Concepts

Element Software

NetApp
October 01, 2024

Sommaire

Concepts

Découvrez les concepts de base du logiciel Element.

- "Présentation du produit"
- Présentation de l'architecture de SolidFire
- Nœuds
- Clusters
- "Sécurité"
- Comptes et autorisations
- "Volumes"
- Protection des données
- La performance et la qualité de service

Trouvez plus d'informations

- "Présentation du stockage 100 % Flash de SolidFire"
- "Documentation SolidFire et Element"

Présentation du produit

Un système de stockage 100 % Flash SolidFire comprend des composants matériels distincts (disques et nœuds) regroupés dans un seul pool de ressources de stockage. Ce cluster unifié présente comme un système de stockage unique utilisable par des clients externes, et est géré à l'aide du logiciel NetApp Element.

Grâce à l'interface Element, aux API ou à d'autres outils de gestion, vous pouvez surveiller la capacité et les performances de stockage du cluster SolidFire et gérer les activités de stockage sur une infrastructure mutualisée.

Fonctionnalités SolidFire

Le système SolidFire offre les fonctionnalités suivantes :

- Offre un stockage haute performance pour votre infrastructure de cloud privé à grande échelle
- Une évolutivité flexible qui permet de répondre à l'évolution des besoins en stockage
- Utilise une interface logicielle de gestion du stockage Element basée sur des API
- Garantit les performances à l'aide des règles de qualité de service
- Équilibrage automatique de la charge sur l'ensemble des nœuds du cluster inclus
- Rééquilibrage automatique des clusters lors de l'ajout ou de la suppression de nœuds

Déploiement SolidFire

Nœuds de stockage fournis par NetApp et intégrés au logiciel NetApp Element

"Présentation de l’architecture de stockage 100 % Flash de SolidFire"

Trouvez plus d’informations

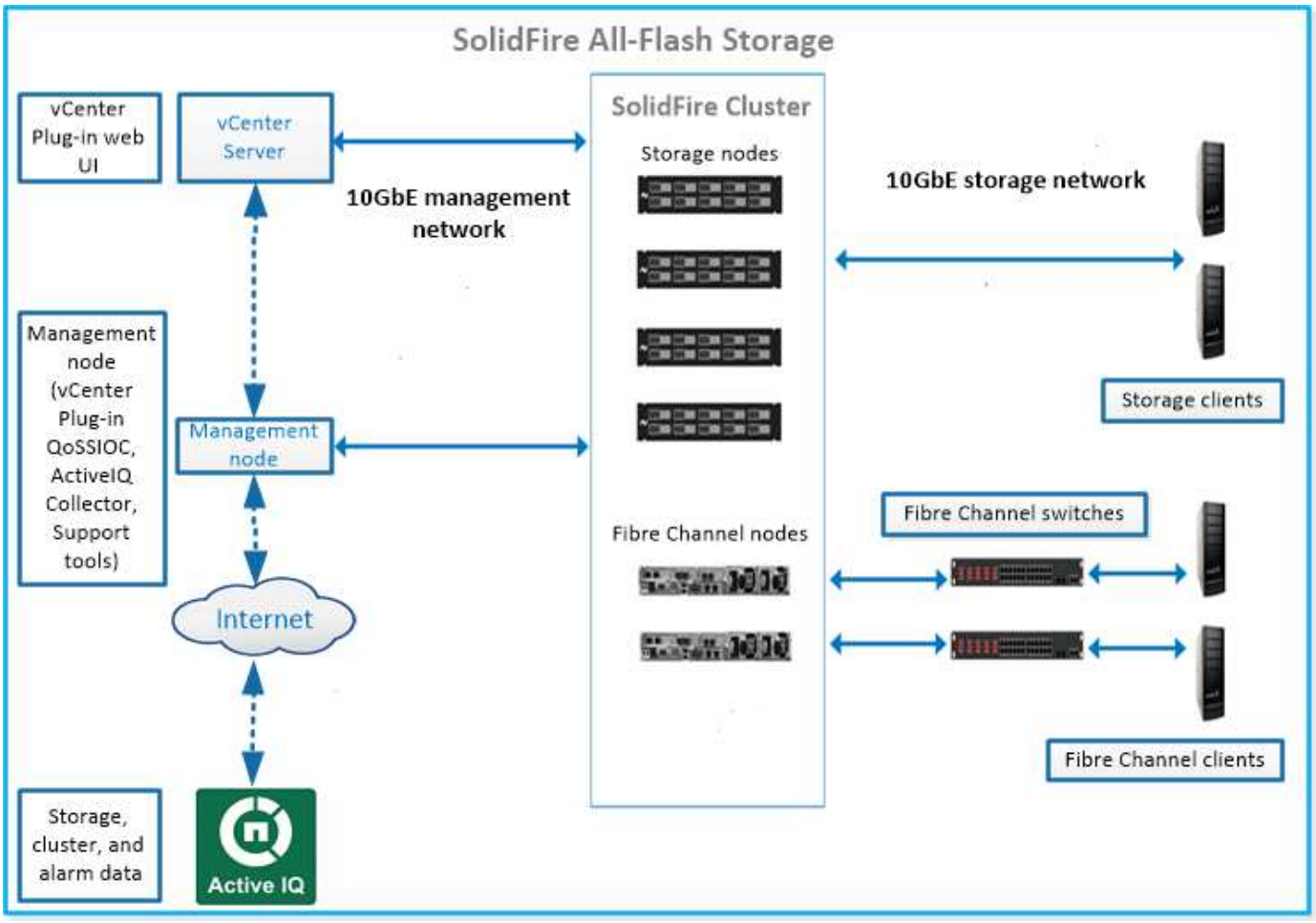
- "Présentation du stockage 100 % Flash de SolidFire"
- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Présentation de l’architecture de SolidFire

Un système de stockage 100 % Flash SolidFire comprend des composants matériels distincts (disques et nœuds) regroupés dans un pool de ressources de stockage avec le logiciel NetApp Element exécuté indépendamment sur chaque nœud. Ce système de stockage unique est géré comme une entité unique via l’interface utilisateur du logiciel Element, l’API et d’autres outils de gestion.

Un système de stockage SolidFire comprend les composants matériels suivants :

- **Cluster** : le hub du système de stockage SolidFire qui est un ensemble de nœuds.
- **Noeuds** : les composants matériels regroupés dans un cluster. Il existe deux types de nœuds :
  - Nœuds de stockage, qui sont des serveurs contenant un ensemble de disques
  - Nœuds Fibre Channel (FC), que vous utilisez pour vous connecter aux clients FC
- **Disques** : utilisés dans les nœuds de stockage pour stocker les données du cluster. Un nœud de stockage contient deux types de disques :
  - Les lecteurs de métadonnées de volume stockent des informations qui définissent les volumes et les autres objets au sein d’un cluster.
  - Les disques de blocs stockent les blocs de données des volumes.



Vous pouvez gérer, contrôler et mettre à jour le système à l'aide de l'interface utilisateur Web d'Element et d'autres outils compatibles :

- "Interfaces logicielles SolidFire"
- "SolidFire Active IQ"
- "Nœud de gestion pour le logiciel Element"
- "Services de gestion"

URL courantes

Les URL suivantes sont couramment utilisées avec les systèmes de stockage 100 % Flash de SolidFire :

URL	Description
`https://[storage cluster MVIP address]`	Accédez à l'interface utilisateur du logiciel NetApp Element.
`https://activeiq.solidfire.com`	Surveillez les données et recevez des alertes en cas de goulot d'étranglement ou de problèmes potentiels au niveau du système.
`https://[management node IP address]`	Accédez à NetApp Hybrid Cloud Control pour mettre à niveau vos services d'installation et de gestion des mises à jour du stockage.

URL	Description
`https://[IP address]:442`	Depuis l'interface utilisateur par nœud, accédez aux paramètres réseau et de cluster et utilisez les tests et utilitaires du système. "En savoir plus ."
`https://[management node IP address]/mnode`	Utilisez l'API REST des services de gestion et d'autres fonctionnalités du nœud de gestion. "En savoir plus ."
`https://[management node IP address]:9443`	Enregistrez le package du plug-in vCenter dans le client Web vSphere. "En savoir plus ."

Trouvez plus d'informations

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

Interfaces logicielles SolidFire

Un système de stockage SolidFire peut être géré à l'aide de différentes interfaces logicielles et utilitaires d'intégration NetApp Element.

Options

- Interface utilisateur du logiciel NetApp Element
- API du logiciel NetApp Element
- Plug-in NetApp Element pour vCenter Server
- Le contrôle des clouds hybrides NetApp
- Interfaces utilisateur de nœud de gestion
- Utilitaires et outils d'intégration supplémentaires

Interface utilisateur du logiciel NetApp Element

Permet de configurer le stockage Element, de surveiller la performance et la capacité du cluster et de gérer l'activité de stockage dans 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 présentées 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.

"Gérez le stockage avec le logiciel Element"

API du logiciel NetApp Element

Permet d'utiliser un ensemble d'objets, de méthodes et de routines pour gérer le stockage Element. L'API Element est basée sur le protocole JSON-RPC sur HTTPS. Vous pouvez surveiller les opérations de l'API dans l'interface utilisateur Element en activant le journal de l'API. Cela vous permet de voir les méthodes qui sont émises vers le système. Vous pouvez activer à la fois les demandes et les réponses pour voir comment le système répond aux méthodes émises.

"Gérez le stockage avec l'API Element"

Plug-in NetApp Element pour vCenter Server

Permet de configurer et de gérer des clusters de stockage exécutant le logiciel Element à l'aide d'une autre interface conçue pour l'interface utilisateur Element dans VMware vSphere.

"Plug-in NetApp Element pour vCenter Server"

Le contrôle des clouds hybrides NetApp

Mise à niveau des services de stockage et de gestion Element et gestion des ressources de stockage avec l'interface NetApp Cloud hybride.

"Présentation de la gestion et du contrôle du stockage avec NetApp Hybrid Cloud Control"

Interfaces utilisateur de nœud de gestion

Le nœud de gestion contient deux interfaces utilisateur : une interface pour la gestion des services REST et une interface utilisateur par nœud pour la gestion des paramètres du réseau et du cluster, ainsi que des tests et utilitaires du système d'exploitation. Depuis l'interface utilisateur de l'API REST, vous pouvez accéder à un menu d'API liées aux services qui contrôlent la fonctionnalité du système basée sur les services à partir du nœud de gestion.

Utilitaires et outils d'intégration supplémentaires

Bien que vous gériez votre stockage à l'aide de NetApp Element, de l'API NetApp Element et du plug-in NetApp Element pour vCenter Server, vous pouvez utiliser des utilitaires et des outils d'intégration supplémentaires pour accéder au stockage.

Interface de ligne de commandes d'Element

"Interface de ligne de commandes d'Element" Vous permet de contrôler un système de stockage SolidFire à l'aide d'une interface de ligne de commandes sans avoir à utiliser l'API Element.

Outils Element PowerShell

"Outils Element PowerShell" Vous pouvez utiliser un ensemble de fonctions Microsoft Windows PowerShell qui utilisent l'API Element pour gérer un système de stockage SolidFire.

Les kits de développement logiciel Element

"Les kits de développement logiciel Element" Possibilité de gérer le cluster SolidFire à l'aide des outils suivants :

- Element Java SDK : permet aux programmeurs d'intégrer l'API Element au langage de programmation Java.
- SDK Element .NET : permet aux programmeurs d'intégrer l'API Element à la plate-forme de programmation .NET.
- Kit de développement logiciel Element Python : permet aux programmeurs d'intégrer l'API Element dans le langage de programmation Python.

Suite de tests API SolidFire Postman

Permet aux programmeurs d'utiliser un ensemble de "Post-man"fonctions qui testent les appels de l'API Element.

Adaptateur de réplication du stockage SolidFire

"Adaptateur de réplication du stockage SolidFire" Intégration à VMware site Recovery Manager (SRM) pour permettre la communication avec les clusters de stockage SolidFire répliqués et exécuter les flux de production pris en charge.

SolidFire VRO

"SolidFire VRO" Permet d'utiliser facilement l'API Element pour administrer votre système de stockage SolidFire avec VMware vRealize Orchestrator.

Fournisseur SolidFire VSS

"Fournisseur SolidFire VSS" Intègre les Shadow Copy VSS avec les snapshots et les clones Element.

Trouvez plus d'informations

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

SolidFire Active IQ

"SolidFire Active IQ" est un outil web qui fournit des vues historiques continuellement mises à jour des données au niveau du cluster. Vous pouvez définir des alertes pour des événements, des seuils ou des metrics spécifiques. SolidFire Active IQ vous permet de surveiller les performances et la capacité du système, ainsi que de rester informé de l'état du cluster.

Les informations suivantes concernant votre système sont disponibles dans SolidFire Active IQ :

- Nombre de nœuds et état des nœuds : sain, hors ligne ou panne
- Représentation graphique du processeur, de l'utilisation de la mémoire et de l'accélération des nœuds
- Détails sur le nœud, par exemple le numéro de série, l'emplacement du slot dans le châssis, le modèle et la version du logiciel NetApp Element s'exécutant sur le nœud de stockage
- Informations relatives aux processeurs et au stockage sur les machines virtuelles

Pour en savoir plus sur SolidFire Active IQ, consultez le "Documentation SolidFire Active IQ".

Pour en savoir plus

- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"
- "Site de support NetApp ; Outils pour Active IQ"

Nœud de gestion pour le logiciel Element

Le "Nœud de gestion (nœud M)" système est une machine virtuelle qui s'exécute en parallèle avec un ou plusieurs clusters de stockage basés sur le logiciel Element. Utilisé pour mettre à niveau et fournir des services système comprenant la surveillance et la télémétrie, gérer les ressources et les paramètres du cluster, exécuter des tests système

et des utilitaires, et activer l'accès au support NetApp pour la résolution de problèmes.

Le nœud de gestion interagit avec un cluster de stockage pour effectuer des actions de gestion, mais il n'est pas membre du cluster de stockage. Les nœuds de gestion recueillent régulièrement des informations sur le cluster via des appels d'API et les signalent à Active IQ à des fins de surveillance à distance (si cette option est activée). Des nœuds de gestion sont également chargés de coordonner les mises à niveau logicielles des nœuds du cluster.

Avec la version 11.3 d'Element, le nœud de gestion fonctionne comme un hôte de microservice, ce qui permet de mettre à jour plus rapidement des services logiciels spécifiques en dehors des versions majeures. Ces microservices ou "services de gestion" sont mis à jour fréquemment en tant que bundles de services.

Services de gestion pour le stockage 100 % Flash de SolidFire

À partir de la version d'Element 11.3, les **services de gestion** sont hébergés sur le "nœud de gestion", ce qui permet des mises à jour plus rapides de certains services logiciels en dehors des versions majeures.

Avec des services de gestion centralisés et étendus pour le stockage 100 % Flash de SolidFire. Ces services incluent "Le contrôle des clouds hybrides NetApp"la télémétrie du système Active IQ, la journalisation et les mises à jour des services, ainsi que le service QoSSIOC pour le plug-in Element pour vCenter.

En savoir plus sur "versions des services de gestion".

Nœuds

Les nœuds sont des ressources matérielles ou virtuelles regroupées dans un cluster afin de fournir des fonctionnalités de calcul et de stockage de blocs.

Le logiciel NetApp Element définit différents rôles de nœud pour un cluster. Les types de rôles de nœud sont les suivants :

- Nœud de gestion
- Nœud de stockage
- Nœud Fibre Channel

L'état des nœuds est indiqué varie en fonction de l'association du cluster.

Nœud de gestion

Un nœud de gestion est une machine virtuelle utilisée pour mettre à niveau et fournir des services système, notamment la surveillance et la télémétrie, gérer les ressources et les paramètres du cluster, exécuter des tests et des utilitaires système et activer l'accès au support NetApp pour le dépannage. "En savoir plus >>"

Nœud de stockage

Un nœud de stockage SolidFire est un serveur qui contient un ensemble de disques qui communiquent entre eux via l'interface réseau Bond10G. Les disques du nœud contiennent des espaces de bloc et de métadonnées pour le stockage et la gestion des données. Chaque nœud contient une image d'usine du logiciel NetApp Element.

Les caractéristiques des nœuds de stockage sont les suivantes :

- Chaque nœud porte un nom unique. Si un nom de nœud n'est pas spécifié par un administrateur, il prend par défaut la valeur SF-XXXX, où XXXX correspond à quatre caractères aléatoires générés par le système.
- Chaque nœud dispose de son propre cache d'écriture NVRAM haute performance pour améliorer les performances globales du système et réduire la latence d'écriture.
- Chaque nœud est relié à deux réseaux, au stockage et à la gestion, chacun disposant de deux liens indépendants pour la redondance et la performance. Chaque nœud requiert une adresse IP sur chaque réseau.
- Vous pouvez créer un cluster avec de nouveaux nœuds de stockage ou ajouter des nœuds de stockage à un cluster existant afin d'augmenter la capacité et les performances de stockage.
- Vous pouvez ajouter ou supprimer des nœuds du cluster à tout moment, sans interruption de service.

Nœud Fibre Channel

Les nœuds Fibre Channel SolidFire assurent la connectivité avec un commutateur Fibre Channel, que vous pouvez connecter aux clients Fibre Channel. Les nœuds Fibre Channel agissent comme un convertisseur de protocole entre les protocoles Fibre Channel et iSCSI. Cela vous permet d'ajouter une connectivité Fibre Channel à tout cluster SolidFire existant ou nouveau.

Caractéristiques des nœuds Fibre Channel :

- Les commutateurs Fibre Channel permettent de gérer l'état de la structure, assurant ainsi des interconnexions optimisées.
- Le trafic entre deux ports traverse uniquement les commutateurs ; il n'est transmis à aucun autre port.
- La défaillance d'un port est isolée et n'affecte pas le fonctionnement des autres ports.
- Plusieurs paires de ports peuvent communiquer simultanément dans une structure.

Etat de fonctionnement du nœud

Un nœud peut être dans l'un des États suivant le niveau de configuration.

- **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.

- **En attente active**

  Le système est en cours d'installation du logiciel d'élément compatible sur le nœud. Une fois l'opération terminée, le nœud passe à l'état actif.

- **Actif**

  Ce nœud participe à un cluster.

Une authentification est requise pour modifier le nœud.

Dans chacun de ces États, certains champs sont en lecture seule.

Trouvez plus d'informations

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

Clusters

Un cluster est le moyeu d'un système de stockage SolidFire et il est composé d'un ensemble de nœuds. Pour réaliser les fonctionnalités d'efficacité du stockage SolidFire, vous devez disposer d'au moins quatre nœuds dans un cluster. Un cluster apparaît sur le réseau comme un seul groupe logique, qui est ensuite accessible en tant que stockage bloc.

La création d'un nouveau cluster initialise un nœud en tant que propriétaire des communications pour un cluster et établit des communications réseau pour chaque nœud du cluster. Ce processus n'est effectué qu'une seule fois pour chaque nouveau cluster. La création d'un cluster peut s'effectuer à l'aide de l'interface utilisateur Element ou de l'API.

Vous pouvez faire évoluer horizontalement un cluster en ajoutant des nœuds supplémentaires. Lorsque vous ajoutez un nouveau nœud, aucune interruption de service n'est constatée, et le cluster utilise automatiquement les performances et la capacité du nouveau nœud.

Les administrateurs et les hôtes peuvent accéder au cluster à l'aide d'adresses IP virtuelles. Tout nœud du cluster peut héberger les adresses IP virtuelles. L'adresse IP virtuelle de gestion (MVIP) permet la gestion des clusters via une connexion 1 GbE, tandis que l'adresse IP virtuelle de stockage (SVIP) permet l'accès de l'hôte au stockage via une connexion 10 GbE. Ces adresses IP virtuelles permettent des connexions cohérentes, quelle que soit la taille ou la composition d'un cluster SolidFire. Si un nœud hébergeant une adresse IP virtuelle échoue, un autre nœud du cluster commence à héberger l'adresse IP virtuelle.

> À partir de la version 11.0 de l'élément, les nœuds peuvent être configurés avec IPv4, IPv6 ou les deux adresses pour leur réseau de gestion. Cela s'applique à la fois aux nœuds de stockage et aux nœuds de gestion, à l'exception du nœud de gestion 11.3 et versions ultérieures qui ne prennent pas en charge IPv6. Lors de la création d'un cluster, seule une seule adresse IPv4 ou IPv6 peut être utilisée pour le MVIP et le type d'adresse correspondant doit être configuré sur tous les nœuds.

Plus d'informations sur les clusters

- Clusters de stockage faisant autorité
- Règle des tiers
- La capacité inutilisée
- Efficacité du stockage
- Quorum du cluster de stockage

Clusters de stockage faisant autorité

Le cluster de stockage faisant autorité est le cluster de stockage que NetApp Hybrid Cloud Control utilise pour authentifier les utilisateurs.

Si votre nœud de gestion ne dispose que d'un seul cluster de stockage, il fait autorité. Si votre nœud de gestion dispose de deux ou plusieurs clusters de stockage, un de ces clusters est désigné comme cluster qui fait autorité, et seuls les utilisateurs de ce cluster peuvent se connecter au contrôle de cloud hybride NetApp. Pour déterminer quel cluster est le cluster faisant autorité, vous pouvez utiliser l' `GET /mnode/about`API. Dans la réponse, l'adresse IP du `token_url` champ est l'adresse IP virtuelle de gestion (MVIP) du cluster de stockage faisant autorité. Si vous tentez de vous connecter à NetApp Hybrid Cloud Control en tant qu'utilisateur qui ne se trouve pas sur le cluster qui fait autorité, la tentative de connexion échoue.

De nombreuses fonctionnalités NetApp Hybrid Cloud Control sont conçues pour fonctionner avec plusieurs clusters de stockage, mais l'authentification et l'autorisation disposent de limites. L'authentification et l'autorisation sont limités par le fait que l'utilisateur du cluster qui fait autorité peut exécuter des actions sur d'autres clusters liés à NetApp Hybrid Cloud Control, même s'ils ne sont pas un utilisateur sur les autres clusters de stockage.

Avant d'administrer plusieurs clusters de stockage, veillez à ce que les utilisateurs définis sur les clusters qui font autorité soient définis sur tous les autres clusters de stockage avec les mêmes autorisations. Vous pouvez gérer les utilisateurs à partir de "Interface utilisateur du logiciel Element".

Pour plus d'informations sur l'utilisation des actifs de cluster de stockage de nœud de gestion, reportez-vous à la section"créer et gérer les ressources du cluster de stockage".

Règle des tiers

Lorsque vous combinez des types de nœuds de stockage dans un cluster de stockage NetApp SolidFire, aucun nœud de stockage ne peut contenir plus de 33 % de la capacité totale du cluster de stockage.

La capacité inutilisée

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. Ce qui reste le cas jusqu'à ce que de la capacité de stockage supplémentaire soit ajoutée. 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.

Efficacité du stockage

Les clusters de stockage NetApp SolidFire utilisent la déduplication, la compression et le provisionnement fin pour réduire la quantité de stockage physique nécessaire au stockage d'un volume.

- **Compression**

  La compression réduit la quantité de stockage physique nécessaire pour un volume en combinant des blocs de données dans des groupes de compression, chacun étant stocké sous forme de bloc unique.

- **Déduplication**

  La déduplication réduit le volume de stockage physique requis pour un volume en abandonnant des blocs de données dupliqués.

- **Provisionnement fin**

  Une LUN ou un volume à provisionnement fin est un volume pour lequel le stockage n'est pas réservé à l'avance. Au contraire, le stockage est alloué de manière dynamique, selon les besoins. L'espace libre est relibéré dans le système de stockage lorsque les données du volume ou de la LUN sont supprimées

Quorum du cluster de stockage

Le logiciel Element crée un cluster de stockage à partir de nœuds sélectionnés, qui tient à jour une base de données répliquée de la configuration du cluster. Un minimum de trois nœuds sont nécessaires pour participer à l'ensemble de groupe afin de maintenir le quorum nécessaire pour la résilience du cluster.

Sécurité

Lorsque vous utilisez votre système de stockage 100 % Flash SolidFire, vos données sont protégées par des protocoles de sécurité standard.

Chiffrement des données au repos (matériel)

Tous les disques des nœuds de stockage sont capables de chiffrer le chiffrement AES 256 bits au niveau du disque. Chaque lecteur dispose de sa propre clé de cryptage, qui est créée lors de l'initialisation initiale du lecteur. Lorsque vous activez la fonctionnalité de cryptage, un mot de passe à l'échelle du cluster est créé et des segments de mot de passe sont ensuite distribués à tous les nœuds du cluster. Aucun nœud ne stocke la totalité du mot de passe. Le mot de passe est alors utilisé pour protéger par mot de passe tous les accès aux lecteurs. Le mot de passe est nécessaire pour déverrouiller le lecteur et ne l'est pas tant que l'alimentation n'est pas coupée du lecteur ou que le lecteur n'est pas verrouillé.

"Activation de la fonctionnalité de chiffrement matériel au repos" n'affecte pas les performances ou l'efficacité sur le cluster. Si un disque ou un nœud compatible avec le chiffrement est retiré de la configuration du cluster avec l'API Element ou l'interface utilisateur d'Element, le chiffrement au repos est désactivé sur les disques. Une fois le lecteur retiré, il peut être effacé en toute sécurité à l'aide de la `SecureEraseDrives` méthode API. Si un disque physique ou un nœud est supprimé de force, les données restent protégées par le mot de passe de l'ensemble du cluster et par les clés de cryptage individuelles du disque.

Chiffrement des données au repos (logiciel)

Un autre type de chiffrement logiciel au repos permet de chiffrer toutes les données écrites sur les SSD du cluster de stockage. "Lorsque cette option est activée", il crypte toutes les données écrites et décrypte toutes les données lues automatiquement dans le logiciel. Le chiffrement logiciel au repos assure la mise en miroir de l'implémentation du lecteur SED (Self-Encrypting Drive) dans le matériel pour assurer la sécurité des données en l'absence de SED.

> 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.

Les solutions logicielles et matérielles de chiffrement au repos peuvent être utilisées de manière indépendante ou en association.

Gestion externe des clés

Vous pouvez configurer le logiciel Element pour qu'il gère les clés de chiffrement du cluster de stockage à

l'aide d'un service tiers de gestion des clés conforme KMIP. Lorsque vous activez cette fonctionnalité, la clé de chiffrement de mot de passe d'accès au disque au niveau du cluster est gérée par un KMS que vous spécifiez.

Element peut utiliser les services de gestion des clés suivants :

- Gemalto SafeNet KeySecure
- SAFENET CHEZ KeySecure
- KeyControl HyTrust
- Gestionnaire de sécurité des données Vormetric
- IBM Security Key Lifecycle Manager

Pour plus d'informations sur la configuration de la gestion externe des clés, reportez-vous à la "vous lancez dans une mise en œuvre externe de la gestion des clés" documentation.

Authentification multifacteur

L'authentification multifacteur (MFA) vous permet de présenter plusieurs types de preuves à l'utilisateur lors NetApp Element de la connexion. Vous pouvez configurer Element pour qu'il accepte uniquement l'authentification multi-facteurs pour les connexions intégrant votre système de gestion des utilisateurs et votre fournisseur d'identités. Vous pouvez configurer Element pour qu'il s'intègre à un fournisseur d'identités SAML 2.0 existant qui peut appliquer plusieurs schémas d'authentification, tels que les mots de passe et les messages texte, les mots de passe et les e-mails, ou d'autres méthodes.

Vous pouvez coupler l'authentification multi-facteurs avec des fournisseurs d'identité compatibles SAML 2.0 (IDP) courants, tels que Microsoft Active Directory Federation Services (ADFS) et Shiboleeth.

Pour configurer MFA, voir la "le système active l'authentification multifacteur" documentation.

FIPS 140-2 pour le chiffrement HTTPS et des données au repos

Les clusters de stockage NetApp SolidFire prennent en charge le chiffrement conforme à la norme FIPS 140-2 (Federal information Processing Standard) pour les modules cryptographiques. Vous pouvez activer la conformité FIPS 140-2 sur votre cluster SolidFire pour les communications HTTPS et le chiffrement de disques.

Lorsque vous activez le mode d'exploitation FIPS 140-2 sur votre cluster, le cluster active NetApp Cryptographic Security module (NCSM) et exploite le chiffrement certifié FIPS 140-2 niveau 1 pour toutes les communications via HTTPS vers l'interface utilisateur et l'API de NetApp Element. Vous utilisez l' `EnableFeature`API Element avec le `fips` paramètre pour activer le chiffrement HTTPS FIPS 140-2-2. Sur les clusters de stockage dotés d'un matériel compatible FIPS, vous pouvez également activer le chiffrement de disque FIPS pour les données au repos à l'aide de l' `EnableFeature`API Element et `FipsDrives` du paramètre.

Pour plus d'informations sur la préparation d'un nouveau cluster de stockage pour le cryptage FIPS 140-2"Créez un cluster prenant en charge les disques FIPS"-2, reportez-vous à la section .

Pour plus d'informations sur l'activation de FIPS 140-2 sur un cluster préparé existant, reportez-vous à "L'API d'élément EnableFeature"la section .

Pour en savoir plus

- "Documentation SolidFire et Element"

- "Plug-in NetApp Element pour vCenter Server"

Comptes et autorisations

Pour administrer et donner l'accès aux ressources de stockage de votre système, vous devez configurer des comptes pour les ressources système.

Avec le stockage Element, vous pouvez créer et gérer les types de compte suivants :

- L'administrateur compte pour le cluster de stockage
- Les comptes utilisateurs de l'accès au volume de stockage
- Comptes utilisateurs de cluster faisant autorité pour NetApp Hybrid Cloud Control

Comptes d'administrateur du cluster de stockage

Deux types de comptes d'administrateur peuvent exister dans un cluster de stockage qui exécute le logiciel NetApp Element :

- **Compte d'administrateur de cluster principal** : ce compte d'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 d'administrateur de cluster** : vous pouvez donner à un compte d'administrateur de cluster une plage limitée d'accès administratif pour 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.

Vous pouvez "gérer les comptes d'administrateur du cluster"créer, supprimer et modifier des comptes d'administrateur de cluster, modifier le mot de passe de l'administrateur de cluster et configurer les paramètres LDAP pour gérer l'accès au système pour les utilisateurs.

Comptes d'utilisateur

Les comptes utilisateur permettent de contrôler l'accès aux ressources de stockage sur un réseau logiciel NetApp Element. Au moins un compte utilisateur est nécessaire avant la création du volume.

Lorsque vous créez un volume, il est affecté à un compte. Si vous avez créé un volume virtuel, le compte est le conteneur de stockage.

Voici quelques considérations supplémentaires :

- Le compte contient l'authentification CHAP requise pour accéder aux volumes qui lui sont affectés.
- Un compte peut avoir jusqu'à 2000 volumes qui lui sont attribués, mais un volume ne peut appartenir qu'à un seul compte.
- Les comptes utilisateur peuvent être gérés à partir du point d'extension NetApp Element Management.

Comptes d’utilisateur de cluster qui font autorité

Les comptes utilisateurs qui font autorité sur le cluster peuvent s’authentifier sur toutes les ressources de stockage associées à l’instance NetApp de contrôle du cloud hybride de nœuds et de clusters. Ce compte vous permet de gérer des volumes, des comptes, des groupes d’accès et bien plus encore dans tous les clusters.

Les comptes utilisateurs qui font autorité sont gérés depuis le menu supérieur droit de l’option de gestion des utilisateurs du contrôle de cloud hybride NetApp.

Le "cluster de stockage faisant autorité" système utilise le cluster de stockage utilisé par le service NetApp Hybrid Cloud Control pour authentifier les utilisateurs.

Tous les utilisateurs créés sur le cluster de stockage qui fait autorité peuvent se connecter au contrôle de cloud hybride NetApp. Les utilisateurs créés sur d’autres clusters de stockage *ne* pas se connecter à Cloud Control hybride.

- Si votre nœud de gestion ne dispose que d’un seul cluster de stockage, il fait autorité.
- Si votre nœud de gestion dispose de deux ou plusieurs clusters de stockage, un de ces clusters est désigné comme cluster qui fait autorité, et seuls les utilisateurs de ce cluster peuvent se connecter au contrôle de cloud hybride NetApp.

Alors que de nombreuses fonctionnalités NetApp de cloud hybride Control fonctionnent avec plusieurs clusters de stockage, l’authentification et l’autorisation disposent des limites nécessaires. L’authentification et l’autorisation sont limités par le fait que les utilisateurs du cluster qui fait autorité peuvent exécuter des actions sur d’autres clusters liés à NetApp Hybrid Cloud Control, même s’ils ne sont pas un utilisateur sur les autres clusters de stockage. Avant d’administrer plusieurs clusters de stockage, veillez à ce que les utilisateurs définis sur les clusters qui font autorité soient définis sur tous les autres clusters de stockage avec les mêmes autorisations. Vous pouvez gérer les utilisateurs NetApp Hybrid Cloud Control.

Comptes de volume

Les comptes spécifiques aux volumes sont uniquement spécifiques au cluster de stockage sur lequel ils ont été créés. Ces comptes vous permettent de définir des autorisations sur des volumes spécifiques sur le réseau, mais n’ont aucun effet en dehors de ces volumes.

Les comptes de volumes sont gérés dans le tableau NetApp Hybrid Cloud Control volumes.

Stockage

Volumes

Le système de stockage NetApp Element 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.

Le stockage Element vous permet de créer, afficher, modifier, supprimer, cloner, sauvegarder ou restaurer des volumes pour les comptes utilisateurs. Vous pouvez également gérer chaque volume d’un cluster, et ajouter ou supprimer des volumes dans des groupes d’accès aux volumes.

Volumes persistants

Les volumes persistants permettent de stocker les données de configuration du nœud de gestion sur un cluster de stockage spécifié, plutôt que localement avec une VM, de sorte que les données puissent être conservées en cas de perte ou de suppression du nœud de gestion. Les volumes persistants sont une configuration de nœud de gestion facultative, mais recommandée.

Une option permettant d'activer les volumes persistants est incluse dans les scripts d'installation et de mise à niveau lorsque "déploiement d'un nouveau nœud de gestion". Les volumes persistants sont des volumes situés sur un cluster de stockage logiciel Element qui contiennent des informations de configuration des nœuds de gestion pour la VM du nœud de gestion hôte dont la persistance est supérieure à la durée de vie de la machine virtuelle. En cas de perte du nœud de gestion, une VM de remplacement peut se reconnecter à et récupérer les données de configuration pour la machine virtuelle perdue.

La fonctionnalité de volumes persistants, si elle est activée pendant l'installation ou la mise à niveau, crée automatiquement plusieurs volumes. Ces volumes, comme tout volume logiciel Element, peuvent être visualisés à l'aide de l'interface utilisateur Web du logiciel Element, du plug-in NetApp Element pour vCenter Server ou de l'API, selon vos préférences et votre installation. Les volumes persistants doivent être actifs et exécutés avec une connexion iSCSI au nœud de gestion afin de conserver les données de configuration actuelles pouvant être utilisées pour la restauration.

> 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

Volumes virtuels (vvols)

Les volumes virtuels vSphere sont un modèle de stockage utilisé par VMware qui permet de déplacer une grande partie de la gestion du stockage pour vSphere du système de stockage vers VMware vCenter. Avec Virtual volumes (vvols), vous pouvez allouer du stockage en fonction des besoins de machines virtuelles individuelles.

Liaisons

Le cluster NetApp Element 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.

Terminaux PE

Les hôtes VMware ESXi utilisent des proxys d'E/S logiques appelés terminaux de protocole pour communiquer avec les volumes virtuels. Les hôtes ESXi lient les volumes virtuels aux terminaux PE pour effectuer des opérations d'E/S. Lorsqu'une machine virtuelle de l'hôte effectue une opération d'E/S, le point de terminaison de protocole associé dirige les E/S vers le volume virtuel auquel elle est couplée.

Les terminaux PE d'un cluster NetApp Element fonctionnent comme des unités logiques d'administration SCSI. Chaque terminal de protocole est créé automatiquement par le cluster. Pour chaque nœud d'un cluster, un terminal de protocole correspondant est créé. Par exemple, un cluster à quatre nœuds possède quatre terminaux de protocole.

ISCSI est le seul protocole pris en charge par le logiciel NetApp Element. Le protocole Fibre Channel n'est pas pris en charge. 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.

Conteneurs de stockage

Les conteneurs de stockage sont des constructions logiques qui sont mappées aux comptes NetApp Element et utilisées pour le reporting et l'allocation des ressources. Ils regroupent des capacités de stockage brutes ou des fonctionnalités de stockage agrégées que le système de stockage peut fournir aux volumes virtuels. Un datastore VVol créé dans vSphere est mappé à un conteneur de stockage individuel. Par défaut, un conteneur de stockage unique dispose de toutes les ressources disponibles depuis le cluster NetApp Element. Si une gouvernance plus granulaire est nécessaire pour la colocation, plusieurs conteneurs de stockage peuvent être créés.

Les conteneurs de stockage fonctionnent comme des comptes classiques et peuvent contenir à la fois des volumes virtuels et des volumes traditionnels. Un maximum de quatre conteneurs de stockage par cluster est pris en charge. Un conteneur de stockage au moins est requis pour utiliser la fonctionnalité VVols. La découverte des conteneurs de stockage dans vCenter lors de la création des volumes virtuels est possible.

Fournisseur VASA

Pour que vSphere soit conscient de la fonctionnalité vVol du cluster NetApp Element, l'administrateur vSphere doit enregistrer le fournisseur NetApp Element VASA auprès de vCenter. Le fournisseur VASA est le chemin de contrôle hors bande entre vSphere et le cluster Element. Il est chargé d'exécuter les demandes sur le cluster Element pour le compte de vSphere, par exemple la création de machines virtuelles, la mise à disposition de machines virtuelles pour vSphere et la publicité des fonctionnalités de stockage pour vSphere.

Le fournisseur VASA s'exécute comme faisant partie du maître de cluster dans le logiciel Element. Le maître de cluster est un service hautement disponible qui bascule vers n'importe quel nœud du cluster si nécessaire. En cas de défaillance du maître de cluster, le fournisseur VASA le déplace tout en assurant une haute disponibilité pour le fournisseur VASA. Toutes les tâches de provisionnement et de gestion du stockage utilisent le fournisseur VASA, qui gère toutes les modifications requises dans le cluster Element.

> Pour Element 12.5 et versions antérieures, ne vous enregistrez pas plusieurs fournisseurs NetApp Element VASA dans une seule instance de vCenter. Ainsi, lorsqu'un deuxième fournisseur NetApp Element VASA est ajouté, tous les data stores VVOL sont inaccessibles.

> Le support VASA pour 10 centres maximum est disponible en tant que correctif de mise à niveau si vous avez déjà enregistré un fournisseur VASA auprès de votre vCenter. Pour l'installer, suivez les instructions du manifeste VASA39 et téléchargez le fichier .tar.gz à partir du "Téléchargements de logiciels NetApp"site. 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

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

Groupes d'accès de volume

La création et l'utilisation de groupes d'accès aux volumes vous permettent de contrôler l'accès à un ensemble de volumes. Lorsque vous associez un ensemble de volumes et un ensemble d'initiateurs à un groupe d'accès de volume, le groupe d'accès accorde à ces initiateurs l'accès à cet ensemble de volumes.

Les groupes d'accès aux volumes du stockage NetApp SolidFire permettent d'accéder à une collection de volumes via des IQN ou des WWPN des initiateurs iSCSI Fibre Channel. Chaque IQN que vous ajoutez à un groupe d'accès peut accéder à chaque volume du groupe sans utiliser l'authentification CHAP. 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 128 initiateurs par groupe d'accès de volume.
- Un maximum de 64 groupes d'accès par volume.
- 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 de volume.
- Pour les clusters Fibre Channel, un seul volume peut appartenir à un maximum de quatre groupes d'accès.

Initiateurs

Les initiateurs permettent aux clients externes d'accéder aux volumes d'un cluster, servant de point d'entrée pour la communication entre les clients et les volumes. Vous pouvez utiliser des initiateurs pour l'accès CHAP aux volumes de stockage plutôt qu'en fonction du compte. Un seul initiateur, lorsqu'il est ajouté à un groupe d'accès de volume, permet aux membres du groupe d'accès de volume d'accéder à tous les volumes de stockage ajoutés au groupe sans nécessiter d'authentification. Un initiateur ne peut appartenir à qu'un seul groupe d'accès.

Protection des données

Les fonctionnalités de protection des données incluent la réplication à distance, les copies Snapshot de volume, le clonage de volume, les domaines de protection et la haute disponibilité avec la technologie double Helix.

La protection des données du stockage Element repose sur plusieurs concepts :

- Types de réplication distante
- Snapshots de volumes pour la protection des données
- Clones de volumes
- Présentation des processus de sauvegarde et de restauration pour le stockage Element
- Domaines de protection
- Domaines de protection personnalisés
- Double haute disponibilité Helix

Types de réplication distante

La réplication à distance des données peut prendre les formes suivantes :

- Réplication synchrone et asynchrone entre les clusters
- Réplication snapshot uniquement

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

Pour plus d'informations, voir "Tr-4741 : réplication à distance du logiciel NetApp Element".

Réplication synchrone et asynchrone entre les clusters

Pour les clusters exécutant le logiciel NetApp 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.

Réplication synchrone

La réplication synchrone réplique en continu les données du cluster source vers le cluster cible et est affectée par la latence, la perte de paquets, la gigue et la bande passante.

La réplication synchrone est adaptée aux situations suivantes :

- Réplication de plusieurs systèmes sur une courte distance
- Un site de reprise sur incident qui est géographiquement local à la source
- Les applications urgentes et la protection des bases de données
- Les applications de continuité de l'activité qui requièrent que le site secondaire fonctionne comme site principal lorsque le site primaire est en panne

Réplication asynchrone

La réplication asynchrone réplique continuellement les données d'un cluster source vers un cluster cible sans attendre les accusés de réception du cluster cible. Pendant la réplication asynchrone, les écritures sont réceptionnées sur le client (l'application) après qu'elles sont validées sur le cluster source.

La réplication asynchrone est adaptée aux situations suivantes :

- Le site de reprise après sinistre est loin de la source et l'application ne tolère pas les latences induites par le réseau.
- La bande passante est limitée sur le réseau qui connecte les clusters source et cible.

Réplication snapshot uniquement

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.

Vous pouvez définir la fréquence des réplications de snapshot.

La réplication Snapshot n'affecte pas la réplication asynchrone ou synchrone.

Réplication entre les clusters Element et ONTAP à l'aide de SnapMirror

Avec la technologie NetApp SnapMirror, vous pouvez répliquer les snapshots qui ont été réalisés à l'aide du logiciel NetApp Element sur ONTAP à des fins de reprise après incident. Dans une relation SnapMirror, Element est un terminal et ONTAP l'autre.

SnapMirror est une technologie de réplication NetApp Snapshot qui facilite la reprise sur incident et permet le basculement de l'infrastructure de stockage primaire vers un stockage secondaire sur un site distant. La technologie SnapMirror crée une réplique, ou miroir, des données de travail dans un système de stockage secondaire, à partir duquel vous pouvez continuer à transmettre des données en cas de panne sur le site primaire. Les données sont mises en miroir au niveau du volume.

La relation entre le volume source du stockage primaire et le volume de destination du stockage secondaire est appelée « relation de protection des données ». Les clusters sont appelés « terminaux » dans lesquels se trouvent les volumes, tandis que les volumes qui contiennent les données répliquées doivent être associés. Cette relation de type peer-to-peer permet aux clusters et aux volumes d'échanger les données de manière sécurisée.

SnapMirror s'exécute de façon native sur les contrôleurs NetApp ONTAP. Il est intégré dans Element et s'exécute sur les clusters NetApp HCI et SolidFire. La logique de contrôle de SnapMirror réside dans le logiciel ONTAP. Par conséquent, toutes les relations SnapMirror doivent impliquer au moins un système ONTAP afin d'effectuer les tâches de coordination. Les utilisateurs gèrent les relations entre les clusters Element et ONTAP principalement via l'interface utilisateur Element, mais certaines tâches de gestion résident dans NetApp ONTAP System Manager. Les utilisateurs peuvent également gérer SnapMirror via l'interface de ligne de commande et l'API, qui sont tous les deux disponibles dans ONTAP et Element.

Voir "Tr-4651 : Architecture et configuration de NetApp SolidFire SnapMirror" (connexion requise)

Vous devez activer manuellement la fonctionnalité SnapMirror au niveau du cluster à l'aide du logiciel Element. La fonctionnalité SnapMirror est désactivée par défaut et n'est pas automatiquement activée dans le cadre d'une nouvelle installation ou mise à niveau.

Après avoir activer SnapMirror, vous pouvez créer des relations SnapMirror à partir de l'onglet protection des données dans le logiciel Element.

Le logiciel NetApp Element 10.1 et versions supérieures prennent en charge la fonctionnalité SnapMirror pour copier et restaurer des snapshots avec les systèmes ONTAP.

Les systèmes exécutant Element 10.1 et versions ultérieures intègrent un code permettant de communiquer directement avec SnapMirror sur des systèmes ONTAP exécutant la version 9.3 ou ultérieure. L'API Element propose des méthodes d'activation de la fonctionnalité SnapMirror sur les clusters, les volumes et les snapshots. De plus, l'interface utilisateur d'Element inclut des fonctionnalités permettant de gérer les relations SnapMirror entre le logiciel Element et les systèmes ONTAP.

À partir des systèmes Element 10.3 et ONTAP 9.4, 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.

Snapshots de volumes pour la protection des données

Un snapshot de volume est une copie instantanée d'un volume que vous pouvez utiliser par la suite pour restaurer un volume à un moment précis.

Bien que les snapshots soient similaires aux clones de volume, les snapshots constituent simplement des répliques de métadonnées de volume, ce qui vous permet de les monter ou d'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 répliquer des snapshots sur un cluster distant et les utiliser comme copie de sauvegarde du volume. Cela permet de restaurer un volume à un point dans le temps en utilisant le snapshot répliqué ; vous

pouvez également créer un clone d'un volume à partir d'un snapshot répliqué.

Vous pouvez sauvegarder des snapshots depuis un cluster Element vers un magasin d'objets externe ou vers un autre cluster Element. 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.

Pour la protection des données, il est possible de créer un snapshot pour un ou plusieurs volumes individuels.

Clones de volumes

Un clone d'un ou plusieurs volumes est une copie instantanée des données. 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.

Présentation des processus de sauvegarde et de restauration pour le stockage Element

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

Vous pouvez sauvegarder un volume dans les éléments suivants :

- Un cluster de stockage SolidFire
- Un magasin d'objets Amazon S3
- Un magasin d'objets 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.

Domaines de protection

Un domaine de protection est un nœud ou un ensemble de nœuds regroupés de manière à ce qu'une partie ou l'ensemble des nœuds puissent tomber en panne, tout en maintenant la disponibilité des données. Les domaines de protection permettent à un cluster de stockage de se réparer automatiquement contre la perte d'un châssis (affinité de châssis) ou d'un domaine entier (groupe de châssis).

Vous pouvez activer manuellement la surveillance du domaine de protection à l'aide du point d'extension de la configuration NetApp Element dans le plug-in NetApp Element pour vCenter Server. Vous pouvez sélectionner un seuil de domaine de protection en fonction des domaines de nœud ou de châssis. Vous pouvez également activer la surveillance du domaine de protection à l'aide de l'API Element ou de l'interface utilisateur Web.

Une disposition de domaine de protection affecte chaque nœud à un domaine de protection spécifique.

Deux dispositions de domaine de protection différentes, appelées niveaux de domaine de protection, sont prises en charge.

- Au niveau du nœud, chaque nœud se trouve dans son propre domaine de protection.
- Au niveau du châssis, seuls les nœuds qui partagent un châssis se trouvent dans le même domaine de protection.
  - L'organisation au niveau du châssis est automatiquement déterminée par le matériel lors de l'ajout d'un nœud au cluster.
  - Dans un cluster où chaque nœud se trouve dans un châssis distinct, ces deux niveaux sont fonctionnellement identiques.

Lors de la création d'un nouveau cluster, si vous utilisez des nœuds de stockage résidant dans un châssis partagé, il est préférable de concevoir une protection contre les défaillances au niveau du châssis à l'aide de la fonction domaines de protection.

domaines de protection personnalisés

Vous pouvez définir une disposition de domaine de protection personnalisée qui correspond à votre disposition spécifique de châssis et de nœud, et où chaque nœud est associé à un seul domaine de protection personnalisé. Par défaut, chaque nœud est affecté au même domaine de protection personnalisé par défaut.

Si aucun domaine de protection personnalisé n'est attribué :

- L'opération de cluster n'est pas affectée.
- Le niveau personnalisé n'est ni tolérant ni résilient.

Lorsque vous configurez des domaines de protection personnalisés pour un cluster, trois niveaux de protection sont possibles, à partir du tableau de bord de l'interface utilisateur Web d'Element :

- Non protégé : le cluster de stockage n'est pas protégé contre la défaillance de l'un de ses domaines de protection personnalisés. Pour résoudre ce problème, ajoutez de la capacité de stockage supplémentaire au cluster ou reconfigurez les domaines de protection personnalisés du cluster afin de protéger le cluster d'éventuelles pertes de données.
- Tolérance aux pannes : le cluster de stockage dispose d'une capacité suffisante pour éviter la perte de données suite à la défaillance de l'un de ses domaines de protection personnalisés.
- Résilience des pannes : le cluster de stockage dispose de suffisamment de capacité libre pour permettre l'auto-rétablissement après la panne de l'un de ses domaines de protection personnalisés. Une fois le processus de réparation terminé, le cluster est protégé contre la perte de données en cas d'échec des domaines supplémentaires.

Si plusieurs domaines de protection personnalisés sont affectés, chaque sous-système affecte des doublons à des domaines de protection personnalisés distincts. Si ce n'est pas possible, il revient à attribuer des doublons à des nœuds distincts. Chaque sous-système (par exemple, bacs, tranches, fournisseurs de points de terminaison de protocole et ensemble) le fait indépendamment.

Vous pouvez utiliser l'interface utilisateur Element pour "Configurez les domaines de protection personnalisés"ou les méthodes d'API suivantes :

- "GetProtectionDomainLayout" - Indique le châssis et le domaine de protection personnalisé dans lequel se trouve chaque nœud.
- "SetProtectionDomainLayout" - Permet d'affecter un domaine de protection personnalisé à chaque nœud.

Double haute disponibilité Helix

La protection des données Helix double est une méthode de réplication qui répartit au moins deux copies redondantes des données sur tous les disques d'un système. L'approche « sans RAID » permet à un système d'absorber plusieurs défaillances simultanées à tous les niveaux du système de stockage et de les réparer rapidement.

La performance et la qualité de service

Un cluster de stockage SolidFire propose des paramètres de qualité de service (QoS) par volume. Vous pouvez garantir les performances des clusters mesurées en entrées et sorties par seconde (IOPS) à l'aide de trois paramètres configurables pour définir la QoS : IOPS min, IOPS max et IOPS en rafale.

SolidFire Active IQ dispose d'une page de recommandations de QoS qui fournit des conseils sur la configuration optimale et la configuration des paramètres de QoS.

Paramètres de qualité de service

Les paramètres IOPS sont définis de l'une des manières suivantes :

- **IOPS minimum** - le nombre minimal d'entrées et de sorties soutenues par seconde (IOPS) que le cluster de stockage fournit à un volume. La valeur d'IOPS minimale configurée pour un volume correspond au niveau de performance garanti pour un volume. Les performances ne tombent pas en dessous de ce niveau.
- **Nombre maximal d'IOPS** - nombre maximal d'IOPS en continu que le cluster de stockage fournit à un volume. Lorsque les niveaux d'IOPS du cluster sont extrêmement élevés, ce niveau de performance d'IOPS n'est pas dépassé.
- **IOPS en rafale** - le nombre maximal d'IOPS autorisé dans un scénario en rafale courte. Si un volume s'exécute en dessous du nombre maximal d'IOPS, les crédits de bursting sont cumulés. Lorsque les niveaux de performance deviennent très élevés et vont jusqu'à des niveaux maximum, de courtes IOPS sont autorisées sur le volume.

  Le logiciel Element utilise IOPS en rafale lorsqu'un cluster fonctionne à faible taux d'utilisation des IOPS du cluster.

  Un seul volume peut augmenter le nombre d'IOPS en rafale et utiliser les crédits pour dépasser le nombre d'IOPS max. Jusqu'à son niveau d'IOPS en rafale pendant une « période de rafale » définie. Un volume peut augmenter jusqu'à 60 secondes si le cluster est capable de prendre en charge cette rafale. Un volume atteint une seconde de crédit en rafale (jusqu'à 60 secondes maximum) par seconde que le volume s'exécute en dessous de sa limite IOPS max.

  Les IOPS en rafale sont limitées de deux manières :

  - Un volume peut augmenter de plusieurs secondes au-dessus de ses IOPS max., ce qui équivaut au nombre de crédits de bursting que le volume a courus.
  - Lorsqu'un volume dépasse sa valeur d'IOPS max, il est limité par son paramètre d'IOPS en rafale. Par conséquent, les IOPS en rafale ne dépassent jamais le paramètre d'IOPS de rafale pour le volume.
- **Bande passante effective max** - la bande passante maximale est calculée en multipliant le nombre d'IOPS (sur la base de la courbe QoS) par la taille d'E/S.

Exemple : les paramètres de QoS de 100 IOPS min, de 1000 IOPS max et de 1500 000 IOPS en rafale ont plusieurs effets sur la qualité de performance :

- Les charges de travail peuvent atteindre et maintenir un maximum de 1000 000 IOPS jusqu'à ce que les conflits entre charges de travail pour les IOPS apparaissent sur le cluster. Les IOPS sont ensuite réduites de manière incrémentielle jusqu'à ce que les IOPS sur tous les volumes se situent dans les plages de QoS désignées, et les conflits pour les performances sont éliminés.
- Les performances de tous les volumes sont poussées vers le IOPS minimum de 100. Les niveaux ne tombent pas en dessous du paramètre min. D'IOPS, mais peuvent rester supérieurs à 100 000 IOPS en cas de conflit de charge de travail.
- Les performances ne sont jamais supérieures à 1000 100 IOPS, ou inférieures à 80 000 IOPS pendant une période prolongée. Les performances de 1500 000 IOPS (IOPS en rafale) sont autorisées, mais uniquement pour les volumes qui ont accumulé des crédits de bursting, car ils sont inférieurs aux IOPS max. Et ne sont autorisés que sur de courtes périodes. Les niveaux en rafale ne sont jamais durables.

Limites de valeur de QoS

Voici les valeurs minimales et maximales possibles pour la QoS.

Paramètres	Valeur min	Valeur par défaut	4 KO	5 8 KO	6 16 KO	262KO
IOPS min	50	50	15 000	9,375*	5556*	385*
IOPS max	100	15 000	200,000**	125 000	74 074	5128
IOPS en rafale	100	15 000	200,000**	125 000	74,074	5128

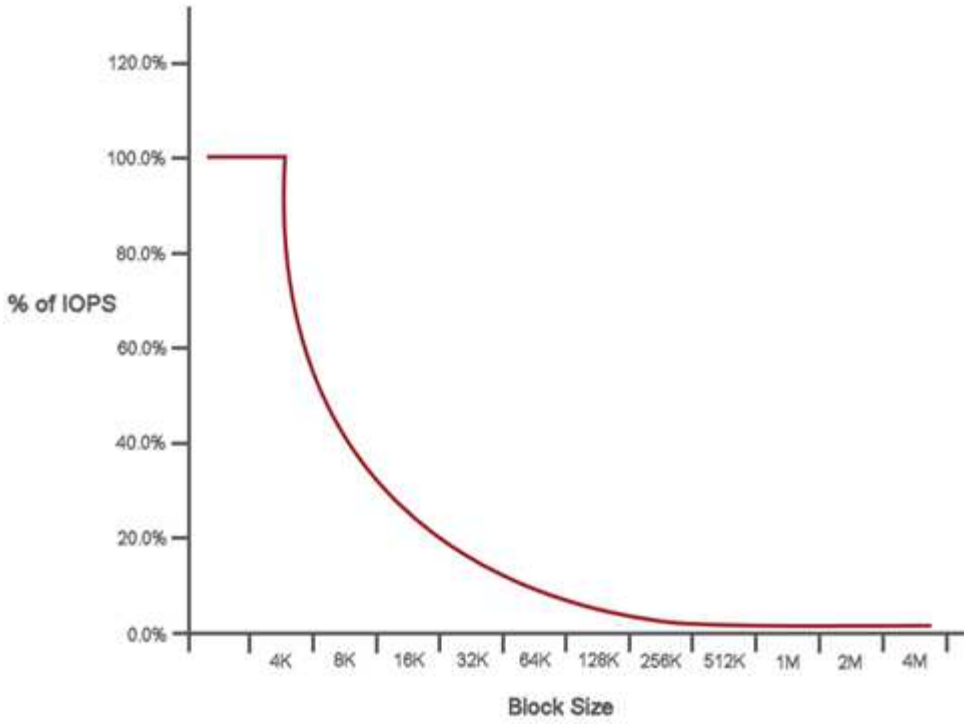
*Ces estimations sont approximatives. **IOPS max et IOPS en rafale peuvent être définis sur 200,000 ; cependant, ce paramètre est uniquement autorisé à uncaréellement les performances d'un volume. Les performances maximales réelles d'un volume sont limitées par l'utilisation du cluster et les performances par nœud.

Performances de QoS

La courbe des performances de QoS indique la relation entre la taille de bloc et le pourcentage d'IOPS.

La taille et la bande passante des blocs ont un impact direct sur le nombre d'IOPS qu'une application peut obtenir. Pour le logiciel Element, il prend en compte la taille des blocs reçus en normalisant ces tailles à la taille des blocs jusqu'à la taille 4 ko. En fonction des charges de travail, le système peut augmenter la taille des blocs. Lorsque la taille de bloc augmente, le système augmente la bande passante jusqu'au niveau nécessaire pour traiter les tailles de bloc de taille supérieure. Plus la bande passante augmente le nombre d'IOPS, plus le système peut atteindre une baisse.

La courbe des performances de QoS indique la relation entre l'augmentation de la taille des blocs et la diminution du pourcentage d'IOPS :



Par exemple, si les tailles de bloc sont de 4 ko et que la bande passante est de 4000 kbit/s, le nombre d'IOPS est de 1000. Si les tailles de bloc augmentent à 8 Ko, la bande passante augmente à 5000 kbit/s et les IOPS diminuent à 625. En prenant en compte la taille des blocs, le système s'assure que des charges de travail moins prioritaires qui utilisent des tailles de blocs plus élevées, comme les sauvegardes et les activités de l'hyperviseur, n'utilisent pas trop les performances requises par le trafic prioritaire utilisant des blocs de tailles plus petite.

Des règles de QoS

Une règle de QoS vous permet de créer et d'enregistrer des paramètres de qualité de service standardisés qui peuvent être appliqués à de nombreux volumes.

Les règles de qualité de service sont idéales pour les environnements de services, par exemple avec des serveurs de bases de données, d'applications ou d'infrastructure qui ne redémarrent pas et ont besoin d'un accès constant égal au stockage. La qualité de service des volumes individuels est optimale pour les machines virtuelles à utilisation légère, telles que les postes de travail virtuels ou les machines virtuelles de type kiosque spécialisées, qui peuvent être redémarrés, mis sous tension ou arrêtées tous les jours ou plusieurs fois par jour.

Les règles de QoS et de QoS ne doivent pas être combinées. 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.

Le cluster sélectionné doit être Element 10.0 ou version ultérieure pour utiliser les règles de QoS ; sinon, les fonctions de politique de QoS ne sont pas disponibles.

Trouvez plus d'informations

- "Documentation SolidFire et Element"