacité globale du cluster est réduite par la capacité du disque.
- La protection des données Double Helix garantit l'existence de deux copies valides des données.

> Les systèmes de stockage SolidFire ne prennent pas en charge le retrait d'un disque si cela entraîne une capacité de stockage insuffisante pour migrer les données.

Pour plus d'informations

- Supprimer les disques défaillants du cluster
- Dépannage de base des lecteurs MDSS
- Retirer les lecteurs MDSS
- "Remplacement des disques par des nœuds de stockage SolidFire"
- "Remplacement des disques pour les nœuds de stockage de la série H600S"
- "Informations matérielles H410S et H610S"
- "Informations matérielles de la série SF"

Supprimer les disques défaillants du cluster

Le système SolidFire place un disque en état de panne si l'autodiagnostic du disque indique au nœud qu'il est défaillant ou si la communication avec le disque est interrompue pendant cinq minutes et demie ou plus. Le système affiche la liste des disques défaillants. Vous devez supprimer un disque défaillant de la liste des disques défaillants dans le logiciel NetApp Element .

Les disques figurant dans la liste **Alertes** apparaissent comme **blockServiceUnhealthy** lorsqu'un nœud est hors ligne. Lors du redémarrage du nœud, si le nœud et ses disques se remettent en ligne en moins de cinq minutes et demie, les disques se mettent à jour automatiquement et continuent de fonctionner comme disques actifs dans le cluster.

1. Dans l'interface utilisateur d'Element, sélectionnez **Cluster** > **Disques**.
2. Cliquez sur **Échec** pour afficher la liste des disques défaillants.
3. Notez le numéro d'emplacement du disque défaillant.

   Vous avez besoin de ces informations pour localiser le disque défectueux dans le châssis.

4. Retirez les disques défaillants en utilisant l'une des méthodes suivantes :

Option	Étapes
Pour retirer des disques individuels	a. Cliquez sur **Actions** pour le lecteur que vous souhaitez supprimer. b. Cliquez sur **Supprimer**.

Pour retirer plusieurs disques	a. Sélectionnez tous les disques que vous souhaitez supprimer, puis cliquez sur **Actions groupées**. b. Cliquez sur **Supprimer**.

Dépannage de base des lecteurs MDSS

Vous pouvez récupérer les disques de métadonnées (ou de partition) en les réintégrant au cluster si l'un ou les deux disques de métadonnées tombent en panne. Vous pouvez effectuer l'opération de récupération dans l'interface utilisateur de NetApp Element si la fonctionnalité MDSS est déjà activée sur le nœud.

Si l'un ou les deux disques de métadonnées d'un nœud tombent en panne, le service de découpage s'arrêtera et les données des deux disques seront sauvegardées sur des disques différents du nœud.

Les scénarios suivants décrivent les cas de défaillance possibles et fournissent des recommandations de base pour corriger le problème :

Le disque de partition système tombe en panne.

- Dans ce scénario, l'emplacement 2 est vérifié et remis dans un état disponible.
- Le lecteur de partition système doit être rempli à nouveau avant que le service de partition puisse être remis en ligne.
- Vous devriez remplacer le disque système. Lorsque celui-ci sera disponible, ajoutez-le ainsi que le disque de l'emplacement 2.

Vous ne pouvez pas ajouter le disque dans l'emplacement 2 seul en tant que disque de métadonnées. Vous devez rajouter les deux disques au nœud simultanément.

L'emplacement 2 est défaillant

- Dans ce scénario, le lecteur de partition système est vérifié et remis dans un état disponible.
- Vous devriez remplacer l'emplacement 2 par un emplacement de rechange. Lorsque l'emplacement 2 sera disponible, ajoutez simultanément le disque système et le disque de l'emplacement 2.

Le disque système et l'emplacement 2 tombent en panne.

- Vous devriez remplacer à la fois le disque système et le lecteur d'emplacement 2 par un disque de rechange. Lorsque les deux disques seront disponibles, ajoutez simultanément le disque système et le disque de l'emplacement 2.

Ordre des opérations

- Remplacez le disque dur défectueux par un disque de rechange (remplacez les deux disques si les deux sont défectueux).
- Réintégrez les disques au cluster une fois qu'ils auront été réutilisés et seront disponibles.

Vérifier les opérations

- Vérifiez que les disques dans l'emplacement 0 (ou interne) et l'emplacement 2 sont identifiés comme disques de métadonnées dans la liste des disques actifs.
- Vérifiez que l'équilibrage de toutes les tranches est terminé (aucun autre message de déplacement de tranches ne doit apparaître dans le journal des événements pendant au moins 30 minutes).

Pour plus d'informations

Ajouter des lecteurs MDSS

Ajouter des lecteurs MDSS

Vous pouvez ajouter un deuxième lecteur de métadonnées sur un nœud SolidFire en convertissant le lecteur de blocs de l'emplacement 2 en un lecteur de tranches. Ceci est réalisé en activant la fonction de service de découpage multi-lecteurs (MDSS). Pour activer cette fonctionnalité, vous devez contacter le support NetApp .

Pour rendre un disque de partition disponible, il peut être nécessaire de remplacer un disque défaillant par un disque neuf ou de rechange. Vous devez ajouter le disque système en même temps que le disque pour l'emplacement 2. Si vous essayez d'ajouter le lecteur de tranche de l'emplacement 2 seul ou avant d'ajouter le lecteur de tranche système, le système générera une erreur.

1. Cliquez sur **Cluster** > **Disques**.
2. Cliquez sur **Disponible** pour afficher la liste des disques disponibles.
3. Sélectionnez les disques de tranches à ajouter.
4. Cliquez sur **Actions groupées**.
5. Cliquez sur **Ajouter**.
6. Vérifiez dans l'onglet **Lecteurs actifs** que les lecteurs ont bien été ajoutés.

Retirer les lecteurs MDSS

Vous pouvez supprimer les disques du service de découpage multi-lecteurs (MDSS). Cette procédure s'applique uniquement si le nœud possède plusieurs disques de partition.

> Si le disque de la tranche système et le disque de l'emplacement 2 tombent en panne, le système arrêtera les services de tranche et retirera les disques. S'il n'y a pas de panne et que vous retirez les disques, les deux disques doivent être retirés simultanément.

1. Cliquez sur **Cluster** > **Disques**.
2. Dans l'onglet **Disponibles**, cochez la case correspondant aux disques de partition à supprimer.
3. Cliquez sur **Actions groupées**.
4. Cliquez sur **Supprimer**.
5. Confirmez l'action.

Dépannage des nœuds

Supprimer des nœuds d'un cluster

Vous pouvez retirer des nœuds d'un cluster pour maintenance ou remplacement. Vous devez utiliser l'interface utilisateur ou l'API de NetApp Element pour supprimer les nœuds avant de les mettre hors ligne.

Voici un aperçu de la procédure de suppression des nœuds de stockage :

- Assurez-vous que le cluster dispose d'une capacité suffisante pour créer une copie des données sur le nœud.
- Supprimez les disques du cluster à l'aide de l'interface utilisateur ou de la méthode API RemoveDrives.

  Cela a pour conséquence que le système migre les données des disques du nœud vers d'autres disques du cluster. La durée de ce processus dépend de la quantité de données à migrer.

- Supprimez le nœud du cluster.

Avant de mettre hors tension ou sous tension un nœud, tenez compte des points suivants :

- La mise hors tension des nœuds et des clusters comporte des risques si elle n'est pas effectuée correctement.

  La mise hors tension d'un nœud doit être effectuée sous la direction du support NetApp .

- Si un nœud est hors service pendant plus de 5,5 minutes dans n'importe quelle condition d'arrêt, la protection des données Double Helix commence la tâche d'écriture de blocs répliqués un par un sur un autre nœud pour répliquer les données. Dans ce cas, contactez le support NetApp pour obtenir de l'aide concernant l'analyse du nœud défaillant.
- Pour redémarrer ou mettre hors tension un nœud en toute sécurité, vous pouvez utiliser la commande d'API Shutdown.
- Si un nœud est en panne ou hors tension, vous devez contacter le support NetApp avant de le remettre en ligne.
- Une fois un nœud remis en ligne, vous devez réintégrer les disques au cluster, en fonction de la durée de son indisponibilité.

Pour plus d'informations

"Remplacement d'un châssis SolidFire défectueux"

"Remplacement d'un nœud de la série H600S défectueux"

Mise hors tension d'un groupe

Pour mettre hors tension un cluster entier, procédez comme suit.

Étapes

1. (Facultatif) Contactez le support NetApp pour obtenir de l'aide concernant les étapes préliminaires.
2. Vérifiez que toutes les entrées/sorties sont arrêtées.
3. Déconnectez toutes les sessions iSCSI :

a. Accédez à l'adresse IP virtuelle de gestion (MVIP) sur le cluster pour ouvrir l'interface utilisateur Element.

b. Notez les nœuds répertoriés dans la liste des nœuds.

c. Exécutez la méthode d'API Shutdown avec l'option halt spécifiée sur chaque ID de nœud du cluster.

Lorsque vous redémarrez le cluster, vous devez suivre certaines étapes pour vérifier que tous les nœuds sont mis en ligne :

1. Vérifiez que tous les niveaux de gravité critique et `volumesOffline` Les défauts du cluster ont été résolus.
2. Attendez 10 à 15 minutes que l'amas se stabilise.
3. Commencez par mettre en service les hôtes pour accéder aux données.

Si vous souhaitez prévoir plus de temps lors de la mise sous tension des nœuds et de la vérification de leur bon fonctionnement après la maintenance, contactez le support technique pour obtenir de l'aide concernant le report de la synchronisation des données afin d'éviter une synchronisation inutile des fichiers binaires.

Trouver plus d'informations

"Comment arrêter et redémarrer correctement un cluster de stockage NetApp Solidfire/HCI"

Utilisez les utilitaires par nœud pour les nœuds de stockage

Utilisez les utilitaires par nœud pour les nœuds de stockage

Vous pouvez utiliser les utilitaires par nœud pour résoudre les problèmes de réseau si les outils de surveillance standard de l'interface utilisateur du logiciel NetApp Element ne vous fournissent pas suffisamment d'informations pour le dépannage. Les utilitaires par nœud fournissent des informations et des outils spécifiques qui peuvent vous aider à résoudre les problèmes de réseau entre les nœuds ou avec le nœud de gestion.

Trouver plus d'informations

- Accédez aux paramètres par nœud via l'interface utilisateur de chaque nœud.
- Détails des paramètres réseau depuis l'interface utilisateur de chaque nœud
- Détails des paramètres du cluster depuis l'interface utilisateur de chaque nœud
- Exécutez des tests système à l'aide de l'interface utilisateur par nœud
- Exécutez les utilitaires système à l'aide de l'interface utilisateur par nœud.

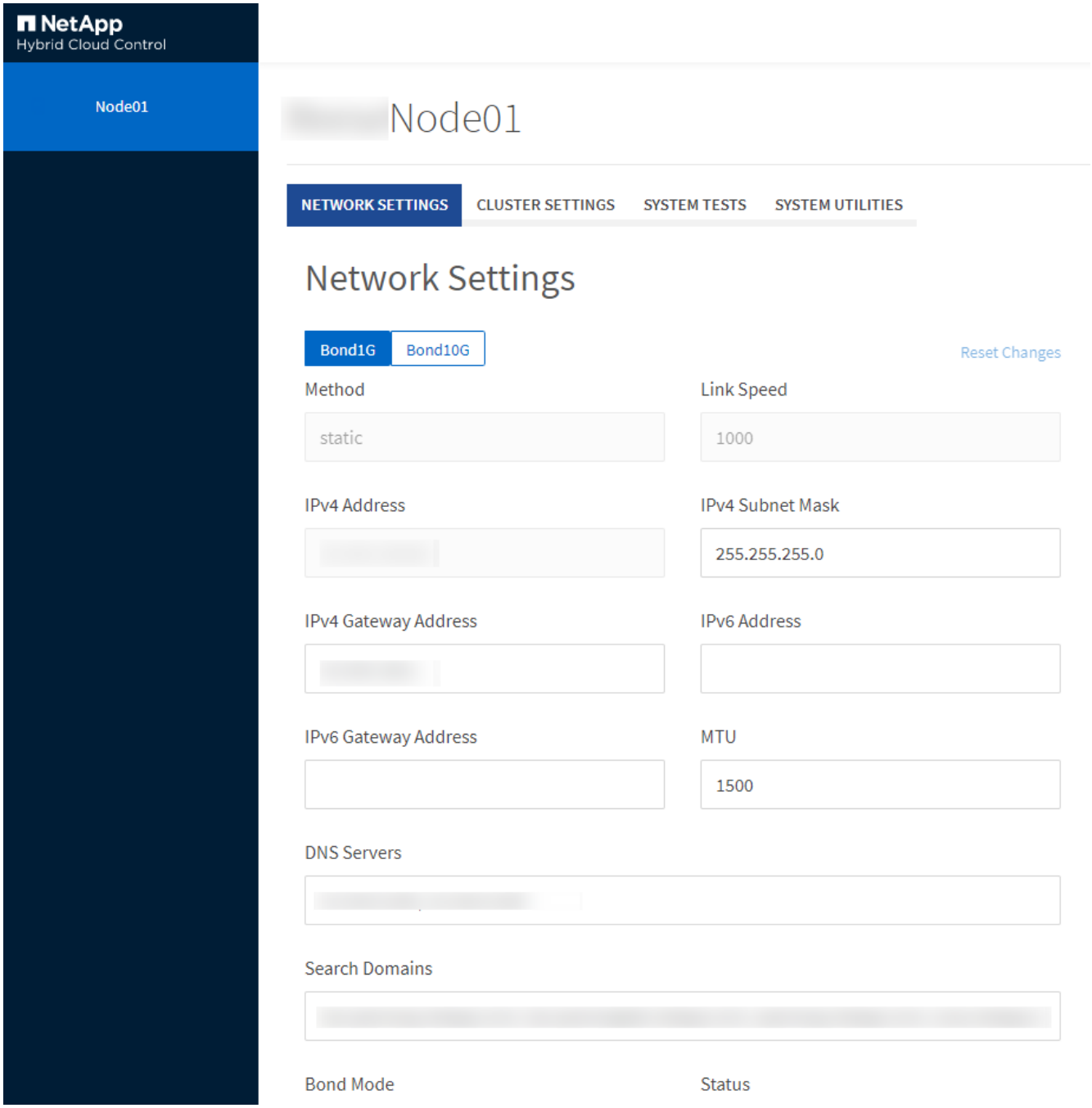
Accédez aux paramètres par nœud via l'interface utilisateur de chaque nœud.

Vous pouvez accéder aux paramètres réseau, aux paramètres du cluster, ainsi qu'aux tests et utilitaires système dans l'interface utilisateur de chaque nœud après avoir saisi l'adresse IP du nœud de gestion et vous être authentifié.

Si vous souhaitez modifier les paramètres d'un nœud à l'état Actif faisant partie d'un cluster, vous devez vous connecter en tant qu'administrateur du cluster.

Vous devez configurer ou modifier un nœud à la fois. Vous devez vous assurer que les paramètres réseau spécifiés produisent l'effet escompté et que le réseau est stable et fonctionne correctement avant d'apporter des modifications à un autre nœud.

1. Ouvrez l'interface utilisateur par nœud en utilisant l'une des méthodes suivantes :
   - Saisissez l'adresse IP de gestion suivie de :442 dans une fenêtre de navigateur, puis connectez-vous à l'aide d'un nom d'utilisateur et d'un mot de passe d'administrateur.
   - Dans l'interface utilisateur d'Element, sélectionnez **Cluster** > **Nœuds**, puis cliquez sur le lien de l'adresse IP de gestion du nœud que vous souhaitez configurer ou modifier. Dans la fenêtre du navigateur qui s'ouvre, vous pouvez modifier les paramètres du nœud.



Détails des paramètres réseau depuis l'interface utilisateur de chaque nœud

Vous pouvez modifier les paramètres réseau du nœud de stockage pour lui attribuer un nouvel ensemble d'attributs réseau.

Vous pouvez consulter les paramètres réseau d'un nœud de stockage sur la page **Paramètres réseau** une fois connecté au nœud. (`https://<node_IP>:442/hcc/node/network-settings`). Vous pouvez sélectionner les paramètres **Bond1G** (gestion) ou **Bond10G** (stockage). La liste suivante décrit les paramètres que vous pouvez modifier lorsqu'un nœud de stockage est à l'état Disponible, En attente ou Actif :

- **Méthode**

  La méthode utilisée pour configurer l'interface. Méthodes possibles :

  - interface de bouclage : utilisée pour définir l'interface de bouclage IPv4.
  - manuel : Permet de définir les interfaces pour lesquelles aucune configuration n'est effectuée par défaut.
  - DHCP : Utilisé pour obtenir une adresse IP via DHCP.
  - statique : Utilisé pour définir des interfaces Ethernet avec des adresses IPv4 allouées statiquement.
- **Vitesse de liaison**

  La vitesse négociée par la carte réseau virtuelle.
- **Adresse IPv4**

  L'adresse IPv4 du réseau eth0.
- **Masque de sous-réseau IPv4**

  Subdivisions d'adresses du réseau IPv4.
- **Adresse de la passerelle IPv4**

  Adresse réseau du routeur pour envoyer des paquets hors du réseau local.
- **Adresse IPv6**

  L'adresse IPv6 du réseau eth0.
- **Adresse de passerelle IPv6**

  Adresse réseau du routeur pour envoyer des paquets hors du réseau local.
- **MTU**

  Taille maximale des paquets qu'un protocole réseau peut transmettre. Doit être supérieur ou égal à 1500. Si vous ajoutez une deuxième carte réseau de stockage, la valeur doit être de 9000.
- **Serveurs DNS**

  Interface réseau utilisée pour la communication au sein du cluster.
- **Rechercher des domaines**

Rechercher les adresses MAC supplémentaires disponibles pour le système.

- **Mode Bond**

  Peut prendre l'un des modes suivants :

  - Actif/Passif (par défaut)
  - ALB
  - LACP
- **Statut**

  Valeurs possibles :

  - Opérationnel
  - Vers le bas
  - En haut
- **Étiquette de réseau virtuel**

  Étiquette attribuée lors de la création du réseau virtuel.

- **Itinéraires**

  Routes statiques vers des hôtes ou des réseaux spécifiques via l'interface associée que les routes sont configurées pour utiliser.

Détails des paramètres du cluster depuis l'interface utilisateur de chaque nœud

Vous pouvez vérifier les paramètres du cluster pour un nœud de stockage après la configuration du cluster et modifier le nom d'hôte du nœud.

La liste suivante décrit les paramètres de cluster pour un nœud de stockage indiqué sur la page **Paramètres de cluster** de l'interface utilisateur du nœud. (`https://<node_IP>:442/hcc/node/cluster-settings`).

- **Rôle**

  Rôle du nœud dans le cluster. Valeurs possibles :

  - Stockage : Nœud de stockage ou Fibre Channel.
  - Gestion : Node est un nœud de gestion.
- **Nom d'hôte**

  Nom du nœud.

- **Grappe**

  Nom du cluster.

- **Adhésion au groupe**

  État du nœud. Valeurs possibles :

- Disponible : Ce nœud n'a pas de nom de cluster associé et ne fait pas encore partie d'un cluster.
- En attente : le nœud est configuré et peut être ajouté à un cluster désigné. L'authentification n'est pas requise pour accéder au nœud.
- En attente : Le système est en train d'installer un logiciel compatible sur le nœud. Une fois l'opération terminée, le nœud passera à l'état Actif.
- Actif : Le nœud participe à un cluster. L'authentification est requise pour modifier le nœud.

- **Version**

  Version du logiciel Element exécutée sur le nœud.

- **Ensemble**

  Nœuds faisant partie de l'ensemble de bases de données.

- **ID du nœud**

  Un identifiant est attribué lorsqu'un nœud est ajouté au cluster.

- **Interface de cluster**

  Interface réseau utilisée pour la communication au sein du cluster.

- **Interface de gestion**

  Interface réseau de gestion. Par défaut, il s'agit de Bond1G, mais Bond10G peut également être utilisé.

- **Interface de stockage**

  Interface réseau de stockage utilisant Bond10G.

- **Compatible avec le chiffrement**

  Indique si le nœud prend en charge ou non le chiffrement du disque.

Exécutez des tests système à l'aide de l'interface utilisateur par nœud

Vous pouvez tester les modifications apportées aux paramètres réseau après les avoir enregistrées dans la configuration réseau. Vous pouvez exécuter les tests pour vous assurer que le nœud de stockage est stable et peut être mis en ligne sans problème.

Vous vous êtes connecté à l'interface utilisateur spécifique à chaque nœud de stockage.

1. Cliquez sur **Tests système**.
2. Cliquez sur **Exécuter le test** à côté du test que vous souhaitez exécuter ou sélectionnez **Exécuter tous les tests**.

   L'exécution de toutes les opérations de test peut prendre du temps et ne doit être effectuée que sur instruction du support NetApp .

   - **Test de l'ensemble connecté**

Teste et vérifie la connectivité à un ensemble de bases de données. Par défaut, le test utilise l'ensemble du cluster auquel le nœud est associé. Vous pouvez également fournir un ensemble différent pour tester la connectivité.

- **Test Connect Mvip**

  Effectue un ping sur l'adresse IP virtuelle de gestion (MVIP) spécifiée, puis exécute un simple appel API vers la MVIP pour vérifier la connectivité. Par défaut, le test utilise le MVIP du cluster auquel le nœud est associé.

- **Test Connect Svip**

  Effectue un ping sur l'adresse IP virtuelle de stockage (SVIP) spécifiée en utilisant des paquets ICMP (Internet Control Message Protocol) correspondant à la taille de l'unité de transmission maximale (MTU) définie sur la carte réseau. Il se connecte ensuite au SVIP en tant qu'initiateur iSCSI. Par défaut, le test utilise le SVIP du cluster auquel le nœud est associé.

- **Configuration matérielle de test**

  Il vérifie que toutes les configurations matérielles sont correctes, valide les versions du firmware et confirme que tous les disques sont installés et fonctionnent correctement. C'est la même chose que les tests en usine.

  Ce test nécessite beaucoup de ressources et ne doit être exécuté que sur demande du support NetApp .

- **Tester la connectivité locale**

  Teste la connectivité à tous les autres nœuds du cluster en effectuant un ping sur l'adresse IP du cluster (CIP) de chaque nœud. Ce test ne s'affichera sur un nœud que si celui-ci fait partie d'un cluster actif.

- **Test de localisation du cluster**

  Vérifie que le nœud peut localiser le cluster spécifié dans la configuration du cluster.

- **Test de configuration réseau**

  Vérifie que les paramètres réseau configurés correspondent aux paramètres réseau utilisés sur le système. Ce test n'est pas destiné à détecter les pannes matérielles lorsqu'un nœud participe activement à un cluster.

- **Test de ping**

  Effectue un ping sur une liste spécifiée d'hôtes ou, si aucune n'est spécifiée, construit dynamiquement une liste de tous les nœuds enregistrés dans le cluster et effectue un ping sur chacun d'eux pour une connectivité simple.

- **Test de connectivité à distance**

  Teste la connectivité à tous les nœuds dans les clusters appariés à distance en effectuant un ping sur l'adresse IP du cluster (CIP) de chaque nœud. Ce test ne s'affichera sur un nœud que si celui-ci fait partie d'un cluster actif.

Exécutez les utilitaires système à l'aide de l'interface utilisateur par nœud.

Vous pouvez utiliser l'interface utilisateur par nœud pour le nœud de stockage afin de créer ou de supprimer des ensembles de support, de réinitialiser les paramètres de configuration des disques et de redémarrer les services réseau ou de cluster.

Vous vous êtes connecté à l'interface utilisateur spécifique à chaque nœud de stockage.

1. Cliquez sur **Utilitaires système**.
2. Cliquez sur le bouton correspondant à l'utilitaire système que vous souhaitez exécuter.
   - **Contrôle de la puissance**

     Redémarre, met hors tension ou arrête le nœud.

     Cette opération entraîne une perte temporaire de connectivité réseau.

     Spécifiez les paramètres suivants :

     - Action : Les options incluent Redémarrer et Arrêter (mise hors tension).
     - Délai de réveil : tout temps supplémentaire avant que le nœud ne se remette en ligne.
   - **Collecte des journaux des nœuds**

     Crée un ensemble de support dans le répertoire /tmp/bundles du nœud.

     Spécifiez les paramètres suivants :

     - Nom du pack : Nom unique pour chaque pack de support créé. Si aucun nom n'est fourni, alors « supportbundle » et le nom du nœud sont utilisés comme nom de fichier.
     - Arguments supplémentaires : ce paramètre est transmis au script sf_make_support_bundle. Ce paramètre ne doit être utilisé qu'à la demande du support NetApp .
     - Délai d'attente (secondes) : Spécifiez le nombre de secondes à attendre pour chaque réponse ping.
   - **Supprimer les journaux du nœud**

     Supprime tous les bundles de support actuellement présents sur le nœud qui ont été créés à l'aide de **Créer un bundle de support de cluster** ou de la méthode d'API CreateSupportBundle.
   - **Réinitialiser les disques**

     Initialise les disques et supprime toutes les données actuellement présentes sur le disque. Vous pouvez réutiliser le disque dans un nœud existant ou dans un nœud mis à niveau.

     Spécifiez le paramètre suivant :

     - Lecteurs : Liste des noms de périphériques (et non des identifiants de lecteur) à réinitialiser.
   - **Réinitialiser la configuration réseau**

     Permet de résoudre les problèmes de configuration réseau d'un nœud individuel et de réinitialiser la configuration réseau de ce nœud aux paramètres d'usine par défaut.

- **Réinitialiser le nœud**

  Réinitialise un nœud aux paramètres d'usine. Toutes les données sont supprimées, mais les paramètres réseau du nœud sont préservés pendant cette opération. Les nœuds ne peuvent être réinitialisés que s'ils ne sont pas affectés à un cluster et sont à l'état Disponible.

  > Lorsque vous utilisez cette option, toutes les données, les paquets (mises à jour logicielles), les configurations et les fichiers journaux sont supprimés du nœud.

- **Relancer le réseautage**

  Redémarre tous les services réseau sur un nœud.

  > Cette opération peut entraîner une perte temporaire de connectivité réseau.

- **Services de redémarrage**

  Redémarre les services logiciels Element sur un nœud.

  > Cette opération peut entraîner une interruption temporaire du service du nœud. Vous ne devez effectuer cette opération que sur instruction du support NetApp .

  Spécifiez les paramètres suivants :

  - Service : Nom du service à redémarrer.
  - Action : Action à effectuer sur le service. Les options incluent démarrer, arrêter et redémarrer.

Collaborer avec le nœud de gestion

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

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

Voir"documentation du nœud de gestion" pour plus d'informations.

Comprendre les niveaux de remplissage des grappes

Le cluster exécutant le logiciel Element génère des erreurs de cluster pour avertir l'administrateur de stockage lorsque le cluster atteint sa capacité maximale. Il existe trois niveaux de remplissage du cluster, tous affichés dans l'interface utilisateur de NetApp Element : avertissement, erreur et critique.

Le système utilise le code d'erreur BlockClusterFull pour signaler un niveau de saturation du stockage des blocs du cluster. Vous pouvez consulter les niveaux de gravité du remplissage du cluster depuis l'onglet Alertes de l'interface utilisateur d'Element.

La liste suivante contient des informations sur les niveaux de gravité de BlockClusterFull :

- **Avertissement**

  Il s'agit d'un avertissement configurable par le client qui apparaît lorsque la capacité de bloc du cluster approche le niveau de gravité d'erreur. Par défaut, ce niveau est fixé à trois pour cent en dessous du niveau d'erreur et peut être ajusté via l'interface utilisateur et l'API d'Element. Vous devez augmenter votre capacité, ou libérer de la capacité dès que possible.

- **Erreur**

  Lorsque le cluster est dans cet état, si un nœud est perdu, la capacité du cluster sera insuffisante pour reconstruire la protection des données Double Helix. La création de nouveaux volumes, de clones et de snapshots est bloquée tant que le cluster est dans cet état. Il ne s'agit pas d'un état sûr ni recommandé pour un cluster. Vous devez augmenter sa capacité ou en libérer immédiatement.

- **Critique**

  Cette erreur critique s'est produite car le cluster est consommé à 100 %. Il est en mode lecture seule et aucune nouvelle connexion iSCSI ne peut être établie avec le cluster. Lorsque ce stade est atteint, vous devez immédiatement libérer ou ajouter de la capacité.

Le système utilise le code d'erreur MetadataClusterFull pour signaler un niveau de saturation du stockage des métadonnées du cluster. Vous pouvez consulter le taux de remplissage du stockage des métadonnées du cluster dans la section Capacité du cluster de la page Vue d'ensemble de l'onglet Rapports de l'interface utilisateur Element.

La liste suivante contient des informations sur les niveaux de gravité de MetadataClusterFull :

- **Avertissement**

  Il s'agit d'un avertissement configurable par le client qui apparaît lorsque la capacité des métadonnées du cluster approche du niveau de gravité d'erreur. Par défaut, ce niveau est fixé à trois pour cent en dessous du niveau d'erreur et peut être ajusté via l'API Element. Vous devez augmenter votre capacité, ou libérer de la capacité dès que possible.

- **Erreur**

  Lorsque le cluster est dans cet état, si un nœud est perdu, la capacité du cluster sera insuffisante pour reconstruire la protection des données Double Helix. La création de nouveaux volumes, de clones et de snapshots est bloquée tant que le cluster est dans cet état. Il ne s'agit pas d'un état sûr ni recommandé pour un cluster. Vous devez augmenter sa capacité ou en libérer immédiatement.

- **Critique**

  Cette erreur critique s'est produite car le cluster est consommé à 100 %. Il est en mode lecture seule et aucune nouvelle connexion iSCSI ne peut être établie avec le cluster. Lorsque ce stade est atteint, vous devez immédiatement libérer ou ajouter de la capacité.

Les dispositions suivantes s'appliquent aux seuils des clusters à deux nœuds :

- Le taux d'erreur de complétude des métadonnées est inférieur de 20 % au seuil critique.
- L'erreur de remplissage des blocs est inférieure d'un disque de stockage (capacité inutilisée incluse) à la

capacité critique ; ce qui signifie qu’elle est inférieure de deux disques de stockage à la capacité critique.