Gérez le stockage avec le logiciel Element

Element Software

NetApp
January 15, 2024

Sommaire

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 les activités de stockage sur une infrastructure mutualisée.

Element est le système d'exploitation du stockage au cœur d'un cluster SolidFire. Le logiciel Element s'exécute de façon indépendante sur tous les nœuds du cluster et permet aux nœuds du cluster de combiner les ressources et de présenter comme un système de stockage unique aux clients externes. Le logiciel Element est chargé de la coordination, de l'évolutivité et de la gestion du cluster dans son ensemble.

L'interface logicielle repose sur l'API Element.

- "Accédez à l'interface utilisateur du logiciel Element"
- "Configuration des options du système SolidFire après le déploiement"
- "Mise à niveau des composants du système de stockage"
- "Utilisez les options de base de l'interface utilisateur du logiciel Element"
- "Gestion des comptes"
- "Gérez votre système"
- "Gérez les volumes et les volumes virtuels"
- "Protégez vos données"
- "Dépanner votre système"

Trouvez plus d'informations

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

Accédez à l'interface utilisateur du logiciel Element

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

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 à l'aide d'un adressage IPv4 ou IPv6, en fonction de la configuration durant la création du cluster.

1. Options au choix :
   - IPv6 : saisissez l'adresse MVIP https://[IPv6] par exemple :

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

   - IPv4 : saisissez l'adresse MVIP https://[IPv4] par exemple :

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

2. Pour DNS, entrez le nom d'hôte.
3. Cliquez sur les messages de certificat d'authentification.

Trouvez plus d'informations

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

Configuration des options du système SolidFire après le déploiement

Une fois le système SolidFire configuré, vous pouvez effectuer certaines tâches facultatives.

Si vous modifiez les informations d'identification dans le système, vous pouvez connaître l'impact sur les autres composants.

En outre, vous pouvez configurer les paramètres de l'authentification multifacteur, de la gestion externe des clés et de la sécurité FIPS (Federal information Processing Standards). Vous devez également examiner la mise à jour des mots de passe si nécessaire.

Trouvez plus d'informations

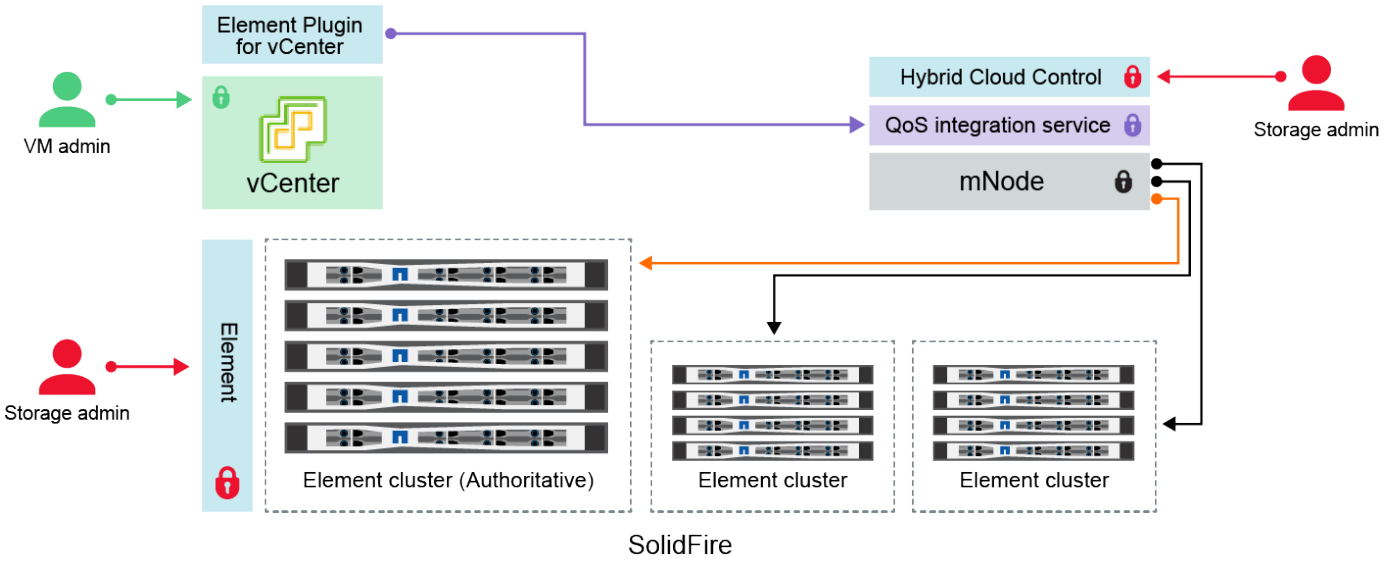
- "Modifiez les identifiants dans NetApp HCI et NetApp SolidFire"
- "Modifiez le certificat SSL par défaut du logiciel Element"
- "Modifiez le mot de passe IPMI pour les nœuds"
- "Activez l'authentification multifacteur"
- "Commencez par une gestion externe des clés"
- "Créez un cluster prenant en charge les disques FIPS"

Modifiez les identifiants dans NetApp HCI et NetApp SolidFire

Selon les politiques de sécurité établies dans l'entreprise qui ont déployé NetApp HCI ou NetApp SolidFire, il est souvent possible de modifier des identifiants ou des mots de passe. Avant de modifier les mots de passe, vous devez connaître l'impact sur les autres composants logiciels du déploiement.

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

Interactions des composants avec NetApp SolidFire
:



Type et icône d'informations d'identification	Utilisation par l'administrateur	Reportez-vous à ces instructions
Informations d'identification d'élément 	**S'applique à**: NetApp HCI et SolidFire Les administrateurs utilisent ces informations d'identification 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 identifiants d'administration des clusters de stockage, appelés « cluster qui fait autorité », pour lesquels le nœud a été initialement configuré. Pour les clusters de stockage ajoutés ultérieurement au contrôle du cloud hybride, mNode stocke en toute sécurité les informations d'identification d'administration. Si les informations d'identification des clusters de stockage ajoutés ultérieurement sont modifiées, les informations d'identification doivent également être mises à jour dans le mNode à l'aide de l'API mNode.	• "Mettre à jour les mots de passe d'administration du cluster de stockage." • Mettez à jour les informations d'identification d'administrateur du cluster de stockage dans le nœud mNode à l'aide du "API modifyclusteradmin".

Type et icône d'informations d'identification	Utilisation par l'administrateur	Reportez-vous à ces instructions
Identifiants d'authentification unique vSphere 	**S'applique à**: NetApp HCI seulement Les administrateurs utilisent ces informations d'identification pour se connecter au client VMware vSphere. Lorsque vCenter fait partie de l'installation de NetApp HCI, les identifiants sont configurés dans le moteur de déploiement NetApp comme suit : • nomutilisateur@vsphere.locusmabl avec le mot de passe spécifié, et • admin@vsphere.locks.com avec le mot de passe spécifié. Lorsqu'un vCenter existant est utilisé pour déployer NetApp HCI, les identifiants d'authentification unique vSphere sont gérés par les administrateurs IT VMware.	"Mettre à jour les identifiants vCenter et ESXi".
Informations d'identification du contrôleur BMC (Baseboard Management Controller) 	**S'applique à**: NetApp HCI seulement Les administrateurs utilisent ces identifiants pour se connecter au BMC des nœuds de calcul NetApp dans un déploiement NetApp HCI. Le contrôleur BMC propose des fonctions de base de surveillance du matériel et de console virtuelle. Les identifiants BMC (parfois appelés *IPMI*) pour chaque nœud de calcul NetApp sont stockés de manière sécurisée sur le nœud mNode dans les déploiements NetApp HCI. NetApp Hybrid Cloud Control utilise les identifiants BMC dans la capacité d'un compte de service pour communiquer avec le BMC dans les nœuds de calcul lors des mises à niveau du micrologiciel du nœud de calcul. Lorsque les informations d'identification BMC sont modifiées, les informations d'identification des nœuds de calcul respectifs doivent également être mises à jour sur mNode pour conserver toutes les fonctionnalités de contrôle du cloud hybride.	• "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". • "Modifiez les informations d'identification BMC sur le nœud de gestion".

Type et icône d'informations d'identification	Utilisation par l'administrateur	Reportez-vous à ces instructions
Identifiants ESXi 	**S'applique à**: NetApp HCI seulement Les administrateurs peuvent se connecter à des hôtes ESXi à l'aide de SSH ou de DCUI local 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 le moteur de déploiement NetApp. Les identifiants root ESXi pour chaque nœud de calcul NetApp sont stockés en toute sécurité sur le nœud mNode dans les déploiements NetApp HCI. NetApp Hybrid Cloud Control utilise les identifiants se trouvant dans la capacité d'un compte de service pour communiquer avec les hôtes ESXi directement pendant les mises à niveau du firmware du nœud de calcul et les vérifications de l'état de santé. Lorsque les identifiants root ESXi sont modifiés par un administrateur VMware, les informations d'identification des nœuds de calcul respectifs doivent être mises à jour sur le nœud mNode pour conserver la fonctionnalité de contrôle du cloud hybride.	"Mettez à jour les informations d'identification pour les hôtes vCenter et ESXi".
Mot de passe d'intégration de la QoS 	**S'applique à**: NetApp HCI et optionnel en SolidFire Non utilisé pour les connexions interactives par les administrateurs. L'intégration de QoS entre VMware vSphere et Element Software s'effectue via : • Le plug-in Element pour vCenter Server, et • Service de qualité de service 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 NetApp Element Plug-in for vCenter Server SIOC est également appelé *QoSSIOC password*. Consultez l'article Element Plug-in for vCenter Server KB.

Type et icône d'informations d'identification	Utilisation par l'administrateur	Reportez-vous à ces instructions
Identifiants de l'appliance vCenter Service 	**S'applique à** : NetApp HCI uniquement si configuré par le moteur de déploiement NetApp 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 d'authentification unique vSphere peuvent également se connecter à l'appliance. Aucun impact sur les autres composants.	Aucune modification requise.
Identifiants d'administrateur du nœud de gestion NetApp 	**S'applique à**: NetApp HCI et optionnel en SolidFire Les administrateurs peuvent se connecter aux ordinateurs virtuels de nœud de gestion NetApp pour obtenir des fonctions avancées de configuration et de dépannage. 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 ont été spécifiés par l'utilisateur lors de l'installation initiale de ce nœud de calcul dans le moteur de déploiement NetApp. Aucun impact sur les autres composants.	Aucune modification requise.

Trouvez plus d'informations

- "Modifiez le certificat SSL par défaut du logiciel Element"
- "Modifiez le mot de passe IPMI pour les nœuds"
- "Activez l'authentification multifacteur"
- "Commencez par une gestion externe des clés"
- "Créez un cluster prenant en charge les disques FIPS"

Modifiez 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, le cluster crée un certificat SSL unique et une clé privée auto-signés qui sont utilisés pour toutes les communications HTTPS via l'interface utilisateur d'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 d'API suivantes pour obtenir plus d'informations sur le certificat SSL par défaut et apporter des modifications.

- **GetSSLCertificate**

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

- **SetSSLCertificate**

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

- **RemoveSSLCertificate**

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

> Le certificat SSL de cluster est automatiquement appliqué à tous les nouveaux nœuds ajoutés au cluster. Tout nœud supprimé 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.

Trouvez plus d'informations

- "Modifiez le certificat SSL par défaut du nœud de gestion"
- "Quelles sont les exigences relatives à la définition de certificats SSL personnalisés dans Element Software ?"
- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Modifiez le mot de passe IPMI par défaut pour les nœuds

Vous pouvez modifier le mot de passe administrateur par défaut de l'interface IPMI (Intelligent Platform Management interface) dès que vous disposez d'un accès IPMI à distance au nœud. Vous pouvez le faire si des mises à jour d'installation sont disponibles.

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

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

- Nœuds H410S
- Nœuds H610S

Modifiez le mot de passe IPMI par défaut pour les 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 avez besoin

Vous devez avoir configuré l'adresse IP IPMI pour chaque nœud de stockage.

Étapes

1. Ouvrez un navigateur Web sur un ordinateur qui peut atteindre le réseau IPMI et naviguez jusqu'à l'adresse IP IPMI du nœud.
2. Entrez le nom d'utilisateur `ADMIN` et mot de passe `ADMIN` dans l'invite de connexion.
3. Lorsque vous vous connectez, cliquez sur l'onglet **Configuration**.
4. Cliquez sur **utilisateurs**.
5. Sélectionner `ADMIN` Et cliquez sur **Modifier l'utilisateur**.
6. Cochez la case **Modifier le mot de passe**.
7. Entrez 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 avec des mots de passe IPMI par défaut.

Modifiez le mot de passe IPMI par défaut pour les 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 avez besoin

Vous devez avoir configuré l'adresse IP IPMI pour chaque nœud de stockage.

Étapes

1. Ouvrez un navigateur Web sur un ordinateur qui peut atteindre le réseau IPMI et naviguez jusqu'à l'adresse IP IPMI du nœud.
2. Entrez le nom d'utilisateur `root` et mot de passe `calvin` dans l'invite de connexion.
3. Lorsque vous vous connectez, cliquez sur l'icône de navigation dans le menu en haut à gauche de la page pour ouvrir le tiroir de la barre latérale.
4. Cliquez sur **Paramètres**.
5. Cliquez sur **gestion des utilisateurs**.
6. Sélectionnez l'utilisateur **Administrateur** dans la liste.
7. Activez la case à cocher **Modifier 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 avec mots de passe IPMI par défaut.

Trouvez plus d'informations

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

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

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

Il permet notamment d'afficher les commandes API activées par l'activité de l'interface utilisateur et de fournir des commentaires.

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

Pour en savoir plus

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

Afficher l'activité API

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

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

Pour plus d'informations sur chaque méthode, reportez-vous à la section "Référence de l'API du logiciel Element".

1. Dans la barre de navigation de l'interface utilisateur Element, cliquez sur **log API**.
2. Pour modifier le type d'activité API affiché dans la fenêtre Journal API, effectuez les opérations suivantes :
   a. Sélectionnez **demandes** pour afficher le trafic de requêtes API.
   b. Sélectionnez **réponses** pour afficher le trafic de réponse API.
   c. Pour filtrer les types de trafic API, sélectionnez l'une des options suivantes :
      - **Utilisateur initié** : trafic API par vos activités au cours de cette session d'interface utilisateur Web.
      - **Interrogation en arrière-plan** : trafic API généré par activité du système en arrière-plan.
      - **Current page** : trafic API généré par des tâches sur la page que vous consultez actuellement.

Trouvez plus d'informations

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

Taux de rafraîchissement de l'interface affecté par la charge du cluster

Selon les temps de réponse de l'API, le cluster peut ajuster automatiquement l'intervalle d'actualisation des données sur certaines parties de la page logicielle NetApp Element que vous affichez.

L'intervalle d'actualisation est réinitialisé par défaut lorsque vous rechargez la page dans votre navigateur. Vous pouvez afficher l'intervalle d'actualisation en cours en cliquant sur le nom du cluster dans le coin supérieur droit de la page. Notez que l'intervalle contrôle la fréquence des requêtes API, et non la rapidité à laquelle les données sont rétraitées par le serveur.

Lorsqu'un cluster est soumis à une charge importante, il peut être possible de mettre en file d'attente les demandes d'API depuis l'interface utilisateur d'Element. Dans de rares cas, lorsque la réponse du système est significativement retardée, comme une connexion réseau lente combinée à un cluster occupé, vous risquez d'être déconnecté de l'interface utilisateur Element si le système ne répond pas suffisamment rapidement aux demandes d'API mises en attente. Si vous êtes redirigé vers l'écran de déconnexion, vous pouvez vous reconnecter après avoir rejeté une invite d'authentification initiale du navigateur. Lorsque vous revenez à la page de présentation, vous pouvez être invité à saisir les informations d'identification du cluster si elles ne sont pas enregistrées par votre navigateur.

Icônes de 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 une référence rapide :

Icône	Description
	Actions
	Sauvegarde sur
	Cloner ou copier
	Supprimer ou purger
	Modifier
	Filtre
	Paire

	Actualisez
	Restaurer
	Source de restauration
	Retour arrière
	Snapshot

Laisser des commentaires

Vous pouvez améliorer l'interface utilisateur Web du logiciel Element et résoudre tous les problèmes liés à l'interface utilisateur à l'aide du formulaire de commentaires accessible via l'interface utilisateur.

1. À partir de n'importe quelle page de l'interface utilisateur de l'élément, cliquez sur le bouton **Feedback**.
2. Entrez les informations pertinentes dans les champs Résumé et Description.
3. Joignez toutes les captures d'écran utiles.
4. Entrez un nom et une adresse e-mail.
5. Cochez la case pour inclure les données relatives à votre environnement actuel.
6. Cliquez sur **soumettre**.

Trouvez plus d'informations

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

Gestion des 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, il 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 à l'aide du protocole CHAP"
- "Gérez les comptes utilisateurs d'administrateur du cluster"

Pour en savoir plus

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

Travailler avec des comptes à l'aide du protocole 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 CHAP (Challenge-Handshake Authentication Protocol) requise pour accéder aux volumes qui lui sont affectés. Lorsque vous créez un volume, il est affecté à un compte spécifique.

Un compte peut comporter jusqu'à deux milliers de volumes qui lui sont attribués, mais un volume ne peut appartenir qu'à un seul compte.

Créez 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. Saisissez un **Nom d'utilisateur**.
4. Dans la section **CHAP Settings**, entrez les informations suivantes :

   Laissez les champs d'informations d'identification vides pour générer automatiquement l'un ou l'autre des mots de passe.

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

Afficher les détails du compte

Vous pouvez afficher l'activité de performances des comptes individuels dans un format graphique.

Le graphique fournit des informations d'E/S et de débit pour le compte. Les niveaux d'activité moyenne et maximale sont indiqués par incréments de périodes de déclaration de 10 secondes. Ces statistiques comprennent l'activité de tous les volumes affectés au compte.

1. Sélectionnez **gestion** > **comptes**.
2. Cliquez sur l'icône actions d'un compte.
3. Cliquez sur **Afficher les détails**.

Voici quelques-uns des détails :

- **Statut** : état du compte. Valeurs possibles :

- Active : un compte actif.
- Verrouillé : un compte verrouillé.
- Supprimé : compte supprimé et purgé.

- **Volumes actifs** : nombre de volumes actifs affectés au compte.
- **Compression** : le score d'efficacité de compression pour les volumes affectés au compte.
- **Déduplication** : score d'efficacité de la déduplication pour les volumes affectés au compte.
- **Provisionnement fin** : le score d'efficacité du provisionnement fin pour les volumes affectés au compte.
- **Efficacité globale** : le score global d'efficacité pour les volumes affectés au compte.

Modifier un compte

Vous pouvez modifier un compte pour modifier son statut, modifier les secrets CHAP ou modifier le nom du compte.

La modification des paramètres CHAP d'un compte ou la suppression d'initiateurs ou de volumes d'un groupe d'accès peut entraîner une perte inattendue de l'accès aux volumes. Pour vérifier que l'accès au volume ne sera pas perdu de façon inattendue, déconnectez toujours les sessions iSCSI qui seront affectées par une modification de compte ou de groupe d'accès. Vérifiez également que les initiateurs peuvent se reconnecter aux volumes après la modification des paramètres de l'initiateur et des paramètres du cluster.

Les volumes persistants associés à des services de gestion sont attribués à un nouveau compte créé lors de l'installation ou de la mise à niveau. Si vous utilisez des volumes persistants, ne modifiez pas ou ne supprimez pas leur compte associé.

1. Sélectionnez **gestion** > **comptes**.
2. Cliquez sur l'icône actions d'un compte.
3. Dans le menu qui s'affiche, sélectionnez **Modifier**.
4. **Facultatif:** modifiez le **Nom d'utilisateur**.
5. **Facultatif :** cliquez sur la liste déroulante **Statut** et sélectionnez un autre état.

   Si vous changez l'état à **Locked**, toutes les connexions iSCSI au compte sont résiliées et le compte n'est plus accessible. Les volumes associés au compte sont conservés, mais ils ne sont pas détectables iSCSI.

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

   Si vous ne modifiez pas les informations d'identification **CHAP Settings**, elles restent les mêmes. Si vous ne renseignez pas les champs d'informations d'identification, 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 supprimez tous les volumes associés au compte avant de supprimer le compte.

Les volumes persistants associés à des services de gestion sont attribués à un nouveau compte créé lors de l'installation ou de la mise à niveau. Si vous utilisez des volumes persistants, ne modifiez pas ou ne supprimez pas leur compte associé.

1. Sélectionnez **gestion** > **comptes**.
2. Cliquez sur l'icône actions du compte à supprimer.
3. Dans le menu qui s'affiche, sélectionnez **Supprimer**.
4. Confirmez l'action.

Trouvez plus d'informations

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

Gérez les comptes utilisateurs d'administrateur du cluster

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

Types de compte d'administrateur du cluster de stockage

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

- **Compte d'administrateur de cluster principal**

  Ce compte administrateur est créé lors de la création du cluster. Il s'agit du compte administratif principal avec le niveau d'accès le plus élevé au cluster. Ce compte est similaire à un utilisateur root dans un système Linux. Vous pouvez modifier le mot de passe de ce compte administrateur.

- **Compte administrateur de cluster**

  Vous pouvez donner à un administrateur de cluster une plage limitée d'accès administratif afin d'effectuer des tâches spécifiques au sein d'un cluster. Les identifiants attribués à chaque compte d'administrateur du cluster sont utilisés pour authentifier les demandes d'interface utilisateur d'API et d'éléments du système de stockage.

Un compte d'administrateur de cluster local (non LDAP) est nécessaire 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 à l'échelle du cluster (non LDAP), effectuez les opérations suivantes :
   a. Cliquez sur **utilisateurs** > **administrateurs de cluster**.

2. Sur la page administrateurs de cluster de l'onglet utilisateurs, vous pouvez afficher les informations suivantes.
   - **ID** : numéro séquentiel attribué au compte administrateur de cluster.
   - **Nom d'utilisateur** : nom donné au compte administrateur de cluster lors de sa création.
   - **Accès** : les autorisations d'utilisateur attribuées au compte d'utilisateur. Valeurs possibles :
     - lecture
     - création de rapports
     - nœuds
     - disques
     - volumes
     - comptes
     - ClusterAdmins
     - administrateur

     Toutes les autorisations sont disponibles pour le type d'accès administrateur.
   - **Type** : le type d'administrateur de cluster. Valeurs possibles :
     - Cluster
     - LDAP
   - **Attributes** : si le compte administrateur de cluster a été créé à l'aide de l'API d'élément, cette colonne affiche toutes les paires nom-valeur qui ont été définies à l'aide de cette méthode.

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

Créez un compte d'administrateur de cluster

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

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

"Activez l'authentification LDAP à l'aide de l'interface utilisateur Element"

Vous pouvez modifier ultérieurement les privilèges du compte administrateur du cluster pour les rapports, les nœuds, les disques, les volumes, les comptes, et l'accès au niveau du cluster. Lorsque vous activez une autorisation, le système attribue un accès en écriture à 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 tout compte utilisateur 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 à l'échelle du cluster (non LDAP), effectuez les opérations suivantes :

a. Cliquez sur **utilisateurs** > **administrateurs de cluster**.
b. Cliquez sur **Créer un administrateur de cluster**.
c. Sélectionnez le type d'utilisateur **Cluster**.
d. Entrez un nom d'utilisateur et un mot de passe pour le compte et confirmez le mot de passe.
e. Sélectionnez les autorisations utilisateur à appliquer au compte.
f. Cochez la case pour accepter le contrat de licence de l'utilisateur final.
g. Cliquez sur **Créer un administrateur de cluster**.

2. Pour créer un compte d'administrateur de cluster dans le répertoire LDAP, effectuez les opérations suivantes :

a. Cliquez sur **Cluster** > **LDAP**.
b. Assurez-vous que l'authentification LDAP est activée.
c. Cliquez sur **Test User Authentication** et copiez le nom distinctif qui apparaît pour l'utilisateur ou l'un des groupes dont l'utilisateur est membre afin de pouvoir le coller ultérieurement.
d. Cliquez sur **utilisateurs** > **administrateurs de cluster**.
e. Cliquez sur **Créer un administrateur de cluster**.
f. Sélectionnez le type d'utilisateur LDAP.
g. Dans le champ Nom unique, suivez l'exemple de la zone de texte pour entrer un nom distinctif complet pour l'utilisateur ou le groupe. Vous pouvez également 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 aura les autorisations de ce compte d'administrateur.

Pour ajouter des utilisateurs ou des groupes LDAP Cluster Admin, le format général du nom d'utilisateur est « LDAP:<Nom unique complet> ».

a. Sélectionnez les autorisations utilisateur à appliquer au compte.
b. Cochez la case pour accepter le contrat de licence de l'utilisateur final.
c. Cliquez sur **Créer un administrateur de cluster**.

Modifiez les autorisations d'administrateur de cluster

Vous pouvez modifier les privilèges du compte administrateur du cluster pour les comptes de rapports, les nœuds, les disques, les volumes, les comptes, et l'accès au niveau du cluster. Lorsque vous activez une autorisation, le système attribue un accès en écriture à 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 de cluster**.
2. Cliquez sur l'icône actions de l'administrateur de 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 du cluster

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

1. Cliquez sur **utilisateurs** > **administrateurs de cluster**.
2. Cliquez sur l'icône actions de l'administrateur de cluster que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Dans le champ Modifier le mot de passe, saisissez un nouveau mot de passe et confirmez-le.
5. Cliquez sur **Enregistrer les modifications**.

Trouvez plus d'informations

- "Activez l'authentification LDAP à l'aide de l'interface utilisateur Element"
- "Désactivez LDAP"
- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Gérez LDAP

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

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

Vous pouvez utiliser les adresses IPv4 et IPv6.

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

1. **Effectuer les étapes de pré-configuration pour la prise en charge du protocole LDAP**. Vérifiez que vous disposez de tous les détails nécessaires à la configuration de l'authentification LDAP.
2. **Activer l'authentification LDAP**. Utilisez l'interface utilisateur Element ou l'API Element.
3. **Valider la configuration LDAP**. Vous pouvez également vérifier que le cluster est configuré avec les valeurs correctes en exécutant la méthode GetLdapConfiguration API ou en vérifiant la configuration LCAP à l'aide de l'interface utilisateur Element.
4. **Tester l'authentification LDAP** (avec le `readonly` utilisateur). Vérifiez que la configuration LDAP est correcte soit en exécutant la méthode TestLdapAuthentication API soit en utilisant l'interface utilisateur Element. Pour ce test initial, utilisez le nom d'utilisateur "sAMAccountName" de l' `readonly` utilisateur. Cela permet de vérifier que votre cluster est configuré correctement pour l'authentification LDAP et de valider également que `readonly` les identifiants et l'accès sont corrects. Si cette étape échoue, répétez les étapes 1 à 3.
5. **Tester l'authentification LDAP** (avec un compte utilisateur que vous souhaitez ajouter). Répétez setp 4 avec un compte utilisateur que vous souhaitez ajouter en tant qu'administrateur de cluster Element. Copiez le `distinguished` Nom (DN) ou utilisateur (ou groupe). Ce DN sera utilisé à l'étape 6.

6. **Ajouter le cluster LDAP admin** (copiez et collez le DN à partir de l'étape d'authentification LDAP de test). En utilisant soit l'interface utilisateur Element soit la méthode de l'API AddapClusterAdmin, créez un nouvel utilisateur administrateur cluster avec le niveau d'accès approprié. Pour le nom d'utilisateur, collez le nom d'utilisateur complet que vous avez copié à l'étape 5. Cela garantit que le DN est correctement formaté.
7. **Tester l'accès admin du cluster**. Connectez-vous au cluster à l'aide du nouvel utilisateur administrateur de cluster LDAP. Si vous avez ajouté un groupe LDAP, vous pouvez vous connecter en tant qu'utilisateur de ce groupe.

Suivez les étapes de pré-configuration pour la prise en charge du protocole LDAP

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

Étapes

1. Configurer un serveur Windows Active Directory.
2. **Facultatif:** activez 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 à l'aide de l'interface utilisateur Element

Vous pouvez configurer l'intégration du système de stockage avec un serveur LDAP existant. Les administrateurs LDAP peuvent ainsi gérer de façon centralisée l'accès au système de stockage pour les utilisateurs.

Vous pouvez configurer LDAP à l'aide de l'interface utilisateur Element ou de l'API Element. Cette procédure explique comment configurer LDAP à l'aide de l'interface utilisateur Element.

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

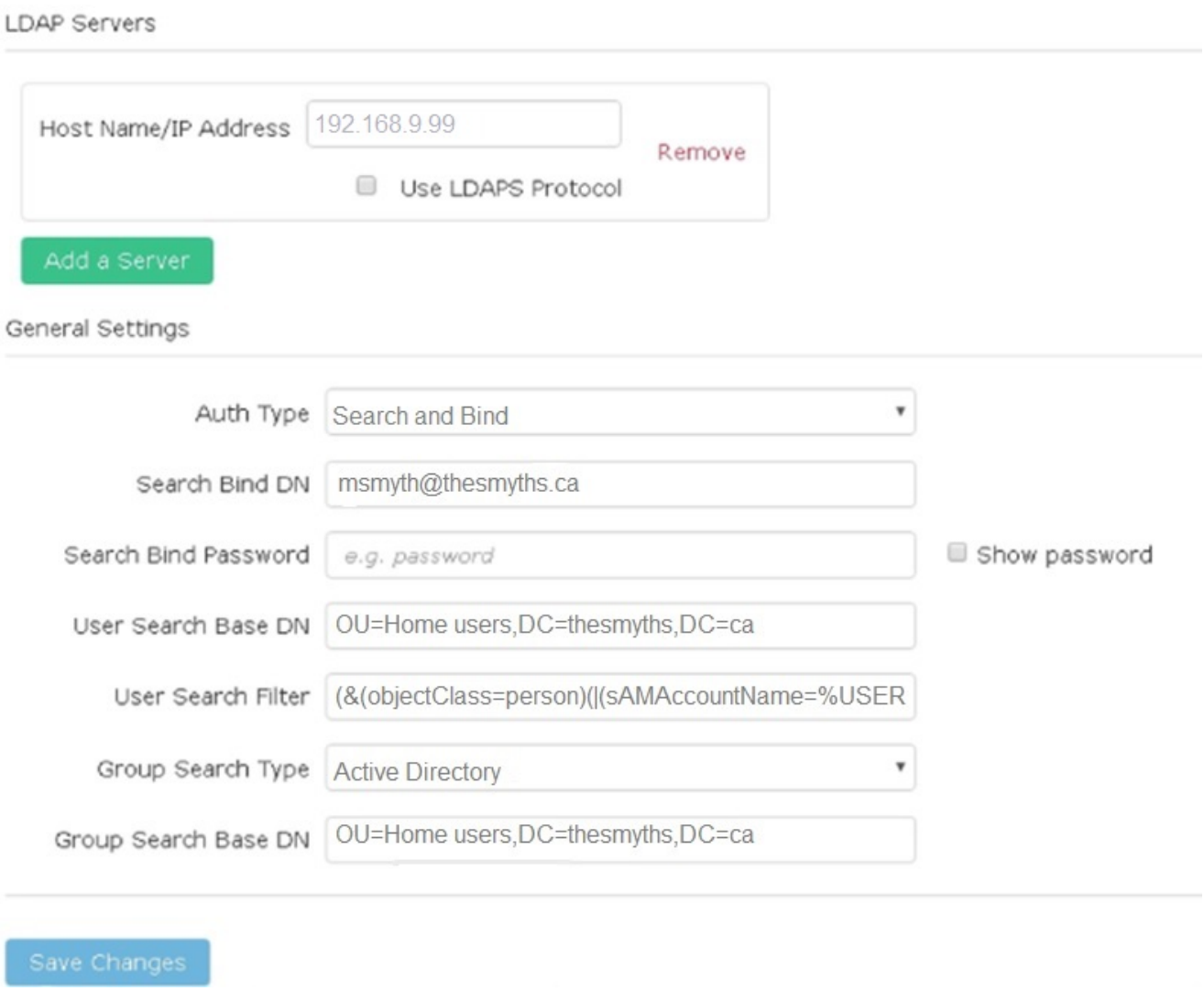
Étapes

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

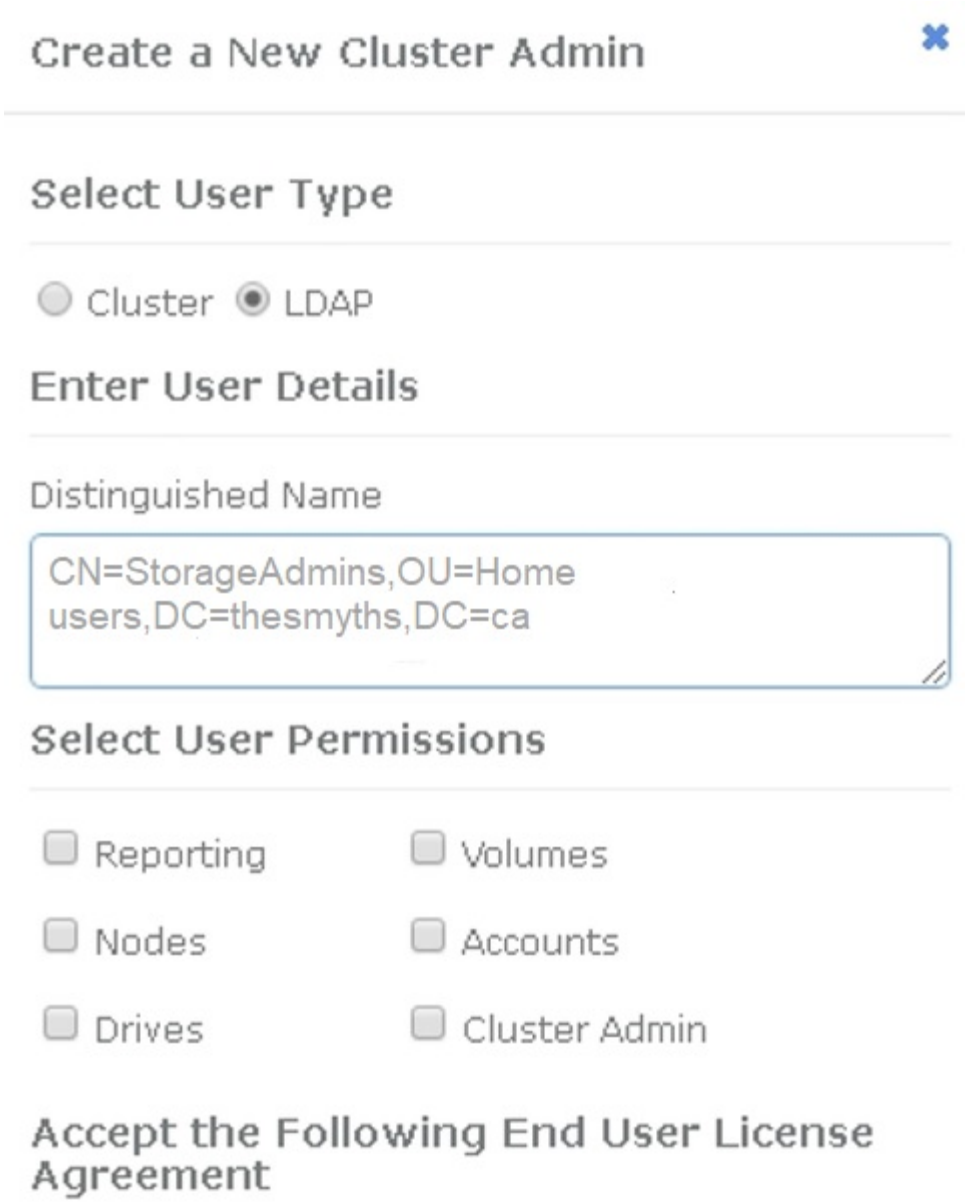
   Un numéro de port personnalisé facultatif peut également être saisi.

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

5. **Facultatif:** sélectionnez **utiliser le protocole LDAPS**.
6. Entrez les informations requises dans **Paramètres généraux**.



7. Cliquez sur **Activer LDAP**.
8. Cliquez sur **Tester l'authentification utilisateur** si vous souhaitez tester l'accès au serveur pour un utilisateur.
9. Copiez le nom distinctif et les informations sur le groupe d'utilisateurs qui s'affichent 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 tout le monde puisse se connecter, procédez comme suit :
    a. Cliquez sur **User** > **View**.



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

   Maintenant, vous avez un utilisateur avec la valeur d'un groupe Active Directory.

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

Activez l'authentification LDAP avec l'API Element

Vous pouvez configurer l'intégration du système de stockage avec un serveur LDAP existant. Les administrateurs LDAP peuvent ainsi gérer de façon centralisée l'accès au système de stockage pour les utilisateurs.

Vous pouvez configurer LDAP à l'aide de l'interface utilisateur Element ou de l'API Element. Cette procédure explique comment configurer LDAP à l'aide de l'API Element.

Pour exploiter l'authentification LDAP sur un cluster SolidFire, vous activez d'abord 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. Entrez 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 readonly pour rechercher d'abord l'utilisateur authentifié et lier ensuite cet utilisateur s'il est trouvé et authentifié.
GroupSearchBaseDN : dc=prodtest,dc=solidfire,dc=net	Spécifie l'emplacement dans l'arborescence LDAP pour commencer la recherche de groupes. Pour cet exemple, nous avons utilisé la racine de notre arbre. Si votre arborescence LDAP est très grande, vous pouvez le définir sur une sous-arborescence plus granulaire pour réduire les temps de recherche.

Paramètres utilisés	Description
UserSearchBaseDN : dc=prodtest,dc=solidfire,dc=net	Indique l'emplacement dans l'arborescence LDAP pour commencer la recherche d'utilisateurs. Pour cet exemple, nous avons utilisé la racine de notre arbre. Si votre arborescence LDAP est très grande, vous pouvez le définir sur une sous-arborescence plus granulaire pour réduire les temps de recherche.
GroupSearchType : ActiveDirectory	Utilise le serveur Windows Active Directory comme serveur LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Pour utiliser userPrincipalName (adresse e-mail pour la connexion), vous pouvez remplacer userSearchFilter par :
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
Ou, pour effectuer une recherche à la fois userPrincipalName et sAMAccountName, vous pouvez utiliser le userSearchFilter suivant :
 	
`"(&(objectClass=person)(`
	(SAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%))» ----

Utilise sAMAccountName comme nom d'utilisateur pour la connexion à la grappe 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 à des entrées dont la valeur est « personne » dans l'attribut objectClass.	SearchBindDN
Il s'agit du nom distinctif de l'utilisateur readonly qui sera utilisé pour effectuer une recherche dans l'annuaire LDAP. Pour le répertoire actif, il est généralement plus facile d'utiliser le nom d'utilisateur en titre (format d'adresse e-mail) pour l'utilisateur.	SearchBindPassword

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

qu'utilisateur dans ce groupe.

Afficher les détails LDAP

Affichez les informations LDAP sur la page LDAP de l'onglet Cluster.

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

1. Pour afficher les détails LDAP avec l'interface utilisateur d'élément, 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
     - Rechercher et lier
   - **Rechercher un DN de liaison** : un DN complet pour se connecter avec pour effectuer une recherche LDAP pour l'utilisateur (nécessite un accès de niveau de liaison à l'annuaire LDAP).
   - **Search Bind Password** : mot de passe utilisé pour authentifier l'accès au serveur LDAP.
   - **Recherche utilisateur DN de base** : le DN de base de l'arborescence utilisée pour lancer la recherche utilisateur. Le système recherche la sous-arborescence à partir de l'emplacement spécifié.
   - **Filtre de recherche d'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.
     - Aucun groupe : aucun support de groupe.
     - DN du membre : groupes de style DN du membre (niveau unique).
   - **Recherche de groupe DN de base** : le DN de base de l'arborescence utilisée pour lancer la recherche de groupe. Le système recherche la sous-arborescence à partir de l'emplacement spécifié.
   - **Tester l'authentification utilisateur** : une fois le protocole LDAP configuré, utilisez-le pour tester le nom d'utilisateur et l'authentification par mot de passe pour le serveur LDAP. Saisissez un compte déjà existant pour le tester. Les informations relatives au nom distinctif et au groupe d'utilisateurs s'affichent, que vous pouvez copier pour une utilisation ultérieure lors de la création d'administrateurs de cluster.

Testez la configuration LDAP

Après avoir configuré LDAP, vous devez le tester à l'aide de l'interface utilisateur d'Element ou de 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 **Test authentification LDAP**.
   c. Pour résoudre les problèmes, utilisez les informations du tableau ci-dessous :

Message d'erreur	Description
`xLDAPUserNotFound`	• L'utilisateur en cours de test est introuvable dans la configuration `userSearchBaseDN` sous-arbre. • Le `userSearchFilter` n'est pas configuré correctement.
`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 incorrecte.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	Le nom d'utilisateur ou le mot de passe en lecture seule n'est pas configuré correctement.
`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 UO imbriquée. Cela peut entraîner des problèmes de permission. La solution consiste à inclure l'UO dans les entrées DN de base d'utilisateur et de 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. Passez en revue les résultats. Si l'appel API réussit, les résultats incluent le nom distinctif de l'utilisateur spécifié et une liste de groupes dans lesquels 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"
     }
}
```

Désactivez LDAP

Vous pouvez désactiver l'intégration LDAP à l'aide de l'interface utilisateur Element.

Avant de commencer, notez tous les paramètres de configuration, car la désactivation du protocole LDAP efface tous les paramètres.

Étapes

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

Trouvez plus d'informations

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

Gérez votre système

Vous pouvez gérer votre système dans l'interface utilisateur Element. C'est notamment l'activation de l'authentification multifacteur, la gestion des paramètres de cluster, la prise

en charge de la norme FIPS (Federal information Processing Standards) et la gestion des clés externe.

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

Pour en savoir plus

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

Activez l'authentification multifacteur

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

Configuration de l'authentification multifacteur

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

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

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

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

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

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

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

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

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

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

Trouvez plus d'informations

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

Informations supplémentaires pour l'authentification multifacteur

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

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

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

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

Trouvez plus d'informations

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

Configurez les paramètres du cluster

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

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

Options

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

Trouvez plus d'informations

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

Activez et désactivez le cryptage des données au repos pour un cluster

Avec les clusters SolidFire, vous pouvez chiffrer toutes les données au repos stockées sur les disques du cluster. Vous pouvez activer la protection des lecteurs à autochiffrement (SED) au niveau du cluster à l'aide de l'une ou l'autre "chiffrement matériel ou logiciel pour les données au repos".

Vous pouvez activer le chiffrement matériel au repos à l'aide de l'interface utilisateur et de l'API d'Element. L'activation de la fonctionnalité de chiffrement matériel au repos n'a aucune incidence sur les performances ou l'efficacité du cluster. Vous pouvez activer le chiffrement logiciel au repos uniquement à l'aide de l'API Element.

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

> Pour les clusters de stockage 100 % Flash SolidFire, le chiffrement logiciel au repos doit être activé au cours de la création du cluster et ne peut pas être désactivé une fois le cluster créé.

Ce dont vous avez besoin

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

Vérifiez le chiffrement des données au repos

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

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

Options

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

Chiffrement matériel des données au repos

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

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

Chiffrement logiciel des données au repos

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

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

Désactivation du chiffrement matériel des données au repos

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

Trouvez plus d'informations

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

Définissez le seuil maximal du cluster

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

Ce dont vous avez besoin

Vous devez disposer des privilèges d'administrateur de cluster.

Étapes

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

Trouvez plus d'informations

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

Activez et désactivez l'accès au support

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

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

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

Gérez la bannière Conditions d'utilisation

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

Options

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

Activez la bannière Conditions d'utilisation

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

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

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

   Ne pas dépasser 4096 caractères.

3. Cliquez sur **Activer**.

Modifiez la bannière Conditions d'utilisation

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

Ce dont vous avez besoin

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

Étapes

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

   Ne pas dépasser 4096 caractères.

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

Désactivez la bannière Conditions d'utilisation

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

Ce dont vous avez besoin

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

Étapes

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

Définissez le protocole de temps du réseau

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

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

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

Vous pouvez demander à chaque nœud d'un cluster d'interroger un serveur NTP (Network Time Protocol) pour les mises à jour. Le cluster contacte uniquement les serveurs configurés et demande les informations NTP à leur place.

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

L'utilisation du FQDN dépend de la mise en place et de l'exploitation des paramètres DNS de chaque nœud de

stockage. Pour ce faire, configurez les serveurs DNS sur chaque nœud de stockage et assurez-vous que les ports sont ouverts en consultant la page Configuration requise du port réseau.

Vous pouvez entrer jusqu'à cinq serveurs NTP différents.

Vous pouvez utiliser les adresses IPv4 et IPv6.

Ce dont vous avez besoin

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

Étapes

1. Configurez une liste d'adresses IP et/ou de FQDN dans les paramètres du serveur.
2. Assurez-vous que le DNS est correctement défini sur les nœuds.
3. Cliquez sur **Cluster** > **Paramètres**.
4. Sous Paramètres du protocole d'heure du réseau, sélectionnez **non**, qui utilise la configuration NTP standard.
5. Cliquez sur **Enregistrer les modifications**.

Trouvez plus d'informations

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

Configurez le cluster pour écouter les diffusions NTP

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

Ce dont vous avez besoin

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

Étapes

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

Trouvez plus d'informations

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

Gérer SNMP

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

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

Vous pouvez utiliser les adresses IPv4 et IPv6.

Détails SNMP

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

- **MIB SNMP**

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

- **Paramètres SNMP généraux**

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

- **Paramètres de déroutement SNMP**

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

Configurez un demandeur SNMP

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

1. Cliquez sur Menu:Cluster[SNMP].
2. Sous **Paramètres SNMP généraux**, cliquez sur **Oui** pour activer SNMP.
3. Dans la liste **version**, sélectionnez **version 2**.
4. Dans la section **Requetors**, saisissez les informations **Community String** et **Network**.

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

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

Trouvez plus d'informations

- Configurer les traps SNMP

Configurez un utilisateur SNMP USM

Lorsque vous activez SNMP version 3, vous devez configurer un utilisateur USM pour qu'il reçoive les requêtes SNMP autorisées.

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

Configurer les traps SNMP

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

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

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

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

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

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

- Statistiques du cluster
- Statistiques de volume

- Volumes par statistiques de compte
- Statistiques de nœud
- Autres données telles que les rapports, les erreurs et les événements système

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

Étapes

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

Gérer les disques

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

Pour en savoir plus

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

Détails sur le disque

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

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

Les éléments suivants apparaissent dans la liste des lecteurs actifs.

- **ID de lecteur**

  Numéro séquentiel attribué au disque.

- **ID de nœud**

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

- **Nom du noeud**

  Nom du nœud qui héberge le disque.

- **Slot**

  Numéro de logement où le lecteur est physiquement situé.

- **Capacité**

  Taille du lecteur, en Go.

- **Série**

  Numéro de série du disque.

- **Usure restante**

  L'indicateur de niveau d'usure.

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

- **Type**

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

Gérer des nœuds

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

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

Trouvez plus d'informations

Ajout d'un nœud à un cluster

Ajout d'un nœud à un cluster

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

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

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

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

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

Vous pouvez ajouter des nœuds aux appliances NetApp HCI.

Étapes

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

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

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

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

   Le nœud apparaît dans la liste des nœuds actifs.

Trouvez plus d'informations

Gestion des versions de nœud et compatibilité

Gestion des versions de nœud et compatibilité

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

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

- **Majeur**

  Le premier numéro désigne une version logicielle. Un nœud avec un numéro de composant majeur ne

peut pas être ajouté à un cluster contenant des nœuds d'un numéro de patch majeur différent, ni un cluster peut être créé avec des nœuds de versions majeures mixtes.

- **Mineur**

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

- **Micro**

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

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

Capacité du cluster dans un environnement de nœuds mixtes

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

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

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

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

- SF3010
- SF6010
- SF9010

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

Afficher les détails du nœud

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

Étapes

1. Cliquez sur **Cluster** > **Nodes**.

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

Afficher les détails des ports Fibre Channel

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

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

Étapes

1. Cliquez sur **Cluster** > **FC ports**.
2. Pour filtrer les informations de cette page, cliquez sur **Filter**.
3. Consultez les détails :
   - **ID de nœud** : nœud hébergeant la session pour la connexion.
   - **Nom du nœud** : nom du nœud généré par le système.
   - **Slot** : numéro de logement où se trouve le port Fibre Channel.
   - **Port HBA** : port physique sur l'adaptateur de bus hôte Fibre Channel (HBA).

- **WWNN** : le nom de nœud mondial.
- **WWPN** : nom du port mondial cible.
- **WWN du commutateur** : nom mondial du commutateur Fibre Channel.
- **Etat du port** : état actuel du port.
- **NPort ID** : ID du port de nœud sur la structure Fibre Channel.
- **Vitesse** : vitesse Fibre Channel négociée. Les valeurs possibles sont les suivantes :
  - 4 Gbit/s
  - 8 Go/s.
  - 16 Gbits/s

Trouvez plus d'informations

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

Gérer des réseaux virtuels

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

Trouvez plus d'informations

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

Ajouter un réseau virtuel

Vous pouvez ajouter un nouveau réseau virtuel à une configuration de cluster pour permettre la connexion d'un environnement mutualisé à un cluster exécutant le logiciel Element.

Ce dont vous avez besoin

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

Vous devez tenir compte des critères suivants pour cette configuration :

- Les VLAN qui ne sont pas activés par VRF exigent que les initiateurs se trouvent dans le même sous-réseau que le SVIP.
- Les VLAN activés par VRF ne nécessitent pas que les initiateurs se trouvent sur le même sous-réseau que le SVIP, et le routage est pris en charge.

- Le SVIP par défaut ne requiert pas que les initiateurs se trouvent dans le même sous-réseau que le SVIP, et le routage est pris en charge.

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

Étapes

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

Afficher les détails des réseaux virtuels

Étapes

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

Activer le routage et le transfert virtuels

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

Vous ne pouvez activer VRF qu'au moment de la création d'un VLAN. Si vous souhaitez revenir à une fonction

non VRF, vous devez supprimer et recréer le VLAN.

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

Trouvez plus d'informations

Ajouter un réseau virtuel

Modifier un réseau virtuel

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

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

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

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

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

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

Lien vers les articles de la base de connaissances de dépannage

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

- "Avertissement IP en double après ajout d'un nœud de stockage dans VLAN sur le cluster Element"

- "Comment déterminer les adresses IP VLAN utilisées et les nœuds auxquels ces adresses IP sont affectées dans l'élément"

Modifier les VLAN VRF

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

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

Supprimer un réseau virtuel

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

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

Trouvez plus d'informations

Modifier un réseau virtuel

Créez un cluster prenant en charge les disques FIPS

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

- "Évitez de mélanger les nœuds pour les disques FIPS"
- "Activation du chiffrement des données au repos"
- "Identifiez si les nœuds sont prêts pour la fonctionnalité disques FIPS"
- "Activez la fonctionnalité disques FIPS"
- "Vérifiez l'état du lecteur FIPS"
- "Dépannez la fonctionnalité de lecteur FIPS"

Évitez de mélanger les nœuds pour les disques FIPS

Pour préparer l'activation de la fonctionnalité de lecteurs FIPS, évitez de combiner les

nœuds où certains prennent en charge des disques FIPS et d'autres non.

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

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

Activation du chiffrement des données au repos

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

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

Trouvez plus d'informations

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

Identifiez si les nœuds sont prêts pour la fonctionnalité disques FIPS

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

Le rapport obtenu affiche l'un des États suivants :

- Aucun : le nœud ne peut pas prendre en charge la fonctionnalité disques FIPS.
- Partiel : les nœuds sont compatibles FIPS, mais tous les disques ne sont pas des disques FIPS.
- Prêt : le nœud est compatible FIPS et tous les disques sont des disques FIPS ou pas de disque.

Étapes

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

   ```
   GetFipsReport
   ```

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

prendre en charge la fonctionnalité disques FIPS.

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

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

Trouvez plus d'informations

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

Activez la fonctionnalité disques FIPS

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

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

Étape

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

   ```
   EnableFeature params: FipsDrives
   ```

Trouvez plus d'informations

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

Vérifiez l'état du lecteur FIPS

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

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

   ```
   GetFeatureStatus
   ```

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

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

Trouvez plus d'informations

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

Dépannez la fonctionnalité de lecteur FIPS

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

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

Trouvez plus d'informations

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

Activez FIPS 140-2 pour HTTPS sur votre cluster

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

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

> Une fois le mode FIPS 140-2 activé, celui-ci ne peut pas être désactivé. Lorsque le mode FIPS 140-2-2 est activé, chaque nœud du cluster redémarre et s'exécute automatiquement pour assurer le bon fonctionnement de NCSM en mode certifié FIPS 140-2. Cela entraîne une interruption des connexions de stockage et de gestion du cluster. Vous devez planifier soigneusement et activer ce mode uniquement si votre environnement a besoin du mécanisme de chiffrement qu'il offre.

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

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

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

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

Trouvez plus d'informations

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

Chiffrement SSL

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

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

- **FIPS 140-2 désactivé**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A.

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A.

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C

  TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A.

TLS_RSA_WAS_AES_128_GCM_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (RSA 2048) - A

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (RSA 2048) - A

TLS_RSA_WITH_IDEA_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_RC4_128_MD5 (RSA 2048) - C

TLS_RSA_WITH_RC4_128_SHA (RSA 2048) - C.

TLS_RSA_WITH_SEED_CBC_SHA (RSA 2048) - A.

- **FIPS 140-2 activé**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A.

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECT571R1) - A.

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C

  TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A.

  TLS_RSA_WAS_AES_128_GCM_SHA256 (RSA 2048) - A.

  TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.

Trouvez plus d'informations

Activez FIPS 140-2 pour HTTPS sur votre cluster

Commencez par une gestion externe des clés

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

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

Trouvez plus d'informations

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

Configurez la gestion externe des clés

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

Ce dont vous avez besoin

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

Étapes

1. Établissez une relation de confiance avec le serveur de clés externe (EKS).
   a. Créez une paire de clés publique/privée pour le cluster Element qui est utilisé pour établir une relation de confiance avec le serveur clé en appelant la méthode API suivante : "CreatePublicPrivateKeypair"
   b. Obtenir la demande de signature de certificat (CSR) que l'autorité de certification doit signer. La RSC permet au serveur de clés de vérifier que le cluster d'éléments qui accédera aux clés est authentifié comme cluster d'éléments. Appelez la méthode API suivante : "GetClientCertificateSignRequest"
   c. Utilisez EKS/Certificate Authority pour signer la RSC récupérée. Pour plus d'informations, consultez la documentation d'un fournisseur tiers.

2. Créez un serveur et un fournisseur sur le cluster pour communiquer avec EKS. Un fournisseur clé définit l'endroit où une clé doit être obtenue et un serveur définit les attributs spécifiques de l'EKS qui seront communiqués.
   a. Créez un fournisseur de clés où résident les détails du serveur de clés en appelant la méthode API suivante : "CreateKeyProviderKmip"
   b. Créez un serveur de clés fournissant le certificat signé et le certificat de clé publique de l'autorité de certification en appelant les méthodes API suivantes : "CreateKeyServerKmip" "TestKeyServerKmip"

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

   c. Ajoutez le serveur de clés dans le conteneur du fournisseur de clés en appelant les méthodes d'API suivantes :"AddKeyServerToProviderKmip" "TestKeyProviderKmip"

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

3. Pour le chiffrement au repos, effectuez l'une des opérations suivantes :
   a. (Pour le chiffrement matériel des données au repos) Activer "chiffrement matériel au repos" En fournissant l'ID du fournisseur de clés qui contient le serveur de clés utilisé pour stocker les clés en appelant le "EnableEncryptionAtRest" Méthode API.

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

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

Trouvez plus d'informations

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

Chiffrement logiciel de nouvelle clé pour la clé principale REST

Vous pouvez utiliser l'API Element pour re-saisir une clé existante. Ce processus crée une nouvelle clé principale de remplacement pour votre serveur de gestion de clés externe. Les clés principales sont toujours remplacées par de nouvelles clés principales et ne sont jamais dupliquées ou remplacées.

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

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

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

Ce dont vous avez besoin

- Vous avez activé le chiffrement logiciel au repos à l'aide du "CreateCluster" D'une nouvelle méthode située sur un nouveau cluster, qui ne contient pas de volumes et n'a pas d'E/S. Utilisez le lien :../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] pour confirmer que l'état est `enabled` avant de continuer.
- Vous avez "établissement d'une relation de confiance" Entre le cluster SolidFire et un serveur de clés externe (EKS). Exécutez le "TestKeyProviderKmip" méthode permettant de vérifier qu'une connexion au fournisseur de clés est établie.

Étapes

1. Exécutez le "ListeKeyProvidersKmip" Commande et copie l'ID du fournisseur de clés (`keyProviderID`).
2. Exécutez le "RekeySoftwareEncryptionAtResteMasterKey" avec le `keyManagementType` ens. paramètre `external` et `keyProviderID` Comme numéro d'ID du fournisseur de clés de l'étape précédente :

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

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

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

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

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

Trouvez plus d'informations

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

Récupérer les clés d'authentification inaccessibles ou non valides

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

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

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

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

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

Étapes à supprimer :

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

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

Commandes d'API de gestion externe des clés

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

Utilisé pour établir une relation de confiance entre le cluster et les serveurs appartenant à un client externe :

- CreatePublicPrivateKeypair
- GetClientCertificateSignRequest

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

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

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

- CreateKeyProviderKmip
- DeleteKeyProviderKmip

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

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

Gérez les volumes et les volumes virtuels

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

- "Utilisation de volumes"
- "Utilisation des volumes virtuels"
- "Utilisation des groupes d'accès de volumes et des initiateurs"

Pour en savoir plus

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

Utilisation de volumes

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

Trouvez plus d'informations

- "Gestion des règles de qualité de service"
- "Créer un volume"
- "Consultez les détails de performances de chaque volume"
- "Modifier les volumes actifs"
- "Supprimer un volume"
- "Restaurer un volume supprimé"
- "Purger un volume"
- "Clonez un volume"
- "Attribuez des LUN aux volumes Fibre Channel"

- "Appliquer une policy de QoS aux volumes"
- "Ne supprime pas l'association de la policy QoS d'un volume"

Gestion des règles de qualité de service

Les règles de qualité de service (QoS) vous permettent de créer et de sauvegarder des paramètres de qualité de service standardisés qui peuvent être appliqués à de nombreux volumes. Vous pouvez créer, modifier et supprimer des règles de QoS à partir de la page règles de QoS de l'onglet gestion.

> Si vous utilisez des règles de QoS, n'utilisez pas la QoS personnalisée sur un volume. La QoS personnalisée remplace et ajuste les valeurs des règles de QoS pour les paramètres de QoS du volume.

"Vidéo NetApp : règles de qualité de service SolidFire"

Voir "La performance et la qualité de service".

- Création d'une règle de QoS
- Modifiez une règle QoS
- Suppression d'une règle QoS

Création d'une règle de QoS

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

1. Sélectionnez **Management** > **QoS Policies**.
2. Cliquez sur **Créer une stratégie QoS**.
3. Entrez **Nom de la stratégie**.
4. Saisissez les valeurs de **min**, **Max IOPS** et **Burst IOPS**.
5. Cliquez sur **Créer une stratégie QoS**.

Modifiez une règle QoS

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

1. Sélectionnez **Management** > **QoS Policies**.
2. Cliquez sur l'icône actions de la stratégie QoS que vous souhaitez modifier.
3. Dans le menu qui s'affiche, sélectionnez **Modifier**.
4. Dans la boîte de dialogue **Modifier la stratégie QoS**, modifiez les propriétés suivantes comme requis :
   - Nom de la règle
   - IOPS min
   - IOPS max
   - IOPS en rafale
5. Cliquez sur **Enregistrer les modifications**.

Suppression d'une règle QoS

Vous pouvez supprimer une règle QoS s'il n'est plus nécessaire. Lorsque vous supprimez une policy de QoS, tous les volumes associés à la règle gèrent les paramètres de QoS mais ne sont plus associés à une policy.

> Si vous tentez de dissocier un volume d'une règle de QoS, vous pouvez modifier les paramètres de QoS de ce volume sur personnalisé.

1. Sélectionnez **Management** > **QoS Policies**.
2. Cliquez sur l'icône actions de la stratégie QoS que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, sélectionnez **Supprimer**.
4. Confirmez l'action.

Trouvez plus d'informations

- "Ne supprime pas l'association de la policy QoS d'un volume"
- "Documentation SolidFire et Element"
- "Plug-in 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 bloc accessibles sur le réseau par des clients iSCSI ou Fibre Channel.

Dans la page volumes de l'onglet gestion, vous pouvez créer, modifier, cloner et supprimer des volumes d'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 à l'aide des informations d'identification CHAP.

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

1. Sélectionnez **Management** > **volumes**.
2. Cliquez sur **Créer un volume**.
3. Dans la boîte de dialogue **Créer un nouveau volume**, entrez **Nom du volume**.
4. Entrez la taille totale du volume.

   > La taille de volume par défaut est en Go. Vous pouvez créer des volumes en utilisant des tailles mesurées en Go ou 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 devrait avoir accès au volume.

   Si aucun compte n'existe, cliquez sur le lien **Créer un compte**, entrez 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. Commencer à taper et la fonction de saisie semi-automatique affiche les valeurs possibles que vous pouvez choisir.

7. Pour définir la **qualité de service**, effectuez l'une des opérations suivantes :
   a. Sous **Policy**, vous pouvez sélectionner une stratégie de qualité de service existante, si disponible.
   b. Sous **Paramètres personnalisés**, définissez les valeurs minimum, maximum et rafale personnalisées pour IOPS ou utilisez les valeurs QoS par défaut.

      Pour les volumes dont la valeur IOPS max ou Burst supérieure à 20,000, il faut des files d'attente très poussées 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 **Management** > **volumes**.
2. Vérifiez les détails.
   - **ID** : ID généré par le système pour le volume.
   - **Nom** : nom donné au volume lors de sa création.
   - **Compte** : le nom du compte attribué au volume.
   - **Access Groups** : nom du ou des groupes d'accès au volume auxquels le volume appartient.
   - **Access** : 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 activités de lecture sont autorisées ; aucune écriture n'est autorisée.
     - Verrouillé : seul l'accès administrateur est autorisé.
     - ReplicationTarget : désigné comme volume cible dans une paire de volumes répliqués.
   - **Utilisé** : pourcentage d'espace utilisé dans le volume.
   - **Taille** : taille totale (en Go) du volume.
   - **Snapshots** : nombre de snapshots créés pour le volume.
   - **QoS Policy** : nom et lien vers la stratégie QoS définie par l'utilisateur.
   - **Min IOPS** : nombre minimum d'IOPS garanties pour le volume.
   - **IOPS max** : nombre maximal d'IOPS autorisé pour le volume.
   - **IOPS en rafale** : le nombre maximal d'IOPS autorisé sur une courte période pour le volume. Valeur par défaut = 15,000.
   - **Attributs** : attributs qui ont été affectés au volume en tant que paire clé/valeur via une méthode API.
   - **512e** : indique si 512e est activé sur un volume. Valeurs possibles :
     - Oui.
     - Non
   - **Créé le** : date et heure de création du volume.

Afficher les détails individuels du volume

Vous pouvez afficher les statistiques de performances des volumes individuels.

1. Sélectionnez **Reporting** > **Volume Performance**.
2. Dans la liste de volumes, cliquez sur l'icône actions d'un volume.
3. Cliquez sur **Afficher les détails**.

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

4. Pour plus d'informations sur le volume, cliquez sur **Voir plus de détails**.

   Le système affiche des informations détaillées ainsi que les graphiques de performance du volume.

Modifier les volumes actifs

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

Vous pouvez redimensionner un volume lorsque l'espace est suffisant sur le cluster dans les conditions suivantes :

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

Étapes

1. Sélectionnez **Management** > **volumes**.
2. Dans la fenêtre **Active**, cliquez sur l'icône actions du volume que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. **Facultatif:** modifiez la taille totale du volume.
   - Vous avez la possibilité d'augmenter la taille du volume, mais pas de la réduire. Vous ne pouvez redimensionner qu'un volume dans une seule opération de redimensionnement. Les opérations de collecte des données superflues et les mises à niveau logicielles n'interrompent pas l'opération de redimensionnement.
   - Si vous réglez la taille du volume pour la réplication, vous devez d'abord augmenter la taille du volume affecté en tant que cible de réplication. Vous pouvez alors redimensionner le volume source. Le volume cible peut être supérieur ou égal au volume source, mais il ne peut pas être plus petit.

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

   - 1 Go = 1 000 000 000 octets
   - 1 Gio = 1 073 741 824 octets
5. **Facultatif:** sélectionnez un niveau d'accès de compte différent de l'un des niveaux suivants :
   - Lecture seule

- Lecture/écriture
- Verrouillé
- Cible de réplication

6. **Facultatif:** sélectionnez le compte qui devrait avoir accès au volume.

   Si le compte n'existe pas, cliquez sur le lien **Créer un compte**, entrez 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. Commencer à taper et la fonction de saisie semi-automatique affiche les valeurs possibles que vous pouvez choisir.

7. **Facultatif:** pour modifier la sélection dans **qualité de service**, effectuez l'une des opérations suivantes :

   a. Sous **Policy**, vous pouvez sélectionner une stratégie de qualité de service existante, si disponible.

   b. Sous **Paramètres personnalisés**, définissez les valeurs minimum, maximum et rafale personnalisées pour IOPS ou utilisez les valeurs QoS par défaut.

   Si vous utilisez des règles de QoS sur un volume, vous pouvez définir une QoS personnalisée afin de supprimer l'affiliation de la « QoS policy » avec ce volume. La QoS personnalisée remplace et ajuste les valeurs des règles de QoS pour les paramètres de QoS du volume.

   Si vous modifiez les valeurs d'IOPS, vous devez augmenter l'incrément de plusieurs dizaines ou centaines. Les valeurs d'entrée nécessitent des nombres entiers valides.

   Configurez des volumes avec une valeur de bursting extrêmement élevée. Le système peut ainsi traiter rapidement des charges de travail séquentielles de 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 purge pas immédiatement un volume supprimé. Le volume reste disponible pendant environ huit heures. Si vous restaurez un volume avant que le système ne le purge, le volume est à nouveau en ligne et les connexions iSCSI sont restaurées.

Si un volume utilisé pour créer un snapshot est supprimé, ses snapshots associés deviennent inactifs. Lorsque les volumes source supprimés sont purgés, les snapshots inactifs associés sont également supprimés du système.

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

Étapes

1. Sélectionnez **Management** > **volumes**.

2. Pour supprimer un seul volume, effectuez les opérations suivantes :

   a. Cliquez sur l'icône actions du volume à supprimer.
   b. Dans le menu qui s'affiche, cliquez sur **Supprimer**.
   c. Confirmez l'action.

   Le système déplace le volume dans 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 **supprimé** de la page **volumes**.

Restaurer un volume supprimé

Vous pouvez restaurer un volume dans le 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 **Management** > **volumes**.
2. Cliquez sur l'onglet **supprimé** pour afficher la liste des volumes supprimés.
3. Cliquez sur l'icône actions du volume à 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 restaurées.

Purger un volume

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

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

1. Sélectionnez **Management** > **volumes**.
2. Cliquez sur le bouton **supprimé**.
3. Effectuez les étapes de purge d'un ou plusieurs volumes.

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

Clonez un volume

Vous pouvez créer un clone d'un ou plusieurs volumes pour effectuer une copie des données à un point dans le temps. Lorsque vous clonez un volume, le système crée un snapshot du volume, puis crée une copie des données référencées par le snapshot. Il s'agit d'un processus asynchrone, et la durée nécessaire de ce processus dépend de la taille du volume que vous clonez et de la charge actuelle du cluster.

Le cluster prend en charge jusqu'à deux demandes de clones en cours d'exécution par volume et jusqu'à huit opérations de clonage de volumes actifs à la fois. Les demandes dépassant ces limites sont placées en file d'attente pour traitement ultérieur.

Les systèmes d'exploitation diffèrent dans leur mode de traitement des volumes clonés. VMware ESXi traitera un volume cloné comme une copie de volume ou un volume Snapshot. Le volume sera un périphérique disponible à utiliser pour créer un nouveau datastore. Pour plus d'informations sur le montage de volumes clones et la gestion des LUN de snapshot, reportez-vous à la documentation VMware sur "Montage d'une copie de datastore VMFS" et "Gérer les datastores VMFS en double".

Avant de tronquer un volume cloné, veillez à cloner ce dernier à une taille plus petite, assurez-vous de préparer les partitions de sorte qu'elles s'adaptent au volume plus petit.

Étapes

1. Sélectionnez **Management** > **volumes**.
2. Pour cloner un seul volume, effectuez les opérations suivantes :
   a. Dans la liste des volumes de la page **Active**, cliquez sur l'icône actions du volume à cloner.
   b. Dans le menu qui s'affiche, cliquez sur **Clone**.
   c. Dans la fenêtre **Clone Volume**, entrez un nom de volume pour le nouveau volume cloné.
   d. Sélectionnez une taille et une mesure pour le volume à l'aide de la zone de sélection et de la liste taille de volume *.

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

      - 1 Go = 1 000 000 000 octets

- 1 Gio = 1 073 741 824 octets

e. Sélectionnez le type d'accès pour le volume récemment cloné.

f. Sélectionnez un compte à associer au volume nouvellement cloné dans la liste **compte**.

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

3. Pour cloner plusieurs volumes, effectuez les opérations suivantes :

   a. Dans la liste des volumes de la page **Active**, cochez la case en regard des volumes que vous souhaitez cloner.

   b. Cliquez sur **actions groupées**.

   c. Dans le menu qui s'affiche, sélectionnez **Clone**.

   d. Dans la boîte de dialogue **Clone multiple volumes**, entrez un préfixe pour les volumes clonés dans le champ **Nouveau préfixe de 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**.

> L'augmentation de la taille du volume d'un clone entraîne la création d'un nouveau volume avec de l'espace libre supplémentaire à l'extrémité du volume. En fonction de l'utilisation du volume, vous devrez peut-être étendre les partitions ou créer de nouvelles partitions dans l'espace libre pour l'utiliser.

Pour en savoir plus

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

Attribuez des LUN aux volumes Fibre Channel

Vous pouvez modifier l'affectation de LUN pour un volume Fibre Channel dans un groupe d'accès de volume. Vous pouvez également attribuer des LUN de volume Fibre Channel lorsque vous créez un groupe d'accès de volume.

L'attribution de nouvelles LUN Fibre Channel est une fonction avancée qui peut avoir des conséquences inconnues sur l'hôte de connexion. Par exemple, il se peut que le nouvel ID de LUN ne soit pas détecté automatiquement sur l'hôte, et que l'hôte nécessite une nouvelle analyse pour détecter le nouvel ID de LUN.

1. Sélectionnez **Management** > **Access Groups**.
2. Cliquez sur l'icône actions du groupe d'accès à modifier.
3. Dans le menu qui s'affiche, sélectionnez **Modifier**.
4. Sous **attribuer des ID de LUN** dans la boîte de dialogue **Modifier un groupe d'accès de volume**, cliquez sur la flèche de la liste **affectations de LUN**.
5. Pour chaque volume de la liste auquel vous souhaitez affecter une LUN, entrez une nouvelle valeur dans le champ **LUN** correspondant.

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

Appliquer une policy de QoS aux volumes

Vous pouvez appliquer une règle de QoS existante à un ou plusieurs volumes en bloc.

La politique de QoS que vous souhaitez appliquer en bloc doit exister.

1. Sélectionnez **Management** > **volumes**.
2. Dans la liste des volumes, cochez la case en regard des volumes à appliquer la politique de QoS.
3. Cliquez sur **actions groupées**.
4. Dans le menu qui s'affiche, cliquez sur **appliquer la stratégie de qualité de service**.
5. Sélectionnez la stratégie QoS dans la liste déroulante.
6. Cliquez sur **appliquer**.

Trouvez plus d'informations

Règles de qualité de service

Ne supprime pas l'association de la policy QoS d'un volume

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

Le volume à modifier doit être associé à une politique de QoS.

1. Sélectionnez **Management** > **volumes**.
2. Cliquez sur l'icône actions d'un volume contenant une stratégie QoS à 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**.

Trouvez plus d'informations

Suppression d'une règle QoS

Utilisation des volumes virtuels

Vous pouvez afficher 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 de volumes virtuels (VVol) désactivée. Vous devez effectuer une tâche ponctuelle pour activer manuellement la fonctionnalité VVol vSphere via l'interface utilisateur Element.

Une fois que vous avez activé la fonctionnalité VVol, un onglet VVol apparaît dans l'interface utilisateur avec laquelle offre une surveillance liée aux VVol et des options de gestion limitées. De plus, un composant logiciel

côté stockage appelé VASA Provider sert de service de sensibilisation du stockage pour vSphere. La plupart des commandes VVol, comme la création, le clonage et la modification de VVol, sont lancées par un hôte vCenter Server ou ESXi et traduites par le fournisseur VASA en API Element pour le système de stockage du logiciel Element. Les commandes de création, de suppression et de gestion de conteneurs de stockage et de suppression de volumes virtuels peuvent être lancées à l'aide de l'interface utilisateur Element.

La majorité des configurations nécessaires à l'utilisation de la fonctionnalité Virtual volumes avec les systèmes de stockage logiciels Element sont effectuées dans vSphere. Consultez le *VMware vSphere Virtual volumes pour le stockage SolidFire* pour enregistrer le fournisseur VASA dans vCenter, créer et gérer des datastores VVol, et gérer le stockage conformément aux règles.

N'enregistrez pas plusieurs fournisseurs NetApp Element VASA vers une seule instance de vCenter. Ainsi, lorsqu'un deuxième fournisseur NetApp Element VASA est ajouté, tous les data stores VVOL sont inaccessibles.

La prise en charge de VASA pour plusieurs vCenters est disponible en tant que 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 à partir du "Téléchargements de logiciels NetApp" et suivez les instructions dans le manifeste. Le fournisseur NetApp Element VASA utilise un certificat NetApp. Avec ce correctif, le certificat est utilisé non modifié par vCenter pour prendre en charge plusieurs vCenters pour VASA et VVol. Ne modifiez pas le certificat. Les certificats SSL personnalisés ne sont pas pris en charge par VASA.

Trouvez plus d'informations

- Activer les volumes virtuels
- Afficher les détails des volumes virtuels
- Supprimer un volume virtuel
- Créer un conteneur de stockage
- Modifiez un conteneur de stockage
- Supprime un conteneur de stockage
- Terminaux PE
- Liaisons
- Détails sur l'hôte

Activer les volumes virtuels

Vous devez activer manuellement la fonctionnalité volumes virtuels vSphere (VVol) via le logiciel NetApp Element. Les VVol sont désactivés par défaut, mais le système du logiciel Element n'est pas automatiquement activé dans le cadre d'une nouvelle installation ou d'une mise à niveau. L'activation des VVol est une tâche de configuration ponctuelle.

Ce dont vous avez besoin

- Le cluster doit exécuter Element 9.0 ou version ultérieure.
- Le cluster doit être connecté à un environnement ESXi 6.0 ou version ultérieure compatible avec les VVol.
- Si vous utilisez Element 11.3 ou version ultérieure, le cluster doit être connecté à un environnement ESXi 6.0 Update 3 ou version ultérieure.

L'activation de la fonctionnalité des volumes virtuels vSphere modifie définitivement la configuration du logiciel Element. Vous ne devriez activer la fonctionnalité VVols que si le cluster est connecté à un environnement compatible avec les VVol VMware ESXi. Vous ne pouvez désactiver la fonctionnalité VVol et restaurer les paramètres par défaut qu'en retournant le cluster à l'image d'usine, qui supprime toutes les données du système.

Étapes

1. Sélectionnez **clusters** > **Paramètres**.
2. Rechercher les paramètres propres 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 de l'élément.

   Lorsque les VVol sont activés, le cluster SolidFire démarre le fournisseur VASA, ouvre le port 8444 pour le trafic VASA et crée des terminaux 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 (VVol) dans **clusters** > **Paramètres**. Vous utiliserez cette URL pour enregistrer VASA Provider dans vCenter.
6. Créez un conteneur de stockage dans **VVol** > **conteneurs de stockage**.

   Vous devez créer au moins un conteneur de stockage afin que les VM puissent être provisionnées vers un datastore VVol.

7. Sélectionnez **VVol** > **points d'extrémité de protocole**.
8. Vérifiez qu'un noeud final de protocole a été créé pour chaque noeud du cluster.

   D'autres tâches de configuration sont requises dans vSphere. Consultez le *VMware vSphere Virtual volumes pour le stockage SolidFire* pour enregistrer le fournisseur VASA dans vCenter, créer et gérer des datastores VVol, et gérer le stockage conformément aux règles.

Trouvez plus d'informations

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

Afficher les détails des volumes virtuels

Vous pouvez consulter les informations sur le volume virtuel de tous les volumes virtuels actifs du cluster dans l'interface utilisateur d'Element. Vous pouvez également consulter les activités de performances de chaque volume virtuel, y compris l'entrée, la sortie, le débit, la latence informations sur la profondeur de la file d'attente et le volume.

Ce dont vous avez besoin

- Vous devez avoir activé les VVol dans l'interface d'Element pour le cluster.
- Vous devez avoir créé un conteneur de stockage associé.

- Vous devez avoir configuré votre cluster vSphere pour utiliser les VVol du logiciel Element.
- Vous devez avoir créé au moins une machine virtuelle dans vSphere.

Étapes

1. Cliquez sur **VVol** > **volumes virtuels**.

   Les informations relatives à tous les volumes virtuels actifs s'affichent.

2. Cliquez sur l'icône **actions** pour le 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 de volume, l'ID de snapshot, l'ID de volume virtuel parent et l'ID de volume virtuel.

- **ID de volume** : ID du volume sous-jacent.
- **ID d'instantané** : ID de l'instantané de volume sous-jacent. La valeur est 0 si le volume virtuel ne représente pas un snapshot SolidFire.
- **ID du volume virtuel parent** : ID du volume virtuel du volume virtuel parent. Si l'ID est tous des zéros, le volume virtuel est indépendant sans lien avec un parent.
- **ID de volume virtuel** : UUID du volume virtuel.
- **Nom** : nom attribué au volume virtuel.
- **Conteneur de stockage** : le conteneur de stockage propriétaire du volume virtuel.
- **Type de système d'exploitation invité** : système d'exploitation associé au volume virtuel.
- **Type de volume virtuel** : Type de volume virtuel : config, données, mémoire, échange ou autre.
- **Access** : autorisations de lecture/écriture attribuées au volume virtuel.
- **Size** : taille du volume virtuel en Go ou Gio.
- **Snapshots** : le nombre de snapshots associés. Cliquez sur le numéro à associer aux détails de l'instantané.
- **IOPS min** : paramètre de qualité de service d'IOPS minimum du volume virtuel.
- **Max IOPS** : paramètre de qualité de service d'IOPS maximum du volume virtuel.
- **IOPS Burst** : paramètre de qualité de service maximum en rafale du volume virtuel.
- **VMW_VMID** : les informations dans les champs précéd'« VMW_ » sont définies par VMware.
- **Heure de création** : heure à laquelle la tâche de création de volume virtuel a été terminée.

Détails des volumes virtuels individuels

La page volumes virtuels de l'onglet VVol fournit les informations suivantes lorsque vous sélectionnez un volume virtuel individuel et consultez ses détails.

- **VMW_XXX** : les informations dans les champs précéd'« VMW_ » sont définies par VMware.
- **ID du volume virtuel parent** : ID du volume virtuel du volume virtuel parent. Si l'ID est tous des zéros, le volume virtuel est indépendant sans lien avec un parent.
- **ID de volume virtuel** : UUID du volume virtuel.

- **Type de volume virtuel** : Type de volume virtuel : config, données, mémoire, échange ou autre.
- **ID de volume** : ID du volume sous-jacent.
- **Access** : autorisations de lecture/écriture attribuées au volume virtuel.
- **Nom du compte** : nom du compte contenant le volume.
- **Access Groups** : groupes d'accès de volume associés.
- **Taille totale du volume** : capacité totale provisionnée en octets.
- **Blocs non nuls** : nombre total de blocs de 4 Ko avec données après la dernière opération de collecte des déchets.
- **Blocs nuls** : nombre total de blocs de 4Kio sans données après la dernière opération de collecte des déchets.
- **Snapshots** : le nombre de snapshots associés. Cliquez sur le numéro à associer aux détails de l'instantané.
- **IOPS min** : paramètre de qualité de service d'IOPS minimum du volume virtuel.
- **Max IOPS** : paramètre de qualité de service d'IOPS maximum du volume virtuel.
- **IOPS Burst** : paramètre de qualité de service maximum en rafale du volume virtuel.
- **Activer 512**: Puisque les volumes virtuels utilisent toujours l'émulation de taille de bloc de 512 octets, la valeur est toujours oui.
- **Volumes couplés** : indique si un volume est apparié.
- **Heure de création** : heure à laquelle la tâche de création de volume virtuel a été terminée.
- **Blocs Size** : taille des blocs sur le volume.
- **Écritures non alignées** : pour les volumes de 512e, le nombre d'opérations d'écriture qui n'étaient pas sur une limite de secteur de 4 ko. Un nombre élevé d'écritures non alignées peut indiquer un alignement incorrect des partitions.
- * Lectures non alignées* : pour les volumes de 512 e, le nombre d'opérations de lecture qui n'étaient pas sur une limite de secteur de 4 ko. Un grand nombre de lectures non alignées peut indiquer un alignement incorrect des partitions.
- **ScsiEUIDeveiceID** : identificateur de périphérique SCSI unique au niveau mondial pour le volume au format 16 octets basé sur EUI-64.
- **ScsiNADeviceID** : identificateur de périphérique SCSI unique global pour le volume au format étendu agréé NAA IEEE.
- **Attributes** : liste des paires nom-valeur au format d'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 des volumes virtuels est activée à partir de l'interface utilisateur Element. Vous devez uniquement supprimer un volume virtuel de l'interface utilisateur Element lorsque cela est absolument nécessaire, par exemple lorsque vSphere ne parvient pas à nettoyer les volumes virtuels sur du stockage SolidFire.

1. Sélectionnez **VVol** > **volumes virtuels**.
2. Cliquez sur l'icône actions du 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 sans limites avant la suppression. Vous devez uniquement supprimer un volume virtuel de l'interface utilisateur Element lorsque cela est absolument nécessaire, par exemple lorsque vSphere ne parvient pas à nettoyer les volumes virtuels sur du stockage SolidFire. Si vous supprimez un volume virtuel de l'interface utilisateur Element, le volume sera immédiatement purgé.

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

Gérez les conteneurs de stockage

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

Les conteneurs de stockage sont créés et liés aux comptes NetApp Element. Un conteneur de stockage créé sur un système de stockage Element apparaît en tant que datastore vSphere dans vCenter et ESXi. Les conteneurs de stockage n'allouent aucun espace dans le stockage Element. Elles sont utilisées pour associer des volumes virtuels de façon logique.

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

Créer un conteneur de stockage

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

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

Étapes

1. Sélectionnez **VVol** > **conteneurs de stockage**.
2. Cliquez sur le bouton **Créer des conteneurs de stockage**.
3. Entrez les informations relatives au conteneur de stockage dans la boîte de dialogue **Créer un nouveau conteneur de stockage** :
   a. Entrez un nom pour le conteneur de stockage.
   b. Configurer les secrets d'initiateur et de cible pour CHAP.

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

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

Un ID de compte NetApp Element créé automatiquement et attribué au conteneur de stockage permet donc de créer manuellement un compte.

Afficher les détails du conteneur de stockage

La page conteneurs de stockage de l'onglet VVol permet d'afficher les informations de tous les conteneurs de stockage actifs sur le cluster.

- **ID de compte** : ID du compte NetApp Element associé au conteneur de stockage.
- **Nom** : le nom du conteneur de stockage.
- **Status** : état du conteneur de stockage. Valeurs possibles :
  - Active : le conteneur de stockage est en cours d'utilisation.
  - Verrouillé : le conteneur de stockage est verrouillé.
- **PE Type** : type de point final du protocole (SCSI est le seul protocole disponible pour le logiciel Element).
- **ID du conteneur de stockage** : UUID du conteneur de stockage de volume virtuel.
- **Volumes virtuels actifs** : nombre de volumes virtuels actifs associés au conteneur de stockage.

Affichez les détails de chaque conteneur de stockage

Vous pouvez afficher les informations du conteneur de stockage d'un conteneur de stockage individuel en les sélectionnant dans la page conteneurs de stockage de l'onglet VVol.

- **ID de compte** : ID du compte NetApp Element associé au conteneur de stockage.
- **Nom** : le nom du conteneur de stockage.
- **Status** : état du conteneur de stockage. Valeurs possibles :
  - Active : le conteneur de stockage est en cours d'utilisation.
  - Verrouillé : le conteneur de stockage est verrouillé.
- **Secret de l'initiateur CHAP** : le secret CHAP unique de l'initiateur.
- **Secret cible CHAP** : le secret CHAP unique pour la cible.
- **ID du conteneur de stockage** : UUID du conteneur de stockage de volume virtuel.
- **Protocol Endpoint Type** : indique le type de noeud final du protocole (SCSI est le seul protocole disponible).

Modifiez un conteneur de stockage

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

1. Sélectionnez **VVol** > **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. Sous Paramètres CHAP, modifiez les informations d'identification Secret de l'initiateur et Secret de la cible utilisées pour l'authentification.

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

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

Supprime un conteneur de stockage

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

Ce dont vous avez besoin

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

Étapes

1. Sélectionnez **VVol** > **conteneurs de stockage**.
2. Cliquez sur l'icône **actions** du conteneur de stockage à supprimer.
3. Dans le menu qui s'affiche, sélectionnez **Supprimer**.
4. Confirmez l'action.
5. Actualisez la liste des conteneurs de stockage dans le sous-onglet **conteneurs de stockage** pour confirmer que le conteneur de stockage a été supprimé.

Terminaux PE

Les terminaux PE sont des points d'accès utilisés par un hôte pour gérer le stockage sur un cluster exécutant le logiciel NetApp Element. Les terminaux de protocole ne peuvent pas être supprimés ou modifiés par un utilisateur, ne sont pas associés à un compte et ne peuvent pas être ajoutés à un groupe d'accès de volume.

Un cluster exécutant le logiciel Element crée automatiquement un terminal de protocole par nœud de stockage dans le cluster. Par exemple, un cluster de stockage à six nœuds comporte six terminaux de protocole mappés à chaque hôte ESXi. Les terminaux PE sont gérés de manière dynamique par le logiciel Element et sont créés, déplacés ou supprimés en fonction des besoins, sans aucune intervention. Les terminaux PE constituent la cible des chemins d'accès multiples et servent de proxy d'E/S pour les LUN secondaires. Chaque terminal PE utilise une adresse SCSI disponible, comme une cible iSCSI standard. Les terminaux Protocol 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 terminaux de protocole

La page Protocol Endpoints de l'onglet VVols fournit des informations sur le terminal de protocole.

- **ID fournisseur principal**

  ID du fournisseur de point final du protocole principal.

- **ID fournisseur secondaire**

  ID du fournisseur de point final du protocole secondaire.

- **ID point final du protocole**

  UUID du noeud final du protocole.

- **Protocole Etat du noeud final**

  État du noeud final du protocole. Les valeurs possibles sont les suivantes :

  - Active : le noeud final du protocole est en cours d'utilisation.
  - Démarrage : le point final du protocole démarre.
  - Basculement : le point final du protocole a échoué.
  - Réservé : le terminal protocole est réservé.

- **Type de fournisseur**

  Type de fournisseur du terminal de protocole. Les valeurs possibles sont les suivantes :

  - Primaire
  - Secondaire

- **ID PÉRIPHÉRIQUE NAA SCSI**

  Identifiant de périphérique SCSI unique au niveau mondial pour le point de terminaison de protocole dans le format étendu enregistré NAA IEEE.

Liaisons

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 noeud final de protocole optimal, crée une liaison qui associe l'hôte ESXi et le volume virtuel au noeud final du protocole et renvoie la 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 liaisons

La page liaisons de l'onglet VVol fournit des informations de liaison sur chaque volume virtuel.

Les informations suivantes s'affichent :

- **ID hôte**

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

- **ID point final du protocole**

  ID de terminal du protocole qui correspondent à chaque nœud du cluster SolidFire.

- **Point final de protocole dans ID de bande**

  ID de périphérique SCSI NAA du noeud final du protocole.

- **Type de point final de protocole**

  Type de noeud final du protocole.

- **ID liaison VVol**

  UUID de liaison du volume virtuel.

- **ID VVol**

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

- **ID secondaire VVol**

  ID secondaire du volume virtuel qui est un ID de LUN SCSI de second niveau.

Détails sur l'hôte

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

Les informations suivantes s'affichent :

- **ID hôte**

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

- **Adresse hôte**

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

- **Liaisons**

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

- **ID de cluster ESX**

  ID de cluster hôte vSphere ou GUID vCenter.

- **IQN de l'initiateur**

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

- **ID de point final du protocole SolidFire**

  Les noeuds finaux de protocole actuellement visibles pour l'hôte ESXi.

Utilisation des groupes d'accès de volumes et des initiateurs

Vous pouvez utiliser des initiateurs iSCSI ou des initiateurs Fibre Channel pour accéder aux volumes définis au sein des groupes d'accès de volume.

Vous pouvez créer des groupes d'accès en mappant les IQN des initiateurs 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 une cible CHAP unique et des secrets 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.

Si vous le souhaitez, vous pouvez également appliquer l'autorisation d'initiateur et l'authentification CHAP par initiateur. Ces options peuvent être définies par initiateur et un groupe d'accès peut contenir plusieurs 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 de volume ont les limites suivantes :

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

Trouvez plus d'informations

- Créer un groupe d'accès de volume
- Ajout de volumes à un groupe d'accès
- Supprimer des volumes d'un groupe d'accès
- Créer un initiateur
- Modifier un initiateur
- Ajout d'un seul initiateur à un groupe d'accès de volume
- Ajoutez plusieurs initiateurs à un groupe d'accès de volume
- Supprimez des initiateurs d'un groupe d'accès
- Supprimer un groupe d'accès
- Supprimer un initiateur

Créer un groupe d'accès de volume

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

Si vous utilisez le protocole CHAP basé sur un initiateur, vous pouvez ajouter des informations d'identification CHAP pour un seul initiateur dans un groupe d'accès de volume, offrant ainsi une sécurité accrue. Cela vous permet d'appliquer cette option aux groupes d'accès aux volumes qui existent déjà.

Étapes

1. Cliquez sur **Management** > **Access Groups**.
2. Cliquez sur **Créer un groupe d'accès**.
3. Entrez un nom pour le groupe d'accès au volume dans le champ **Nom**.
4. Ajoutez un initiateur au groupe d'accès de 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. b. Cliquez sur **Ajouter 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**. Une fois que vous avez créé, le système ajoute automatiquement l'initiateur à la liste des initiateurs. 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 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**. Une fois que vous avez créé, le système ajoute automatiquement l'initiateur à la liste des initiateurs. 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 **View Details** dans le menu actions du volume dans la liste **Management** > **volumes** > **Active**. Lorsque vous modifiez un initiateur, vous pouvez basculer l'attribut requiredCHAP sur vrai, ce qui vous permet de définir le secret de l'initiateur cible. Pour plus d'informations, reportez-vous à la section informations sur l'API relative à la méthode ModilyInitiator. "Gérez le stockage avec l'API Element"

5. **Facultatif:** Ajouter d'autres initiateurs si nécessaire.
6. Sous Ajouter des volumes, sélectionnez un volume dans la liste **volumes**.

Le volume apparaît dans la liste **volumes attachés**.

7. **Facultatif:** Ajouter plus de volumes selon les besoins.
8. Cliquez sur **Créer un groupe d'accès**.

Trouvez plus d'informations

Ajout de volumes à un groupe d'accès

Afficher les détails des groupes d'accès individuels

Vous pouvez afficher les détails d'un groupe d'accès individuel, comme les volumes attachés et les initiateurs, dans un format graphique.

1. Cliquez sur **Management** > **Access Groups**.
2. Cliquez sur l'icône actions d'un groupe d'accès.
3. Cliquez sur **Afficher les détails**.

Détails du groupe d'accès de volume

La page Access Groups de l'onglet Management fournit des informations sur les groupes d'accès de volume.

Les informations suivantes s'affichent :

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

Ajout de volumes à un groupe d'accès

Vous pouvez ajouter des volumes à un groupe d'accès de volume. Chaque volume peut appartenir à plusieurs groupes d'accès de volume ; vous pouvez voir 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 de volume Fibre Channel.

1. Cliquez sur **Management** > **Access Groups**.
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 supprimez un volume d'un groupe d'accès, celui-ci n'a plus accès à ce volume.

La modification des paramètres CHAP d'un compte ou la suppression d'initiateurs ou de volumes d'un groupe d'accès peut entraîner une perte inattendue de l'accès aux volumes. Pour vérifier que l'accès au volume ne sera pas perdu de manière inattendue, déconnectez toujours 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 après la modification des paramètres de l'initiateur et des paramètres du cluster.

1. Cliquez sur **Management** > **Access Groups**.
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 au volume**, 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 supprimer le volume de la liste.

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

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

Créer un initiateur

Vous pouvez créer des initiateurs iSCSI ou Fibre Channel et éventuellement leur attribuer des alias.

Vous pouvez également attribuer des attributs CHAP basés sur initator à l'aide d'un appel d'API. Pour ajouter un nom de compte CHAP et des informations d'identification par initiateur, vous devez utiliser le `CreateInitiator` Appel API pour supprimer et ajouter un accès CHAP et des attributs. L'accès des initiateurs peut être limité à un ou plusieurs VLAN en spécifiant un ou plusieurs virtualNetworkID 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, reportez-vous aux informations de référence de l'API."Gérez le stockage avec l'API Element"

Étapes

1. Cliquez sur **Management** > **Initiators**.
2. Cliquez sur **Créer initiateur**.
3. Effectuez les étapes de création d'un ou plusieurs initiateurs :

Option	Étapes
Créer un seul initiateur	a. Cliquez sur **Créer un seul initiateur**. 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 initiateur**.
Créer plusieurs initiateurs	a. Cliquez sur **Bulk Create Initiators**. b. Entrez une liste d'IQN ou de WWPN dans la zone de texte. c. Cliquez sur **Ajouter initiateurs**. d. Choisissez un initiateur dans la liste des résultats 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 initiateurs**.

Modifier un initiateur

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

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

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

Étapes

1. Cliquez sur **Management** > **Initiators**.
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**.

Ajout d'un seul initiateur à un groupe d'accès de volume

Vous pouvez ajouter un initiateur à un groupe d'accès de volume existant.

Lorsque vous ajoutez un initiateur à un groupe d'accès de volume, celui-ci a accès à tous les volumes de ce groupe.

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

Si vous utilisez le protocole CHAP basé sur un initiateur, vous pouvez ajouter des informations d'identification CHAP pour un seul initiateur dans un groupe d'accès de volume, offrant ainsi une sécurité accrue. Cela vous permet d'appliquer cette option aux groupes d'accès aux volumes qui existent déjà.

Étapes

1. Cliquez sur **Management** > **Access Groups**.
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 de volume, effectuez les opérations suivantes :

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

   b. Cliquez sur **Ajouter 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**. Après avoir créé l'initiateur, le système ajoute automatiquement l'initiateur à la liste **Initiators**.

   Voici un exemple de format :

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

5. Pour ajouter un initiateur iSCSI au groupe d'accès de 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**. Après avoir créé l'initiateur, le système ajoute automatiquement l'initiateur à la liste **Initiators**.

   Le format accepté d'un IQN initiateur est le suivant : iqn.aaaa-mm, dans lequel y et m sont des chiffres, suivi 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 à partir de la page **Management** > **volumes** Active volumes en cliquant sur l'icône actions, puis en sélectionnant **View Details** pour le volume.

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

Ajoutez plusieurs initiateurs à un groupe d'accès de volume

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

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

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

Vous pouvez ajouter plusieurs initiateurs à un groupe d'accès de volume existant pour permettre l'accès aux volumes et attribuer des informations d'identification CHAP uniques à chaque initiateur de ce groupe d'accès de volume. Cela vous permet d'appliquer cette option aux groupes d'accès aux volumes qui existent déjà.

Vous pouvez attribuer des attributs CHAP basés sur initator à l'aide d'un appel d'API. Pour ajouter un nom de compte CHAP et des informations d'identification par initiateur, vous devez utiliser l'appel API ModimodiyInitiator pour supprimer et ajouter des droits d'accès et des attributs CHAP.

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

Étapes

1. Cliquez sur **Management** > **Initiators**.
2. Sélectionnez les initiateurs à ajouter à un groupe d'accès.
3. Cliquez sur le bouton **actions groupées**.
4. Cliquez sur **Ajouter au groupe d'accès de volume**.
5. Dans la boîte de dialogue Ajouter au groupe d'accès au volume, sélectionnez un groupe d'accès dans la liste **Groupe d'accès au volume**.
6. Cliquez sur **Ajouter**.

Supprimez des initiateurs d'un groupe d'accès

Lorsque vous supprimez un initiateur d'un groupe d'accès, il ne peut plus accéder aux volumes de ce groupe. L'accès normal au compte du volume n'est pas interrompu.

La modification des paramètres CHAP d'un compte ou la suppression d'initiateurs ou de volumes d'un groupe d'accès peut entraîner une perte inattendue de l'accès aux volumes. Pour vérifier que l'accès au volume ne sera pas perdu de manière inattendue, déconnectez toujours 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 après la modification des paramètres de l'initiateur et des paramètres du cluster.

Étapes

1. Cliquez sur **Management** > **Access Groups**.
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 au volume**, cliquez sur la flèche de la liste **initiateurs**.
5. Sélectionnez l'icône x pour chaque initiateur que vous souhaitez supprimer 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 de volume du groupe d'accès au volume avant de supprimer ce groupe. Après avoir supprimé le groupe d'accès, l'accès de groupe aux volumes est interrompu.

1. Cliquez sur **Management** > **Access Groups**.
2. Cliquez sur l'icône **actions** du groupe d'accès à 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 dans ce groupe d'accès**.
5. Confirmez l'action.

Supprimer un initiateur

Vous pouvez supprimer un initiateur après celui-ci n'est plus nécessaire. Lorsque vous supprimez un initiateur, le système le supprime de tout groupe d'accès de volume associé. Toutes les connexions utilisant l'initiateur restent valides jusqu'à ce que la connexion soit réinitialisée.

Étapes

1. Cliquez sur **Management** > **Initiators**.
2. Effectuez les étapes de suppression d'un ou plusieurs initiateurs :

Option	Étapes
Supprimer un initiateur unique	a. Cliquez sur l'icône **actions** de l'initiateur que vous souhaitez supprimer. b. Cliquez sur **Supprimer**. c. Confirmez l'action.
Supprimez plusieurs initiateurs	a. Cochez les cases en regard des initiateurs à supprimer. b. Cliquez sur le bouton **actions groupées**. c. Dans le menu qui s'affiche, sélectionnez **Supprimer**. d. Confirmez l'action.

Protégez vos données

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

- **Snapshots**

  La protection des données snapshot uniquement réplique les données modifiées au point spécifique de temps sur un cluster distant. Seuls les snapshots créés sur le cluster source sont répliqués. Les écritures actives du volume source ne sont pas.

  Utilisation des snapshots de volumes pour la protection des données

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

Il peut répliquer des données de volume de manière synchrone ou asynchrone depuis l'un des clusters d'une paire de clusters qui s'exécute sous Element pour les scénarios de basculement et de retour arrière.

Réplication à distance entre les clusters exécutant le logiciel NetApp Element

- **La réplication entre des clusters Element et ONTAP à l'aide de la technologie SnapMirror**

  Avec la technologie NetApp SnapMirror, vous pouvez répliquer les snapshots pris en utilisant Element vers ONTAP à des fins de reprise après incident. Dans une relation SnapMirror, Element est un terminal et ONTAP l'autre.

  Utilisez la réplication SnapMirror entre les clusters Element et ONTAP

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

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

  Sauvegarde et restauration de volumes dans des magasins d'objets SolidFire, S3 ou Swift

Pour en savoir plus

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

Utilisation des snapshots de volumes pour la protection des données

Un snapshot de volume est une copie instantanée d'un volume. Vous pouvez créer un snapshot d'un volume et l'utiliser ultérieurement si vous devez restaurer un volume à son état au moment de sa création.

Les copies Snapshot sont similaires aux clones de volumes. Toutefois, les snapshots sont simplement des répliques de métadonnées de volume ; vous ne pouvez donc pas les monter ou les écrire. La création d'un snapshot de volume ne prend qu'une petite quantité de ressources système et d'espace, ce qui accélère la création de snapshots que le clonage.

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

Il est également possible de répliquer les snapshots sur un cluster distant et de les utiliser comme copie de sauvegarde du volume. Cela permet de restaurer un volume à un point dans le temps spécifique à l'aide du snapshot répliqué. Vous pouvez également créer un clone de volume à partir d'un snapshot répliqué.

Trouvez plus d'informations

- Utilisation de snapshots de volumes individuels pour la protection des données
- Utilisation de snapshots de groupe pour la tâche de protection des données
- Planification d'un snapshot

Utilisation de snapshots de volumes individuels pour la protection des données

Un snapshot de volume est une copie instantanée d'un volume. Vous pouvez utiliser un volume individuel plutôt qu'un groupe de volumes pour le snapshot.

Trouvez plus d'informations

- Créer un snapshot de volume
- Modifier la conservation des snapshots
- Suppression d'un snapshot
- Clonage d'un volume à partir d'un snapshot
- Retour arrière d'un volume à un snapshot
- Sauvegarde d'un snapshot de volume dans un magasin d'objets Amazon S3
- Sauvegarde d'un snapshot de volume dans un magasin d'objets OpenStack Swift
- Sauvegarde d'un snapshot de volume sur un cluster SolidFire

Créer un snapshot de volume

Vous pouvez créer un snapshot d'un volume actif pour préserver l'image du volume à tout moment. Vous pouvez créer jusqu'à 32 copies Snapshot pour un seul volume.

1. Cliquez sur **Management** > **volumes**.
2. Cliquez sur l'icône **actions** du volume que vous souhaitez utiliser pour l'instantané.
3. Dans le menu qui s'affiche, sélectionnez **instantané**.
4. Dans la boîte de dialogue **Créer un instantané de volume**, entrez le nouveau nom d'instantané.
5. **Facultatif:** cochez la case **inclure l'instantané dans la réplication lorsqu'il est couplé** pour vous assurer que l'instantané est capturé dans la réplication lorsque le volume parent est couplé.
6. Pour définir la conservation de l'instantané, sélectionnez l'une des options suivantes :
   - Cliquez sur **conserver indéfiniment** pour conserver indéfiniment l'instantané sur le système.
   - Cliquez sur **Set Retention Period** et utilisez les champs de spin de date pour choisir une durée pour le système de conservation de l'instantané.
7. Pour créer un seul snapshot immédiat, effectuez les opérations suivantes :
   a. Cliquez sur **prendre un instantané maintenant**.
   b. Cliquez sur **Créer un instantané**.
8. Pour planifier l'exécution ultérieure de l'instantané, effectuez les opérations suivantes :
   a. Cliquez sur **Créer une planification d'instantanés**.
   b. Saisissez un **Nouveau nom d'horaire**.
   c. Choisissez un **Type d'horaire** dans la liste.
   d. **Facultatif :** cochez la case **Programme récurrent** pour répéter l'instantané programmé périodiquement.
   e. Cliquez sur **Créer un programme**.

Trouvez plus d'informations

Planifier un snapshot

Modifier la conservation des snapshots

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

Étapes

1. Cliquez sur **Data protection** > **snapshots**.
2. Cliquez sur l'icône **actions** pour le snapshot que vous souhaitez modifier.
3. Dans le menu qui s'affiche, cliquez sur **Modifier**.
4. **Facultatif:** cochez la case **inclure l'instantané dans la réplication lorsqu'il est couplé** pour vous assurer que l'instantané est capturé dans la réplication lorsque le volume parent est couplé.
5. **Facultatif :** sélectionnez une option de rétention pour l'instantané :
   - Cliquez sur **conserver indéfiniment** pour conserver indéfiniment l'instantané sur le système.
   - Cliquez sur **Set Retention Period** et utilisez les zones de spin de date pour sélectionner une durée pour le système de conservation de l'instantané.
6. Cliquez sur **Enregistrer les modifications**.

Supprime un snapshot

Vous pouvez supprimer un snapshot 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 snapshots en cours de réplication à partir du cluster source. Si un snapshot est en cours de synchronisation avec le cluster cible lorsque vous le supprimez, la réplication de synchronisation est terminée et l'instantané est supprimé du cluster source. Le snapshot n'est pas supprimé du cluster cible.

Vous pouvez également supprimer les snapshots qui ont été répliqués sur la cible du cluster cible. L'instantané supprimé est conservé dans une liste de snapshots 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 le snapshot source, la cible arrête la réplication du snapshot.

Lorsque vous supprimez un snapshot du cluster source, le snapshot de cluster cible n'est pas affecté (l'inverse est également vrai).

1. Cliquez sur **Data protection** > **snapshots**.
2. Cliquez sur l'icône **actions** pour le snapshot que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, sélectionnez **Supprimer**.
4. Confirmez l'action.

Cloner un volume à partir d'un snapshot

Vous pouvez créer un nouveau volume à partir d'un snapshot d'un volume. Dans ce cas, le système utilise les informations de snapshot pour cloner un nouveau volume à l'aide

des données contenues sur le volume au moment de la création de l'instantané. Ce processus stocke des informations sur les autres instantanés du volume dans le nouveau volume.

1. Cliquez sur **Data protection** > **snapshots**.
2. Cliquez sur l'icône **actions** du snapshot que vous souhaitez utiliser pour le clone de volume.
3. Dans le menu qui s'affiche, cliquez sur **Cloner le volume à partir de l'instantané**.
4. Entrez un **Nom du volume** dans la boîte de dialogue **Cloner le volume à partir de snapshot**.
5. Sélectionnez un **taille totale** et unités de taille pour le nouveau volume.
6. Sélectionnez un type **Access** pour le volume.
7. Sélectionnez un **compte** dans la liste à associer au nouveau volume.
8. Cliquez sur **Démarrer le clonage**.

Restaurer un volume vers un snapshot

Vous pouvez restaurer un volume à un instantané précédent à tout moment. Cette opération rétablit les modifications apportées au volume depuis la création du snapshot.

Étapes

1. Cliquez sur **Data protection** > **snapshots**.
2. Cliquez sur l'icône **actions** de 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 **revenir à l'instantané**, sélectionnez **Enregistrer l'état actuel du volume en tant qu'instantané**.
   b. Entrez un nom pour le nouvel instantané.
5. Cliquez sur **Restaurer instantané**.

Sauvegarder un snapshot de volume

Vous pouvez utiliser la fonctionnalité de sauvegarde intégrée pour sauvegarder un snapshot de volume. Vous pouvez sauvegarder des snapshots depuis un cluster SolidFire vers un magasin d'objets externe ou vers un autre cluster SolidFire. Lorsque vous sauvegardez un snapshot dans un magasin d'objets externe, vous devez disposer d'une connexion au magasin d'objets qui permet des opérations de lecture/écriture.

- "Sauvegarder un snapshot de volume dans un magasin d'objets Amazon S3"
- "Sauvegardez un snapshot de volume dans un magasin d'objets OpenStack Swift"
- "Sauvegarder un snapshot de volume sur un cluster SolidFire"

Sauvegarder un snapshot de volume dans un magasin d'objets Amazon S3

Vous pouvez sauvegarder des snapshots SolidFire dans des magasins d'objets externes compatibles avec Amazon S3.

1. Cliquez sur **protection des données** > **snapshots**.
2. Cliquez sur l'icône **actions** pour le snapshot que vous souhaitez sauvegarder.
3. Dans le menu qui s'affiche, cliquez sur **Sauvegarder sur**.
4. Dans la boîte de dialogue **Integrated Backup** sous **Backup to**, sélectionnez **S3**.
5. Sélectionnez une option sous **format de données** :
   - **Natif** : format compressé lisible uniquement par les systèmes de stockage SolidFire.
   - **Non compressé** : format non compressé compatible avec d'autres systèmes.
6. Entrez un nom d'hôte à utiliser pour accéder au magasin d'objets dans le champ **Nom d'hôte**.
7. Saisissez un ID de clé d'accès pour le compte dans le champ **ID de clé d'accès**.
8. Saisissez la clé secrète pour le 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 **nametag**.
11. Cliquez sur **Démarrer lecture**.

Sauvegardez un snapshot de volume dans un magasin d'objets OpenStack Swift

Vous pouvez sauvegarder des snapshots SolidFire dans des magasins d'objets secondaires compatibles avec OpenStack Swift.

1. Cliquez sur **Data protection** > **snapshots**.
2. Cliquez sur l'icône **actions** pour le snapshot que vous souhaitez sauvegarder.
3. Dans le menu qui s'affiche, cliquez sur **Sauvegarder sur**.
4. Dans la boîte de dialogue **Integrated Backup**, sous **Backup to**, sélectionnez **Swift**.
5. Sélectionnez une option sous **format de données** :
   - **Natif** : format compressé lisible uniquement par les systèmes de stockage SolidFire.
   - **Non compressé** : format non compressé compatible avec d'autres systèmes.
6. Saisissez une **URL** à utiliser pour accéder au magasin d'objets.
7. Saisissez un **Nom d'utilisateur** pour le compte.
8. Saisissez la **clé d'authentification** pour le compte.
9. Saisissez le **conteneur** dans lequel stocker la sauvegarde.
10. **Facultatif** : saisissez un **nom**.
11. Cliquez sur **Démarrer lecture**.

Sauvegarder un snapshot de volume sur un cluster SolidFire

Vous pouvez sauvegarder des snapshots 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 à utiliser pour l'authentification entre les clusters. Cette clé d'écriture de volume en bloc permet au cluster source de

s'authentifier auprès du cluster de destination, offrant 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 bloc à partir du volume de destination avant de démarrer l'opération.

1. Sur le cluster de destination, cliquez sur **Management** > **volumes**.
2. Cliquez sur l'icône **actions** pour le volume de destination.
3. Dans le menu résultant, cliquez sur **Restaurer depuis**.
4. Dans la boîte de dialogue **Restauration intégrée** sous **Restaurer depuis**, sélectionnez **SolidFire**.
5. Sélectionnez un format de données sous **format de données** :
   - **Natif** : format compressé lisible uniquement par les systèmes de stockage SolidFire.
   - **Non compressé** : format non compressé compatible avec d'autres systèmes.
6. Cliquez sur **générer clé**.
7. Copiez la clé de la case **clé d'écriture de volume en masse** dans votre presse-papiers.
8. Sur le cluster source, cliquez sur **Data protection** > **snapshots**.
9. Cliquez sur l'icône actions correspondant au snapshot que vous souhaitez utiliser pour la sauvegarde.
10. Dans le menu qui s'affiche, cliquez sur **Sauvegarder sur**.
11. Dans la boîte de dialogue **de la boîte de dialogue** sauvegarde intégrée de la section **sauvegarde vers**, sélectionnez **SolidFire**.
12. Sélectionnez le même format de données que celui sélectionné précédemment dans le champ **format de données**.
13. Entrez l'adresse IP virtuelle de gestion du cluster du volume de destination dans le champ **Remote Cluster MVIP**.
14. Entrez 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 de volume en bloc**, collez la clé que vous avez générée précédemment sur le cluster de destination.
17. Cliquez sur **Démarrer lecture**.

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

Vous pouvez créer un snapshot de groupe d'un ensemble de volumes associé afin de conserver une copie instantanée des métadonnées de chaque volume. Vous pouvez utiliser l'instantané de groupe ultérieurement comme sauvegarde ou restauration pour restaurer l'état du groupe de volumes à un état précédent.

Trouvez plus d'informations

- Créez un snapshot de groupe
- Modifier les instantanés de groupe
- Modifier les membres de l'instantané de groupe
- Supprimer un snapshot de groupe
- Restaurer les volumes dans un snapshot de groupe
- Clonage de plusieurs volumes

- Cloner plusieurs volumes à partir d'un snapshot de groupe

Détails de l'instantané de groupe

La page snapshots de groupe de l'onglet protection des données fournit des informations sur les instantanés de groupe.

- **ID**

  ID généré par le système pour l'instantané de groupe.

- **UUID**

  ID unique du snapshot de groupe.

- **Nom**

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

- **Créer heure**

  Heure à laquelle le snapshot de groupe a été créé.

- **Statut**

  État actuel du snapshot. Valeurs possibles :

  - Préparation : le snapshot est en cours de préparation et n'est pas encore accessible en écriture.
  - Terminé : cet instantané a terminé sa préparation et est maintenant utilisable.
  - Active : l'instantané est la branche active.

- **# volumes**

  Nombre de volumes dans le groupe.

- * Conserver jusqu'à*

  Le jour et l'heure de la suppression du snapshot.

- **Réplication à distance**

  Indique si le snapshot est activé ou non pour la réplication vers un cluster SolidFire distant. Valeurs possibles :

  - Activé : l'instantané est activé pour la réplication à distance.
  - Désactivé : le snapshot n'est pas activé pour la réplication à distance.

Création d'un snapshot de groupe

Vous pouvez créer un snapshot d'un groupe de volumes et créer un planning de snapshots de groupe pour automatiser les snapshots de groupe. Un snapshot de groupe unique peut effectuer des snapshots de manière cohérente jusqu'à 32 volumes à la fois.

Étapes

1. Cliquez sur **Management** > **volumes**.
2. Utilisez les cases à cocher pour sélectionner plusieurs volumes pour un groupe de volumes.
3. Cliquez sur **actions groupées**.
4. Cliquez sur **instantané de groupe**.
5. Entrez un nouveau nom d'instantané de groupe dans la boîte de dialogue Créer un instantané de groupe de volumes.
6. **Facultatif :** cochez la case **inclure chaque membre de snapshot de groupe dans la réplication lorsqu'il est couplé** pour vous assurer que chaque snapshot est capturé dans la réplication lorsque le volume parent est couplé.
7. Sélectionnez une option de conservation pour l'instantané de groupe :
   - Cliquez sur **conserver indéfiniment** pour conserver indéfiniment l'instantané sur le système.
   - Cliquez sur **Set Retention Period** et utilisez les champs de spin de date pour choisir une durée pour le système de conservation de l'instantané.
8. Pour créer un seul snapshot immédiat, effectuez les opérations suivantes :
   a. Cliquez sur **prendre l'instantané de groupe maintenant**.
   b. Cliquez sur **Créer instantané de groupe**.
9. Pour planifier l'exécution ultérieure de l'instantané, effectuez les opérations suivantes :
   a. Cliquez sur **Créer planification Snapshot de groupe**.
   b. Saisissez un **Nouveau nom d'horaire**.
   c. Sélectionnez un **Type d'horaire** dans la liste.
   d. **Facultatif :** cochez la case **Programme récurrent** pour répéter l'instantané programmé périodiquement.
   e. Cliquez sur **Créer un programme**.

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** > **snapshots de groupe**.
2. Cliquez sur l'icône actions correspondant au snapshot de groupe que vous souhaitez modifier.
3. Dans le menu qui s'affiche, sélectionnez **Modifier**.
4. **Facultatif:** pour modifier le paramètre de réplication du snapshot de groupe :
   a. Cliquez sur **Modifier** en regard de **réplication actuelle**.
   b. Cochez la case **inclure chaque membre de snapshot de groupe dans la réplication lorsqu'il est couplé** pour vous assurer que chaque instantané est capturé dans la réplication lorsque le volume parent est couplé.
5. **Facultatif :** pour modifier le paramètre de rétention de l'instantané de groupe, sélectionnez l'une des options suivantes :
   a. Cliquez sur **Modifier** en regard de **rétention actuelle**.
   b. Sélectionnez une option de conservation pour l'instantané de groupe :
      - Cliquez sur **conserver indéfiniment** pour conserver indéfiniment l'instantané sur le système.

- Cliquez sur **Set Retention Period** et utilisez les champs de spin de date pour choisir une durée pour le système de conservation de l'instantané.

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

Suppression d'un snapshot de groupe

Vous pouvez supprimer un instantané de groupe du système. Lorsque vous supprimez le snapshot de groupe, vous pouvez choisir de supprimer ou de conserver tous les instantanés associés au groupe en tant que snapshots individuels.

Si vous supprimez un volume ou un snapshot membre d'un snapshot de groupe, vous ne pouvez plus revenir au snapshot de groupe. Toutefois, vous pouvez restaurer chaque volume individuellement.

1. Cliquez sur **protection des données** > **snapshots de groupe**.
2. Cliquez sur l'icône actions du snapshot que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, cliquez sur **Supprimer**.
4. Sélectionnez l'une des options suivantes dans la boîte de dialogue de confirmation :
   - Cliquez sur **Supprimer l'instantané de groupe ET tous les membres de l'instantané de groupe** pour supprimer l'instantané de groupe et tous les snapshots membres.
   - Cliquez sur **conserver les membres de snapshot de groupe en tant que snapshots individuels** pour supprimer l'instantané de groupe, mais conserver tous les snapshots membres.
5. Confirmez l'action.

Restaurer les volumes dans un snapshot de groupe

Vous pouvez restaurer un groupe de volumes à tout moment vers un instantané de groupe.

Lorsque vous restaurez un groupe de volumes, tous les volumes du groupe sont restaurés à leur état au moment de la création de l'instantané de groupe. L'annulation restaure également les tailles de volume à la taille enregistrée dans le snapshot d'origine. Si le système a purgé un volume, tous les snapshots de ce volume ont également été supprimés au moment de la purge ; le système ne restaure pas les snapshots de volume supprimés.

1. Cliquez sur **protection des données** > **snapshots de groupe**.
2. Cliquez sur l'icône actions correspondant au snapshot de groupe que vous souhaitez utiliser pour la restauration de volume.
3. Dans le menu qui s'affiche, sélectionnez **Restaurer les volumes pour regrouper l'instantané**.
4. **Facultatif** : pour enregistrer l'état actuel des volumes avant de revenir au snapshot :
   a. Dans la boîte de dialogue **revenir à l'instantané**, sélectionnez **Enregistrer l'état actuel des volumes comme instantané de groupe**.
   b. Entrez un nom pour le nouvel instantané.
5. Cliquez sur **Restaurer l'instantané de groupe**.

Modification des membres de l'instantané de groupe

Vous pouvez modifier les paramètres de conservation des membres d'un snapshot de

groupe existant.

1. Cliquez sur **Data protection** > **snapshots**.
2. Cliquez sur l'onglet **membres**.
3. Cliquez sur l'icône actions du membre de snapshot de groupe que vous souhaitez modifier.
4. Dans le menu qui s'affiche, sélectionnez **Modifier**.
5. Pour modifier le paramètre de réplication de l'instantané, sélectionnez l'une des options suivantes :
   - Cliquez sur **conserver indéfiniment** pour conserver indéfiniment l'instantané sur le système.
   - Cliquez sur **Set Retention Period** et utilisez les champs de spin de date pour choisir une durée pour le système de conservation de l'instantané.
6. Cliquez sur **Enregistrer les modifications**.

Clonage de plusieurs volumes

Vous pouvez créer plusieurs clones de volumes en une seule opération pour créer une copie instantanée des données d'un groupe de volumes.

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

La taille du volume et la charge actuelle du cluster affectent le temps nécessaire à une opération de clonage.

Étapes

1. Cliquez sur **Management** > **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 **Clone** dans le menu résultant.
6. Entrez un **Nouveau préfixe de nom de volume** dans la boîte de dialogue **Clone multiple volumes**.

   Le préfixe est appliqué à tous les volumes du groupe.

7. **Facultatif:** sélectionnez un autre compte auquel le clone appartient.

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

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

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

Vous pouvez cloner un groupe de volumes à partir d'un snapshot de groupe instantané.

Cette opération nécessite qu'un snapshot de groupe des volumes existe déjà, car l'instantané de groupe est utilisé comme base pour créer les 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 affectent le temps nécessaire à une opération de clonage.

1. Cliquez sur **protection des données** > **snapshots de groupe**.
2. Cliquez sur l'icône actions correspondant au snapshot de groupe que vous souhaitez utiliser pour les clones de volume.
3. Dans le menu qui s'affiche, sélectionnez **Cloner volumes à partir de l'instantané de groupe**.
4. Entrez un **Nouveau préfixe de nom de volume** dans la boîte de dialogue **Cloner volumes à partir de l'instantané de groupe**.

   Le préfixe est appliqué à tous les volumes créés à partir du snapshot de groupe.

5. **Facultatif:** sélectionnez un autre compte auquel le clone appartient.

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

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

Planifier un snapshot

Vous pouvez protéger les données d'un volume ou d'un groupe de volumes en planifiant les copies Snapshot de volume pour qu'elles s'effectuent à intervalles spécifiés. Vous pouvez planifier l'exécution automatique des snapshots d'un seul volume ou de groupes.

Lorsque vous configurez un planning de snapshots, vous pouvez choisir entre des intervalles de temps basés sur des jours de la semaine ou des jours du mois. Vous pouvez également indiquer les jours, heures et minutes avant le prochain instantané. Vous pouvez stocker les snapshots résultants sur un système de stockage distant si le volume est en cours de réplication.

Trouvez plus d'informations

- Créer un planning de snapshots
- Modifier un planning de snapshots
- Supprime une planification de snapshots
- Copier un planning de snapshots

Détails de la planification des snapshots

Sur la page protection des données > plannings, vous pouvez afficher les informations suivantes dans la liste des planifications Snapshot.

- **ID**

ID généré par le système pour l'instantané.

- **Type**

  Type de planification. Le snapshot est actuellement le seul type pris en charge.

- **Nom**

  Nom donné au planning lors de sa création. Les noms de planning de snapshot peuvent comporter jusqu'à 223 caractères et contenir des caractères a-z, 0-9 et tiret (-).

- **Fréquence**

  Fréquence d'exécution de la planification. La fréquence peut être définie en heures, minutes, semaines ou mois.

- **Récurrent**

  Indique si le programme doit être exécuté une seule fois ou à intervalles réguliers.

- **Pause manuelle**

  Indique si la planification a été mise en pause manuelle ou non.

- **ID de volume**

  ID du volume utilisé par la planification lors de l'exécution de la planification.

- **Dernière exécution**

  Date de la dernière exécution de la planification.

- **État du dernier passage**

  Résultat de la dernière exécution du planning. Valeurs possibles :

  - Réussite
  - Panne

Créer un planning de snapshots

Vous pouvez planifier l'exécution automatique d'un ou de plusieurs volumes à des intervalles spécifiques.

Lorsque vous configurez un planning de snapshots, vous pouvez choisir entre des intervalles de temps basés sur des jours de la semaine ou des jours du mois. Vous pouvez également créer un programme récurrent et spécifier les jours, heures et minutes avant la prochaine capture d'écran.

Si vous planifiez l'exécution d'un instantané à une période qui n'est pas divisible d'ici 5 minutes, l'instantané s'exécute à la période suivante divisible d'ici 5 minutes. Par exemple, si vous planifiez l'exécution d'un snapshot à 12:42:00 UTC, il s'exécutera à 12:45:00 UTC. Vous ne pouvez pas programmer l'exécution d'un instantané à des intervalles inférieurs à 5 minutes.

Étapes

1. Cliquez sur **Data protection** > **Schedules**.

2. Cliquez sur **Créer un programme**.
3. Dans le champ **ID de volume CSV**, entrez un ID de volume unique ou une liste d'ID de volume séparée par des virgules à inclure dans l'opération d'instantané.
4. Saisissez un nouveau nom d'horaire.
5. Sélectionnez un type de programme et définissez le programme dans les options proposées.
6. **Facultatif:** sélectionnez **Programme récurrent** pour répéter indéfiniment la programmation d'instantanés.
7. **Facultatif :** Entrez un nom pour le nouvel instantané dans le champ **Nouveau nom d'instantané**.

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

8. **Facultatif:** cochez la case **inclure les instantanés dans la réplication lorsqu'ils sont couplés** pour vous assurer que les instantanés sont capturés en réplication lorsque le volume parent est couplé.
9. Pour définir la conservation de l'instantané, sélectionnez l'une des options suivantes :
   - Cliquez sur **conserver indéfiniment** pour conserver indéfiniment l'instantané sur le système.
   - Cliquez sur **Set Retention Period** et utilisez les champs de spin de date pour choisir une durée pour le système de conservation de l'instantané.
10. Cliquez sur **Créer un programme**.

Modifier un planning de snapshots

Vous pouvez modifier des plannings de snapshots existants. Après modification, la prochaine fois que le planning s'exécute, il utilise les attributs mis à jour. Tous les snapshots créés par le planning d'origine restent sur le système de stockage.

Étapes

1. Cliquez sur **Data protection** > **Schedules**.
2. Cliquez sur l'icône **actions** pour le programme que vous souhaitez modifier.
3. Dans le menu qui s'affiche, cliquez sur **Modifier**.
4. Dans le champ **ID de volume CSV**, modifiez l'ID de volume unique ou la liste des ID de volume séparés par des virgules actuellement inclus dans l'opération de snapshot.
5. Pour interrompre ou reprendre la programmation, sélectionnez l'une des options suivantes :
   - Pour interrompre un programme actif, sélectionnez **Oui** dans la liste **Pause manuel du programme**.
   - Pour reprendre un horaire en pause, sélectionnez **non** dans la liste **Pause manuel du programme**.
6. Entrez un nom différent pour l'horaire dans le champ **Nouveau nom d'horaire** si vous le souhaitez.
7. Pour modifier l'horaire à exécuter sur différents jours de la semaine ou du mois, sélectionnez **Type d'horaire** et modifiez l'horaire dans les options proposées.
8. **Facultatif:** sélectionnez **Programme récurrent** pour répéter indéfiniment la programmation d'instantanés.
9. **Facultatif :** Entrez ou modifiez le nom du nouvel instantané dans le champ **Nouveau nom d'instantané**.

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

10. **Facultatif:** cochez la case **inclure les instantanés dans la réplication lorsqu'ils sont couplés** pour vous assurer que les instantanés sont capturés en réplication lorsque le volume parent est couplé.
11. Pour modifier le paramètre de rétention, sélectionnez l'une des options suivantes :

- Cliquez sur **conserver indéfiniment** pour conserver indéfiniment l'instantané sur le système.
- Cliquez sur **Set Retention Period** et utilisez les zones de spin de date pour sélectionner une durée pour le système de conservation de l'instantané.

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

Copier un planning de snapshots

Vous pouvez copier un planning et conserver ses attributs actuels.

1. Cliquez sur **Data protection** > **Schedules**.
2. Cliquez sur l'icône actions correspondant au programme que vous souhaitez copier.
3. Dans le menu qui s'affiche, cliquez sur **faire une copie**.

   La boîte de dialogue **Créer un programme** apparaît, avec les attributs actuels du planning.

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

Supprime une planification de snapshots

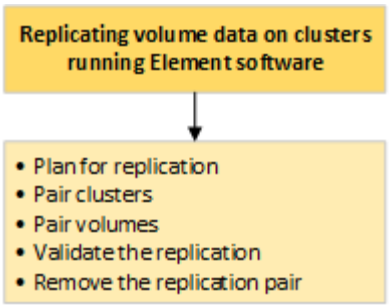
Vous pouvez supprimer un planning de snapshots. Une fois que vous avez supprimé le planning, il n'exécute pas de snapshots planifiés futurs. Tous les snapshots créés par la planification restent sur le système de stockage.

1. Cliquez sur **Data protection** > **Schedules**.
2. Cliquez sur l'icône **actions** pour le programme que vous souhaitez supprimer.
3. Dans le menu qui s'affiche, cliquez sur **Supprimer**.
4. Confirmez l'action.

Réplication à distance entre les clusters exécutant le logiciel NetApp Element

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

Le processus de réplication comprend les étapes suivantes :



- "Planifiez l'association des clusters et des volumes pour la réplication en temps réel"
- "Coupler les clusters pour la réplication"
- "Coupler les volumes"
- "Validation de la réplication de volume"
- "Supprime une relation de volume après la réplication"
- "Gestion des relations de volume"

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

La réplication à distance en temps réel implique de coupler deux clusters de stockage exécutant le logiciel Element, de coupler des volumes sur chaque cluster et de valider la réplication. Une fois la réplication terminée, vous devez supprimer la relation de volume.

Ce dont vous avez besoin

- Vous devez disposer des privilèges d'administrateur de cluster sur un ou les deux clusters en cours d'association.
- Toutes les adresses IP de nœud à la fois sur les réseaux de stockage et de gestion des clusters jumelés sont acheminées les unes aux autres.
- La MTU de tous les nœuds jumelés doit être identique et prise en charge de bout en bout entre les clusters.
- Les deux clusters de stockage doivent avoir des noms de cluster uniques, des adresses MVIP, des adresses IP de nœud et toutes les adresses IP de nœud.
- La différence entre les versions des logiciels Element sur les clusters est supérieure à une version principale. Si la différence est supérieure, l'un des clusters doit être mis à niveau pour effectuer la réplication des données.

> Les appliances WAN Accelerator n'ont pas été qualifiées par NetApp pour la réplication des données. Ces appliances peuvent interférer avec la compression et la déduplication si elles sont déployées entre deux clusters qui répliquant les données. Assurez-vous de bien qualifier les effets de tout accélérateur WAN avant de le déployer dans un environnement de production.

Trouvez plus d'informations

- Coupler les clusters pour la réplication
- Coupler les volumes
- Attribuez une source et une cible de réplication aux volumes couplés

Coupler les clusters pour la réplication

Vous devez coupler deux clusters pour utiliser la fonctionnalité de réplication en temps réel. Une fois que vous avez couplé et connecté deux clusters, vous pouvez configurer des volumes actifs sur un cluster pour qu'ils soient répliqués en continu sur un second cluster, assurant ainsi la protection continue des données (CDP).

Ce dont vous avez besoin

- Vous devez disposer des privilèges d'administrateur de cluster sur un ou les deux clusters en cours d'association.
- Tous les MIP et SIP de nœud sont acheminés les uns vers les autres.
- Moins de 2000 ms de latence aller-retour entre les clusters.
- Les deux clusters de stockage doivent avoir des noms de cluster uniques, des adresses MVIP, des adresses SVIP et toutes les adresses IP de nœud.
- La différence entre les versions des logiciels Element sur les clusters est supérieure à une version principale. Si la différence est supérieure, l'un des clusters doit être mis à niveau pour effectuer la réplication des données.

> L'association de cluster requiert une connectivité complète entre les nœuds du réseau de gestion. La réplication nécessite une connectivité entre les différents nœuds du réseau de cluster de stockage.

Vous pouvez coupler un cluster avec quatre autres clusters au maximum pour répliquer des volumes. Vous pouvez également coupler les clusters au sein du groupe de clusters.

Trouvez plus d'informations

Configuration requise pour les ports réseau

Couplez des clusters à l'aide de MVIP ou d'une clé de couplage

Vous pouvez coupler un cluster source et cible à l'aide du MVIP du cluster cible si un administrateur de cluster a accès aux deux clusters. Si l'accès à l'administrateur de cluster n'est disponible que sur un seul cluster d'une paire de clusters, une clé de couplage peut être utilisée sur le cluster cible pour terminer le couplage du cluster.

1. Sélectionnez l'une des méthodes suivantes pour coupler les clusters :
    - Coupler les clusters à l'aide de MVIP : utilisez cette méthode si l'administrateur de cluster a accès aux deux clusters. Cette méthode utilise le MVIP du cluster distant pour coupler deux clusters.
    - Couplez des clusters à l'aide d'une clé de couplage : utilisez cette méthode si l'administrateur de cluster n'a accès qu'à un seul cluster. Cette méthode génère une clé de couplage qui peut être utilisée sur le cluster cible pour terminer le couplage du cluster.

Trouvez plus d'informations

- Couplez des clusters à l'aide de MVIP
- Couplez des clusters à l'aide d'une clé de couplage

Couplez des clusters à l'aide de MVIP

Vous pouvez coupler deux clusters pour la réplication en temps réel en utilisant le MVIP d'un cluster pour établir une connexion avec l'autre cluster. Cette méthode doit permettre à l'administrateur du cluster d'accéder aux deux clusters. Le nom d'utilisateur et le mot de passe de l'administrateur du cluster permettent d'authentifier l'accès au cluster avant de pouvoir apparier les clusters.

1. Sur le cluster local, sélectionnez **Data protection** > **Cluster paires**.
2. Cliquez sur **pair Cluster**.
3. Cliquez sur **Démarrer le couplage** et cliquez sur **Oui** pour indiquer que vous avez accès au cluster distant.
4. Saisissez l'adresse MVIP du cluster distant.
5. Cliquez sur **effectuer le couplage sur le cluster distant**.

   Dans la fenêtre **Authentication required**, entrez le nom d'utilisateur et le mot de passe de l'administrateur de cluster du cluster distant.
6. Sur le cluster distant, sélectionnez **Data protection** > **Cluster paires**.
7. Cliquez sur **pair Cluster**.
8. Cliquez sur **Terminer le couplage**.
9. Cliquez sur le bouton **Terminer le couplage**.

Trouvez plus d'informations

- Couplez des clusters à l'aide d'une clé de couplage
- "Couplage de clusters à l'aide de MVIP (vidéo)"

Couplez des clusters à l'aide d'une clé de couplage

Si un administrateur de cluster a accès à un cluster local, mais pas au cluster distant, vous pouvez coupler les clusters à l'aide d'une clé de couplage. Une clé de couplage est générée sur un cluster local, puis envoyée en toute sécurité à un administrateur de cluster sur un site distant pour établir une connexion et réaliser l'association du cluster pour une réplication en temps réel.

1. Sur le cluster local, sélectionnez **Data protection** > **Cluster paires**.
2. Cliquez sur **pair Cluster**.
3. Cliquez sur **Démarrer le couplage** et cliquez sur **non** pour indiquer que vous n'avez pas accès au cluster distant.
4. Cliquez sur **générer clé**.

   Cette action génère une clé de texte pour le couplage et crée une paire de clusters non configurée sur le cluster local. Si vous ne terminez pas la procédure, vous devez supprimer manuellement la paire de clusters.
5. Copiez la clé de couplage du cluster dans le presse-papiers.

6. Rendez la clé de couplage accessible à l'administrateur du cluster sur le site distant du cluster.

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

> Ne modifiez aucun des caractères de la clé de couplage. La clé devient non valide si elle est modifiée.

7. Sur le cluster distant, sélectionnez **Data protection** > **Cluster paires**.
8. Cliquez sur **pair Cluster**.
9. Cliquez sur **Terminer le couplage** et entrez la clé de couplage dans le champ **touche de couplage** (le collage est la méthode recommandée).
10. Cliquez sur **Terminer le couplage**.

Trouvez plus d'informations

- Couplez des clusters à l'aide de MVIP
- "Association de clusters à l'aide d'une clé de couplage de cluster (vidéo)"

Valider la connexion de la paire de clusters

Une fois le couplage du cluster terminé, vous pouvez vérifier la connexion de la paire de clusters pour assurer la réussite de la réplication.

1. Sur le cluster local, sélectionnez **Data protection** > **Cluster paires**.
2. Dans la fenêtre **Cluster paires**, vérifiez que la paire cluster est connectée.
3. **Facultatif:** revenez au cluster local et à la fenêtre **Cluster paires** et vérifiez que la paire cluster est connectée.

Coupler les volumes

Une fois la connexion entre les clusters d'une paire de clusters établie, vous pouvez coupler un volume sur un cluster avec un volume sur l'autre cluster de la paire. Lorsqu'une relation de couplage de volume est établie, vous devez identifier le volume cible de réplication.

Vous pouvez coupler deux volumes pour une réplication en temps réel stockée sur différents clusters de stockage dans une paire de clusters connectée. Une fois que vous associez deux clusters, vous pouvez configurer des volumes actifs sur un cluster pour qu'ils soient répliqués en continu sur un second cluster, assurant ainsi la protection continue des données (CDP). Vous pouvez également attribuer un volume à la source ou à la cible de la réplication.

Les demandes de volume sont toujours une à une. Lorsqu'un volume fait partie d'une association avec un volume d'un autre cluster, vous ne pouvez plus le coupler avec un autre volume.

Ce dont vous avez besoin

- Vous avez établi une connexion entre les clusters dans une paire de clusters.
- Vous disposez des privilèges d'administrateur de cluster sur un ou les deux clusters en cours d'association.

Étapes

1. Créez un volume cible avec un accès en lecture ou en écriture
2. Couplez des volumes à l'aide d'un ID de volume ou d'une clé de couplage
3. Attribuez une source et une cible de réplication aux volumes couplés

Créez un volume cible avec un accès en lecture ou en écriture

Le processus de réplication implique deux terminaux : la source et le volume cible. Lorsque vous créez le volume cible, celui-ci est automatiquement défini en mode lecture/écriture pour accepter les données pendant la réplication.

1. Sélectionnez **Management** > **volumes**.
2. Cliquez sur **Créer un volume**.
3. Dans la boîte de dialogue Créer un nouveau volume, entrez le Nom du volume.
4. Entrez la taille totale du volume, sélectionnez une taille de bloc pour le volume, puis 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**.

Couplez des volumes à l'aide d'un ID de volume ou d'une clé de couplage

Le processus de couplage implique le couplage de deux volumes à l'aide d'un ID de volume ou d'une clé de couplage.

1. Couplez les volumes en sélectionnant l'une des méthodes suivantes :
   - Utilisation d'un ID de volume : utilisez cette méthode si vous avez accès des administrateurs du cluster aux deux clusters sur lesquels les volumes doivent être appariés. Cette méthode utilise l'ID du volume du cluster distant pour établir une connexion.
   - Utilisation d'une clé de couplage : utilisez cette méthode si l'administrateur de cluster n'a accès qu'au cluster source. Cette méthode génère une clé de couplage qui peut être utilisée sur le cluster distant pour terminer la paire de volumes.

> La clé de couplage de volume contient une version chiffrée des informations relatives au volume et peut contenir des informations sensibles. Partagez cette clé de manière sécurisée uniquement.

Trouvez plus d'informations

- Couplez des volumes à l'aide d'un ID de volume

- Couplez des volumes à l'aide d'une clé de couplage

Couplez des volumes à l'aide d'un ID de volume

Vous pouvez coupler un volume à un autre volume sur un cluster distant si vous disposez des informations d'identification d'administrateur de cluster pour le cluster distant.

Ce dont vous avez besoin

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

> Vous pouvez affecter une source et une cible de réplication après le processus de couplage. Une source ou une cible de réplication peut être un volume dans une paire de volumes. Vous devez créer un volume cible qui ne contient aucune donnée et qui présente les caractéristiques exactes du volume source, comme la taille, la taille de bloc pour les volumes (512 octets ou 4 ko) et la configuration de la qualité de service. Si vous attribuez un volume existant comme cible de réplication, les données de ce volume sont écrasées. Le volume cible peut être supérieur ou égal au volume source, mais il ne peut pas être plus petit.

- Connaître l'ID du volume cible.

Étapes

1. Sélectionnez **Management** > **volumes**.
2. Cliquez sur l'icône **actions** pour le volume que vous souhaitez coupler.
3. Cliquez sur **paire**.
4. Dans la boîte de dialogue **pair Volume**, sélectionnez **Start couplage**.
5. Sélectionnez **Je fais** pour indiquer que vous avez accès au cluster distant.
6. Sélectionnez un **mode de réplication** dans la liste :
   - **Temps réel (asynchrone)** : les écritures sont reconnues au client après leur validation sur le cluster source.
   - **Temps réel (synchrone)** : les écritures sont reconnues au client après leur validation sur les clusters source et cible.
   - **Snapshots uniquement** : seuls les snapshots créés sur le cluster source sont répliqués. Les écritures actives 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 le couplage**.

   Le système ouvre un onglet de navigateur Web qui se connecte à l'interface utilisateur Element du cluster distant. Vous devrez peut-être vous connecter au cluster distant avec les informations d'identification de l'administrateur du cluster.

10. Dans l'interface utilisateur de l'élément du cluster distant, sélectionnez **Complete Pairing**.
11. Confirmez les détails dans **confirmer le couplage de volume**.
12. Cliquez sur **Terminer le couplage**.

Après avoir confirmé le couplage, les deux clusters commencent à connecter les volumes pour le couplage. Pendant le processus de couplage, vous pouvez afficher les messages dans la colonne **Volume Status** de la fenêtre **Volume paires**. La paire de volumes s'affiche `PausedMisconfigured` jusqu'à ce que la source et la cible de la paire de volumes soient affectées.

Une fois le couplage terminé, vous devez actualiser la table volumes pour supprimer l'option **pair** de la liste **actions** du volume couplé. Si vous n'actualisez pas la table, l'option **paire** reste disponible pour la sélection. Si vous sélectionnez à nouveau l'option **paire**, un nouvel onglet s'ouvre et comme le volume est déjà couplé, le système signale un `StartVolumePairing Failed: xVolumeAlreadyPaired` Message d'erreur dans la fenêtre **pair Volume** de la page de l'interface utilisateur de l'élément.

Trouvez plus d'informations

- Messages de couplage de volume
- Avertissements de couplage de volume
- Attribuez une source et une cible de réplication aux volumes couplés

Couplez des volumes à l'aide d'une clé de couplage

Si vous ne disposez pas d'informations d'identification administrateur de cluster pour un cluster distant, vous pouvez coupler un volume à un autre volume d'un cluster distant à l'aide d'une clé de couplage.

Ce dont vous avez besoin

- Assurez-vous que les clusters contenant les volumes sont appariés.
- Assurez-vous qu'il y a un volume sur le cluster distant à utiliser pour le couplage.

> Vous pouvez affecter une source et une cible de réplication après le processus de couplage. Une source ou une cible de réplication peut être un volume dans une paire de volumes. Vous devez créer un volume cible qui ne contient aucune donnée et qui présente les caractéristiques exactes du volume source, comme la taille, la taille de bloc pour les volumes (512 octets ou 4 ko) et la configuration de la qualité de service. Si vous attribuez un volume existant comme cible de réplication, les données de ce volume sont écrasées. Le volume cible peut être supérieur ou égal au volume source, mais il ne peut pas être plus petit.

Étapes

1. Sélectionnez **Management** > **volumes**.
2. Cliquez sur l'icône **actions** pour le volume que vous souhaitez coupler.
3. Cliquez sur **paire**.
4. Dans la boîte de dialogue **pair Volume**, sélectionnez **Start couplage**.
5. Sélectionnez **Je ne** pas 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 reconnues au client après leur validation sur le cluster source.
   - **Temps réel (synchrone)** : les écritures sont reconnues au client après leur validation sur les clusters source et cible.

- **Snapshots uniquement** : seuls les snapshots créés sur le cluster source sont répliqués. Les écritures actives du volume source ne sont pas répliquées.

7. Cliquez sur **générer clé**.

   Cette action génère une clé de texte pour le couplage et crée une paire de volumes non configurés sur le cluster local. Si vous n'avez pas terminé la procédure, vous devrez supprimer manuellement la paire de volumes.

8. Copiez la clé de couplage dans le presse-papiers de votre ordinateur.
9. Mettez la clé de couplage à la disposition de l'administrateur du cluster sur le site distant du cluster.

   La clé de couplage de volume doit être traitée de manière sécurisée et ne pas être utilisée de manière à permettre un accès accidentel ou non sécurisé.

   Ne modifiez aucun des caractères de la clé de couplage. La clé devient non valide si elle est modifiée.

10. Dans l'interface utilisateur de l'élément de cluster distant, sélectionnez **Management** > **volumes**.
11. Cliquez sur l'icône actions du volume à coupler.
12. Cliquez sur **paire**.
13. Dans la boîte de dialogue **pair Volume**, sélectionnez **Complete couplage**.
14. Collez la clé de couplage de l'autre groupe dans la case **clé de couplage**.
15. Cliquez sur **Terminer le couplage**.

    Après avoir confirmé le couplage, les deux clusters commencent à connecter les volumes pour le couplage. Pendant le processus de couplage, vous pouvez afficher les messages dans la colonne **Volume Status** de la fenêtre **Volume paires**. La paire de volumes s'affiche `PausedMisconfigured` jusqu'à ce que la source et la cible de la paire de volumes soient affectées.

    Une fois le couplage terminé, vous devez actualiser la table volumes pour supprimer l'option **pair** de la liste **actions** du volume couplé. Si vous n'actualisez pas la table, l'option **paire** reste disponible pour la sélection. Si vous sélectionnez à nouveau l'option **paire**, un nouvel onglet s'ouvre et comme le volume est déjà couplé, le système signale un `StartVolumePairing Failed: xVolumeAlreadyPaired` Message d'erreur dans la fenêtre **pair Volume** de la page de l'interface utilisateur de l'élément.

Trouvez plus d'informations

- Messages de couplage de volume
- Avertissements de couplage de volume
- Attribuez une source et une cible de réplication aux volumes couplés

Attribuez une source et une cible de réplication aux volumes couplés

Une fois les volumes couplés, vous devez affecter un volume source et son volume cible de réplication. Une source ou une cible de réplication peut être un volume dans une paire de volumes. Vous pouvez également utiliser cette procédure pour rediriger les données envoyées vers un volume source vers un volume cible distant en cas d'indisponibilité du

volume source.

Ce dont vous avez besoin

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

Étapes

1. Préparation du volume source :

   a. Dans le cluster contenant le volume que vous souhaitez attribuer en tant que source, sélectionnez **Management** > **volumes**.

   b. Cliquez sur l'icône **actions** du volume que vous souhaitez attribuer en tant que source et cliquez sur **Modifier**.

   c. Dans la liste déroulante **Access**, sélectionnez **Read/Write**.

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

   La modification de l'accès interrompt la réplication du volume et entraîne 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. Préparation du volume cible :

   a. Dans le cluster contenant le volume que vous souhaitez attribuer en tant que cible, sélectionnez **Management** > **volumes**.

   b. Cliquez sur l'icône actions du volume que vous souhaitez attribuer en tant que cible et cliquez sur **Modifier**.

   c. Dans la liste déroulante **Access**, sélectionnez **cible de réplication**.

   > Si vous attribuez un volume existant comme cible de réplication, les données de ce volume sont écrasées. Vous devez utiliser un nouveau volume cible qui ne contient aucune donnée et qui présente les caractéristiques exactes du volume source, comme la taille, le paramètre 512 et la configuration de la qualité de service. Le volume cible peut être supérieur ou égal au volume source, mais il ne peut pas être plus petit.

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

Trouvez plus d'informations

- Couplez des volumes à l'aide d'un ID de volume
- Couplez des volumes à l'aide d'une clé de couplage

Validation de la réplication de volume

Après la réplication d'un volume, assurez-vous que les volumes source et cible sont actifs. Dans un état actif, les volumes sont jumelés, les données sont envoyées de la source au volume cible et les données sont synchronisées.

1. Dans les deux clusters, sélectionnez **Data protection** > **Volume paires**.

2. Vérifiez que l'état du volume est actif.

Trouvez plus d'informations

Avertissements de couplage de volume

Supprime une relation de volume après la réplication

Une fois la réplication terminée et vous n'avez plus besoin de la relation de paire de volumes, vous pouvez supprimer la relation de volume.

1. Sélectionnez **Data protection** > **Volume paires**.
2. Cliquez sur l'icône **actions** de la paire de volumes à supprimer.
3. Cliquez sur **Supprimer**.
4. Confirmez le message.

Gestion des relations de volume

Vous pouvez gérer les relations de volume de plusieurs façons, comme mettre en pause la réplication, inverser le couplage de volumes, changer le mode de réplication, supprimer une paire de volumes ou supprimer une paire de clusters.

Trouvez plus d'informations

- Interrompre la réplication
- Changer le mode de réplication
- Supprimez les paires de volumes

Interrompre la réplication

Vous pouvez suspendre la réplication manuellement si vous devez interrompre le traitement des E/S pendant une courte période. Vous pouvez interrompre la réplication en cas de pic de traitement des E/S et en cas de réduction de la charge de traitement.

1. Sélectionnez **Data protection** > **Volume paires**.
2. Cliquez sur l'icône actions de la paire de volumes.
3. Cliquez sur **Modifier**.
4. Dans le volet **Edit Volume pair**, interrompez manuellement le processus de réplication.

> La mise en pause ou la reprise manuelle de la réplication du 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**.

Changer le mode de réplication

Vous pouvez modifier les propriétés de la paire de volumes pour modifier le mode de

réplication de la relation de la paire de volumes.

1. Sélectionnez **Data protection** > **Volume paires**.
2. Cliquez sur l'icône actions de la paire de volumes.
3. Cliquez sur **Modifier**.
4. Dans le volet **Edit Volume pair**, sélectionnez un nouveau mode de réplication :
   - **Temps réel (asynchrone)** : les écritures sont reconnues au client après leur validation sur le cluster source.
   - **Temps réel (synchrone)** : les écritures sont reconnues au client après leur validation sur les clusters source et cible.
   - **Snapshots uniquement** : seuls les snapshots créés sur le cluster source sont répliqués. Les écritures actives du volume source ne sont pas répliquées. **Attention:** changer 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**.

Supprimez les paires de volumes

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

1. Sélectionnez **Data protection** > **Volume paires**.
2. Cliquez sur l'icône actions de la paire de volumes à supprimer.
3. Cliquez sur **Supprimer**.
4. Confirmez le message.

Supprime une paire de clusters

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

1. Cliquez sur **Data protection** > **Cluster paires**.
2. Cliquez sur l'icône actions d'une paire de clusters.
3. Dans le menu qui s'affiche, cliquez sur **Supprimer**.
4. Confirmez l'action.
5. Effectuez de nouveau les étapes à partir du second cluster au sein du jumelage des clusters.

Détails des paires de clusters

La page paires de clusters de l'onglet protection des données fournit des informations sur les clusters qui ont été appariés ou en cours de couplage. Le système affiche des messages de couplage et de progression dans la colonne État.

- **ID**

  ID généré par le système donné à chaque paire du cluster.

- **Nom du cluster distant**

Nom de l’autre cluster de la paire.

- **MVIP à distance**

  Adresse IP virtuelle de gestion de l’autre cluster de la paire.

- **Statut**

  État de réplication du cluster distant

- **Volumes de réplication**

  Nombre de volumes contenus par le cluster jumelés pour la réplication.

- **UUID**

  ID unique attribué à chaque cluster de la paire.

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 en cours de couplage. Le système affiche des messages de couplage et de progression dans la colonne État du volume.

- **ID**

  ID généré par le système pour le volume.

- **Nom**

  Nom donné au volume lors de sa création. Les noms de volume peuvent comporter jusqu’à 223 caractères et contenir a-z, 0-9 et tiret (-).

- **Compte**

  Nom du compte attribué au volume.

- **Etat du volume**

  État de réplication du volume

- **État de l’instantané**

  État du volume snapshot.

- **Mode**

  Méthode de réplication d’écriture client. Les valeurs possibles sont les suivantes :

  - Asynchrone
  - Snapshot uniquement
  - Synchrone

- **Direction**

Direction des données du volume :

- Icône du volume source (→) indique que des données sont écrites sur une cible en dehors du cluster.
- Icône du volume cible (←) indique que les 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 de volume distant**

  ID de volume du volume sur le cluster distant.

- **Nom du volume distant**

  Nom attribué au volume distant lors de sa création.

Messages de couplage de volume

Vous pouvez afficher les messages de couplage de volume pendant le processus de couplage initial à partir de la page paires de volumes sous l'onglet protection des données. Ces messages peuvent s'afficher aux extrémités source et cible de la paire dans la vue liste volumes de réplication.

- **PausedDisconnected**

  Expiration de la réplication source ou de la synchronisation des RPC. La connexion au cluster distant a été perdue. Vérifiez les connexions réseau au cluster.

- **ResumingConnected**

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

- **ResuminingRRSync**

  Une seule copie Helix des métadonnées du volume est créée dans le cluster couplée.

- **ResumingLocalSync**

  Une copie double hélice des métadonnées du volume est créée dans le cluster associé.

- **ResumingDataTransfer**

  Le transfert des données a repris.

- **Actif**

Les volumes sont appariés et les données sont envoyées depuis la source vers le volume cible. Les données sont en cours de synchronisation.

- **Ralenti**

  Aucune activité de réplication n'a lieu.

Avertissements de couplage de volume

La page paires de volumes de l'onglet protection des données fournit ces messages après la paire de volumes. Ces messages peuvent s'afficher aux extrémités source et cible de la paire (sauf indication contraire) dans la vue de liste volumes de réplication.

- **PausedClusterFull**

  Étant donné que le cluster cible est plein, la réplication source et le transfert de données en bloc ne peuvent pas se faire. Le message s'affiche uniquement à l'extrémité source de la paire.

- **PausedExcededMaxSnapshotCount**

  Le volume cible dispose déjà du nombre maximal de snapshots et ne peut pas répliquer d'autres snapshots.

- **PausedManual**

  Le volume local a été mis en pause manuellement. Il doit être mis en pause avant la reprise de la réplication.

- **PausedManualRemote**

  Le volume distant est en mode pause manuelle. Intervention manuelle requise pour annuler la pause du volume distant avant la reprise de la réplication.

- **PausedMisConfigured**

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

- **PausedQoS**

  La qualité de service cible n'a pas pu supporter les E/S entrantes. Reprises automatiques de la réplication. Le message s'affiche uniquement à l'extrémité source de la paire.

- **PausedSlowLink**

  Liaison lente détectée et interruption de la réplication. Reprises automatiques de la réplication. Le message s'affiche uniquement à l'extrémité source de la paire.

- **PausedVolumeSizeMatch**

  La taille du volume cible n'est pas identique à celle du volume source.

- **PausedXCopy**

  Une commande SCSI XCOPY est envoyée vers un volume source. La commande doit se terminer avant que la réplication puisse reprendre. Le message s'affiche uniquement à l'extrémité source de la paire.

- **StoppedMisConfigured**

  Une erreur de configuration permanente a été détectée. Le volume distant a été purgé ou non apparié. Aucune action corrective n'est possible ; une nouvelle association doit être établie.

Utilisez la réplication SnapMirror entre les clusters Element et ONTAP

Vous pouvez créer des relations SnapMirror à partir de l'onglet protection des données dans l'interface utilisateur de NetApp Element. La fonctionnalité SnapMirror doit être activée pour que ce type de fonctionnalité soit visible 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"

Les systèmes exécutant le logiciel NetApp Element prennent en charge la fonctionnalité SnapMirror pour copier et restaurer les copies Snapshot avec les systèmes NetApp ONTAP. Cette technologie repose en premier lieu sur la reprise après incident de NetApp HCI vers ONTAP. Ces terminaux incluent ONTAP, ONTAP Select et Cloud Volumes ONTAP. Consultez le document TR-4641 protection des données NetApp HCI.

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

Trouvez plus d'informations

- "Bâtissez votre Data Fabric avec NetApp HCI, ONTAP et l'infrastructure convergée"
- "Réplication entre le logiciel NetApp Element et ONTAP"

Présentation de SnapMirror

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

Les systèmes exécutant Element peuvent communiquer directement avec SnapMirror sur les systèmes ONTAP versions 9.3 ou ultérieures. L'API NetApp Element propose des méthodes d'activation de la fonctionnalité SnapMirror sur les clusters, les volumes et les snapshots. De plus, l'interface utilisateur Element inclut toutes les fonctionnalités nécessaires pour gérer les relations SnapMirror entre le logiciel Element et les systèmes ONTAP.

Vous pouvez répliquer des volumes ONTAP émis vers des volumes Element dans des cas d'utilisation spécifiques avec une fonctionnalité limitée. Pour plus d'informations, consultez la documentation ONTAP.

Trouvez plus d'informations

"Réplication entre le logiciel Element et ONTAP"

Activation de SnapMirror sur le cluster

Vous devez activer manuellement la fonctionnalité SnapMirror au niveau du cluster via l'interface utilisateur NetApp Element. Le système est fourni avec la fonctionnalité SnapMirror désactivée par défaut, qui n'est pas automatiquement activé dans le cadre d'une nouvelle installation ou 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 d'un système NetApp ONTAP. Vous devez activer la fonctionnalité SnapMirror uniquement si le cluster est connecté pour une utilisation avec les volumes NetApp ONTAP.

Ce dont vous avez besoin

Le cluster de stockage doit exécuter le logiciel NetApp Element.

Étapes

1. Cliquez sur **clusters** > **Paramètres**.
2. Recherchez les paramètres cluster pour SnapMirror.
3. Cliquez sur **Activer SnapMirror**.

> L'activation de la fonctionnalité SnapMirror modifie définitivement la configuration du logiciel Element. Vous ne pouvez désactiver la fonctionnalité SnapMirror et restaurer les paramètres par défaut que en retournant le cluster à l'image d'usine.

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

Activer 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. Cette autorisation est autorisée par l'administrateur du cluster exécutant le logiciel NetApp Element pour SnapMirror afin de contrôler un volume.

Ce dont vous avez besoin

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

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

Étapes

1. Cliquez sur **Management** > **volumes**.
2. Cliquez sur l'icône **actions** du 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 terminal SnapMirror

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

Un terminal 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 terminal SnapMirror.

Vous pouvez créer et gérer jusqu'à quatre terminaux SnapMirror dans un cluster de stockage exécutant le logiciel Element.

> Si un noeud final 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 noeud final 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 noeud final ne peut alors être géré qu'à l'aide de l'API Element.

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

Ce dont vous avez besoin

- Vous devez avoir activé SnapMirror dans l'interface utilisateur Element pour le cluster de stockage.
- Vous connaissez les informations d'identification ONTAP pour le noeud final.

Étapes

1. Cliquez sur **Data protection** > **SnapMirror Endpoints**.
2. Cliquez sur **Créer un point final**.
3. Dans la boîte de dialogue **Créer un nouveau point final**, entrez l'adresse IP de gestion de cluster du système ONTAP.
4. Entrez les informations d'identification de l'administrateur ONTAP associées au noeud final.
5. Consultez les informations complémentaires :
   - LIFs : liste les interfaces logiques ONTAP intercluster utilisées pour communiquer avec Element.
   - Status : affiche l'état actuel du noeud final SnapMirror. Les valeurs possibles sont : connecté, déconnecté et non géré.
6. Cliquez sur **Créer un point final**.

Créer une relation SnapMirror

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

> Lorsqu'un volume n'est pas encore activé pour SnapMirror et que vous sélectionnez de créer une relation dans l'interface utilisateur d'Element, SnapMirror est automatiquement activé sur ce volume.

Ce dont vous avez besoin

SnapMirror est activé sur le volume.

Étapes

1. Cliquez sur **Management** > **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 noeud final dans la liste **Endpoint**.
5. Sélectionnez 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 Element, cliquez sur **Créer un nouveau volume**.
   a. Sélectionnez **Storage Virtual machine** pour cette relation.
   b. Sélectionnez **Aggregate** dans la liste déroulante.
   c. Dans le champ **Nom du volume suffixe**, entrez un suffixe.

      Le système détecte le nom du volume source et le copie dans le champ **Nom du volume**. Le suffixe que vous entrez ajoute le nom.

   d. Cliquez sur **Créer un volume de destination**.
7. Pour utiliser un volume ONTAP existant, cliquez sur **utiliser un volume existant**.
   a. Sélectionnez **Storage Virtual machine** pour cette relation.
   b. Sélectionnez le volume cible de cette nouvelle relation.
8. Dans la section **Détails de la relation**, sélectionnez une stratégie. Si la stratégie sélectionnée possède des règles de conservation, la table règles affiche les règles et les étiquettes associées.
9. **Facultatif** : sélectionnez un programme.

   Cette valeur détermine la fréquence à laquelle la relation crée des copies.

10. **Facultatif** : dans le champ **Limit Bandwidth to**, entrez la quantité maximale de bande passante qui peut être utilisée par les transferts de données associés à cette relation.
11. Consultez les informations complémentaires :
    - **État** : état de relation actuel du volume de destination. Les valeurs possibles sont :
      - Non initialisé : le volume de destination n'a pas été initialisé.
      - Snapmiroité : le volume de destination a été initialisé et prêt à recevoir les mises à jour SnapMirror.
      - Broken-off : le volume de destination est en lecture/écriture et des instantanés sont présents.
    - **Statut** : état actuel de la relation. Les valeurs possibles sont inactive, transférer, vérifier, suspendre, suspendre, en file d'attente, préparation, finalisation, abandon et interruption.
    - **Temps de décalage** : durée en secondes pendant laquelle le système de destination est en retard derrière le système source. Le temps de décalage ne doit pas dépasser l'intervalle de planification de transfert.
    - **Limite de bande passante** : la quantité maximale de bande passante qui peut être consommée par les transferts de données associés à cette relation.
    - **Dernier transfert** : horodatage du dernier instantané transféré. Cliquez pour plus d'informations.
    - **Nom de la politique** : nom de la règle ONTAP SnapMirror pour la relation.
    - **Type de politique** : type de règle ONTAP SnapMirror sélectionnée pour la relation. Les valeurs possibles sont :
      - async_mirror
      - coffre-fort_miroir
    - **Nom de l'horaire** : nom de l'horaire préexistant sur le système ONTAP sélectionné pour cette relation.
12. Pour ne pas s'initialiser à ce stade, assurez-vous que la case **Initialize** n'est pas cochée.

L'initialisation peut prendre beaucoup de temps. Il peut être préférable de l'exécuter pendant les heures creuses. L'initialisation effectue un transfert de base ; elle effectue une copie Snapshot du volume source, puis transfère cette copie ainsi que tous les blocs de données qu'elle référence au volume de destination. Vous pouvez initialiser manuellement ou utiliser une planification pour démarrer le processus d'initialisation (et les mises à jour suivantes) en fonction du planning.

13. Cliquez sur **Créer relation**.
14. Cliquez sur **Data protection** > **SnapMirror Relationship** pour afficher cette nouvelle relation SnapMirror.

Actions relatives aux relations SnapMirror

Vous pouvez configurer une relation à partir de la page relations SnapMirror de l'onglet protection des données. Les options de l'icône actions sont décrites ici.

- **Modifier** : modifie la stratégie utilisée ou le calendrier de la relation.
- **Delete** : supprime la relation SnapMirror. Cette fonction ne supprime pas le volume de destination.
- **Initialize** : effectue le premier transfert initial de données de base pour établir une nouvelle relation.
- **Mise à jour** : effectue une mise à jour à la demande de la relation, en répliquant toutes les nouvelles données et copies Snapshot incluses depuis la dernière mise à jour vers la destination.
- **Quiesce**: Empêche toute mise à jour supplémentaire pour une relation.
- **Reprendre** : reprend une relation qui est mise au repos.
- **Break**: Rend le volume de destination lecture-écriture et arrête tous les transferts actuels et futurs. Déterminez 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.
- **Resync** : rétablit une relation rompue dans la même direction avant que la rupture ne se produise.
- **Reverse Resync** : automatise les étapes nécessaires pour créer et initialiser une nouvelle relation dans la direction opposée. Ceci peut être effectué uniquement si la relation existante est à l'état rompu. Cette opération ne supprimera pas la relation actuelle. Le volume source d'origine rétablit la copie Snapshot commune la plus récente et resynchronise avec la destination. Toute modification apportée au volume source d'origine depuis la dernière mise à jour SnapMirror réussie est perdue. Toute modification apportée ou toute nouvelle donnée écrite dans le volume de destination actuel est renvoyée au volume source d'origine.
- **Abort** : annule un transfert en cours. Si une mise à jour SnapMirror est publiée pour une relation abandonnée, la relation se poursuit avec le dernier transfert depuis le dernier point de contrôle de redémarrage qui a été créé avant l'abandon.

Étiquettes SnapMirror

Une étiquette SnapMirror sert de marqueur pour transférer un snapshot spécifié selon les règles de conservation de la relation.

L'application d'une étiquette à un Snapshot la marque en tant que cible de la réplication SnapMirror. Le rôle de la relation est d'appliquer les règles lors du transfert de données en sélectionnant l'instantané étiqueté correspondant, en le copiant vers le volume de destination, et en veillant à ce que le nombre correct de copies soit conservé. Il se réfère à la politique pour déterminer le nombre de conserver et la période de conservation. La police peut avoir un nombre illimité de règles et chaque règle a un libellé unique. Cette étiquette sert de lien entre l'instantané et la règle de conservation.

Il s'agit de l'étiquette SnapMirror qui indique la règle appliquée au snapshot sélectionné, au snapshot de groupe ou à la planification.

Ajoutez des étiquettes SnapMirror aux snapshots

Les étiquettes SnapMirror spécifient la règle de conservation des snapshots sur le terminal SnapMirror. Vous pouvez ajouter des étiquettes aux instantanés et aux instantanés de groupe.

Vous pouvez afficher les étiquettes disponibles dans la boîte de dialogue existante relative à la relation SnapMirror ou dans NetApp ONTAP System Manager.

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

Ce dont vous avez besoin

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

Étapes

1. Cliquez sur **protection des données** > **snapshots** ou **snapshots de groupe**.
2. Cliquez sur l'icône **actions** pour le snapshot ou le snapshot de groupe auquel vous souhaitez ajouter une étiquette SnapMirror.
3. Dans la boîte de dialogue **Edit snapshot**, entrez du texte dans le champ **SnapMirror Label**. L'étiquette doit correspondre à une étiquette de règle dans la règle appliquée à la relation SnapMirror.
4. Cliquez sur **Enregistrer les modifications**.

Ajoutez des étiquettes SnapMirror aux planifications de snapshots

Vous pouvez ajouter des étiquettes SnapMirror aux planifications Snapshot afin de vous assurer qu'une règle SnapMirror est appliquée. Vous pouvez afficher les étiquettes disponibles dans la boîte de dialogue correspondante ou dans NetAppONTAP System Manager.

Ce dont vous avez besoin

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

Étapes

1. Cliquez sur **Data protection** > **Schedules**.
2. Ajoutez une étiquette SnapMirror à une planification de l'une des manières suivantes :

Option	Étapes
Création d'une planification	a. Sélectionnez **Créer un programme**. b. Entrez tous les autres détails pertinents. c. Sélectionnez **Créer un programme**.

Option	Étapes
Modification d'un planning existant	a. Cliquez sur l'icône **actions** pour le programme auquel vous souhaitez ajouter un libellé et sélectionnez **Modifier**. b. Dans la boîte de dialogue qui s'affiche, entrez du texte dans le champ **libellé SnapMirror**. c. Sélectionnez **Enregistrer les modifications**.

Trouvez plus d'informations

Créer un planning de snapshots

Reprise sur incident avec SnapMirror

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

Si le cluster d'origine est totalement défaillant ou inexistant, contactez le support NetApp pour obtenir de l'aide.

Effectuer un basculement à partir d'un cluster Element

Vous pouvez effectuer un basculement depuis le cluster Element pour rendre le volume de destination accessible en lecture/écriture et aux hôtes côté destination. Avant d'effectuer un basculement à partir du cluster Element, vous devez interrompre 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 l'interface de ligne de commandes ONTAP pour lancer la commande « interrompre la relation ».

Ce dont vous avez besoin

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

Étapes

1. Dans l'interface utilisateur Element, cliquez sur **Data protection** > **SnapMirror relations**.
2. Recherchez la relation avec le volume source que vous souhaitez basculer.
3. Cliquez sur l'icône **actions**.
4. Cliquez sur **Break**.
5. Confirmez l'action.

   Le volume du cluster de destination dispose désormais d'un accès en lecture/écriture et peut être monté sur les hôtes de l'application pour reprendre les workloads de production. Toutes les réplications SnapMirror sont interrompues à la suite de cette opération. La relation montre un état de rupture.

Effectuez un rétablissement de l'élément

Lorsque le problème du côté principal a été réduit, vous devez resynchroniser le volume source d'origine et revenir au logiciel NetApp Element. Les étapes que vous effectuez varient selon que le volume source d'origine existe toujours ou si vous devez revenir à un volume nouvellement créé.

Trouvez plus d'informations

- Effectuez une restauration lorsque le volume source existe toujours
- Effectuez une restauration lorsque le volume source n'existe plus
- Scénarios de restauration SnapMirror

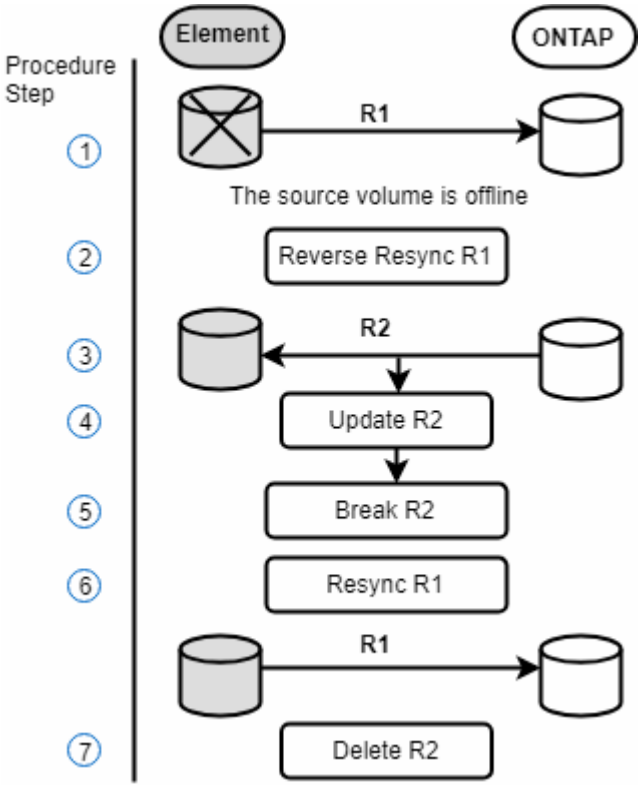
Scénarios de restauration SnapMirror

La fonctionnalité de reprise sur incident SnapMirror est illustrée dans deux scénarios de restauration. Ceux-ci supposent que la relation d'origine a été rompue.

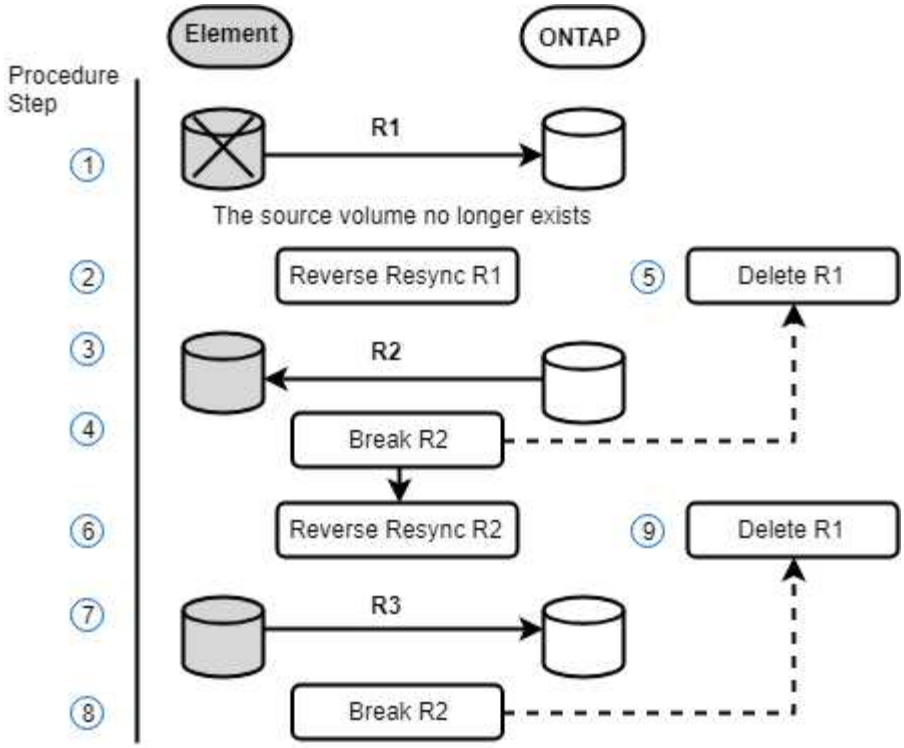
Les étapes des procédures correspondantes sont ajoutées pour référence.

> Dans les exemples ci-dessous, R1 = relation initiale où le cluster exécutant le logiciel NetApp Element est le volume source d'origine (Element) et ONTAP le volume de destination d'origine (ONTAP). R2 et R3 représentent les relations inverses créées via l'opération de resynchronisation inverse.

L'image suivante montre le scénario de retour arrière lorsque le volume source est toujours présent :



L'image suivante montre le scénario de retour arrière lorsque le volume source n'existe plus :



Trouvez plus d'informations

- Effectuez une restauration lorsque le volume source existe toujours
- Effectuez une restauration lorsque le volume source n'existe plus

Effectuez 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 situations où le volume source d'origine existe toujours.

1. Dans l'interface utilisateur Element, recherchez la relation que vous avez rompue le basculement.
2. Cliquez sur l'icône actions et cliquez sur **Reverse Resync**.
3. Confirmez l'action.

> L'opération Reverse Resync crée une nouvelle relation dans laquelle les rôles des volumes source et de destination d'origine sont inversés (cela entraîne deux relations comme la relation d'origine persiste). Dans le cadre de l'opération de resynchronisation inverse, toutes les nouvelles données du volume de destination d'origine sont transférées vers le volume source d'origine. Vous pouvez continuer à accéder aux données et à les écrire sur le volume actif du côté de destination, mais vous devez déconnecter tous les hôtes du volume source et effectuer une mise à jour SnapMirror avant de rediriger vers le volume primaire d'origine.

4. Cliquez sur l'icône actions de la relation inverse que vous venez de créer et cliquez sur **mettre à jour**.

   Maintenant que vous avez terminé la resynchronisation inverse et que vous avez veillé à ce que aucune session active ne soit connectée au volume côté destination et que les données les plus récentes se trouvent sur le volume primaire d'origine, pour terminer le retour arrière et réactiver le volume principal

d'origine, procédez comme suit :

5. Cliquez sur l'icône actions de la relation inverse et cliquez sur **Break**.
6. Cliquez sur l'icône actions de la relation d'origine et cliquez sur **Resync**.

> Le volume primaire d'origine peut désormais être monté pour reprendre les workloads de production sur le volume primaire d'origine. La réplication SnapMirror d'origine reprend en fonction de la règle et du planning configurés pour la relation.

7. Après avoir confirmé que le statut de la relation d'origine est "napmiroité", cliquez sur l'icône actions de la relation inverse et cliquez sur **Supprimer**.

Trouvez plus d'informations

Scénarios de restauration SnapMirror

Effectuez 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 le cluster d'origine est toujours intact. Pour obtenir des instructions sur la restauration vers un nouveau cluster, consultez la documentation disponible sur le site de support NetApp.

Ce dont vous avez besoin

- Vous disposez d'une relation de réplication rompue entre les volumes Element et ONTAP.
- Le volume de l'élément est irrémédiablement perdu.
- Le nom du volume d'origine apparaît comme INTROUVABLE.

Étapes

1. Dans l'interface utilisateur Element, recherchez la relation que vous avez rompue le basculement.

   Meilleure pratique : notez les détails de la règle SnapMirror et du calendrier de la relation initiale interrompue. Ces informations seront nécessaires lors de la recréation de la relation.

2. Cliquez sur l'icône **actions** et cliquez sur **Reverse Resync**.
3. Confirmez l'action.

> L'opération Reverse Resync crée une nouvelle relation dans laquelle les rôles du volume source d'origine et du volume de destination sont inversés (cela entraîne deux relations comme la relation d'origine persiste). Comme le volume d'origine n'existe plus, le système crée un nouveau volume Element avec le même nom de volume et la même taille de volume que le volume source d'origine. Le nouveau volume se voit attribuer une politique de 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 règle de qualité de services pour tous les volumes créés par SnapMirror pour remplacer les volumes source d'origine qui ont été détruits.

Les données du dernier snapshot sont transférées vers le nouveau volume dans le cadre de l'opération de resynchronisation inverse. Vous pouvez continuer à accéder aux données et à les écrire sur le volume actif

du côté de la destination, mais vous devez déconnecter tous les hôtes du volume actif et effectuer une mise à jour de SnapMirror avant de réintégrer la relation principale d'origine dans une étape ultérieure. Une fois la resynchronisation inverse terminée et assurez-vous qu'aucune session active n'est connectée au volume côté 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 arrière et réactiver le volume principal d'origine :

4. Cliquez sur l'icône **actions** de la relation inverse créée pendant l'opération Reverse Resync et cliquez sur **Break**.
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 **Inverser la resynchronisation**.
7. La source et la destination sont ainsi inversés et la relation avec la même source de volume et la même destination de volume que la relation d'origine s'effectue.
8. Cliquez sur l'icône **actions** et sur **Modifier** pour mettre à jour cette relation avec la stratégie de QoS d'origine et les paramètres de planification que vous avez pris en compte.
9. Maintenant, vous pouvez supprimer la relation inverse que vous avez resynchronisés à l'étape 6.

Trouvez plus d'informations

Scénarios de restauration SnapMirror

Effectuez un transfert ou une migration ponctuelle de ONTAP vers Element

En général, lorsque vous utilisez SnapMirror pour la reprise d'activité à partir d'un cluster de stockage SolidFire exécutant le logiciel NetApp Element vers le logiciel ONTAP, Element est la source et ONTAP, destination. Cependant, dans certains cas, le système de stockage ONTAP peut servir de source et d'élément comme destination.

- Deux scénarios existent :
  - Aucune relation de reprise après incident antérieure n'existe. Suivre toutes les étapes de cette procédure.
  - Il existe une relation antérieure de reprise après incident, mais pas entre les volumes utilisés pour cette atténuation. Dans ce cas, suivez uniquement les étapes 3 et 4 ci-dessous.

Ce dont vous avez besoin

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

Vous devez spécifier le chemin de destination d'élément sous la forme hostip:/lun/<ID_number>, où lun est la chaîne réelle « LUN » et ID_number l'ID du volume élément.

Étapes

1. Avec 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. Vérifier que la relation SnapMirror a été créée à l'aide de la commande ONTAP snapmirror show.

   Pour plus d'informations sur la création d'une relation de réplication dans la documentation ONTAP et pour connaître la syntaxe complète des commandes, reportez-vous à la page de manuel ONTAP.

3. À l'aide du `ElementCreateVolume` API, créer le volume cible et définir le mode d'accès du 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 de ONTAP `snapmirror initialize` commande :

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

Sauvegarde et restauration de volumes

Vous pouvez sauvegarder et restaurer des volumes dans d'autres systèmes de stockage SolidFire, ainsi que des magasins 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 devez disposer d'informations de manifeste à partir du processus de sauvegarde d'origine. Si vous restaurez un volume sauvegardé sur un système de stockage SolidFire, aucune information manifeste n'est requise.

Trouvez plus d'informations

- Sauvegarde d'un volume dans un magasin d'objets Amazon S3
- Sauvegardez un volume dans un magasin d'objets OpenStack Swift
- Sauvegarder un volume sur un cluster de stockage SolidFire
- Restauration d'un volume à partir d'une sauvegarde sur un magasin d'objets Amazon S3
- Restauration d'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

Sauvegarde d'un volume dans un magasin d'objets Amazon S3

Vous pouvez sauvegarder des volumes dans des magasins d'objets externes compatibles avec Amazon S3.

1. Cliquez sur **Management** > **volumes**.
2. Cliquez sur l'icône actions correspondant au volume à sauvegarder.
3. Dans le menu qui s'affiche, cliquez sur **Sauvegarder sur**.
4. Dans la boîte de dialogue **Integrated Backup** sous **Backup to**, sélectionnez **S3**.
5. Sélectionnez une option sous **format de données** :
   - **Natif** : format compressé lisible uniquement par les systèmes de stockage SolidFire.
   - **Non compressé** : format non compressé compatible avec d'autres systèmes.
6. Entrez un nom d'hôte à utiliser pour accéder au magasin d'objets dans le champ **Nom d'hôte**.
7. Saisissez un ID de clé d'accès pour le compte dans le champ **ID de clé d'accès**.
8. Saisissez la clé secrète pour le compte dans le champ **clé d'accès secrète**.
9. Saisissez le compartiment S3 dans lequel stocker la sauvegarde dans le champ **compartiment S3**.
10. Entrez un nom à ajouter au préfixe dans le champ **nametag**.
11. Cliquez sur **Démarrer lecture**.

Sauvegardez un volume dans un magasin d'objets OpenStack Swift

Vous pouvez sauvegarder des volumes dans des magasins d'objets externes compatibles avec OpenStack Swift.

1. Cliquez sur **Management** > **volumes**.
2. Cliquez sur l'icône actions du volume à sauvegarder.
3. Dans le menu qui s'affiche, cliquez sur **Sauvegarder sur**.
4. Dans la boîte de dialogue **Integrated Backup** sous **Backup to**, sélectionnez **Swift**.
5. Sélectionnez un format de données sous **format de données** :

- **Natif** : format compressé lisible uniquement par les systèmes de stockage SolidFire.
- **Non compressé** : format non compressé compatible avec d'autres systèmes.

6. Saisissez une URL à utiliser pour accéder au magasin d'objets dans le champ **URL**.
7. Entrez 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 **Container**.
10. **Facultatif** : saisissez un nom à ajouter au préfixe dans le champ **nametag**.
11. Cliquez sur **Démarrer lecture**.

Sauvegarder un volume sur un cluster de stockage SolidFire

Vous pouvez sauvegarder des volumes résidant sur un cluster distant pour des clusters de stockage exécutant le logiciel Element.

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

Voir "Coupler les clusters pour la réplication".

Lors de la sauvegarde ou de la restauration d'un cluster à un autre, le système génère une clé à utiliser pour l'authentification entre les clusters. Cette clé d'écriture de volume en bloc permet au cluster source de s'authentifier auprès du cluster de destination, offrant 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 bloc à partir du volume de destination avant de démarrer l'opération.

1. Sur le cluster de destination, **Management** > **volumes**.
2. Cliquez sur l'icône actions du volume de destination.
3. Dans le menu résultant, cliquez sur **Restaurer depuis**.
4. Dans la boîte de dialogue **Restauration intégrée**, sous **Restaurer depuis**, sélectionnez **SolidFire**.
5. Sélectionnez une option sous **format de données** :
   - **Natif** : format compressé lisible uniquement par les systèmes de stockage SolidFire.
   - **Non compressé** : format non compressé compatible avec d'autres systèmes.
6. Cliquez sur **générer clé**.
7. Copiez la clé de la case **clé d'écriture de volume en masse** dans votre presse-papiers.
8. Sur le cluster source, accédez à **Management** > **volumes**.
9. Cliquez sur l'icône actions du volume à sauvegarder.
10. Dans le menu qui s'affiche, cliquez sur **Sauvegarder sur**.
11. Dans la boîte de dialogue **sauvegarde intégrée** sous **sauvegarde vers**, sélectionnez **SolidFire**.
12. Sélectionnez la même option que celle sélectionnée précédemment dans le champ **format de données**.
13. Entrez l'adresse IP virtuelle de gestion du cluster du volume de destination dans le champ **Remote Cluster MVIP**.
14. Entrez 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 de volume en bloc**, collez la clé que vous avez générée précédemment sur

le cluster de destination.

17. Cliquez sur **Démarrer lecture**.

Restauration d'un volume à partir d'une sauvegarde sur un magasin d'objets Amazon S3

Vous pouvez restaurer un volume à partir d'une sauvegarde sur un magasin d'objets Amazon S3.

1. Cliquez sur **Rapport** > **Journal des événements**.
2. Recherchez l'événement de sauvegarde qui a créé la sauvegarde à restaurer.
3. Dans la colonne **Détails** de l'événement, cliquez sur **Afficher les détails**.
4. Copiez les informations du manifeste dans le presse-papiers.
5. Cliquez sur **Management** > **volumes**.
6. Cliquez sur l'icône actions du volume à restaurer.
7. Dans le menu résultant, cliquez sur **Restaurer depuis**.
8. Dans la boîte de dialogue **Integrated Restore** sous **Restore from**, sélectionnez **S3**.
9. Sélectionnez l'option correspondant à la sauvegarde sous **format de données** :
   - **Natif** : format compressé lisible uniquement par les systèmes de stockage SolidFire.
   - **Non compressé** : format non compressé compatible avec d'autres systèmes.
10. Entrez un nom d'hôte à utiliser pour accéder au magasin d'objets dans le champ **Nom d'hôte**.
11. Saisissez un ID de clé d'accès pour le compte dans le champ **ID de clé d'accès**.
12. Saisissez la clé secrète pour le 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 **manifest**.
15. Cliquez sur **Start Write**.

Restauration d'un volume à partir d'une sauvegarde sur un magasin d'objets OpenStack Swift

Vous pouvez restaurer un volume à partir d'une sauvegarde dans un magasin d'objets OpenStack Swift.

1. Cliquez sur **Rapport** > **Journal des événements**.
2. Recherchez l'événement de sauvegarde qui a créé la sauvegarde à restaurer.
3. Dans la colonne **Détails** de l'événement, cliquez sur **Afficher les détails**.
4. Copiez les informations du manifeste dans le presse-papiers.
5. Cliquez sur **Management** > **volumes**.
6. Cliquez sur l'icône actions du volume à restaurer.
7. Dans le menu résultant, cliquez sur **Restaurer depuis**.
8. Dans la boîte de dialogue **Integrated Restore** sous **Restore from**, sélectionnez **Swift**.
9. Sélectionnez l'option correspondant à la sauvegarde sous **format de données** :
   - **Natif** : format compressé lisible uniquement par les systèmes de stockage SolidFire.

- **Non compressé** : format non compressé compatible avec d'autres systèmes.

10. Saisissez une URL à utiliser pour accéder au magasin d'objets dans le champ **URL**.
11. Entrez 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. Entrez le nom du conteneur dans lequel la sauvegarde est stockée dans le champ **Container**.
14. Collez les informations du manifeste dans le champ **manifest**.
15. Cliquez sur **Start Write**.

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 à utiliser pour l'authentification entre les clusters. Cette clé d'écriture de volume en bloc permet au cluster source de s'authentifier auprès du cluster de destination, offrant 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 bloc à partir du volume de destination avant de démarrer l'opération.

1. Sur le cluster de destination, cliquez sur **Management** > **volumes**.
2. Cliquez sur l'icône actions du volume à restaurer.
3. Dans le menu résultant, cliquez sur **Restaurer depuis**.
4. Dans la boîte de dialogue **Restauration intégrée**, sous **Restaurer depuis**, sélectionnez **SolidFire**.
5. Sélectionnez l'option correspondant à la sauvegarde sous **format de données** :
   - **Natif** : format compressé lisible uniquement par les systèmes de stockage SolidFire.
   - **Non compressé** : format non compressé compatible avec d'autres systèmes.
6. Cliquez sur **générer clé**.
7. Copiez les informations **clé d'écriture de volume en masse** dans le presse-papiers.
8. Dans le cluster source, cliquez sur **Management** > **volumes**.
9. Cliquez sur l'icône actions du volume que vous souhaitez utiliser pour la restauration.
10. Dans le menu qui s'affiche, cliquez sur **Sauvegarder sur**.
11. Dans la boîte de dialogue **sauvegarde intégrée**, sélectionnez **SolidFire** sous **sauvegarde sur**.
12. Sélectionnez l'option qui correspond à la sauvegarde sous **format de données**.
13. Entrez l'adresse IP virtuelle de gestion du cluster du volume de destination dans le champ **Remote Cluster MVIP**.
14. Entrez 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 de votre presse-papiers dans le champ **clé d'écriture de volume en vrac**.
17. Cliquez sur **Démarrer lecture**.

Dépanner votre système

Vous devez surveiller le système à des fins de diagnostic et obtenir des informations sur les tendances de performances et les États des différentes opérations du système. Vous devrez peut-être remplacer les nœuds ou les disques SSD à des fins de maintenance.

- "Affiche des informations relatives aux événements système"
- "Afficher l'état des tâches en cours d'exécution"
- "Afficher les alertes système"
- "Afficher l'activité sur les performances du nœud"
- "Afficher les performances des volumes"
- "Afficher les sessions iSCSI"
- "Afficher les sessions Fibre Channel"
- "Résoudre les problèmes liés aux disques"
- "Résoudre les problèmes"
- "Utilisation d'utilitaires par nœud pour les nœuds de stockage"
- "Travaillez avec le nœud de gestion"
- "Comprendre les niveaux de remplissage du cluster"

Pour en savoir plus

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

Affiche des informations relatives aux événements système

Vous pouvez afficher des informations sur les différents événements détectés dans le système. Le système actualise les messages d'événement toutes les 30 secondes. Le journal des événements affiche les principaux événements du cluster.

1. Dans l'interface utilisateur de l'élément, sélectionnez **Rapport** > **Journal des événements**.

   Pour chaque événement, les informations suivantes s'affichent :

Élément	Description
ID	ID unique associé à chaque événement.
Type d'événement	Type d'événement consigné, par exemple, des événements d'API ou des événements de clonage.
Messagerie	Message associé à l'événement.
Détails	Informations permettant d'identifier la raison de l'événement.

ID de service	Service qui a signalé l'incident (le cas échéant).
Nœud	Nœud ayant signalé l'événement (le cas échéant).
ID de disque	Le lecteur qui a signalé l'incident (le cas échéant).
Heure de l'événement	Heure à laquelle l'événement s'est produit.

Trouvez plus d'informations

Types d'événement

Types d'événement

Le système signale plusieurs types d'événements ; chaque événement est une opération que le système a effectuée. Les événements peuvent être de routine, des événements normaux ou des événements nécessitant l'intervention de l'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 ne consigne pas les commandes API en lecture seule dans le journal des événements.

La liste suivante décrit les types d'événements qui s'affichent dans le journal des événements :

- **ApiEvent**

  Événements lancés par un utilisateur via une API ou une interface utilisateur Web qui modifie les paramètres.

- **BinAssignesEvénement**

  Événements liés à l'affectation des bacs de données. Les bacs sont essentiellement des conteneurs qui détiennent des données et qui sont mappés dans le cluster.

- **BinSyncEvent**

  Événements système liés à une réattribution de données entre les services en mode bloc.

- **BsCheckEvent**

  Événements système liés aux contrôles de service de bloc.

- **BsKillEvent**

  Événements système liés aux cessations d'emploi du bloc.

- **BulkOpEvent**

  Événements liés aux opérations effectuées sur un volume entier, comme une sauvegarde, une

restauration, une copie Snapshot ou un clone.

- **CloneEvent**

  Événements liés au clonage de volume.

- **ClusterMasterEvent**

  Événements apparaissant lors de l'initialisation du cluster ou lors des modifications de configuration apportées au cluster, comme l'ajout ou la suppression de nœuds.

- **CsumEvent**

  Événements liés à des checksums de données non valides sur le disque.

- **DataEvent**

  Événements liés à la lecture et à l'écriture des données.

- **DbEvent**

  Événements liés à la base de données globale gérés par des nœuds d'ensemble dans le cluster.

- **Événement de conduite**

  Événements liés aux opérations de conduite.

- **EncryptionAtRestEvent**

  Événements liés au processus de chiffrement sur un cluster.

- **Événement**

  Événements liés à l'augmentation ou à la diminution du nombre de nœuds d'un ensemble.

- **FibroChannelEvent**

  Événements liés à la configuration de et connexions aux nœuds.

- **GcEvent**

  Les événements liés aux processus s'exécutent toutes les 60 minutes pour récupérer du stockage sur des disques en mode bloc. Ce processus est également connu sous le nom de collecte de déchets.

- **IEvent**

  Erreur système interne.

- **Installevent**

  Événements d'installation automatique du logiciel. Le logiciel est automatiquement installé sur un nœud en attente.

- **ISCSIEvent**

  Événements liés aux problèmes iSCSI dans le système.

- **LimEvent**

  Événements liés au nombre de volumes ou de volumes virtuels dans un compte ou dans le cluster proche du maximum autorisé.

- **MainenanceModeEvent**

  Événements liés au mode de maintenance du nœud, tels que la désactivation du nœud.

- **NetworkEvent**

  Événements liés à l'état de la mise en réseau virtuelle.

- **HardwareEvent plateforme**

  Événements liés à des problèmes détectés sur des périphériques matériels.

- **RemoteClusterEvent**

  Événements liés au couplage à distance du cluster.

- **SchedulerEvent**

  Événements liés aux instantanés programmés.

- **ServiceEvent**

  Événements liés à l'état de service du système.

- **SliceEvent**

  Événements liés au serveur de tranches, tels que la suppression d'un lecteur ou d'un volume de métadonnées.

  Il existe trois types d'événements de réaffectation de tranche, qui incluent des informations sur le service dans lequel un volume est affecté :

  - inversion : changement du service principal en un nouveau service principal

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

  - déplacement : déplacement du service secondaire vers un nouveau service secondaire

    ```
    sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
    ```

  - suppression: suppression d'un volume d'un ensemble de services

    ```
    sliceID {oldSecondaryServiceID(s)}
    ```

- **SnmpTrapEvent**

Événements liés aux traps SNMP.

- **StatEvent**

  Événements liés aux statistiques du système.

- **TsEvent**

  Événements liés au service de transport du système.

- **UnexpectedException**

  Événements liés à des exceptions système inattendues.

- **UretEvent**

  Événements liés aux erreurs de lecture irrécupérables qui se produisent 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 d'exécution

Vous pouvez afficher la progression et l'état d'exécution des tâches exécutées dans l'interface utilisateur Web qui sont signalées par les méthodes API ListSyncJobs et ListBulkVolumeJobs. Vous pouvez accéder à la page tâches en cours d'exécution à partir de l'onglet Rapports de l'interface utilisateur de l'élément.

S'il existe 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 en cours de synchronisation. Lorsqu'une tâche est terminée, elle est remplacée par la tâche de synchronisation en file d'attente suivante. La synchronisation des tâches peut continuer à apparaître sur la page tâches en cours d'exécution jusqu'à ce qu'il n'y ait plus de tâches à effectuer.

Vous pouvez voir les données de synchronisation de réplication des volumes en cours de réplication sur la page tâches en cours du cluster contenant le volume cible.

Afficher les alertes système

Vous pouvez afficher les alertes pour obtenir des informations sur les défaillances ou les erreurs de cluster dans le système. Les alertes peuvent être des informations, des avertissements ou des erreurs et constituent un bon indicateur de leur fonctionnement. La plupart des erreurs se résolvent automatiquement.

Vous pouvez utiliser la méthode ListClusterFaults API pour automatiser la surveillance des alertes. Vous serez ainsi informé de toutes les alertes qui se produisent.

1. Dans l'interface utilisateur de l'élément, sélectionnez **Rapport** > **alertes**.

   Le système actualise les alertes de la page toutes les 30 secondes.

Pour chaque événement, les informations suivantes s'affichent :

Élément	Description
ID	ID unique associé à une alerte de cluster.
Gravité	Le degré d'importance de l'alerte. Valeurs possibles : • Avertissement : un problème mineur qui peut bientôt nécessiter une attention particulière. Les mises à niveau du système sont toujours autorisées. • Erreur : défaillance pouvant entraîner une dégradation des performances ou une perte de la haute disponibilité. Les erreurs ne doivent généralement pas affecter le service. • Critique : une défaillance grave qui affecte le service. Le système ne peut pas traiter les demandes d'E/S de l'API ou du client. L'utilisation de cet état peut entraîner une perte potentielle de données. • BEST Practice : aucune pratique recommandée pour la configuration des systèmes n'est en cours d'utilisation.
Type	Composant affecté par le défaut. Peut être un nœud, un disque, un cluster, un service ou un volume.
Nœud	ID de nœud du nœud auquel cette erreur fait référence. Inclus pour les défaillances de nœud et de lecteur, sinon réglé sur - (tableau de bord).
ID de disque	ID du lecteur auquel cette anomalie fait référence. Inclus pour les défauts de conduite, sinon réglé à - (tableau de bord).
Code d'erreur	Code descriptif indiquant la cause du défaut.
Détails	Une description du défaut avec des détails supplémentaires.
Date	La date et l'heure auxquelles le défaut a été enregistré.

2. Cliquez sur **Afficher les détails** pour une alerte individuelle afin d'afficher des informations sur l'alerte.
3. Pour afficher les détails de toutes les alertes sur la page, cliquez sur la colonne Détails.

Une fois que le système a résolu une alerte, toutes les informations concernant l'alerte, y compris la date à laquelle elle a été résolue, sont déplacées vers la zone résolue.

Trouvez plus d'informations

- Codes d'anomalie du bloc d'instruments
- "Gérez le stockage avec l'API Element"

Codes d'anomalie du bloc d'instruments

Le système signale une erreur ou un état qui pourrait être intéressant en générant un code d'erreur, qui est répertorié sur la page alertes. Ces codes vous aident à déterminer quel composant du système a rencontré l'alerte et pourquoi l'alerte a été générée.

La liste suivante présente les différents types de codes :

- **AuthenticationServiceFault**

  Le service d'authentification sur un ou plusieurs nœuds de cluster ne fonctionne pas comme prévu.

  Contactez le support NetApp pour obtenir de l'aide.

- **DisponibleVirtualNetworkIPAddressesLow**

  Le nombre d'adresses réseau virtuelles dans le bloc d'adresses IP est faible.

  Pour résoudre ce problème, ajoutez d'autres adresses IP au bloc d'adresses réseau virtuelles.

- **BlockClusterFull**

  L'espace de stockage bloc est insuffisant pour prendre en charge la perte d'un nœud. Pour plus de détails sur les niveaux de remplissage du cluster, reportez-vous à la méthode GetClusterFullThreshold API. Cette panne du cluster indique l'une des conditions suivantes :

  - Stage3Low (Avertissement) : le seuil défini par l'utilisateur a été franchi. Réglez les paramètres Cluster Full ou ajoutez des nœuds.
  - Stage4Critique (erreur) : l'espace disponible pour la restauration suite à une défaillance d'un nœud est insuffisant. La création de volumes, de snapshots et de clones n'est pas autorisée.
  - Stage5CompletelyConsumied (critique)1 ; aucune écriture ni aucune nouvelle connexion iSCSI ne sont autorisées. Les connexions iSCSI actuelles seront conservées. Les écritures échouent jusqu'à ce que davantage de capacité soit ajoutée au cluster. Pour résoudre cette défaillance, purgez ou supprimez des volumes ou ajoutez un autre nœud de stockage au cluster de stockage.

- **Blocs Degraded**

  Les données de bloc ne sont plus intégralement répliquées en raison d'une défaillance.

Gravité	Description
Avertissement	Seules deux copies complètes des données de bloc sont accessibles.

Erreur	Seule une seule copie complète des données du bloc est accessible.
Primordial	Aucune copie complète des données de bloc n'est accessible.

Remarque : l'état d'avertissement ne peut se produire que sur un système Triple Helix.

Pour résoudre ce problème, restaurez tout nœud hors ligne ou service de bloc, ou contactez le support NetApp pour obtenir de l'aide.

- **BlockServiceTooFull**

  Un service de bloc utilise trop d'espace.

  Pour résoudre cette erreur, ajoutez de la capacité provisionnée.

- **BlockServiceIsain**

  Un service de bloc a été détecté comme défectueux :

  - Gravité = Avertissement : aucune action n'est entreprise. Cette période d'avertissement expire dans cTimeUntilBSIsKilledMsec=330000 millisecondes.
  - Gravité = erreur : le système met automatiquement hors service les données et reréplique ses données sur d'autres lecteurs en bon état.
  - Gravité = critique : des services de bloc défaillants sur plusieurs nœuds supérieurs ou égaux au nombre de réplications (2 pour la double hélice). Les données ne sont pas disponibles et la synchronisation des bacs ne se termine pas. Recherchez des problèmes de connectivité réseau et des erreurs matérielles. Il y aura d'autres défauts si des composants matériels spécifiques sont défectueux. Le défaut s'efface lorsque le service de bloc est accessible ou lorsque le service a été déclassé.

- **ClockewExceedsFaiultThreshold**

  L'écart de temps entre le maître de cluster et le nœud présentant un jeton dépasse le seuil recommandé. Le cluster de stockage ne peut pas corriger automatiquement l'écart de temps entre les nœuds.

  Pour résoudre ce problème, utilisez des serveurs NTP internes à votre réseau plutôt que les paramètres par défaut de l'installation. Si vous utilisez un serveur NTP interne, contactez le support NetApp pour obtenir de l'aide.

- **ClusterCannotSync**

  Il existe un manque d'espace et les données des disques de stockage bloc hors ligne ne peuvent pas être synchronisées avec des disques toujours actifs.

  Pour résoudre ce problème, ajoutez de l'espace de stockage supplémentaire.

- **ClusterFull**

  Il n'y a plus d'espace de stockage libre dans le cluster de stockage.

  Pour résoudre ce problème, ajoutez de l'espace de stockage supplémentaire.

- **ClusterIOPSAreprovisionning**

  Les IOPS du cluster sont surprovisionnées. La somme de toutes les IOPS minimales de QoS est supérieure aux IOPS attendues du cluster. Il est impossible de maintenir la qualité de service minimale pour tous les volumes simultanément.

  Pour résoudre ce problème, réduisez les paramètres d'IOPS de QoS minimaux pour les volumes.

- **DisableDriveSecurityFailed**

  Le cluster n'est pas configuré pour activer la sécurité des disques (chiffrement au repos), mais la sécurité d'au moins un disque est activée, ce qui signifie que la désactivation de la sécurité du disque sur ces disques est en panne. Cette anomalie est consignée avec la gravité « Avertissement ».

  Pour résoudre ce problème, vérifiez les détails de l'erreur pour savoir pourquoi la sécurité du lecteur n'a pas pu être désactivée. Les raisons possibles sont :

  - La clé de chiffrement n'a pas pu être acquise, recherchez le problème d'accès à la clé ou au serveur de clés externe.
  - L'opération de désactivation a échoué sur le lecteur, déterminez si la mauvaise clé a pu être acquise. Si aucun de ces éléments n'est la cause du défaut, il est possible que le lecteur doive être remplacé.

  Vous pouvez tenter de récupérer un lecteur qui ne désactive pas la sécurité avec succès, même lorsque la clé d'authentification correcte est fournie. Pour effectuer cette opération, retirez le ou les lecteurs du système en les déplaçant vers disponibles, effectuez une suppression sécurisée sur le lecteur et revenez à actif.

- **DisconnectedClusterpair**

  Une paire de clusters est déconnectée ou configurée de manière incorrecte. Vérifier la connectivité réseau entre les clusters.

- **DisconnectedRemoteNode**

  Un nœud distant est déconnecté ou configuré de manière incorrecte. Vérifiez la connectivité réseau entre les nœuds.

- **DisconnectedSnapMirror orEndpoint**

  Un terminal SnapMirror distant est déconnecté ou configuré de manière incorrecte. Vérifiez la connectivité réseau entre le cluster et le point de terminaison SnapMirror distant.

- **Possible**

  Un ou plusieurs disques sont disponibles dans le cluster. En général, tous les clusters doivent avoir tous des disques ajoutés ou aucun disque n'est à l'état disponible. Si ce défaut apparaît de façon inattendue, contactez le support NetApp.

  Pour résoudre ce problème, ajoutez tout disque disponible au cluster de stockage.

- **Véhicule dégradé**

  Le cluster renvoie cette panne lorsqu'un ou plusieurs disques sont en panne, ce qui indique l'une des conditions suivantes :

- Le gestionnaire de lecteur ne peut pas accéder au lecteur.
- Le service de tranche ou de bloc a échoué trop de fois, probablement à cause des échecs de lecture ou d'écriture du disque, et ne peut pas redémarrer.
- Le lecteur est manquant.
- Le service maître du nœud est inaccessible (tous les disques du nœud sont considérés comme manquants/défaillants).
- Le lecteur est verrouillé et la clé d'authentification du lecteur ne peut pas être acquise.
- Le lecteur est verrouillé et l'opération de déverrouillage échoue. Pour résoudre ce problème :
- Vérifiez la connectivité réseau du nœud.
- Remplacez le lecteur.
- Assurez-vous que la clé d'authentification est disponible.

- **DriveHealthFault**

  Un lecteur a échoué à la vérification de l'état DU LECTEUR INTELLIGENT et, par conséquent, les fonctions du lecteur sont réduites. Il existe un niveau de gravité critique pour ce défaut :

  - Disque avec le numéro de série : <numéro de série> dans le slot : <slot de nœud><slot de disque> a échoué au contrôle global INTELLIGENT de l'état du disque. Pour résoudre ce problème, remplacez le lecteur.

- **Anomalie de la transmission**

  La durée de vie restante d'un disque est inférieure aux seuils, mais il fonctionne toujours.il existe deux niveaux de gravité possibles pour cette anomalie : critique et avertissement :

  - Disque en série : <numéro de série> dans le slot : <slot de nœud><slot de disque> présente des niveaux d'usure stratégiques.
  - Disque avec série : <numéro de série> dans le slot : <slot de nœud><slot de disque> présente une faible usure. Pour résoudre ce problème, remplacez rapidement le lecteur.

- **DupliateClusterMasterCandidates**

  Plusieurs candidats de maître de cluster de stockage ont été détectés. Contactez le support NetApp pour obtenir de l'aide.

- **EnableDriveSecurityFailed**

  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. Cette anomalie est consignée avec la gravité « Avertissement ».

  Pour résoudre ce problème, vérifiez les détails de l'anomalie pour savoir pourquoi la sécurité du lecteur n'a pas pu être activée. Les raisons possibles sont :

  - La clé de chiffrement n'a pas pu être acquise, recherchez le problème d'accès à la clé ou au serveur de clés externe.
  - L'opération d'activation a échoué sur le lecteur, déterminez si la clé incorrecte a pu être acquise. Si aucun de ces éléments n'est la cause du défaut, il est possible que le lecteur doive être remplacé.

  Vous pouvez tenter de récupérer un lecteur qui n'active pas la sécurité avec succès, même lorsque la clé d'authentification correcte est fournie. Pour effectuer cette opération, retirez le ou les lecteurs du système

en les déplaçant vers disponibles, effectuez une suppression sécurisée sur le lecteur et revenez à actif.

- **Dégradêtre**

  La connectivité ou l'alimentation réseau a été perdue à un ou plusieurs des nœuds de l'ensemble.

  Pour résoudre ce problème, restaurez la connectivité ou l'alimentation réseau.

- **exception**

  Un défaut signalé qui est autre qu'une anomalie de routine. Ces défauts ne sont pas automatiquement effacés de la file d'attente des pannes. Contactez le support NetApp pour obtenir de l'aide.

- **FailedSpaceTooFull**

  Un service de bloc ne répond pas aux demandes d'écriture de données. Le service de tranche est alors à court d'espace pour stocker les écritures ayant échoué.

  Pour résoudre ce problème, restaurez la fonctionnalité des services de bloc pour permettre aux écritures de continuer normalement et l'espace non disponible pour être vidé du service de tranche.

- **FanSensor**

  Un capteur de ventilateur est défectueux ou est manquant.

  Pour résoudre ce problème, remplacez tout matériel défectueux.

- **FibroChannelAccessDegraded**

  Un nœud Fibre Channel ne répond pas aux autres nœuds du cluster de stockage sur son IP de stockage pendant un certain temps. Dans cet état, le nœud est alors considéré comme ne répond pas et génère une panne du cluster. Vérifiez la connectivité réseau.

- **FibroChannelAccessUnavailable**

  Tous les nœuds Fibre Channel ne répondent pas. Les ID de nœud sont affichés. Vérifiez la connectivité réseau.

- **FielChannelActiveIxL**

  Le nombre iXL Nexus approche la limite prise en charge de 8000 sessions actives par nœud Fibre Channel.

  - La limite des bonnes pratiques est de 5500.
  - La limite d'avertissement est de 7500.
  - La limite maximale (non appliquée) est de 8192. Pour résoudre ce problème, réduire le nombre de commutateurs iXL Nexus en dessous de la limite des meilleures pratiques de 5500.

- **FibroChannelConfig**

  Cette panne du cluster indique l'une des conditions suivantes :

  - Un port Fibre Channel inattendu est installé sur un slot PCI.
  - Il existe un modèle HBA Fibre Channel inattendu.

- Il y a un problème avec le firmware d'un HBA Fibre Channel.
- Un port Fibre Channel n'est pas en ligne.
- Il existe un problème persistant de configuration du mot de passe Fibre Channel. Contactez le support NetApp pour obtenir de l'aide.

- **FibroChannelIOPS**

  Le nombre total d'IOPS atteint la limite d'IOPS pour les nœuds Fibre Channel du cluster. Les limites sont les suivantes :

  - FC0025 : limite de 450 000 IOPS à une taille de bloc de 4 Ko par nœud Fibre Channel.
  - FCN001 : limite d'opérations de 625 000 IOPS à une taille de bloc de 4 Ko par nœud Fibre Channel. Pour résoudre ce problème, équilibrer la charge sur tous les nœuds Fibre Channel disponibles.

- **FibroChannelStaticIxL**

  Le nombre d'iXL Nexus approche la limite prise en charge de 16000 sessions statiques par nœud Fibre Channel.

  - La limite des bonnes pratiques est de 11000.
  - La limite d'avertissement est de 15000.
  - La limite maximale (appliquée) est de 16384. Pour résoudre ce problème, réduire le nombre de commutateurs iXL Nexus en dessous de la limite des meilleures pratiques de 11000.

- **FileSystemCapacityLow**

  L'espace disponible sur l'un des systèmes de fichiers est insuffisant.

  Pour résoudre ce problème, ajoutez de la capacité au système de fichiers.

- **FipsDriveMismatch**

  Un lecteur non FIPS a été physiquement inséré dans un nœud de stockage compatible FIPS ou un lecteur FIPS a été physiquement inséré dans un nœud de stockage non FIPS. Une seule panne est générée par nœud et répertorie tous les disques affectés.

  Pour résoudre ce problème, retirez ou remplacez le ou les lecteurs non-concordants en question.

- **FipsDriveOutOfCompliance**

  Le système a détecté que le chiffrement au repos a été désactivé après l'activation de la fonctionnalité lecteurs FIPS. Cette panne est également générée lorsque la fonctionnalité lecteurs FIPS est activée et qu'un lecteur ou nœud non FIPS est présent dans le cluster de stockage.

  Pour résoudre ce problème, activez le chiffrement au repos ou retirez le matériel non FIPS du cluster de stockage.

- **FipsSelfTestFailure**

  Le sous-système FIPS a détecté une défaillance au cours de l'autotest.

  Contactez le support NetApp pour obtenir de l'aide.

- **HardwareConfigMismatch**

Cette panne du cluster indique l'une des conditions suivantes :

- La configuration ne correspond pas à la définition du nœud.
- La taille de disque de ce type de nœud est incorrecte.
- Un lecteur non pris en charge a été détecté. Une raison possible est que la version de l'élément installé ne reconnaît pas ce lecteur. Il est recommandé de mettre à jour le logiciel Element sur ce nœud.
- Le firmware du disque ne correspond pas.
- L'état compatible du cryptage de disque ne correspond pas au nœud. Contactez le support NetApp pour obtenir de l'aide.

- **IdPCertificateExexpiration**

  Le certificat SSL du fournisseur de services du cluster à utiliser avec un fournisseur d'identités tiers approche de son 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 un délai de 30 jours.
Erreur	Le certificat expire dans un délai de 7 jours.
Primordial	Le certificat expire dans un délai de 3 jours ou a déjà expiré.

  Pour résoudre ce problème, mettez à jour le certificat SSL avant qu'il n'expire. Utilisez la méthode UpdateIdpConfiguration API avec `refreshCertificateExpirationTime=true` Fournir le certificat SSL mis à jour.

- **InConsistenBondmodes**

  Les modes de liaison sur le périphérique VLAN sont manquants. Ce défaut affiche le mode de liaison attendu et le mode de liaison en cours d'utilisation.

- **Inconstant InterfaceConfiguration**

  La configuration de l'interface est incohérente.

  Pour résoudre ce problème, assurez-vous que les interfaces de nœud du cluster de stockage sont configurées de manière cohérente.

- **Inconstant Mtus**

  Cette panne du cluster indique l'une des conditions suivantes :

  - Bond1G non-concordance : des MTUs incohérents ont été détectés sur les interfaces Bond1G.
  - Bond10G : des MTUs incohérents ont été détectés sur les interfaces Bond10G. Cette erreur affiche le ou les nœuds en question ainsi que la valeur MTU associée.

- **InConsistenRoutingRules**

  Les règles de routage pour cette interface sont incohérentes.

- **InConsistenSubnetmasques**

  Le masque de réseau du périphérique VLAN ne correspond pas au masque de réseau enregistré en interne pour le VLAN. Ce défaut affiche le masque de réseau attendu et le masque de réseau actuellement utilisé.

- **IncorrictBondPortCount**

  Le nombre de ports de liaison est incorrect.

- **InvalidConfiguredFibreChannelNodeCount**

  L'une des deux connexions de nœud Fibre Channel attendues est en état de dégradation. Cette erreur s'affiche lorsqu'un seul nœud Fibre Channel est connecté.

  Pour résoudre ce problème, vérifiez la connectivité du réseau et le câblage réseau du cluster, puis recherchez les services défaillants. En l'absence de problèmes de réseau ou de service, contactez le support NetApp pour obtenir un remplacement de nœud Fibre Channel.

- **IrqBalanceed**

  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 (AC) arrive à expiration.

    Pour résoudre ce problème, acquérez un nouveau certificat de l'autorité de certification racine avec une date d'expiration d'au moins 30 jours et utilisez ModityKeyServerKmip pour fournir le certificat d'autorité de certification racine mis à jour.

  - Le certificat client arrive à expiration.

    Pour résoudre ce problème, créez une nouvelle RSC à l'aide de GetClientCertificateSigningRequest, demandez-lui de vous assurer que la nouvelle date d'expiration est au moins 30 jours et utilisez ModityKeyServerKmip pour remplacer le certificat client KMIP arrivant à expiration par le nouveau certificat.

  - Le certificat de l'autorité de certification racine (CA) a expiré.

    Pour résoudre ce problème, acquérez un nouveau certificat de l'autorité de certification racine avec une date d'expiration d'au moins 30 jours et utilisez ModityKeyServerKmip pour fournir le certificat d'autorité de certification racine mis à jour.

  - Le certificat client a expiré.

    Pour résoudre ce problème, créez une nouvelle RSC à l'aide de GetClientCertificateSigningRequest, demandez-lui de vous assurer que la nouvelle date d'expiration est au moins 30 jours et utilisez ModityKeyServerKmip 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, réacquérez le certificat à partir de l'autorité de certification racine. Utilisez ModityKeyServerKmip pour installer le

certificat de client KMIP correct.

- Erreur de certificat client.

  Pour résoudre cette erreur, vérifiez que le certificat client KMIP correct est installé. L'autorité de certification racine du certificat client doit être installée sur le système EKS. Utilisez ModityKeyServerKmip pour installer le certificat de client KMIP correct.

- **KmipServerFault**
  - Échec de la connexion

    Pour résoudre ce problème, vérifiez que le serveur de clés externe est sous tension 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 de client de l'autorité de certification racine et KMIP corrects sont utilisés, et que la clé privée et le certificat du client KMIP correspondent.

  - Erreur du serveur

    Pour résoudre ce problème, vérifiez les détails de l'erreur. Le dépannage du serveur de clés externe peut être nécessaire en fonction de l'erreur renvoyée.

- **MemoryEccThreshold**

Un grand nombre d'erreurs ECC corrigibles ou non corrigibles ont été détectées. Ce défaut utilise les niveaux de gravité suivants en fonction de l'urgence :

Événement	Gravité	Description
Un seul module DIMM cErrorCount atteint cDimmCorrectTableErrWarnThreshold.	Avertissement	Correction des erreurs de mémoire ECC au-dessus du seuil sur DIMM : <processeur> <emplacement DIMM>
Un seul module DIMM cErrorCount reste au-dessus de cDimmCorrectTableErrWarnThreshold jusqu'à ce que cErrorFaultTimer expire pour le module DIMM.	Erreur	Correction des erreurs de mémoire ECC au-dessus du seuil sur DIMM : <processeur> <DIMM>
Un contrôleur de mémoire signale cErrorCount au-dessus de cMemCtlrCorrectTableErrWarnThreshold, et cMemCtlrCorrecttableErrWarnDuration est spécifié.	Avertissement	Erreurs de mémoire ECC corrigibles au-dessus du seuil sur le contrôleur de mémoire : <processeur> <contrôleur de mémoire>

Un contrôleur de mémoire signale cErrorCount au-dessus de cMemCtlrCorrectTableErrWarnThreshold jusqu'à ce que cErrorFaultTimer expire pour le contrôleur de mémoire.	Erreur	Correction des erreurs de mémoire ECC au-dessus du seuil sur DIMM : <processeur> <DIMM>
Un seul module DIMM signale un uErrorCount supérieur à zéro, mais inférieur à cDimmUncorrectTableErraultThreshold.	Avertissement	Erreur(s) de mémoire ECC non réparable(s) détectée(s) sur DIMM : <processeur> <emplacement DIMM>
Un seul module DIMM signale un uErrorCount d'au moins cDimmUncorrectleErraultThreshold.	Erreur	Erreur(s) de mémoire ECC non réparable(s) détectée(s) sur DIMM : <processeur> <emplacement DIMM>
Un contrôleur de mémoire signale un uErrorCount supérieur à zéro, mais inférieur à cMemCtlrUncorrectTableErraultThreshold.	Avertissement	Erreur(s) de mémoire ECC non réparable(s) détectée(s) sur le contrôleur de mémoire : <processeur> <contrôleur de mémoire>
Un contrôleur de mémoire signale un uErrorCount d'au moins cMemCtlrUncorrectleErrultThreshold.	Erreur	Erreur(s) de mémoire ECC non réparable(s) détectée(s) sur le contrôleur de mémoire : <processeur> <contrôleur de mémoire>

Pour résoudre ce problème, contactez le support NetApp pour obtenir de l'aide.

- **MemoryUsageThreshold**

  L'utilisation de la mémoire est supérieure à la normale. Ce défaut utilise les niveaux de gravité suivants en fonction de l'urgence :

  Pour plus d'informations sur le type de défaut, reportez-vous à l'en-tête **Détails** dans le défaut d'erreur.

Gravité	Description
Avertissement	La mémoire système est faible.
Erreur	La mémoire système est très faible.
Primordial	La mémoire système est totalement consommée.

Pour résoudre ce problème, contactez le support NetApp pour obtenir de l'aide.

- **MetadataClusterFull**

  L'espace de stockage des métadonnées est insuffisant pour prendre en charge la perte d'un nœud. Pour plus de détails sur les niveaux de remplissage du cluster, reportez-vous à la méthode GetClusterFullThreshold API. Cette panne du cluster indique l'une des conditions suivantes :

  - Stage3Low (Avertissement) : le seuil défini par l'utilisateur a été franchi. Réglez les paramètres Cluster Full ou ajoutez des nœuds.
  - Stage4Critique (erreur) : l'espace disponible pour la restauration suite à une défaillance d'un nœud est insuffisant. La création de volumes, de snapshots et de clones n'est pas autorisée.
  - Stage5CompletelyConsumied (critique)1 ; aucune écriture ni aucune nouvelle connexion iSCSI ne sont autorisées. Les connexions iSCSI actuelles seront conservées. Les écritures échouent jusqu'à ce que davantage de capacité soit ajoutée au cluster. Supprimez ou supprimez des données ou ajoutez des nœuds. Pour résoudre cette défaillance, purgez ou supprimez des volumes ou ajoutez un autre nœud de stockage au cluster de stockage.
- **MtuCheckFailure**

  Un périphérique réseau n'est pas configuré pour la taille de MTU appropriée.

  Pour résoudre ce problème, assurez-vous que toutes les interfaces réseau et tous les ports de switch sont configurés pour les trames jumbo (MTU jusqu'à 9000 octets).

- **NetworkConfig**

  Cette panne du cluster indique l'une des conditions suivantes :

  - Une interface attendue n'est pas présente.
  - Une interface dupliquée est présente.
  - Une interface configurée est en panne.
  - Un redémarrage du réseau est nécessaire. Contactez le support NetApp pour obtenir de l'aide.
- **NoAvailableVirtualNetworkIPAddresses**

  Aucune adresse de réseau virtuel n'est disponible dans le bloc d'adresses IP.

  - VirtualNetworkID # TAG(#) n'a pas d'adresses IP de stockage disponibles. Impossible d'ajouter des nœuds supplémentaires au cluster. Pour résoudre ce problème, ajoutez d'autres adresses IP au bloc d'adresses réseau virtuelles.
- **NodeHardwareFault (l'interface réseau <nom> est en panne ou le câble est débranché)**

  Une interface réseau est en panne ou le câble est débranché.

  Pour résoudre ce problème, vérifiez la connectivité réseau du ou des nœuds.

- **NodeHardwareFault (l'état de cryptage de disque compatible correspond à l'état de cryptage du nœud compatible pour le lecteur dans le logement <node slot><drive slot>)**

  Un disque ne correspond pas aux capacités de chiffrement avec le nœud de stockage dans lequel il est installé.

- **NodeHardwareFault (<type de disque> taille du disque <taille réelle> pour le lecteur dans le logement <logement de nœud><logement de disque> pour ce type de nœud - taille attendue <taille attendue>)**

Un nœud de stockage contient un disque dont la taille est incorrecte pour ce nœud.

- **NodeHardwareFault (disque non pris en charge détecté dans le logement <logement de nœud><logement de disque> ; les statistiques de disque et les informations d'intégrité seront indisponibles)**

  Un nœud de stockage contient un lecteur qu'il ne prend pas en charge.

- **NodeHardwareFault (le lecteur dans le logement <logement de nœud><logement de lecteur> doit utiliser la version de micrologiciel <version attendue>, mais utilise la version non prise en charge <version réelle>)**

  Un nœud de stockage contient un lecteur exécutant une version de micrologiciel non prise en charge.

- **NodeMaintenance**

  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 de maintenance.
Erreur	Indique que le mode de maintenance n'a pas pu être désactivé, probablement en raison d'un standard actif ou défectueux.

  Pour résoudre cette erreur, désactivez le mode de maintenance une fois la maintenance terminée. Si le problème de niveau d'erreur persiste, contactez le support NetApp pour obtenir de l'aide.

- **NodeOffline**

  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 cette défaillance, utilisez la liaison LACP lors du déploiement de nœuds de stockage. Les clients peuvent rencontrer des problèmes de performances si LACP n'est pas activé et configuré correctement.

- **NtpServerUnreaaccessible**

  Le cluster de stockage ne peut pas communiquer avec le serveur NTP ou les serveurs spécifiés.

  Pour résoudre cette erreur, 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 spécifiée 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 paramètres 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 défaillant ou a échoué. Ce défaut présente les niveaux de gravité suivants :

Gravité	Description
Avertissement	Un avertissement a été détecté par le matériel. Cette condition peut être transitoire, comme un avertissement de température. • NvmLifetimeError • NvmLifetimeStatus • EnergySourceLifetimeStatus • ErgySourceTemperatureStatus • WarningThresholdExcerespecté
Erreur	Une erreur ou un état critique a été détecté par le matériel. Le maître de cluster tente de supprimer le disque de coupe de l'opération (cela génère un événement de suppression de disque). Si les services de tranche secondaire ne sont pas disponibles, le lecteur ne sera pas supprimé. Erreurs renvoyées en plus des erreurs de niveau d'avertissement : • Le point de montage du périphérique NVRAM n'existe pas. • La partition de périphérique NVRAM n'existe pas. • La partition de périphérique NVRAM existe mais n'est pas montée.
Primordial	Une erreur ou un état critique a été détecté par le matériel. Le maître de cluster tente de supprimer le disque de coupe de l'opération (cela génère un événement de suppression de disque). Si les services de tranche secondaire ne sont pas disponibles, le lecteur ne sera pas supprimé. • Persistance • ArmStatusSaveNarmé • CsaveStatusError

Remplacez tout matériel défectueux dans le nœud. Si ce problème ne se résout pas, contactez le support NetApp pour obtenir de l'aide.

- **PowerSupplyError**

  Cette panne du cluster indique l'une des conditions suivantes :

  - Aucune alimentation n'est présente.
  - Un bloc d'alimentation est défectueux.
  - Une entrée d'alimentation est manquante ou hors plage. Pour résoudre ce problème, vérifiez que l'alimentation redondante est fournie à tous les nœuds. Contactez le support NetApp pour obtenir de l'aide.

- **Provisionne uneSpaceTooFull**

  La capacité globale provisionnée du cluster est trop pleine.

  Pour résoudre ce problème, ajoutez de l'espace provisionné ou supprimez et purgez des volumes.

- **RemoteRepAsyncDelayExceeceema**

  Le délai asynchrone configuré pour la réplication a été dépassé. Vérifier la connectivité réseau entre les clusters.

- **RemoteRepClusterFull**

  Les volumes ont mis en pause la réplication distante car le cluster de stockage cible est trop plein.

  Pour résoudre ce problème, libérez de l'espace sur le cluster de stockage cible.

- **RemoteRepSnapshotFull**

  Les volumes ont mis en pause la réplication distante des snapshots car le cluster de stockage cible est trop plein.

  Pour résoudre ce problème, libérez de l'espace sur le cluster de stockage cible.

- **RemoteRepSnapshotsExceededLimit**

  Les volumes ont mis en pause la réplication distante des snapshots car le volume du cluster de stockage cible a dépassé sa limite de snapshots.

  Pour résoudre ce défaut, augmentez la limite snapshot sur le cluster de stockage cible.

- **ScheduleActionError**

  Une ou plusieurs activités planifiées ont été exécutées, mais elles ont échoué.

  Le défaut disparaît si l'activité programmée s'exécute de nouveau et réussit, si l'activité planifiée est supprimée ou si l'activité est interrompue et reprise.

- **Sensorielle ReadingFailed**

  L'auto-test du contrôleur BMC (Baseboard Management Controller) a échoué ou un capteur n'a pas pu communiquer avec le contrôleur 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.

- **SliceServiceTooFull**

  Un service de tranche possède trop peu de capacité provisionnée qui lui est attribuée.

  Pour résoudre cette erreur, ajoutez de la capacité provisionnée.

- **SliceServiceUnHealthy**

  Le système a détecté qu'un service de tranche est défectueux et qu'il est automatiquement mis hors service.

  - Gravité = Avertissement : aucune action n'est entreprise. Ce délai d'avertissement expire dans 6 minutes.
  - Gravité = erreur : le système met automatiquement hors service les données et reréplique ses données sur d'autres lecteurs en bon état. Recherchez des problèmes de connectivité réseau et des erreurs matérielles. Il y aura d'autres défauts si des composants matériels spécifiques sont défectueux. Le défaut s'efface lorsque le service de tranche est accessible ou lorsque le service a été mis hors service.

- **SshEnabled**

  Le service SSH est activé sur un ou plusieurs nœuds du cluster de stockage.

  Pour résoudre cette panne, désactivez le service SSH sur le ou les nœuds appropriés ou contactez le support NetApp pour obtenir de l'aide.

- **SslCertificateExexpiration**

  Le certificat SSL associé à ce nœud arrive 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 un délai de 30 jours.
Erreur	Le certificat expire dans un délai de 7 jours.
Primordial	Le certificat expire dans un délai de 3 jours ou a déjà expiré.

  Pour résoudre ce problème, renouvelez le certificat SSL. Si nécessaire, contactez le support NetApp pour obtenir de l'aide.

- **StrandedCapacity**

  Un seul nœud représente plus de la moitié de la capacité du cluster de stockage.

  Afin de préserver la redondance des données, le système réduit la capacité du nœud le plus grand, de

sorte qu'une partie de sa capacité de bloc soit inutilisée.

Pour résoudre ce problème, ajoutez des disques aux nœuds de stockage existants ou ajoutez des nœuds de stockage au cluster.

- **TempSensor**

  Un capteur de température signale des températures supérieures à la normale. Cette anomalie peut être déclenchée en même temps que les pannes de l'alimentation électrique ou du ventilateur.

  Pour résoudre ce problème, vérifiez qu'il n'y a pas d'obstruction du débit d'air à proximité du cluster de stockage. Si nécessaire, contactez le support NetApp pour obtenir de l'aide.

- **mise à niveau**

  Une mise à niveau 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.

- **Non responsable**

  Un service ne répond plus.

  Contactez le support NetApp pour obtenir de l'aide.

- **VirtualNetworkConfig**

  Cette panne du cluster indique l'une des conditions suivantes :

  - Aucune interface n'est présente.
  - Un namespace incorrect sur une interface.
  - Le masque de réseau est incorrect.
  - L'adresse IP est incorrecte.
  - Une interface n'est pas opérationnelle.
  - Il y a une interface superflue sur un noeud. Contactez le support NetApp pour obtenir de l'aide.

- **VolumesDegded**

  Les volumes secondaires n'ont pas terminé la réplication et la synchronisation. Le message est effacé lorsque la synchronisation est terminée.

- **VolumesOffline**

  Un ou plusieurs volumes du cluster de stockage sont hors ligne. La panne **Volume Degraded** est également présente.

  Contactez le support NetApp pour obtenir de l'aide.

Afficher l'activité sur les performances du nœud

Vous pouvez afficher les activités de performances de chaque nœud au format graphique. Ces informations fournissent des statistiques en temps réel pour les

opérations d'E/S de lecture/écriture par seconde (IOPS) et pour chaque lecteur du nœud. Le graphique d'utilisation est mis à jour toutes les cinq secondes et le graphique des statistiques sur les lecteurs est mis à jour toutes les dix secondes.

1. Cliquez sur **Cluster** > **Nodes**.
2. Cliquez sur **actions** pour le noeud que vous souhaitez afficher.
3. Cliquez sur **Afficher les détails**.

> Vous pouvez voir des points spécifiques dans le temps sur la ligne et les graphiques à barres en positionnant le curseur sur la ligne ou la barre.

Afficher les performances des volumes

Vous pouvez afficher des informations détaillées de performances pour tous les volumes du cluster. Vous pouvez trier les informations par ID de volume ou par colonne de performance. Vous pouvez également filtrer les informations en fonction de certains critères.

Vous pouvez modifier la fréquence à laquelle le système actualise les informations de performances sur la page en cliquant sur la liste **Actualiser chaque** et en choisissant une valeur différente. L'intervalle d'actualisation par défaut est de 10 secondes si le cluster possède moins de 1000 volumes ; sinon, la valeur par défaut est de 60 secondes. Si vous choisissez une 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 de l'élément, sélectionnez **Reporting** > **Volume Performance**.
2. Dans la liste de volumes, cliquez sur l'icône actions d'un volume.
3. Cliquez sur **Afficher les détails**.

   Un bac s'affiche en bas de la page contenant des informations générales sur le volume.

4. Pour plus d'informations sur le volume, cliquez sur **Voir plus de détails**.

   Le système affiche des informations détaillées ainsi que les graphiques de performance du volume.

Trouvez plus d'informations

Détails des performances des volumes

Détails des performances des volumes

Vous pouvez afficher les statistiques de performance des volumes à partir de la page Volume Performance de l'onglet Reporting dans l'interface utilisateur Element.

La liste suivante décrit les détails qui vous sont disponibles :

- **ID**

  ID généré par le système pour le volume.

- **Nom**

  Nom donné au volume lors de sa création.

- **Compte**

  Nom du compte attribué au volume.

- **Groupes d'accès**

  Nom du ou des groupes d'accès de volume auxquels appartient le volume.

- **Utilisation du volume**

  Valeur de pourcentage décrivant la quantité d'utilisation du volume par le client.

  Valeurs possibles :

  - 0 = le client n'utilise pas le volume
  - 100 = le client utilise le max
  - Pour 100 = le client utilise la rafale

- **IOPS totales**

  Le nombre total d'IOPS (lecture et écriture) actuellement exécuté sur le volume.

- **Lecture d'IOPS**

  Nombre total d'IOPS de lecture en cours d'exécution sur le volume.

- **IOPS d'écriture**

  Nombre total d'IOPS d'écriture actuellement exécutées sur le volume.

- **Débit total**

  Débit total (lecture et écriture) actuellement exécuté sur le volume.

- **Débit de lecture**

  Quantité totale du débit de lecture actuellement exécuté sur le volume.

- **Débit d'écriture**

  Quantité totale du débit d'écriture actuellement exécuté sur le volume.

- * Latence totale*

  Temps moyen, en microsecondes, pour effectuer les opérations de lecture et d'écriture sur un volume.

- * Latence de lecture*

  Temps moyen, en microsecondes, pour mener à bien les opérations de lecture vers le volume au cours des 500 dernières millisecondes.

- **Latence d'écriture**

  Temps moyen, en microsecondes, pour traiter les opérations d'écriture sur un volume au cours des 500 dernières millisecondes.

- **Profondeur de file d'attente**

  Nombre d'opérations de lecture et d'écriture en attente dans le volume.

- **Taille d'E/S moyenne**

  Taille moyenne en octets des E/S récentes au volume au cours des 500 dernières millisecondes.

Afficher les sessions iSCSI

Vous pouvez afficher les sessions iSCSI connectées au cluster. Vous pouvez filtrer les informations pour n'inclure que les sessions souhaitées.

1. Dans l'interface utilisateur de l'élément, sélectionnez **Rapport** > **sessions iSCSI**.
2. Pour afficher les champs des critères de filtre, cliquez sur **Filter**.

Trouvez plus d'informations

Détails de la session iSCSI

Détails de la session iSCSI

Vous pouvez afficher des informations concernant les sessions iSCSI connectées au cluster.

La liste suivante décrit les informations que vous trouverez sur les sessions iSCSI :

- **Nœud**

  Nœud hébergeant la partition de métadonnées primaire du volume.

- **Compte**

  Nom du compte qui détient le volume. Si la valeur est vide, un tiret (-) s'affiche.

- **Volume**

  Nom du volume identifié sur le nœud.

- **ID de volume**

  ID du volume associé à l'IQN cible.

- **ID initiateur**

  ID généré par le système pour l'initiateur.

- **Alias initiateur**

Nom facultatif de l'initiateur qui permet de trouver plus facilement l'initiateur lorsque cette liste est longue.

- **IP de l'Initator**

  Adresse IP du noeud final qui initie la session.

- **IQN de l'initiateur**

  IQN du noeud final qui initie la session.

- **IP cible**

  Adresse IP du nœud hébergeant le volume.

- **IQN cible**

  L'IQN du volume.

- **Créé le**

  Date à laquelle la session a été établie.

Afficher les sessions Fibre Channel

Vous pouvez afficher les sessions Fibre Channel (FC) connectées au cluster. Vous pouvez filtrer les informations pour n'inclure que les connexions que vous souhaitez afficher dans la fenêtre.

1. Dans l'interface utilisateur de l'élément, sélectionnez **Rapport** > **sessions FC**.
2. Pour afficher les champs des critères de filtre, cliquez sur **Filter**.

Trouvez plus d'informations

Détails de la session Fibre Channel

Détails de la session Fibre Channel

Vous pouvez trouver des informations concernant les sessions Fibre Channel (FC) actives connectées au cluster.

La liste suivante décrit les informations que vous pouvez trouver à propos des sessions FC connectées au cluster :

- **ID de nœud**

  Nœud hébergeant la session pour la connexion.

- **Nom du noeud**

  Nom de nœud généré par le système.

- **ID initiateur**

ID généré par le système pour l'initiateur.

- **WWPN initiateur**

  Le nom du port mondial de lancement.

- **Alias initiateur**

  Nom facultatif de l'initiateur qui permet de trouver plus facilement l'initiateur lorsque cette liste est longue.

- **WWPN cible**

  Nom du port cible dans le monde entier.

- **Groupe d'accès au volume**

  Nom du groupe d'accès au volume auquel appartient la session.

- **ID de groupe d'accès de volume**

  ID généré par le système pour le groupe d'accès.

Résoudre les problèmes liés aux disques

Vous pouvez remplacer un disque SSD défectueux. Le remplacement à chaud des disques SSD pour les nœuds de stockage SolidFire. Si vous pensez qu'un disque SSD est défaillant, contactez le support NetApp pour vérifier la défaillance et suivez la procédure de résolution adéquate. Le support NetApp travaille également avec vous pour obtenir un disque de remplacement conformément à votre contrat de niveau de service.

Le mode de remplacement dans ce cas vous permet de supprimer un disque défectueux d'un nœud actif et de le remplacer par un nouveau disque SSD de NetApp. Il n'est pas recommandé de supprimer les disques non défectueux sur un cluster actif.

Vous devez conserver des pièces de rechange sur site suggérées par le support NetApp pour permettre un remplacement immédiat du disque en cas de panne.

> À des fins de test, si vous simulez une panne de disque en tirant un disque d'un nœud, vous devez attendre 30 secondes avant de réinsérer le disque dans le slot.

En cas de panne d'un disque, Double Helix redistribue les données du disque vers les nœuds restants sur le cluster. En effet, plusieurs pannes de disque sur le même nœud ne sont pas un problème, car le logiciel Element protège contre deux copies de données résidant sur le même nœud. Une défaillance de disque se traduit par les événements suivants :

- Migration des données hors du disque.
- La capacité globale du cluster est réduite par la capacité du disque.
- La protection des données par double Helix assure que deux copies des données sont valides.

> Les systèmes de stockage SolidFire ne prennent pas en charge la suppression d'un disque si la migration des données entraîne une quantité insuffisante de stockage.

Pour en savoir plus

- Retirer les disques défectueux du cluster
- Dépannage de base du lecteur MDSS
- Retirez les lecteurs MDSS
- "Remplacement des disques des nœuds de stockage SolidFire"
- "Remplacement des disques pour les nœuds de stockage de la gamme H600S"
- "Informations sur le matériel H410S et H610S"
- "Informations sur le matériel SF-Series"

Retirer les disques défectueux du cluster

Le système SolidFire met un disque en panne si l'auto-diagnostic du disque indique au nœud qu'il est en panne ou si la communication avec le disque s'arrête pendant cinq minutes et demie au moins. Le système affiche la liste des disques défectueux. Vous devez supprimer un disque défectueux de la liste des disques défaillants du logiciel NetApp Element.

Les lecteurs de la liste **Alerts** s'affichent sous la forme **blockServiceUnHealthy** lorsqu'un nœud est hors ligne. Lors du redémarrage du nœud, si le nœud et ses disques sont de nouveau en ligne en cinq minutes et demi, les disques se mettent automatiquement à jour et continuent de jouer le rôle de disques actifs dans le cluster.

1. Dans l'interface utilisateur de l'élément, sélectionnez **Cluster** > **Drives**.
2. Cliquez sur **FAILED** pour afficher la liste des disques défectueux.
3. Notez le numéro de slot du disque défaillant.

   Vous avez besoin de ces informations pour localiser le lecteur défectueux dans le châssis.

4. Retirez les disques défectueux à l'aide de l'une des méthodes suivantes :

Option	Étapes
Pour supprimer des lecteurs individuels	a. Cliquez sur **actions** pour le lecteur que vous souhaitez supprimer. b. Cliquez sur **Supprimer**.
Pour supprimer plusieurs lecteurs	a. Sélectionnez tous les lecteurs que vous souhaitez supprimer, puis cliquez sur **actions groupées**. b. Cliquez sur **Supprimer**.

Dépannage de base du lecteur MDSS

Vous pouvez récupérer des disques de métadonnées (ou de tranche) en les ajoutant au cluster en cas de panne d'un ou des deux disques de métadonnées. Vous pouvez effectuer l'opération de récupération dans l'interface utilisateur NetApp Element si la

fonction MDSS est déjà activée sur le nœud.

En cas de défaillance de l'un des disques de métadonnées ou des deux disques d'un nœud, le service de tranche s'arrête et les données des deux disques sont sauvegardées sur différents disques du nœud.

Les scénarios suivants présentent les scénarios de défaillance possibles et fournissent des recommandations de base pour corriger le problème :

Le disque de coupe du système est défaillant

- Dans ce scénario, l'emplacement 2 est vérifié et renvoyé à un état disponible.
- Le lecteur de tranche système doit être rempli à nouveau avant que le service de tranche puisse être remis en ligne.
- Vous devez remplacer le lecteur de tranche système, lorsque le lecteur de tranche système devient disponible, ajoutez le lecteur et le lecteur de logement 2 en même temps.

> Vous ne pouvez pas ajouter le lecteur dans l'emplacement 2 en tant que lecteur de métadonnées. Vous devez ajouter les deux disques simultanément au nœud.

Le slot 2 est défaillant

- Dans ce scénario, le lecteur de tranche système est vérifié et renvoyé à un état disponible.
- Vous devez remplacer le logement 2 par un logement de rechange, lorsque le logement 2 devient disponible, ajoutez simultanément le lecteur de tranche système et le lecteur de logement 2.

Le lecteur de tranche système et le logement 2 sont défectueux

- Vous devez remplacer le lecteur de tranche système et le logement 2 par un lecteur de rechange. Lorsque les deux lecteurs deviennent disponibles, ajoutez simultanément le lecteur de tranche système et le lecteur de logement 2.

Ordre des opérations

- Remplacez le lecteur matériel défectueux par un lecteur de rechange (remplacez les deux disques en cas de défaillance des deux disques).
- Ajoutez des disques au cluster une fois qu'ils ont été reremplis et qu'ils sont disponibles.

Vérifiez les opérations

- Vérifiez que les lecteurs du logement 0 (ou interne) et du logement 2 sont identifiés comme des lecteurs de métadonnées dans la liste lecteurs actifs.
- Vérifiez que l'équilibrage des coupes est terminé (il n'y a plus de messages de tranches mobiles dans le journal des événements pendant au moins 30 minutes).

Pour en savoir plus

Ajouter des lecteurs MDSS

Ajouter des lecteurs MDSS

Vous pouvez ajouter un second lecteur de métadonnées sur un nœud SolidFire en convertissant le lecteur de blocs dans l'emplacement 2 en un lecteur de tranche. Pour ce

faire, activez la fonction MDSS (Multi-Drive Slice Service). Pour activer cette fonctionnalité, contactez le support NetApp.

L'obtention d'un lecteur de tranche dans un état disponible peut nécessiter le remplacement d'un lecteur défectueux par un nouveau lecteur ou un lecteur de rechange. Vous devez ajouter le lecteur de tranche système en même temps que vous ajoutez le lecteur pour le logement 2. Si vous essayez d'ajouter le lecteur de tranche de slot 2 seul ou avant d'ajouter le lecteur de tranche système, le système génère une erreur.

1. Cliquez sur **Cluster** > **Drives**.
2. Cliquez sur **disponible** pour afficher la liste des lecteurs disponibles.
3. Sélectionnez les lecteurs de tranche à ajouter.
4. Cliquez sur **actions groupées**.
5. Cliquez sur **Ajouter**.
6. Confirmez à partir de l'onglet **disques actifs** que les lecteurs ont été ajoutés.

Retirez les lecteurs MDSS

Vous pouvez supprimer les lecteurs MDSS (Multi-Drive Slice Service). Cette procédure s'applique uniquement si le nœud possède plusieurs unités de coupe.

> Si le lecteur de tranche du système et le lecteur de logement 2 tombent en panne, le système arrête les services de tranche et supprime les lecteurs. En l'absence de panne et si vous retirez les lecteurs, les deux lecteurs doivent être retirés en même temps.

1. Cliquez sur **Cluster** > **Drives**.
2. Dans l'onglet **lecteurs disponibles**, cochez la case correspondant aux lecteurs de tranche en cours de retrait.
3. Cliquez sur **actions groupées**.
4. Cliquez sur **Supprimer**.
5. Confirmez l'action.

Résoudre les problèmes

Vous pouvez supprimer des nœuds d'un cluster à des fins de maintenance ou de remplacement. Vous devez utiliser l'interface ou l'API NetApp Element pour supprimer les nœuds avant de les mettre hors ligne.

La procédure à suivre pour supprimer les nœuds de stockage est la suivante :

- Assurez-vous que la capacité du cluster est suffisante pour créer une copie des données sur le nœud.
- Supprimez des disques du cluster à l'aide de l'interface utilisateur ou de la méthode API RemoveDrives.

  Ainsi, le système est-il en mesure de migrer les données des disques du nœud vers d'autres disques du cluster. Le temps nécessaire à ce processus dépend de la quantité de données à migrer.

- Ne supprime pas du cluster le nœud.

Avant de mettre un nœud hors tension ou sous tension, gardez les points suivants à l'esprit :

- La mise hors tension des nœuds et des clusters comporte des risques s'ils ne sont pas correctement effectués.

  Mettre un nœud hors tension doit s'effectuer sous la direction du support NetApp.

- Si un nœud a été arrêté plus de 5.5 minutes sous n'importe quel type de condition d'arrêt, la protection des données Double Helix débute la tâche d'écrire des blocs répliqués sur un autre nœud afin de répliquer les données. Dans ce cas, contactez le support NetApp pour obtenir de l'aide sur l'analyse du nœud défaillant.
- Pour redémarrer ou mettre un nœud hors tension en toute sécurité, vous pouvez utiliser la commande Shutdown API.
- Si un nœud est en panne ou hors ligne, vous devez contacter le support NetApp avant de le remettre en ligne.
- Une fois qu'un nœud est remis en ligne, vous devez réintégrer les disques dans le cluster, selon sa durée de mise hors service.

Pour en savoir plus

"Remplacement d'un châssis SolidFire défectueux"

"Remplacement d'un nœud de la série H600S défectueux"

Mettez un cluster hors tension

Pour mettre l'ensemble du cluster hors tension, effectuez la procédure suivante.

Étapes

1. (Facultatif) Contactez le support NetApp pour obtenir de l'aide concernant la réalisation des étapes préliminaires.
2. Vérifiez que toutes les E/S sont arrêtées.
3. Déconnecter toutes les sessions iSCSI :
   a. Accédez à l'adresse IP virtuelle de gestion (MVIP) du cluster pour ouvrir l'interface utilisateur Element.
   b. Notez les nœuds répertoriés dans la liste nœuds.
   c. Exécutez la méthode de l'API Shutdown avec l'option halt spécifiée sur chaque ID de noeud 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 critiques et `volumesOffline` les défaillances de cluster ont été résolues.
> 2. Attendez 10 à 15 minutes que le cluster se stabilise.
> 3. Commencez à amener les hôtes pour accéder aux données.
>
> Si vous souhaitez consacrer plus de temps à la mise sous tension des nœuds et à la vérification de leur bon fonctionnement après la maintenance, contactez le support technique pour obtenir de l'aide afin de retarder la synchronisation des données et d'éviter une synchronisation inutile des bacs.

Trouvez plus d'informations

"Comment mettre hors tension et hors tension en toute simplicité un cluster de stockage NetApp SolidFire/HCI"

Utilisation d'utilitaires par nœud pour les nœuds de stockage

Vous pouvez utiliser les utilitaires par nœud pour résoudre des problèmes réseau si les outils de surveillance standard de l'interface utilisateur du logiciel NetApp Element ne fournissent pas suffisamment d'informations pour la résolution de problèmes. Les utilitaires par nœud fournissent des informations et des outils spécifiques qui vous aident à résoudre des problèmes de réseau entre les nœuds ou avec le nœud de gestion.

Trouvez plus d'informations

- Accès aux paramètres par nœud à l'aide de l'interface utilisateur par nœud
- Détails des paramètres réseau à partir de l'interface utilisateur par nœud
- Détails des paramètres de cluster depuis l'interface de chaque nœud
- Exécutez les tests système à l'aide de l'interface utilisateur par nœud
- Exécutez les utilitaires système à l'aide de l'interface utilisateur par nœud

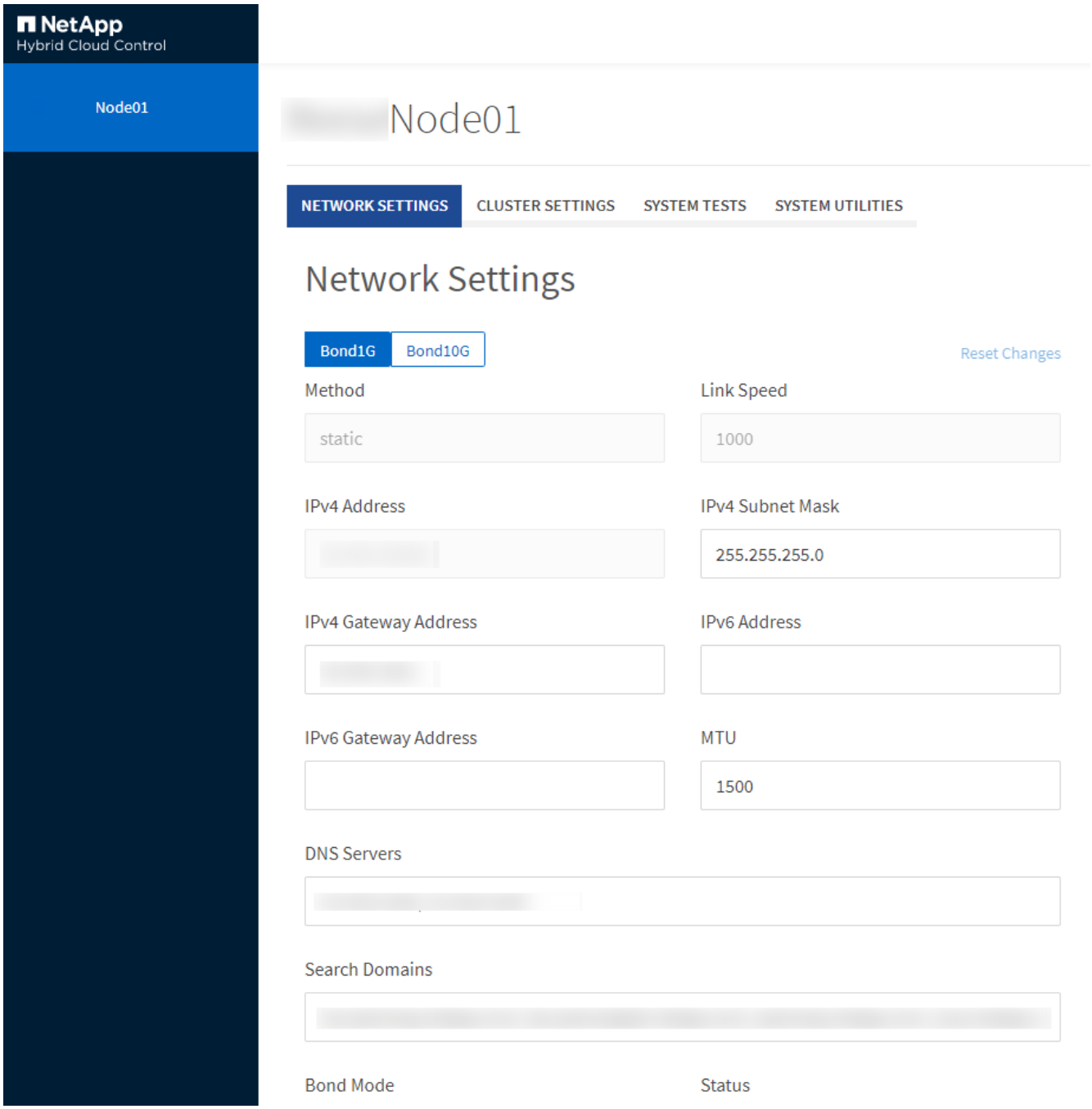
Accès aux paramètres par nœud à l'aide de l'interface utilisateur par nœud

Vous pouvez accéder aux paramètres réseau, aux paramètres de cluster, aux tests et aux utilitaires système dans l'interface utilisateur par nœud après avoir saisi l'adresse IP du nœud de gestion et vous authentifier.

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 de cluster.

Vous devez configurer ou modifier un nœud à la fois. Assurez-vous que les paramètres réseau spécifiés ont l'effet attendu et que le réseau est stable et fonctionne bien avant d'apporter des modifications à un autre nœud.

1. Ouvrez l'interface utilisateur par nœud à l'aide de l'une des méthodes suivantes :
   - Entrez l'adresse IP de gestion suivie de :442 dans une fenêtre de navigateur et connectez-vous à l'aide d'un nom d'utilisateur et d'un mot de passe admin.
   - Dans l'interface utilisateur de l'élément, sélectionnez **Cluster** > **Nodes**, puis cliquez sur le lien de l'adresse IP de gestion correspondant au 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 à partir de l'interface utilisateur par nœud

Vous pouvez modifier les paramètres réseau du nœud de stockage pour donner au nœud un nouvel ensemble d'attributs réseau.

Vous pouvez voir les paramètres réseau d'un noeud de stockage sur la page **Paramètres réseau** lorsque vous vous connectez au noeud (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**

  Méthode utilisée pour configurer l'interface. Méthodes possibles :

- Bouclage : permet de définir l'interface de bouclage IPv4.
- Manual : permet de définir les interfaces pour lesquelles aucune configuration n'est effectuée par défaut.
- dhcp : permet d'obtenir une adresse IP via DHCP.
- Statique : permet de définir des interfaces Ethernet avec des adresses IPv4 allouées de manière statique.

- **Vitesse de liaison**

  Vitesse négociée par la carte réseau virtuelle.

- **Adresse IPv4**

  Adresse IPv4 du réseau eth0.

- **Masque de sous-réseau IPv4**

  Subdivisions d'adresse du réseau IPv4.

- **Adresse de passerelle IPv4**

  Adresse réseau du routeur pour envoyer des paquets hors du réseau local.

- **Adresse IPv6**

  Adresse IPv6 du réseau eth0.

- **Adresse de passerelle IPv6**

  Adresse réseau du routeur pour envoyer des paquets hors du réseau local.

- **MTU**

  La plus grande taille de paquet 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 9000.

- **Serveurs DNS**

  Interface réseau utilisée pour la communication avec le cluster.

- **Domaines de recherche**

  Recherchez les adresses MAC supplémentaires disponibles pour le système.

- **Mode bond**

  Peut être l'un des modes suivants :

  - Activepassive (par défaut)
  - ALB
  - LACP

- **Statut**

  Valeurs possibles :

- UpAndRunning
- Vers le bas
- Haut

- **Numéro de réseau virtuel**

  Balise attribuée lors de la création du réseau virtuel.

- **Routes**

  Routes statiques vers des hôtes ou des réseaux spécifiques via l'interface associée que les routes sont configurées pour utiliser.

Détails des paramètres de cluster depuis l'interface de chaque nœud

Vous pouvez vérifier les paramètres du cluster d'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 d'un nœud de stockage indiqué dans la page **Paramètres de cluster** de l'interface utilisateur par nœud (https://<node IP>:442/hcc/node/cluster-settings).

- **Rôle**

  Rôle qui lui est attribué dans le cluster. Valeurs possibles :

  - Stockage : nœud de stockage ou Fibre Channel.
  - Gestion : nœud est un nœud de gestion.

- **Nom d'hôte**

  Nom du nœud.

- **Cluster**

  Nom du cluster.

- * Adhésion au groupe*

  État du nœud. Valeurs possibles :

  - Disponible : le nœud ne possède 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.
  - PendingActive : le système est en cours d'installation de logiciels compatibles sur le nœud. Une fois l'opération terminée, le nœud passe à l'état actif.
  - Actif : le nœud participe à un cluster. Une authentification est requise pour modifier le nœud.

- **Version**

  Version du logiciel Element exécutée sur le nœud.

- **Ensemble**

Nœuds faisant partie de l'ensemble de base de données.

- **ID de nœud**

  ID attribué lorsqu'un nœud est ajouté au cluster.

- **Interface de cluster**

  Interface réseau utilisée pour la communication avec le cluster.

- **Interface de gestion**

  Interface de réseau de gestion. Par défaut, il s'agit de Bond1G, mais peut également utiliser Bond10G.

- **Interface de stockage**

  Interface de réseau de stockage utilisant Bond10G.

- **Prise en charge du cryptage**

  Indique si le nœud prend en charge le chiffrement de disque.

Exécutez les tests système à l'aide de l'interface utilisateur par nœud

Vous pouvez tester les modifications apportées aux paramètres réseau après les avoir configurées sur le réseau. Vous pouvez exécuter les tests pour vous assurer que le nœud de stockage est stable et que celui-ci peut être mis en ligne sans aucun problème.

Vous avez ouvert une session sur l'interface utilisateur par nœud pour le nœud de stockage.

1. Cliquez sur **tests système**.
2. Cliquez sur **Exécuter le test** en regard du test à exécuter ou sélectionnez **Exécuter tous les tests**.

   L'exécution de toutes les opérations de test peut prendre du temps et doit être effectuée uniquement selon les directives du support NetApp.

   - **Test ensemble connecté**

     Teste et vérifie la connectivité à un ensemble de base 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**

     Envoie un ping à l'adresse MVIP (Management Virtual IP) spécifiée, puis exécute un appel d'API simple vers le MVIP pour vérifier la connectivité. Par défaut, le test utilise le MVIP pour le cluster auquel le nœud est associé.

   - **Test connexion Svip**

     Ping adresse IP virtuelle de stockage (SVIP) spécifiée à l'aide de paquets ICMP (Internet Control message Protocol) qui correspondent à la taille MTU (maximum transmission Unit) définie sur la carte réseau. Il se connecte ensuite au SVIP en tant qu'initiateur iSCSI. Par défaut, le test utilise le SVIP

pour le cluster auquel le nœud est associé.

- **Tester la configuration matérielle**

  Vérifie que toutes les configurations matérielles sont correctes, valide les versions de firmware correctes et vérifie que tous les disques sont installés et fonctionnent correctement. Ceci est le même que les tests d'usine.

  > Ce test consomme beaucoup de ressources et doit être exécuté uniquement sur demande du support NetApp.

- **Tester la connectivité locale**

  Teste la connectivité à tous les autres nœuds du cluster en envoyant une commande ping à l'adresse IP (CIP) du cluster sur chaque nœud. Ce test s'affiche uniquement sur un nœud si ce dernier fait partie d'un cluster actif.

- **Tester le cluster de localisation**

  Confirme que le nœud peut localiser le cluster spécifié dans la configuration du cluster

- **Tester la 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 défaillances matérielles lorsqu'un nœud participe activement à un cluster.

- **Test Ping**

  Ping une liste d'hôtes spécifiée ou, si aucun n'est spécifié, génère dynamiquement une liste de tous les nœuds enregistrés dans le cluster et envoie des commandes ping à chacun pour une connectivité simple.

- **Tester la connectivité distante**

  Teste la connectivité sur tous les nœuds des clusters couplés à distance en envoyant une requête ping à l'adresse IP du cluster (CIP) sur chaque nœud. Ce test s'affiche uniquement sur un nœud si ce dernier 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 de stockage pour créer ou supprimer des bundles de support, réinitialiser les paramètres de configuration des disques et redémarrer les services réseau ou de cluster.

Vous avez ouvert une session sur l'interface utilisateur par nœud pour le nœud de stockage.

1. Cliquez sur **Utilitaires système**.
2. Cliquez sur le bouton de l'utilitaire système que vous souhaitez exécuter.
   - **Puissance de contrôle**

     Redémarre ou arrête le nœud.

Cette opération entraîne une perte temporaire de la connectivité réseau.

Spécifiez les paramètres suivants :

- Action : les options incluent redémarrage et arrêt (arrêt).
- Délai d'activation : tout délai supplémentaire avant la remise en ligne du nœud.

◦ **Recueillir les journaux de noeud**

Crée un bundle de support sous le répertoire /tmp/bundles du nœud.

Spécifiez les paramètres suivants :

- Nom du bundle : nom unique pour chaque bundle de support créé. Si aucun nom n'est fourni, « supportbundle » et le nom du nœud sont utilisés comme nom de fichier.
- Args supplémentaires : ce paramètre est envoyé au script sf_marque_support_bundle. Ce paramètre doit être utilisé uniquement à la demande du support NetApp.
- Timeout sec : spécifiez le nombre de secondes d'attente pour chaque réponse ping individuelle.

◦ **Supprimer les journaux de nœud**

Supprime tous les packs de support en cours sur le nœud créés à l'aide de la méthode de création de bundle de support de cluster* ou de l'API CreateSupportBundle.

◦ **Réinitialiser les lecteurs**

Initialise les lecteurs et supprime toutes les données qui se trouvent actuellement sur le lecteur. 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 transmission) à réinitialiser.

◦ **Réinitialiser la configuration réseau**

Permet de résoudre les problèmes de configuration réseau d'un nœud individuel et de rétablir les paramètres d'usine par défaut d'un nœud individuel.

◦ **Réinitialiser le noeud**

Réinitialise les paramètres d'usine d'un nœud. Toutes les données sont supprimées, mais les paramètres réseau du nœud sont conservés pendant cette opération. Les nœuds ne peuvent être réinitialisés que s'ils sont non assignés à un cluster et sont en état disponible.

Toutes les données, les packages (mises à niveau logicielles), les configurations et les fichiers journaux sont supprimés du nœud lorsque vous utilisez cette option.

◦ **Redémarrer le réseau**

Redémarre tous les services réseau sur un nœud.

Cette opération peut entraîner une perte temporaire de la connectivité réseau.

◦ **Redémarrer les services**

Redémarre les services logiciels Element sur un nœud.

> Cette opération peut entraîner une interruption temporaire du service des nœuds. Vous devez effectuer cette opération uniquement selon la direction du support NetApp.

Spécifiez les paramètres suivants :

- Service : nom du service à redémarrer.
- Action : action à effectuer sur le service. Les options possibles sont le démarrage, l'arrêt et le redémarrage.

Travaillez avec le nœud de gestion

Vous pouvez utiliser le nœud de gestion (nœud M) pour mettre à niveau les services du système, gérer les ressources et les paramètres du cluster, exécuter des tests et des utilitaires système, configurer Active IQ pour le contrôle du système et activer l'accès au support NetApp pour le dépannage.

> Il est recommandé d'associer un seul nœud de gestion à une instance VMware vCenter et d'éviter de définir les mêmes ressources de stockage et de calcul ou instances vCenter dans plusieurs nœuds de gestion.

Voir "documentation sur le nœud de gestion" pour en savoir plus.

Comprendre les niveaux de remplissage du cluster

Le cluster exécutant le logiciel Element génère des défaillances de cluster pour avertir l'administrateur du stockage lorsque le cluster manque de capacité. Il existe trois niveaux de remplissage du cluster, qui sont tous affichés dans l'interface utilisateur NetApp Element : avertissement, erreur et critique.

Le système utilise le code d'erreur BlockClusterFull pour avertir de la plénitude du stockage du bloc de cluster. Vous pouvez afficher les niveaux de sévérité de la plénitude du cluster depuis l'onglet alertes de l'interface utilisateur Element.

La liste suivante contient des informations sur les niveaux de sévérité des blocs complets :

- **Avertissement**

  Il s'agit d'un avertissement configurable par le client qui s'affiche lorsque la capacité en mode bloc du cluster approche du niveau de gravité de l'erreur. Par défaut, ce niveau est défini à trois pour cent sous le niveau d'erreur et peut être réglé via l'interface utilisateur et l'API de l'élément. Vous devez ajouter de la capacité ou libérer de la capacité dès que possible.

- **Erreur**

  Lorsque le cluster est défini sur cet état, en cas de perte d'un nœud, la capacité du cluster ne sera pas suffisante pour reconstruire la protection des données Double Helix. La création de volumes, les clones et les instantanés sont tous bloqués pendant que le cluster est à cet état. Cet état n'est pas sûr ou recommandé pour tout cluster. Vous devez ajouter de la capacité ou libérer immédiatement de la capacité.

- **Critique**

  Cette erreur critique s'est produite, car le cluster est à 100 % consommé. Elle est en lecture seule et aucune nouvelle connexion iSCSI ne peut être établie au cluster. Dès que vous aurez atteint ce stade, vous devrez libérer ou ajouter immédiatement de la capacité.

Le système utilise le code d'erreur MetadaClusterFull pour avertir de la plénitude du stockage des métadonnées du cluster. Vous pouvez afficher la plénitude du stockage des métadonnées du cluster à partir de la section capacité du cluster sur la page Présentation de l'onglet Rapports de l'interface utilisateur Element.

La liste ci-dessous contient des informations sur les niveaux de sévérité de MetadataClusterFull :

- **Avertissement**

  Il s'agit d'un avertissement configurable par le client qui s'affiche lorsque la capacité de métadonnée du cluster approche du niveau de gravité de l'erreur. Par défaut, ce niveau est défini à trois pour cent sous le niveau d'erreur et peut être réglé via l'API d'élément. Vous devez ajouter de la capacité ou libérer de la capacité dès que possible.

- **Erreur**

  Lorsque le cluster est défini sur cet état, en cas de perte d'un nœud, la capacité du cluster ne sera pas suffisante pour reconstruire la protection des données Double Helix. La création de volumes, les clones et les instantanés sont tous bloqués pendant que le cluster est à cet état. Cet état n'est pas sûr ou recommandé pour tout cluster. Vous devez ajouter de la capacité ou libérer immédiatement de la capacité.

- **Critique**

  Cette erreur critique s'est produite, car le cluster est à 100 % consommé. Elle est en lecture seule et aucune nouvelle connexion iSCSI ne peut être établie au cluster. Dès que vous aurez atteint ce stade, vous devrez libérer ou ajouter immédiatement de la capacité.

Les seuils suivants s'appliquent aux clusters à deux nœuds :

- L'erreur de remplissage des métadonnées est inférieure à 20 % du niveau critique.
- L'erreur de remplissage du bloc est de 1 disque de bloc (dont la capacité inutilisée) en dessous du niveau critique ; cela signifie que deux disques de bloc valent de la capacité en dessous du niveau critique.