Concepts

Element Software

NetApp
November 18, 2025

Sommaire

Concepts

Apprenez les concepts de base liés au logiciel Element.

- "Présentation du produit"
- Présentation de l’architecture SolidFire
- Nœuds
- Groupes
- "Sécurité"
- Comptes et autorisations
- "Volumes"
- Protection des données
- Performance et qualité du service

Présentation du produit

Un système de stockage 100 % flash SolidFire est composé de composants matériels distincts (disques et nœuds) combinés en un seul pool de ressources de stockage. Ce cluster unifié se présente comme un système de stockage unique destiné aux clients externes et est géré par le logiciel NetApp Element .

À l’aide de l’interface Element, de l’API ou d’autres outils de gestion, vous pouvez surveiller la capacité et les performances de stockage du cluster SolidFire et gérer l’activité de stockage sur une infrastructure mutualisée.

Fonctionnalités SolidFire

Un système Solidfire offre les fonctionnalités suivantes :

- Offre un stockage haute performance pour votre infrastructure de cloud privé à grande échelle.
- Offre une capacité de stockage flexible qui vous permet de répondre à vos besoins changeants.
- Utilise une interface logicielle Element de gestion du stockage pilotée par API
- Garantit la performance grâce à des politiques de qualité de service
- Inclut l’équilibrage de charge automatique sur tous les nœuds du cluster
- Rééquilibre automatiquement les clusters lorsque des nœuds sont ajoutés ou supprimés.

Déploiement SolidFire

Utilisez les nœuds de stockage fournis par NetApp et intégrés au logiciel NetApp Element .

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

Trouver plus d’informations

- "Module d’extension NetApp Element pour vCenter Server"

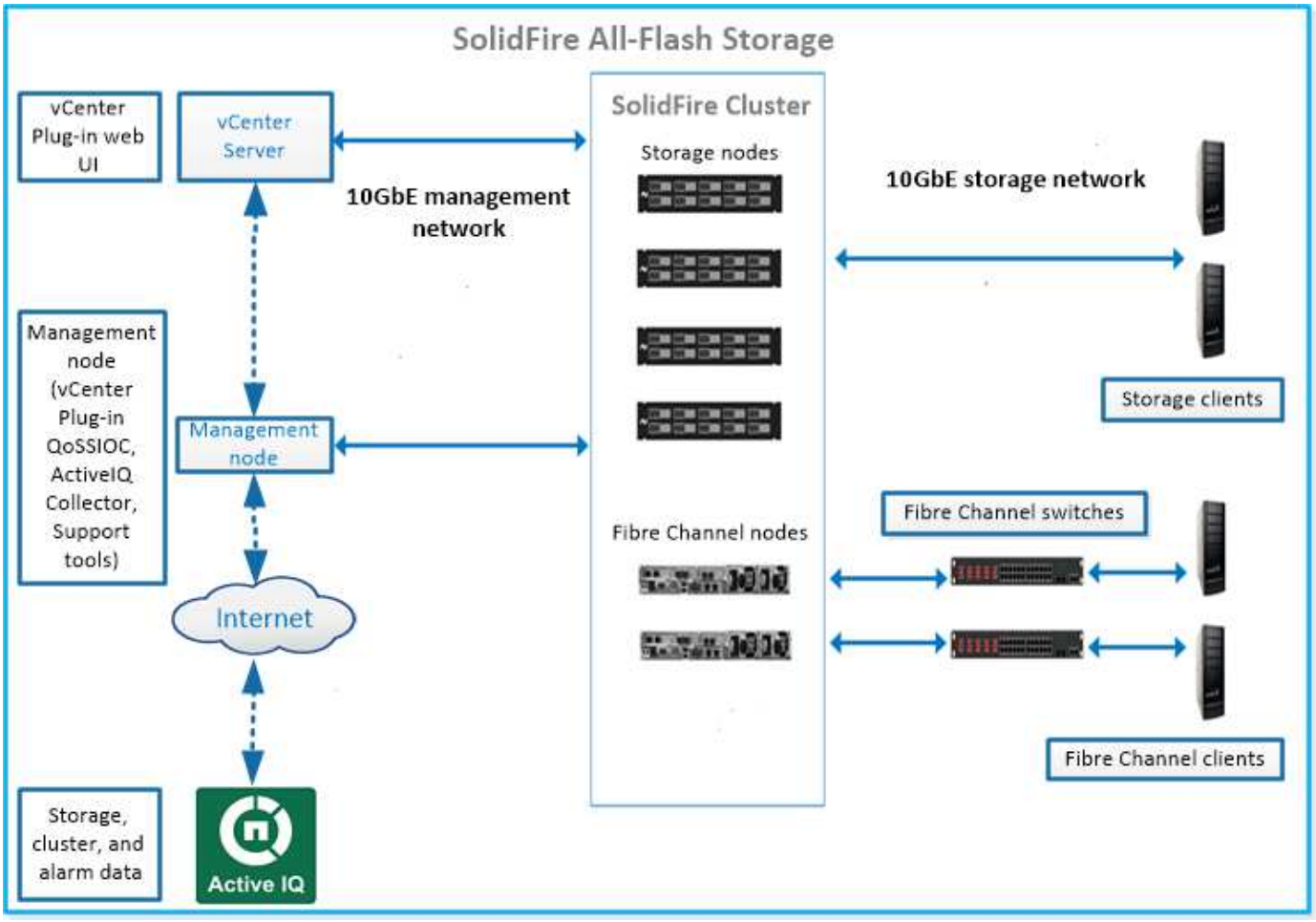
Architecture et composants

Découvrez l'architecture SolidFire

Un système de stockage 100% flash SolidFire est composé de composants matériels discrets (disques et nœuds) combinés en un pool de ressources de stockage avec le logiciel NetApp Element fonctionnant indépendamment sur chaque nœud. Ce système de stockage unique est géré comme une entité unique à l'aide de l'interface utilisateur, de l'API et d'autres outils de gestion du logiciel Element.

Un système de stockage SolidFire comprend les composants matériels suivants :

- **Cluster** : Le centre névralgique du système de stockage SolidFire , constitué d'un ensemble de nœuds.
- **Nœuds** : Les composants matériels regroupés en cluster. Il existe deux types de nœuds :
  - Les nœuds de stockage sont des serveurs contenant un ensemble de disques.
  - Les nœuds Fibre Channel (FC), que vous utilisez pour vous connecter aux clients FC
- **Disques durs** : 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 les informations qui définissent les volumes et autres objets au sein d'un cluster.
  - Les disques de stockage par blocs stockent les blocs de données pour les volumes.



Vous pouvez gérer, surveiller 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

Voici les URL courantes que vous utilisez avec un système de stockage 100 % flash 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 goulots d'étranglement des performances ou de problèmes système potentiels.
`https://[management node IP address]`	Accédez à NetApp Hybrid Cloud Control pour mettre à niveau votre installation de stockage et vos services de gestion.
`https://[IP address]:442`	Depuis l'interface utilisateur de chaque nœud, accédez aux paramètres réseau et de cluster et utilisez les tests et utilitaires système."Apprendre encore plus."
`https://[management node IP address]/mnode`	Utilisez l'API REST des services de gestion et les autres fonctionnalités du nœud de gestion."Apprendre encore plus."
`https://[management node IP address]:9443`	Enregistrez le package du plug-in vCenter dans le client Web vSphere."Apprendre encore plus."

Trouver plus d'informations

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

Interfaces logicielles SolidFire

Vous pouvez gérer un système de stockage SolidFire à l'aide de différentes interfaces logicielles et utilitaires d'intégration NetApp Element .

Options

- interface utilisateur du logiciel NetApp Element
- API logicielle NetApp Element
- Module d'extension NetApp Element pour vCenter Server
- Contrôle du cloud hybride NetApp

- Interfaces utilisateur des nœuds de gestion
- utilitaires et outils d'intégration supplémentaires

interface utilisateur du logiciel NetApp Element

Permet de configurer le stockage Element, de surveiller la capacité et les performances du cluster et de gérer l'activité de stockage sur une infrastructure mutualisée. Element est le système d'exploitation de stockage au cœur d'un cluster SolidFire . Le logiciel Element s'exécute indépendamment sur tous les nœuds du cluster et permet à ces nœuds de combiner des ressources qui sont présentées comme un système de stockage unique aux clients externes. Le logiciel Element est responsable de la coordination, de la mise à l'échelle et de la gestion de l'ensemble du système. L'interface logicielle est construite sur l'API Element.

"Gérez le stockage avec le logiciel Element"

API logicielle NetApp Element

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

"Gérez le stockage avec l'API Element"

Module d'extension NetApp Element pour vCenter Server

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

"Module d'extension NetApp Element pour vCenter Server"

Contrôle du cloud hybride NetApp

Permet de mettre à niveau les services de stockage et de gestion Element et de gérer les ressources de stockage à l'aide de l'interface NetApp Hybrid Cloud Control.

"Gérez et surveillez le stockage avec NetApp Hybrid Cloud Control."

Interfaces utilisateur des nœuds de gestion

Le nœud de gestion contient deux interfaces utilisateur : une interface utilisateur pour la gestion des services basés sur REST et une interface utilisateur par nœud pour la gestion des paramètres réseau et de 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 les fonctionnalités du système basé sur les services à partir du nœud de gestion.

utilitaires et outils d'intégration supplémentaires

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

Element CLI

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

Outils PowerShell d'Element

"Outils PowerShell d'Element"vous permet d'utiliser une collection de fonctions Microsoft Windows PowerShell qui utilisent l'API Element pour gérer un système de stockage SolidFire .

Kits de développement logiciel (SDK) Element

"Kits de développement logiciel (SDK) Element"vous permettent de gérer votre cluster SolidFire à l'aide de ces outils :

- Kit de développement logiciel (SDK) Element Java : permet aux programmeurs d'intégrer l'API Element au langage de programmation Java.
- Kit de développement logiciel (SDK) Element .NET : permet aux programmeurs d'intégrer l'API Element à la plateforme de programmation .NET.
- Kit de développement logiciel (SDK) Element pour Python : permet aux programmeurs d'intégrer l'API Element au langage de programmation Python.

Suite de tests de l'API Postman de SolidFire

Permet aux programmeurs d'utiliser une collection de"Facteur" fonctions qui testent les appels à l'API Element.

Adaptateur de réplication de stockage SolidFire

"Adaptateur de réplication de stockage SolidFire"s'intègre avec VMware Site Recovery Manager (SRM) pour permettre la communication avec les clusters de stockage SolidFire répliqués et exécuter les flux de travail pris en charge.

SolidFire vRO

"SolidFire vRO"offre un moyen pratique d'utiliser l'API Element pour administrer votre système de stockage SolidFire avec VMware vRealize Orchestrator.

Fournisseur SolidFire VSS

"Fournisseur SolidFire VSS"Intègre les copies fantômes VSS aux instantanés et clones Element.

Trouver plus d'informations

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

SolidFire Active IQ

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

Vous trouverez les informations suivantes concernant votre système dans SolidFire Active IQ:

- Nombre de nœuds et leur état : opérationnels, hors ligne ou défaillants
- Représentation graphique de l'utilisation du processeur, de la mémoire et de la limitation du nombre de nœuds
- Détails concernant le nœud, tels que le numéro de série, l'emplacement dans le châssis, le modèle et la version du logiciel NetApp Element exécuté sur le nœud de stockage.
- Informations relatives au processeur et au stockage des machines virtuelles

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

Pour plus d'informations

- "Documentation logicielle SolidFire et Element"
- "Module d'extension NetApp Element pour vCenter Server"
- **Site d'assistance NetApp › Outils pour Active IQ**

Nœud de gestion pour le logiciel Element

Le"nœud de gestion (mNode)" est une machine virtuelle qui fonctionne en parallèle avec un ou plusieurs clusters de stockage basés sur le logiciel Element. Il est utilisé 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 permettre l'accès au support NetApp pour le dépannage.

Le nœud de gestion interagit avec un cluster de stockage pour effectuer des actions de gestion, mais n'est pas membre de ce cluster. Les nœuds de gestion collectent périodiquement des informations sur le cluster via des appels API et transmettent ces informations à Active IQ pour la surveillance à distance (si activée). Les nœuds de gestion sont également responsables de la coordination des mises à jour logicielles des nœuds du cluster.

À partir de la version Element 11.3, le nœud de gestion fonctionne comme un hôte de microservices, permettant des mises à jour plus rapides de certains services logiciels en dehors des versions majeures. Ces microservices ou"services de gestion" sont fréquemment mis à jour sous forme de packs de services.

Services de gestion pour le stockage 100% flash SolidFire

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

Les services de gestion offrent des fonctionnalités de gestion centralisées et étendues pour le stockage 100 % flash SolidFire . Ces services comprennent"Contrôle du cloud hybride NetApp" , la télémétrie du système Active IQ , la journalisation et les mises à jour de service, ainsi que le service QoSSIOC pour le plug-in Element pour vCenter.

En savoir plus sur"mises à jour des services de gestion" .

Nœuds

Les nœuds sont des ressources matérielles ou virtuelles regroupées en cluster pour fournir des capacités de stockage par blocs et de calcul.

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

États des nœudsvarient en fonction de l'association au sein 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 permettre l'accès au support NetApp pour le dépannage."Apprendre encore plus"

Nœud de stockage

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

Les nœuds de stockage présentent les caractéristiques suivantes :

- Chaque nœud possède un nom unique. Si aucun nom de nœud n'est 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 possède son propre cache d'écriture NVRAM(mémoire vive non volatile haute performance) afin d'améliorer les performances globales du système et de réduire la latence d'écriture.
- Chaque nœud est connecté à deux réseaux, stockage et gestion, chacun disposant de deux liaisons indépendantes pour la redondance et les performances. Chaque nœud nécessite 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 pour augmenter la capacité et les performances de stockage.
- Vous pouvez ajouter ou supprimer des nœuds du cluster à tout moment sans interrompre le service.

Nœud Fibre Channel

Les nœuds Fibre Channel de SolidFire assurent la connectivité à un commutateur Fibre Channel, auquel vous pouvez connecter des clients Fibre Channel. Les nœuds Fibre Channel servent de convertisseur de protocole entre les protocoles Fibre Channel et iSCSI ; cela vous permet d'ajouter une connectivité Fibre Channel à tout cluster SolidFire nouveau ou existant.

Les nœuds Fibre Channel présentent les caractéristiques suivantes :

- Les commutateurs Fibre Channel gèrent l'état du réseau, assurant des interconnexions optimisées.
- Le trafic entre deux ports transite uniquement par 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 au sein d'un réseau.

États de fonctionnement des nœuds

Un nœud peut se trouver dans l'un des nombreux états possibles en fonction de son niveau de configuration.

- **Disponible**

  Ce nœud n'a pas de nom de cluster associé et ne fait pas encore partie d'un cluster.

- **En attente**

  Le nœud est configuré et peut être ajouté à un cluster désigné.

  L'authentification n'est pas requise pour accéder au nœud.

- **Activité en attente**

  Le système est en train d'installer le logiciel Element compatible sur le nœud. Une fois l'opération terminée, le nœud passera à l'état Actif.

- **Actif**

  Le nœud participe à un cluster.

  L'authentification est requise pour modifier le nœud.

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

Trouver plus d'informations

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

Groupes

Un cluster est le centre névralgique d'un système de stockage SolidFire et se compose d'un ensemble de nœuds. Pour bénéficier des performances de stockage SolidFire , vous devez disposer d'au moins quatre nœuds dans un cluster. Un cluster apparaît sur le réseau comme un groupe logique unique et peut ensuite être utilisé comme stockage par blocs.

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. Vous pouvez créer un cluster à l'aide de l'interface utilisateur d'Element ou de l'API.

Vous pouvez faire évoluer un cluster en ajoutant des nœuds supplémentaires. Lorsque vous ajoutez un

nouveau nœud, il n'y a aucune interruption de service 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. N'importe quel nœud du cluster peut héberger les adresses IP virtuelles. L'adresse IP virtuelle de gestion (MVIP) permet la gestion du cluster via une connexion 1GbE, tandis que l'adresse IP virtuelle de stockage (SVIP) permet l'accès de l'hôte au stockage via une connexion 10GbE. Ces adresses IP virtuelles permettent des connexions stables quelle que soit la taille ou la composition d'un cluster SolidFire . Si un nœud hébergeant une adresse IP virtuelle tombe en panne, un autre nœud du cluster prend le relais pour héberger cette adresse IP virtuelle.

> À partir de la version 11.0 d'Element, les nœuds peuvent être configurés avec des adresses IPv4, IPv6 ou les deux pour leur réseau de gestion. Ceci s'applique aux nœuds de stockage et aux nœuds de gestion, à l'exception du nœud de gestion 11.3 et versions ultérieures qui ne prend pas en charge IPv6. Lors de la création d'un cluster, 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
- Capacité bloquée
- Efficacité du stockage
- quorum du cluster de stockage

Clusters de stockage faisant autorité

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

Si votre nœud de gestion ne possède qu'un seul cluster de stockage, alors il s'agit du cluster faisant autorité. Si votre nœud de gestion comporte deux clusters de stockage ou plus, l'un de ces clusters est désigné comme cluster faisant autorité et seuls les utilisateurs de ce cluster peuvent se connecter à NetApp Hybrid Cloud Control. Pour déterminer quel cluster fait autorité, vous pouvez utiliser le `GET /mnode/about` API. Dans la réponse, l'adresse IP dans le `token_url` Ce champ correspond à 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 n'appartenant pas au cluster faisant autorité, la tentative de connexion échouera.

De nombreuses fonctionnalités de NetApp Hybrid Cloud Control sont conçues pour fonctionner avec plusieurs clusters de stockage, mais l'authentification et l'autorisation présentent des limitations. La limitation concernant l'authentification et l'autorisation est que l'utilisateur du cluster faisant autorité peut exécuter des actions sur d'autres clusters liés à NetApp Hybrid Cloud Control même s'il n'est pas un utilisateur sur les autres clusters de stockage.

Avant de procéder à la gestion de plusieurs clusters de stockage, vous devez vous assurer que les utilisateurs définis sur les clusters faisant autorité sont définis sur tous les autres clusters de stockage avec les mêmes autorisations. Vous pouvez gérer les utilisateurs depuis le"interface utilisateur du logiciel Element" .

Voir"créer et gérer les ressources du cluster de stockage" pour plus d'informations sur l'utilisation des ressources du cluster de stockage du nœud de gestion.

Règle des tiers

Lorsque vous mélangez différents 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.

Capacité bloquée

Si un nœud nouvellement ajouté représente plus de 50 % de la capacité totale du cluster, une partie de la capacité de ce nœud est rendue inutilisable (« bloquée »), afin qu'il se conforme à la règle de capacité. Cela restera le cas jusqu'à ce que davantage de capacité de stockage soit ajoutée. Si un nœud très volumineux est ajouté et qu'il enfreint également la règle de capacité, le nœud précédemment bloqué ne le sera plus, tandis que le nœud nouvellement ajouté le deviendra. Il convient toujours d'ajouter des capacités par paires pour éviter que cela ne se produise. Lorsqu'un nœud devient indisponible, une erreur 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 requise pour un volume en combinant les blocs de données en groupes de compression, chacun étant stocké comme un seul bloc.

- **Déduplication**

  La déduplication réduit la quantité de stockage physique requise pour un volume en supprimant les blocs de données dupliqués.

- **Provisionnement fin**

  Un volume à provisionnement fin, ou LUN, est un volume pour lequel l'espace de stockage n'est pas réservé à l'avance. L'espace de stockage est alloué dynamiquement, en fonction des besoins. L'espace libre est restitué au système de stockage lorsque des données sont supprimées du volume ou du LUN.

quorum du cluster de stockage

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

Sécurité

Lorsque vous utilisez votre système de stockage 100 % flash SolidFire , vos données sont protégées par des protocoles de sécurité conformes aux normes de l'industrie.

Chiffrement au repos (matériel)

Tous les disques des nœuds de stockage sont capables de chiffrement en utilisant le chiffrement AES 256 bits au niveau du disque. Chaque disque possède sa propre clé de chiffrement, créée lors de sa première initialisation. Lorsque vous activez la fonction de chiffrement, un mot de passe global est créé pour l'ensemble

du cluster, puis des fragments de ce mot de passe sont distribués à tous les nœuds du cluster. Aucun nœud ne stocke l'intégralité du mot de passe. Le mot de passe est ensuite utilisé pour protéger par mot de passe tout accès aux disques. Le mot de passe est nécessaire pour déverrouiller le disque et n'est ensuite plus requis sauf si l'alimentation est coupée ou si le disque est verrouillé.

"Activation de la fonction de chiffrement matériel au repos"n'affecte pas les performances ni l'efficacité du cluster. Si un disque ou un nœud compatible avec le chiffrement est supprimé de la configuration du cluster via l'API Element ou l'interface utilisateur Element, le chiffrement au repos sera désactivé sur les disques. Une fois le disque retiré, il peut être effacé de manière sécurisée à l'aide de la fonction `SecureEraseDrives` Méthode API. Si un disque ou un nœud physique est retiré de force, les données restent protégées par le mot de passe global du cluster et les clés de chiffrement individuelles du disque.

Chiffrement au repos (logiciel)

Un autre type de chiffrement au repos, le chiffrement logiciel au repos, permet de chiffrer toutes les données écrites sur les SSD d'un cluster de stockage. "Lorsqu'il est activé" Il chiffre automatiquement toutes les données écrites et déchiffre toutes les données lues grâce au logiciel. Le chiffrement logiciel au repos reflète l'implémentation du disque auto-chiffrant (SED) 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 lors de la création du cluster et ne peut pas être désactivé après sa création.

Le chiffrement au repos, qu'il soit logiciel ou matériel, peut être utilisé indépendamment ou en combinaison.

Gestion des clés externes

Vous pouvez configurer le logiciel Element pour utiliser un service de gestion de clés (KMS) tiers conforme à la norme KMIP afin de gérer les clés de chiffrement du cluster de stockage. Lorsque vous activez cette fonctionnalité, la clé de chiffrement du mot de passe d'accès aux disques à l'échelle du cluster de stockage est gérée par un KMS que vous spécifiez.

Element peut utiliser les services de gestion de clés suivants :

- Clé de sécurité Gemalto SafeNet
- SafeNet AT KeySecure
- HyTrust KeyControl
- Responsable de la sécurité des données Vormetric
- Gestionnaire de cycle de vie des clés de sécurité IBM

Pour plus d'informations sur la configuration de la gestion des clés externes, consultez"Pour commencer, consultez la gestion des clés externes." documentation.

Authentification multifacteur

L'authentification multifactorielle (MFA) vous permet d'exiger des utilisateurs qu'ils présentent plusieurs types de preuves pour s'authentifier auprès de l'interface utilisateur Web de NetApp Element ou de l'interface utilisateur du nœud de stockage lors de la connexion. Vous pouvez configurer Element pour qu'il n'accepte que l'authentification multifacteurs pour les connexions, en l'intégrant à votre système de gestion des utilisateurs et à votre fournisseur d'identité existants. Vous pouvez configurer Element pour qu'il s'intègre à un fournisseur d'identité SAML 2.0 existant capable d'appliquer plusieurs schémas d'authentification, tels que mot de passe et SMS, mot de passe et e-mail, ou d'autres méthodes.

Vous pouvez associer l'authentification multifactorielle à des fournisseurs d'identité (IdP) compatibles SAML 2.0 courants, tels que Microsoft Active Directory Federation Services (ADFS) et Shibboleth.

Pour configurer l'authentification multifacteur (MFA), consultez "activer l'authentification multifactorielle" documentation.

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

Les clusters de stockage NetApp SolidFire prennent en charge un chiffrement conforme aux exigences de la norme fédérale de traitement de l'information (FIPS) 140-2 pour les modules cryptographiques. Vous pouvez activer la conformité FIPS 140-2 sur votre cluster SolidFire pour les communications HTTPS et le chiffrement des disques.

Lorsque vous activez le mode de fonctionnement FIPS 140-2 sur votre cluster, celui-ci active le module de sécurité cryptographique NetApp (NCSM) et utilise 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 le `EnableFeature` API Element avec l'API Element avec `fips` Paramètre permettant d'activer le chiffrement HTTPS FIPS 140-2. Sur les clusters de stockage dotés de matériel compatible FIPS, vous pouvez également activer le chiffrement FIPS des disques pour les données au repos à l'aide de `EnableFeature` API Element avec l'API Element avec `FipsDrives` paramètre.

Pour plus d'informations sur la préparation d'un nouveau cluster de stockage pour le chiffrement FIPS 140-2, consultez"Créer un cluster prenant en charge les disques FIPS" .

Pour plus d'informations sur l'activation de la norme FIPS 140-2 sur un cluster existant et préparé, consultez"l'API EnableFeature Element" .

Pour plus d'informations

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

Comptes et autorisations

Pour administrer les ressources de stockage de votre système et en fournir l'accès, vous devrez créer des comptes pour ces ressources.

Avec Element Storage, vous pouvez créer et gérer les types de comptes suivants :

- Comptes d'utilisateurs administrateurs pour le cluster de stockage
- Comptes d'utilisateurs pour l'accès au volume de stockage
- Comptes d'utilisateurs de cluster faisant autorité pour NetApp Hybrid Cloud Control

comptes d'administrateur de cluster de stockage

Il existe deux types de comptes d'administrateur pouvant exister dans un cluster de stockage exécutant le logiciel NetApp Element :

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

de passe de ce compte administrateur.

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

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

Tu peux"gérer les comptes d'administrateur de cluster" en créant, supprimant et modifiant les comptes d'administrateur de cluster, en changeant le mot de passe de l'administrateur de cluster et en configurant les paramètres LDAP pour gérer l'accès au système pour les utilisateurs.

Comptes d'utilisateurs

Les comptes utilisateurs permettent de contrôler l'accès aux ressources de stockage sur un réseau basé sur le logiciel NetApp Element . Au moins un compte utilisateur est requis avant qu'un volume puisse être créé.

Lorsque vous créez un volume, celui-ci est affecté à un compte. Si vous avez créé un volume virtuel, le compte fait office de conteneur de stockage.

Voici quelques considérations supplémentaires :

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

comptes d'utilisateurs de cluster faisant autorité

Les comptes d'utilisateurs autorisés du cluster peuvent s'authentifier auprès de n'importe quelle ressource de stockage associée à l'instance de nœuds et de clusters NetApp Hybrid Cloud Control. Ce compte vous permet de gérer les volumes, les comptes, les groupes d'accès et bien plus encore sur tous les clusters.

Les comptes d'utilisateurs autorisés sont gérés depuis l'option Gestion des utilisateurs du menu situé en haut à droite de NetApp Hybrid Cloud Control.

Le"cluster de stockage faisant autorité" il s'agit du cluster de stockage que NetApp Hybrid Cloud Control utilise pour authentifier les utilisateurs.

Tous les utilisateurs créés sur le cluster de stockage principal peuvent se connecter à NetApp Hybrid Cloud Control. Les utilisateurs créés sur d'autres clusters de stockage ne peuvent pas se connecter à Hybrid Cloud Control.

- Si votre nœud de gestion ne possède qu'un seul cluster de stockage, alors il s'agit du cluster faisant autorité.
- Si votre nœud de gestion comporte deux clusters de stockage ou plus, l'un de ces clusters est désigné comme cluster faisant autorité et seuls les utilisateurs de ce cluster peuvent se connecter à NetApp Hybrid Cloud Control.

Bien que de nombreuses fonctionnalités de NetApp Hybrid Cloud Control fonctionnent avec plusieurs clusters

de stockage, l'authentification et l'autorisation présentent des limitations inévitables. La limitation concernant l'authentification et l'autorisation est que les utilisateurs du cluster faisant autorité peuvent exécuter des actions sur d'autres clusters liés à NetApp Hybrid Cloud Control même s'ils ne sont pas utilisateurs sur les autres clusters de stockage. Avant de procéder à la gestion de plusieurs clusters de stockage, vous devez vous assurer que les utilisateurs définis sur les clusters faisant autorité sont définis sur tous les autres clusters de stockage avec les mêmes autorisations. Vous pouvez gérer les utilisateurs depuis NetApp Hybrid Cloud Control.

Comptes de volume

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

Les comptes de volume sont gérés dans la table des volumes de contrôle du cloud hybride NetApp .

Stockage

Volumes

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

Le stockage d'éléments vous permet de créer, visualiser, 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 sur une machine virtuelle, afin que les données puissent être préservées en cas de perte ou de suppression du nœud de gestion. Les volumes persistants constituent une configuration de nœud de gestion optionnelle 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 sur un cluster de stockage basé sur le logiciel Element qui contiennent des informations de configuration du nœud de gestion pour la machine virtuelle du nœud de gestion hôte et qui persistent au-delà de la durée de vie de la machine virtuelle. Si le nœud de gestion est perdu, une machine virtuelle de remplacement peut se reconnecter et récupérer les données de configuration de la machine virtuelle perdue.

La fonctionnalité de volumes persistants, si elle est activée lors de l'installation ou de la mise à niveau, crée automatiquement plusieurs volumes. Ces volumes, comme tout volume basé sur le 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 opérationnels avec une connexion iSCSI au nœud de gestion pour conserver les données de configuration actuelles pouvant être utilisées pour la récupération.

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

Volumes virtuels (vVols)

vSphere Virtual Volumes est un paradigme de stockage pour VMware qui déplace une grande partie de la gestion du stockage de vSphere du système de stockage vers VMware vCenter. Avec les volumes virtuels (vVols), vous pouvez allouer du stockage en fonction des besoins de chaque machine virtuelle.

Reliures

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

Points de terminaison du protocole

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

Les points de terminaison de protocole dans un cluster NetApp Element fonctionnent comme des unités logiques administratives SCSI. Chaque point de terminaison de protocole est créé automatiquement par le cluster. Pour chaque nœud d'un cluster, un point de terminaison de protocole correspondant est créé. Par exemple, un cluster à quatre nœuds aura quatre points de terminaison 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 points de terminaison de protocole ne peuvent être ni supprimés ni modifiés par un utilisateur, ne sont pas associés à un compte et ne peuvent pas être ajoutés à un groupe d'accès aux volumes.

Conteneurs de stockage

Les conteneurs de stockage sont des structures logiques qui correspondent à des comptes NetApp Element et sont utilisés pour la création de rapports et l'allocation des ressources. Ils mettent en commun la capacité de stockage brute ou agrègent les capacités de stockage que le système de stockage peut fournir aux volumes virtuels. Un datastore VVol créé dans vSphere est mappé à un conteneur de stockage individuel. Un seul conteneur de stockage dispose par défaut de toutes les ressources disponibles du cluster NetApp Element . Si une gouvernance plus granulaire est nécessaire pour la mutualisation, plusieurs conteneurs de stockage peuvent être créés.

Les conteneurs de stockage fonctionnent comme des comptes traditionnels 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 minimum est requis pour utiliser les fonctionnalités de VVols. Vous pouvez découvrir les conteneurs de stockage dans vCenter lors de la création des VVols.

Fournisseur VASA

Pour que vSphere prenne en compte la fonctionnalité vVol sur le cluster NetApp Element , l'administrateur vSphere doit enregistrer le fournisseur VASA NetApp Element auprès de vCenter. Le fournisseur VASA constitue le chemin de contrôle hors bande entre vSphere et le cluster Element. Il est chargé d'exécuter les requêtes sur le cluster Element au nom de vSphere, telles que la création de machines virtuelles, la mise à disposition de machines virtuelles à vSphere et la publicité des capacités de stockage auprès de vSphere.

Le fournisseur VASA s'exécute dans le cadre du maître de cluster du logiciel Element. Le nœud maître du

cluster est un service à haute disponibilité qui bascule vers n'importe quel nœud du cluster en cas de besoin. Si le maître du cluster bascule, le fournisseur VASA le suit, garantissant ainsi 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 nécessaires sur le cluster Element.

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

La prise en charge VASA pour un maximum de 10 vCenters est disponible sous forme de 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 depuis le"Téléchargements de logiciels NetApp" site. Le fournisseur NetApp Element VASA utilise un certificat NetApp . Grâce à ce correctif, le certificat est utilisé sans modification par vCenter pour prendre en charge plusieurs vCenters pour l'utilisation de VASA et VVols. Ne modifiez pas le certificat. Les certificats SSL personnalisés ne sont pas pris en charge par VASA.

Trouver plus d'informations

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

groupes d'accès au volume

En créant et en utilisant des groupes d'accès aux volumes, vous pouvez 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 aux volumes, ce groupe d'accès accorde à ces initiateurs l'accès à cet ensemble de volumes.

Les groupes d'accès aux volumes dans le stockage NetApp SolidFire permettent aux IQN d'initiateur iSCSI ou aux WWPN Fibre Channel d'accéder à une collection de volumes. 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 au volume ont les limites suivantes :

- Un maximum de 128 initiateurs par groupe d'accès au volume.
- Un maximum de 64 groupes d'accès par volume.
- Un groupe d'accès peut être composé d'un maximum de 2000 volumes.
- Un IQN ou un WWPN ne peut appartenir qu'à un seul groupe d'accès aux volumes.
- 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 un accès aux volumes de stockage basé sur CHAP

plutôt que sur un compte. Un seul initiateur, lorsqu'il est ajouté à un groupe d'accès aux volumes, permet aux membres du groupe d'accéder à tous les volumes de stockage ajoutés au groupe sans nécessiter d'authentification. Un initiateur ne peut appartenir qu'à un seul groupe d'accès.

Protection des données

Les fonctionnalités de protection des données incluent la réplication à distance, les instantanés de volume, le clonage de volume, les domaines de protection et la haute disponibilité grâce à la technologie Double Helix.

La protection des données stockées dans les éléments comprend les concepts suivants :

- types de réplication à distance
- Instantanés de volume pour la protection des données
- Clones de volume
- Aperçu du processus de sauvegarde et de restauration pour Element Storage
- Domaines de protection
- Domaines de protection personnalisés
- Haute disponibilité de la double hélice

types de réplication à distance

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

- Réplication synchrone et asynchrone entre les clusters
- Réplication par instantané uniquement
- Réplication entre les clusters Element et ONTAP à l'aide de SnapMirror

Pour plus d'informations, consultez "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 la création rapide de copies distantes des données de volume.

Vous pouvez associer un cluster de stockage à un maximum de quatre autres clusters de stockage. Vous pouvez répliquer les données de volume de manière synchrone ou asynchrone à partir de l'un ou l'autre cluster d'une paire de clusters pour les scénarios de basculement et de restauration.

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 appropriée dans les situations suivantes :

- Réplication de plusieurs systèmes sur une courte distance

- Un site de reprise après sinistre situé géographiquement à proximité de la source
- Applications sensibles au temps et protection des bases de données
- Applications de continuité d'activité nécessitant que le site secondaire prenne le relais du site principal en cas d'indisponibilité de ce dernier.

Réplication asynchrone

La réplication asynchrone réplique en continu les données d'un cluster source vers un cluster cible sans attendre les accusés de réception du cluster cible. Lors de la réplication asynchrone, les écritures sont confirmées au client (application) après leur validation sur le cluster source.

La réplication asynchrone est appropriée dans les situations suivantes :

- Le site de reprise après sinistre est éloigné de la source et l'application ne tolère pas les latences induites par le réseau.
- Le réseau reliant les clusters source et cible présente des limitations de bande passante.

Réplication par instantané uniquement

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

Vous pouvez définir la fréquence des réplications d'instantanés.

La réplication par instantané n'affecte pas la réplication asynchrone ou synchrone.

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

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

SnapMirror est une technologie de réplication de snapshots NetApp qui facilite la reprise après sinistre, conçue pour le basculement du stockage principal vers le stockage secondaire sur un site géographiquement distant. La technologie SnapMirror crée une réplique, ou un miroir, des données de travail dans un stockage secondaire à partir duquel vous pouvez continuer à diffuser des données en cas de panne sur le site principal. Les données sont dupliquées au niveau du volume.

La relation entre le volume source dans le stockage principal et le volume de destination dans le stockage secondaire est appelée relation de protection des données. Les clusters sont appelés points de terminaison dans lesquels résident les volumes, et les volumes contenant les données répliquées doivent être appariés. Une relation entre pairs permet aux clusters et aux volumes d'échanger des données en toute sécurité.

SnapMirror fonctionne nativement sur les contrôleurs NetApp ONTAP et est intégré à Element, qui fonctionne 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 pour effectuer le travail de coordination. Les utilisateurs gèrent les relations entre Element et les clusters ONTAP principalement via l'interface utilisateur d'Element ; cependant, certaines tâches de gestion résident dans NetApp ONTAP System Manager. Les utilisateurs peuvent également gérer SnapMirror via l'interface de ligne de commande (CLI) et l'interface de programmation (API), toutes 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 activée automatiquement lors d'une nouvelle installation ou d'une mise à niveau.

Après avoir activé SnapMirror, vous pouvez créer des relations SnapMirror à partir de l'onglet Protection des données du logiciel Element.

Le logiciel NetApp Element 10.1 et versions ultérieures prend en charge la fonctionnalité SnapMirror pour copier et restaurer des instantanés avec les systèmes ONTAP .

Les systèmes exécutant Element 10.1 et versions ultérieures incluent un code qui peut communiquer directement avec SnapMirror sur les systèmes ONTAP exécutant la version 9.3 ou supérieure. L'API Element fournit des méthodes permettant d'activer la fonctionnalité SnapMirror sur les clusters, les volumes et les snapshots. De plus, l'interface utilisateur d'Element inclut 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 d'origine ONTAP vers des volumes Element dans des cas d'utilisation spécifiques avec des fonctionnalités limitées.

Pour plus d'informations, voir "Réplication entre NetApp Element Software et ONTAP (interface de ligne de commande ONTAP)".

Instantanés de volume pour la protection des données

Un instantané de volume est une copie à un instant précis d'un volume que vous pouvez utiliser ultérieurement pour restaurer un volume à ce moment précis.

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

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

Vous pouvez sauvegarder des instantanés d'un cluster Element vers un stockage d'objets externe ou vers un autre cluster Element. Lorsque vous sauvegardez un instantané sur un stockage d'objets externe, vous devez disposer d'une connexion à ce stockage d'objets autorisant les opérations de lecture/écriture.

Vous pouvez prendre un instantané d'un volume individuel ou de plusieurs volumes pour la protection des données.

Clones de volume

Un clone d'un seul volume ou de plusieurs volumes est une copie des données à un instant précis. Lorsque vous clonez un volume, le système crée un instantané du volume, puis une copie des données référencées par cet instantané.

Il s'agit d'un processus asynchrone, et sa durée dépend de la taille du volume à cloner et de la charge actuelle du cluster.

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

Aperçu du processus de sauvegarde et de restauration pour Element Storage

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

Vous pouvez sauvegarder un volume sur les supports 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 avez besoin des informations du manifeste issues du processus de sauvegarde d'origine. Si vous restaurez un volume sauvegardé sur un système de stockage SolidFire , aucune information de manifeste n'est requise.

Domaines de protection

Un domaine de protection est un nœud ou un ensemble de nœuds regroupés de telle sorte que toute partie, voire la totalité, puisse tomber en panne, tout en maintenant la disponibilité des données. Les domaines de protection permettent à un cluster de stockage de se réparer automatiquement en cas de 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 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 nœuds 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 configuration de domaine de protection attribue chaque nœud à un domaine de protection spécifique.

Deux configurations 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 appartiennent au même domaine de protection.
    - La configuration au niveau du châssis est automatiquement déterminée à partir du matériel lorsque le nœud est ajouté au cluster.
    - Dans un cluster où chaque nœud se trouve dans un châssis séparé, ces deux niveaux sont fonctionnellement identiques.

Lors de la création d'un nouveau cluster, si vous utilisez des nœuds de stockage situés dans un châssis partagé, vous pouvez envisager de concevoir une protection contre les pannes au niveau du châssis à l'aide de la fonctionnalité Domaines de protection.

Domaines de protection personnalisés

Vous pouvez définir une configuration de domaine de protection personnalisée qui correspond à la configuration spécifique de votre châssis et de vos nœuds, et dans laquelle chaque nœud est associé à un seul et unique 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 :

- Le fonctionnement du cluster n'est pas affecté.
- Le niveau personnalisé n'est ni tolérant ni résilient.

Lorsque vous configurez des domaines de protection personnalisés pour un cluster, il existe trois niveaux de protection possibles, que vous pouvez voir sur le 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 le protéger contre d'éventuelles pertes de données.
- Tolérance aux pannes : le cluster de stockage dispose d'une capacité libre suffisante pour éviter toute perte de données après la défaillance de l'un de ses domaines de protection personnalisés.
- Résilience aux pannes : le cluster de stockage dispose d'une capacité libre suffisante pour s'auto-réparer après la défaillance de l'un de ses domaines de protection personnalisés. Une fois le processus de réparation terminé, le cluster sera protégé contre toute perte de données en cas de défaillance d'autres domaines.

Si plusieurs domaines de protection personnalisés sont attribués, chaque sous-système attribuera les doublons à des domaines de protection personnalisés distincts. Si cela s'avère impossible, le système attribue les doublons à des nœuds distincts. Chaque sous-système (par exemple, les compartiments, les tranches, les fournisseurs de points de terminaison de protocole et l'ensemble) effectue cette opération indépendamment.

Vous pouvez utiliser l'interface utilisateur Element pour"configurer des domaines de protection personnalisés" , ou vous pouvez utiliser les méthodes API suivantes :

- "ObtenirProtectionDomainLayout"- indique dans quel châssis et dans quel domaine de protection personnalisé chaque nœud se trouve.
- "Définir la disposition du domaine de protection"- permet d'attribuer un domaine de protection personnalisé à chaque nœud.

Haute disponibilité de la double hélice

La protection des données Double Helix 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 de multiples pannes simultanées à tous les niveaux du système de stockage et de se réparer rapidement.

Performance et qualité du service

Un cluster de stockage SolidFire a la capacité de fournir des paramètres de qualité de service (QoS) par volume. Vous pouvez garantir les performances du cluster mesurées en entrées et sorties par seconde (IOPS) à l'aide de trois paramètres configurables qui définissent la QoS : IOPS min, IOPS max et IOPS en rafale.

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

Paramètres de qualité de service

Les paramètres IOPS sont définis de la manière suivante :

- **IOPS minimum** - Le nombre minimum d'entrées et de sorties soutenues par seconde (IOPS) que le cluster de stockage fournit à un volume. Le nombre minimal d'IOPS configuré pour un volume correspond au niveau de performance garanti pour ce volume. Les performances ne descendent pas en dessous de ce niveau.
- **IOPS maximales** - Le nombre maximal d'IOPS soutenues que le cluster de stockage fournit à un volume. Lorsque les niveaux d'IOPS du cluster sont extrêmement élevés, ce niveau de performance IOPS n'est pas dépassé.
- **IOPS en rafale** - Le nombre maximal d'IOPS autorisés dans un scénario de rafale courte. Si un volume a fonctionné en dessous du nombre maximal d'IOPS, des crédits de rafale sont accumulés. Lorsque les niveaux de performance deviennent très élevés et sont poussés à leurs niveaux maximums, de courtes rafales d'IOPS sont autorisées sur le volume.

  Le logiciel Element utilise les IOPS en rafale lorsqu'un cluster fonctionne dans un état de faible utilisation des IOPS du cluster.

  Un seul volume peut accumuler des IOPS en rafale et utiliser ces crédits pour dépasser ses IOPS maximales jusqu'à son niveau d'IOPS en rafale pendant une « période de rafale » définie. Un volume peut exploser pendant une durée maximale de 60 secondes si le cluster a la capacité de supporter cette explosion. Un volume accumule une seconde de crédit de rafale (jusqu'à un maximum de 60 secondes) pour chaque seconde pendant laquelle le volume fonctionne en dessous de sa limite Max IOPS.

  Les IOPS en rafale sont limitées de deux manières :

  - Un volume peut dépasser son nombre maximal d'IOPS pendant un nombre de secondes égal au nombre de crédits de rafale accumulés par le volume.
  - Lorsqu'un volume dépasse son paramètre Max IOPS, il est limité par son paramètre Burst IOPS. Par conséquent, les IOPS en rafale ne dépassent jamais le paramètre IOPS en rafale défini pour le volume.
- **Bande passante maximale effective** - La bande passante maximale est calculée en multipliant le nombre d'IOPS (basé sur la courbe QoS) par la taille des E/S.

  Exemple : Les paramètres QoS suivants : 100 IOPS min., 1 000 IOPS max. et 1 500 IOPS en rafale, ont les effets suivants sur la qualité des performances :

  - Les charges de travail peuvent atteindre et maintenir un maximum de 1000 IOPS jusqu'à ce que la situation de contention des charges de travail pour les IOPS devienne apparente sur le cluster. Les IOPS sont ensuite réduites progressivement jusqu'à ce que les IOPS sur tous les volumes se situent dans les plages QoS désignées et que la contention des performances soit soulagée.
  - Les performances sur tous les volumes sont optimisées pour atteindre le seuil minimal d'IOPS de 100. Les niveaux ne descendent pas en dessous du seuil minimal d'IOPS, mais peuvent rester supérieurs à 100 IOPS lorsque la contention de la charge de travail est soulagée.
  - Les performances ne dépassent jamais 1000 IOPS, ni ne sont inférieures à 100 IOPS de manière prolongée. Une performance de 1500 IOPS (IOPS en rafale) est autorisée, mais uniquement pour les volumes qui ont accumulé des crédits de rafale en fonctionnant en dessous du nombre maximal d'IOPS et seulement pendant de courtes périodes. Les pics de consommation ne sont jamais maintenus.

limites de valeur QoS

Voici les valeurs minimales et maximales possibles pour la QoS.

Paramètres	Valeur minimale	Défaut	4 4KB	5 8 Ko	6 16 Ko	262 Ko
IOPS minimales	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. **Les valeurs maximales d'IOPS et d'IOPS en rafale peuvent être fixées à 200 000 ; toutefois, ce paramètre n'est autorisé que pour débloquer les performances d'un volume. Les performances maximales réelles d'un volume sont limitées par l'utilisation du cluster et les performances de chaque nœud.

performances QoS

La courbe de performance QoS illustre la relation entre la taille des blocs et le pourcentage d'IOPS.

La taille des blocs et la bande passante ont un impact direct sur le nombre d'IOPS qu'une application peut obtenir. Le logiciel Element tient compte de la taille des blocs qu'il reçoit en normalisant cette taille à 4k. En fonction de la charge de travail, le système peut augmenter la taille des blocs. À mesure que la taille des blocs augmente, le système accroît sa bande passante au niveau nécessaire pour traiter ces blocs plus volumineux. À mesure que la bande passante augmente, le nombre d'IOPS que le système est capable d'atteindre diminue.

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

Par exemple, si la taille des blocs est de 4k et la bande passante de 4000 KBps, les IOPS sont de 1000. Si la taille des blocs passe à 8 ko, la bande passante passe à 5000 Ko/s et les IOPS diminuent à 625. En tenant compte de la taille des blocs, le système garantit que les charges de travail de priorité inférieure qui utilisent des tailles de blocs plus importantes, telles que les sauvegardes et les activités de l'hyperviseur, n'accaparent pas une trop grande partie des performances nécessaires au trafic de priorité supérieure utilisant des tailles de blocs plus petites.

Politiques QoS

Une politique QoS vous permet de créer et d'enregistrer un paramètre de qualité de service standardisé qui peut être appliqué à de nombreux volumes.

Les politiques QoS sont idéales pour les environnements de services, par exemple avec des serveurs de bases de données, d'applications ou d'infrastructure qui redémarrent rarement et nécessitent un accès constant et égal au stockage. La QoS de volume individuel est idéale pour les VM à faible utilisation, telles que les bureaux virtuels ou les VM spécialisées de type kiosque, qui peuvent être redémarrées, allumées ou éteintes quotidiennement ou plusieurs fois par jour.

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

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

Trouver plus d’informations

- "Documentation logicielle SolidFire et Element"