Concepts

HCI

NetApp
October 23, 2024

Sommaire

Concepts

Présentation de NetApp HCI

NetApp HCI : une infrastructure de cloud hybride haute performance qui combine le stockage, le calcul, le réseau et l'hyperviseur tout en ajoutant des fonctionnalités de clouds publics et privés.

L'infrastructure désagrégée de cloud hybride de NetApp vous permet de faire évoluer de manière indépendante vos ressources de calcul et de stockage, pour une meilleure adaptation aux workloads et des performances garanties.

- Répond aux besoins du multicloud hybride
- Possibilité de faire évoluer indépendamment les ressources de calcul et de stockage
- Simplifie l'orchestration des services de données dans tous les multiclouds hybrides

Composants de NetApp HCI

Voici un aperçu des différents composants de l'environnement NetApp HCI :

- NetApp HCI fournit à la fois des ressources de stockage et de calcul. Utilisez l'assistant **moteur de déploiement NetApp** pour déployer NetApp HCI. Une fois le déploiement terminé, les nœuds de calcul apparaissent en tant qu'hôtes ESXi et vous pouvez les gérer dans VMware vSphere Web client.
- **Les services de gestion** ou les microservices incluent le collecteur Active IQ, QoSSIOC pour le plug-in vCenter et le service de nœud M; ils sont fréquemment mis à jour en tant que packs de services. À partir de la version Element 11.3, **les services de gestion** sont hébergés sur le noeud de gestion, ce qui permet des mises à jour plus rapides de certains services logiciels en dehors des versions majeures. Le **noeud de gestion** (nœud M) est une machine virtuelle qui s'exécute en parallèle avec un ou plusieurs clusters de stockage basés sur 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.

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

- **Le contrôle du cloud hybride NetApp** vous permet de gérer NetApp HCI. Vous pouvez mettre à niveau des services de gestion, développer votre système, collecter des journaux et surveiller votre installation à l'aide de NetApp SolidFire Active IQ. Vous vous connectez au contrôle du cloud hybride NetApp en accédant à l'adresse IP du nœud de gestion.
- Le plug-in **NetApp Element pour vCenter Server** est un outil basé sur le Web intégré à l'interface utilisateur vSphere. Le plug-in est une extension et une interface conviviale pour VMware vSphere qui peuvent gérer et surveiller les clusters de stockage exécutant **le logiciel NetApp Element**. Le plug-in constitue une alternative à l'interface utilisateur d'Element. Vous pouvez utiliser l'interface utilisateur du plug-in pour détecter et configurer les clusters, ainsi que pour gérer, surveiller et allouer du stockage à partir de la capacité du cluster pour configurer des datastores et des datastores virtuels (pour les volumes virtuels). Un cluster apparaît sur le réseau comme un seul groupe local représenté aux hôtes et aux administrateurs par des adresses IP virtuelles. Vous pouvez également surveiller l'activité du cluster à l'aide de rapports en temps réel, notamment des messages d'erreur et d'alerte pour tout événement susceptible de se produire lors de l'exécution de diverses opérations.

En savoir plus sur "Plug-in NetApp Element pour vCenter Server".

- Par défaut, NetApp HCI envoie des statistiques de performances et d'alerte au service **NetApp SolidFire Active IQ**. Dans le cadre de votre contrat de support standard, le support NetApp surveille ces données et vous alerte en cas de goulot d'étranglement ou de problèmes potentiels au niveau du système. Vous devez créer un compte sur le site de support NetApp si vous ne en possédez pas encore un (même si vous disposez déjà d'un compte SolidFire Active IQ) afin de pouvoir tirer parti de ce service.

  En savoir plus sur "NetApp SolidFire Active IQ".

URL NetApp HCI

Les URL les plus courantes utilisées avec NetApp HCI sont les suivantes :

URL	Description
`https://[IPv4 address of Bond1G interface on a storage node]`	Accédez à l'assistant du moteur de déploiement NetApp pour installer et configurer NetApp HCI. "En savoir plus ."
<code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt; </code>	Accédez à NetApp HCI Hybrid Cloud Control pour mettre à niveau, développer et contrôler votre installation et mettre à jour vos services de gestion. "En savoir plus ."
`https://[IP address]:442`	À partir de l'interface utilisateur par nœud, accédez aux paramètres du réseau et du cluster et utilisez les tests et utilitaires du système. "En savoir plus ."
`https://[management node IP address]:9443`	Enregistrez le module du plug-in vCenter dans le client Web vSphere.
`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://<ManagementNodeIP>/mnode`	Mettre à jour manuellement les services de gestion à l'aide de l'interface d'API REST depuis le nœud de gestion.
`https://[storage cluster MVIP address]`	Accédez à l'interface utilisateur du logiciel NetApp Element.

Trouvez plus d'informations

- "Plug-in NetApp Element pour vCenter Server"
- "Page Ressources NetApp HCI"

Comptes d'utilisateur

Pour accéder aux ressources de stockage de votre système, vous devez configurer des comptes utilisateur.

Gestion des comptes d'utilisateurs

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.

NetApp Hybrid Cloud Control vous permet de créer et de gérer plusieurs types de comptes :

- L'administrateur compte pour le cluster de stockage
- Comptes utilisateurs autorisés
- Les comptes de volume, spécifiques uniquement au cluster de stockage sur lequel ils ont été créés.

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

Comptes utilisateurs autorisés

Les comptes utilisateurs qui font autorité peuvent s'authentifier sur toute ressource de stockage associée 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" Est le cluster de stockage utilisé par 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.

Trouvez plus d'informations

- "Gérez les comptes utilisateurs"
- "Découvrir les clusters"
- "Page Ressources NetApp HCI"
- "Plug-in NetApp Element pour vCenter Server"

Protection des données

Les termes de la protection des données NetApp HCI incluent différents types de réplication à distance, les snapshots de volume, le clonage de volumes, les domaines de protection et la haute disponibilité avec la technologie Helix double.

La protection des données NetApp HCI comprend les concepts suivants :

- 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 SolidFire
- Les domaines de protection
- 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

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 après incident et permet le basculement du stockage primaire vers le 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.

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 SolidFire vers un magasin d'objets externe ou vers un autre cluster SolidFire. Lorsque vous sauvegardez un snapshot dans un magasin d'objets externe, vous devez disposer d'une connexion au magasin d'objets qui permet des opérations de lecture/écriture.

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 SolidFire

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.

Les 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).

Une disposition de domaine de protection attribue 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 des nœuds, 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.

Vous pouvez effectuer manuellement "activez la surveillance du domaine de protection" Utilisation du 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.

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

Vous pouvez définir une disposition de domaine de protection personnalisée, où 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.

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.

Trouvez plus d'informations

- "Page Ressources NetApp HCI"
- "Plug-in NetApp Element pour vCenter Server"

Clusters

Un cluster est un groupe de nœuds qui fonctionne comme un ensemble collectif pour fournir des ressources de stockage ou de calcul. Depuis la version NetApp HCI 1.8, vous pouvez disposer d'un cluster de stockage à deux nœuds. Un cluster de stockage apparaît sur le réseau comme un seul groupe logique, qui est ensuite accessible en tant que stockage bloc.

La couche de stockage de NetApp HCI est fournie par le logiciel NetApp Element et la couche de gestion est fournie par le plug-in NetApp Element pour vCenter Server. Un nœud de stockage est un serveur qui contient un ensemble de disques qui communiquent entre eux via l'interface réseau Bond10G. Chaque nœud de stockage est relié à deux réseaux, au stockage et à la gestion, chacun disposant de deux liens indépendants pour la redondance et les performances. 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.

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 le cluster faisant autorité, vous pouvez utiliser le `GET /mnode/about` API. Dans la réponse, l'adresse IP dans `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.

Gérez les utilisateurs avec NetApp Hybrid Cloud Control.

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. 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.

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.

Clusters de stockage à deux nœuds

Depuis la version NetApp HCI 1.8, vous pouvez configurer un cluster de stockage avec deux nœuds.

- Vous pouvez utiliser certains types de nœuds pour former le cluster de stockage à deux nœuds. Voir "Notes de version de NetApp HCI 1.8".

  Dans un cluster à deux nœuds, les nœuds de stockage sont limités aux nœuds avec des disques de 480 Go et 960 Go, et les nœuds doivent être du même type de modèle.

- Les clusters de stockage à deux nœuds sont particulièrement adaptés aux déploiements à petite échelle, avec des charges de travail qui ne dépendent pas d'exigences de capacité et de performances élevées.
- En plus de deux nœuds de stockage, un cluster de stockage à deux nœuds comprend également deux **NetApp HCI Witness Nodes**.

  En savoir plus sur "Nœuds témoins."

- Vous pouvez faire évoluer un cluster de stockage à deux nœuds vers un cluster de stockage à trois nœuds. Les clusters à trois nœuds améliorent la résilience en offrant la possibilité d'effectuer une réparation automatique en cas de défaillance d'un nœud de stockage.
- Les clusters de stockage à deux nœuds offrent les mêmes fonctionnalités et fonctions de sécurité que les clusters de stockage traditionnels à quatre nœuds.
- Les clusters de stockage à deux nœuds utilisent les mêmes réseaux que les clusters de stockage à quatre nœuds. Les réseaux sont configurés durant le déploiement NetApp HCI à l'aide de l'assistant du moteur de déploiement NetApp.

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. Les nœuds témoins d'un cluster à deux nœuds sont utilisés pour s'assurer qu'il y a suffisamment de nœuds de stockage pour former un quorum d'ensemble valide. Pour la création d'ensemble, les nœuds de stockage sont préférés par rapport à Witness Nodes. Pour l'ensemble à trois nœuds minimum impliquant un cluster de stockage à deux nœuds, deux nœuds de stockage et un nœud témoin sont utilisés.

Dans un ensemble à trois nœuds avec deux nœuds de stockage et un nœud témoin, si un nœud de stockage se met hors ligne, le cluster passe en état dégradé. Parmi les deux nœuds témoins, un seul peut être actif dans l'ensemble. Le second nœud témoin ne peut pas être ajouté à l'ensemble, car il exécute le rôle de sauvegarde. Le cluster reste en état dégradé jusqu'à ce que le nœud de stockage hors ligne revienne à un état en ligne ou qu'un nœud de remplacement soit ajouté au cluster.

Si un noeud témoin échoue, le noeud témoin restant rejoint l'ensemble pour former un ensemble à trois noeuds. Vous pouvez déployer un nouveau nœud témoin pour remplacer le nœud témoin défectueux.

Auto-rétablissement et gestion des pannes dans les clusters de stockage à deux nœuds

Si un composant matériel échoue dans un nœud faisant partie d'un cluster traditionnel, le cluster peut rééquilibrer les données qui se trouvent sur le composant qui a échoué vers d'autres nœuds disponibles du cluster. Cette fonction d'autorétablissement n'est pas disponible dans un cluster de stockage à deux nœuds, car un minimum de trois nœuds de stockage physiques doivent être disponibles pour le cluster afin d'assurer une réparation automatique. Lorsqu'un nœud d'un cluster à deux nœuds tombe en panne, le cluster à deux nœuds ne nécessite pas la régénération d'une seconde copie des données. Les nouvelles écritures sont répliquées pour les données de bloc dans le nœud de stockage actif restant. Lorsque le nœud défaillant est remplacé et rejoint le cluster, les données sont rééquilibrées entre les deux nœuds de stockage physique.

Clusters de stockage avec trois nœuds ou plus

Grâce à l'extension de deux nœuds de stockage à trois nœuds, votre cluster est plus résilient. Il favorise des fonctionnalités d'autorétablissement en cas de panne de nœud et de disque, mais n'offre pas de capacité supplémentaire. Vous pouvez développer à l'aide du "Interface de contrôle du cloud hybride NetApp". Lorsque vous étendez votre système d'un cluster à deux nœuds à un cluster à trois nœuds, la capacité peut être inutilisée (voir la La capacité inutilisée). L'assistant de l'interface utilisateur affiche des avertissements concernant la capacité inutilisée avant l'installation. Un seul nœud témoin est toujours disponible pour conserver le quorum de l'ensemble en cas de défaillance d'un nœud de stockage, avec un second nœud témoin en veille. Lorsque vous étendez un cluster de stockage à trois nœuds à un cluster à quatre nœuds, la capacité et les performances sont améliorées. Dans un cluster à quatre nœuds, Witness Nodes ne sont plus nécessaires pour former le quorum du cluster. Vous pouvez étendre jusqu'à 64 nœuds de calcul et 40 nœuds de stockage.

Trouvez plus d'informations

- "Cluster de stockage à deux nœuds NetApp HCI | TR-4823"
- "Plug-in NetApp Element pour vCenter Server"
- "Centre de documentation des logiciels SolidFire et Element"

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.

Les logiciels NetApp HCI et Element définissent différents rôles de nœud pour un cluster. Les quatre types de rôles de nœud sont **noeud de gestion**, **noeud de stockage**, **noeud de calcul** et **noeud témoin NetApp HCI**.

Nœud de gestion

Le nœud de gestion (parfois abrégé en nœud M) 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.

Le nœud de gestion est une machine virtuelle (VM) qui s'exécute en parallèle avec un ou plusieurs clusters de stockage logiciels Element. Outre les mises à niveau, il fournit des services système comprenant la surveillance et la télémétrie, une gestion des ressources et des paramètres du cluster, des tests système et des utilitaires. Il permet également d'activer l'accès au support NetApp pour la résolution de problèmes. 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, comme le collecteur Active IQ, les QoSSIOC pour le plug-in vCenter et le service de nœuds de gestion, sont fréquemment mis à jour en tant que packs de services.

Nœuds de stockage

Les nœuds de stockage NetApp HCI sont matériels qui fournissent les ressources de stockage d'un système NetApp HCI. 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 nœuds de stockage NetApp HCI peuvent être gérés à l'aide du point d'extension de gestion NetApp Element.

Nœuds de calcul

Les nœuds de calcul NetApp HCI sont matériels qui fournissent des ressources de calcul, telles que le processeur, la mémoire et les ressources réseau, nécessaires à la virtualisation lors de l'installation de NetApp HCI. Comme chaque serveur exécute VMware ESXi, la gestion du nœud de calcul NetApp HCI (ajout ou suppression d'hôtes) doit être effectuée en dehors du plug-in dans le menu hôtes et clusters de vSphere. Qu'il s'agisse d'un cluster de stockage à quatre nœuds ou d'un cluster de stockage à deux nœuds, le nombre minimal de nœuds de calcul reste deux pour un déploiement NetApp HCI.

Nœuds témoins

Les nœuds NetApp HCI Witness sont des machines virtuelles qui s'exécutent sur des nœuds de calcul en parallèle avec un cluster de stockage basé sur le logiciel Element. Les nœuds témoins n'hébergent pas les services de tranche ou de bloc. Un nœud Witness permet la disponibilité du cluster de stockage en cas de défaillance d'un nœud de stockage. Vous pouvez gérer et mettre à niveau les nœuds Witness de la même manière que les autres nœuds de stockage. Un cluster de stockage peut disposer d'un maximum de quatre nœuds témoin. Leur but principal est de s'assurer qu'il existe suffisamment de nœuds de grappe pour former un quorum d'ensemble valide.

Meilleure pratique : configurer les machines virtuelles du nœud témoin pour utiliser le datastore local du nœud de calcul (défini par défaut par NDE), ne les configurer pas sur du stockage partagé, comme les volumes de stockage SolidFire. Pour empêcher la migration automatique des machines virtuelles, définissez le niveau d'automatisation DRS (Distributed Resource Scheduler) de la machine virtuelle Witness Node sur **Disabled**. Cela empêche les deux nœuds témoin de s'exécuter sur le même nœud de calcul et de créer une configuration de paire haute disponibilité.

En savoir plus sur "Conditions requises pour les ressources du nœud témoin" et "Exigences relatives à l'adresse IP du nœud témoin".

Dans un cluster de stockage à deux nœuds, au moins deux nœuds Witness sont déployés pour assurer la redondance en cas de défaillance du nœud témoin. Lorsque le processus d'installation de NetApp HCI installe Witness Nodes, un modèle de machine virtuelle est stocké dans VMware vCenter que vous pouvez utiliser pour redéployer un nœud témoin s'il est accidentellement retiré, perdu ou corrompu. Vous pouvez également utiliser le modèle pour redéployer un nœud témoin si vous devez remplacer un nœud de calcul défaillant qui héberge le nœud Witness. Pour obtenir des instructions, consultez la section **Redeploy Witness Nodes clusters de stockage à deux et trois nœuds** "ici".

Trouvez plus d'informations

- "Cluster de stockage à deux nœuds NetApp HCI | TR-4823"
- "Plug-in NetApp Element pour vCenter Server"
- "Centre de documentation des logiciels SolidFire et Element"

Stockage

Mode Maintenance

Si vous devez mettre un nœud de stockage hors ligne pour des opérations de maintenance telles que les mises à niveau logicielles ou la réparation d'hôte, vous pouvez réduire l'impact sur les E/S au reste du cluster de stockage en activant le mode de maintenance pour ce nœud. Vous pouvez utiliser le mode de maintenance avec les deux nœuds de dispositif et les nœuds SolidFire Enterprise SDS.

Lorsqu'un nœud de stockage est hors tension, il s'affiche sous la forme **indisponible** dans la colonne État du nœud de la page stockage de HCC, car cette colonne affiche l'état du nœud du point de vue du cluster. L'état hors tension du nœud est indiqué par l'icône **hors ligne** en regard du nom d'hôte du nœud.

Vous pouvez passer d'un nœud de stockage en mode maintenance uniquement si le nœud fonctionne correctement (ne présente pas de blocage des défaillances de cluster) et si le cluster de stockage est tolérant à une panne de nœud unique. Une fois que vous activez le mode de maintenance pour un nœud sain et tolérant, le nœud n'est pas immédiatement transféré. Il est surveillé jusqu'à ce que les conditions suivantes soient vraies :

- Tous les volumes hébergés sur le nœud ont fait l'objet d'une panne

- Le nœud n'héberge plus la base d'un volume
- Un nœud de veille temporaire est attribué pour chaque volume en cours de basculement

Lorsque ces critères sont remplis, le nœud est passé en mode maintenance. Si ces critères ne sont pas remplis au cours d'une période de 5 minutes, le nœud n'entrera pas en mode de maintenance.

Lorsque vous désactivez le mode de maintenance pour un nœud de stockage, le nœud est surveillé jusqu'à ce que les conditions suivantes soient vraies :

- Toutes les données sont entièrement répliquées vers le nœud
- Toutes les défaillances de bloc d'instruments de blocage sont résolues
- Toutes les affectations de noeuds de secours temporaires pour les volumes hébergés sur le noeud ont été inactivées

Une fois ces critères remplis, le nœud est mis hors mode maintenance. Si ces critères ne sont pas remplis dans une heure, le nœud ne pourra pas basculer en mode de maintenance à partir du nœud.

Vous pouvez voir les États des opérations en mode maintenance lorsque vous travaillez avec le mode maintenance à l'aide de l'API Element :

- **Désactivé** : aucune maintenance n'a été demandée.
- **FailedToRecover** : le nœud n'a pas pu récupérer à partir de la maintenance.
- **Recovery ingFromMaintenance**: Le noeud est en cours de récupération à partir de la maintenance.
- **PréparingForMaintenance** : des actions sont en cours pour permettre à un noeud d'effectuer la maintenance.
- **ReadyForMaintenance** : le nœud est prêt à effectuer la maintenance.

Trouvez plus d'informations

- "Activez le mode maintenance avec l'API Element"
- "Désactivez le mode de maintenance avec l'API Element"
- "Documentation de l'API NetApp Element"
- "Page Ressources NetApp HCI"
- "Plug-in NetApp Element pour vCenter Server"

Volumes

Le stockage est provisionné dans le système NetApp Element en tant que volumes. Les volumes sont des périphériques de bloc accessibles sur le réseau à l'aide de clients iSCSI ou Fibre Channel.

Le plug-in NetApp Element pour vCenter Server 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.

Si vous déployez un nœud de gestion pour NetApp HCI à l'aide du moteur de déploiement NetApp, les volumes persistants sont automatiquement activés et configurés.

Une option permettant d'activer les volumes persistants est incluse dans l'installation et la mise à niveau des scripts lors du 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 avec NetApp-HCI- prépachevé au nom du cluster attribué. 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

Trouvez plus d'informations

- "Gérer les volumes"
- "Plug-in NetApp Element pour vCenter Server"
- "Centre de documentation des logiciels SolidFire et Element"

Groupes d'accès de volume

Un groupe d'accès de volume est une collection de volumes auxquels les utilisateurs peuvent accéder via des initiateurs iSCSI ou Fibre Channel.

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 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.

Trouvez plus d'informations

- "Gérez les groupes d'accès aux volumes"
- "Plug-in NetApp Element pour vCenter Server"

- "Centre de documentation des logiciels SolidFire et Element"

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.

Trouvez plus d'informations

- "Gestion des initiateurs"
- "Groupes d'accès de volume"
- "Gérez les groupes d'accès aux volumes"
- "Plug-in NetApp Element pour vCenter Server"
- "Centre de documentation des logiciels SolidFire et Element"

Domaines de protection personnalisés

Vous pouvez définir une disposition de domaine de protection personnalisée, où 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 :

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

Si plusieurs domaines de protection personnalisés sont affectés, chaque sous-système attribue 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.

> L'utilisation de domaines de protection personnalisés suppose qu'aucun nœud ne partage de châssis.

Les méthodes d'API Element suivantes exposent ces nouveaux domaines de protection :

- GetProtectionDomainLayout - affiche le châssis et le domaine de protection personnalisé de chaque nœud.
- SetProtectionDomainLayout - permet d'affecter un domaine de protection personnalisé à chaque nœud.

Contactez la prise en charge de NetApp pour plus d'informations sur l'utilisation de domaines de protection personnalisés.

Trouvez plus d'informations

"Gérez le stockage avec l'API Element"

Licences NetApp HCI

Lorsque vous utilisez NetApp HCI, vous devrez peut-être disposer de licences supplémentaires selon ce que vous utilisez.

Licences NetApp HCI et VMware vSphere

La licence VMware vSphere dépend de votre configuration :

Option de mise en réseau	Licences
Option A : deux câbles pour les nœuds de calcul utilisant le balisage VLAN (tous les nœuds de calcul)	Nécessite l'utilisation de vSphere Distributed Switch, qui nécessite une licence VMware vSphere Enterprise plus.
Option B : six câbles pour les nœuds de calcul utilisant des VLAN balisés (nœud de calcul 2RU H410C à 4 nœuds)	Cette configuration utilise le commutateur standard vSphere par défaut. L'utilisation en option du switch distribué vSphere nécessite une licence VMware Enterprise plus.
Option C : six câbles pour les nœuds de calcul utilisant des VLAN natifs et balisés (nœud de calcul H410C, 2RU à 4 nœuds)	Cette configuration utilise le commutateur standard vSphere par défaut. L'utilisation en option du switch distribué vSphere nécessite une licence VMware Enterprise plus.

Licences NetApp HCI et ONTAP Select

Si vous avez reçu une version de ONTAP Select pour une utilisation conjointe avec un système NetApp HCI acheté, les limites supplémentaires suivantes s'appliquent :

- La licence ONTAP Select, qui est intégrée à la vente de systèmes NetApp HCI, ne peut être utilisée qu'avec des nœuds de calcul NetApp HCI.
- Le stockage de ces instances ONTAP Select doit résider uniquement sur les nœuds de stockage NetApp HCI.
- Il est interdit d'utiliser des nœuds de calcul tiers ou des nœuds de stockage tiers.

Trouvez plus d'informations

- "Plug-in NetApp Element pour vCenter Server"
- "Centre de documentation des logiciels SolidFire et Element"

Valeurs maximales de configuration NetApp pour Cloud Control

NetApp HCI inclut NetApp Hybrid Cloud Control pour simplifier la gestion du cycle de vie du calcul et du stockage. Cette solution prend en charge les mises à niveau du logiciel Element sur des nœuds de stockage pour les clusters de stockage NetApp HCI et NetApp SolidFire, ainsi que les mises à niveau du firmware pour les nœuds de calcul NetApp HCI dans NetApp HCI. Elle est disponible par défaut sur les nœuds de gestion dans NetApp HCI.

Outre la communication des composants matériels et logiciels fournis par NetApp dans une installation NetApp HCI, NetApp Hybrid Cloud Control interagit avec des composants tiers dans l'environnement client, tels que VMware vCenter. NetApp qualifie la fonctionnalité de NetApp de cloud hybride Control et son interaction avec ces composants tiers dans l'environnement du client à une certaine échelle. Pour optimiser l'expérience avec NetApp Hybrid Cloud Control, NetApp recommande de rester dans la plage maximale de configuration.

Si vous dépassez ces limites testées, la commande de cloud hybride NetApp peut rencontrer des problèmes avec une interface utilisateur et des réponses d'API plus lentes ou fonctionnalité n'étant pas disponible. Si vous faites appel à NetApp pour la prise en charge des produits avec NetApp Cloud Control dans des environnements configurés en dehors des limites de configuration, le support NetApp vous demande de modifier la configuration afin qu'elle respecte les valeurs maximales de configuration documentées.

Valeurs maximales de configuration

NetApp Hybrid Cloud Control prend en charge les environnements VMware vSphere avec jusqu'à 500 nœuds de calcul NetApp. Il prend en charge jusqu'à 20 clusters de stockage NetApp Element avec 40 nœuds de stockage par cluster.

Sécurité NetApp HCI

Lorsque vous utilisez NetApp HCI, les données sont protégées par des protocoles de sécurité standard.

Chiffrement des données au repos pour les nœuds de stockage

NetApp HCI vous permet de chiffrer toutes les données stockées sur le cluster de stockage.

Tous les disques d'un nœud de stockage qui peuvent être chiffrées utilisent 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 au niveau du cluster de stockage 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. Vous avez besoin du mot de passe pour déverrouiller le lecteur, et puisque le lecteur cryptage toutes les données, vos données sont sécurisées en permanence.

Lorsque le chiffrement est activé au repos, les performances et l'efficacité du cluster de stockage ne sont pas affectées. En outre, si vous supprimez un disque ou un nœud compatible avec le chiffrement du cluster de stockage avec l'API Element ou l'interface utilisateur d'Element, le chiffrement au repos est désactivé sur les disques et les disques sont supprimés de manière sécurisée, ce qui protège les données précédemment stockées sur ces disques. Après avoir retiré le lecteur, vous pouvez l'effacer en toute sécurité avec le `SecureEraseDrives` Méthode API. Si vous retirez de force un disque ou un nœud du cluster de stockage, les données restent protégées par le mot de passe de tout le cluster et les clés de cryptage individuelles du

disque.

Pour plus d'informations sur l'activation et la désactivation du chiffrement au repos, reportez-vous à la section "Activation et désactivation du cryptage pour un cluster" Dans le Centre de documentation SolidFire et Element.

Chiffrement logiciel au repos

Le chiffrement logiciel au repos permet le chiffrement de toutes les données écrites sur les disques SSD d'un cluster de stockage. Cela fournit une couche principale de cryptage dans les nœuds SolidFire Enterprise SDS, qui n'incluent pas les disques à autocryptage (SED).

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 section "Mise en route de la gestion externe des clés" Dans le Centre de documentation SolidFire et Element.

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 "Activation de l'authentification multifacteur" Dans le Centre de documentation SolidFire et Element.

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

Les clusters de stockage NetApp SolidFire et les systèmes NetApp HCI prennent en charge le chiffrement conforme à la norme FIPS 140-2 pour les modules cryptographiques. Vous pouvez activer la conformité FIPS 140-2 sur votre cluster NetApp HCI ou SolidFire pour les communications HTTPS et le chiffrement de disque.

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 le

`EnableFeature` API d'Element avec le `fips` Paramètre pour activer le chiffrement FIPS 140-2 HTTPS. Sur les clusters de stockage avec du matériel compatible FIPS, vous pouvez également activer le chiffrement de disque FIPS pour les données au repos à l'aide du `EnableFeature` API d'Element avec le `FipsDrives` paramètre.

Pour plus d'informations sur la préparation d'un nouveau cluster de stockage à des fins de chiffrement FIPS 140-2, reportez-vous à la section "Création d'un cluster prenant en charge les disques FIPS".

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

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 ses IOPS max. Jusqu'à son niveau d'IOPS en rafale pour une « période définie ». Un volume peut monter en charge jusqu'à 60 secondes si le cluster est capable de répondre aux besoins en 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

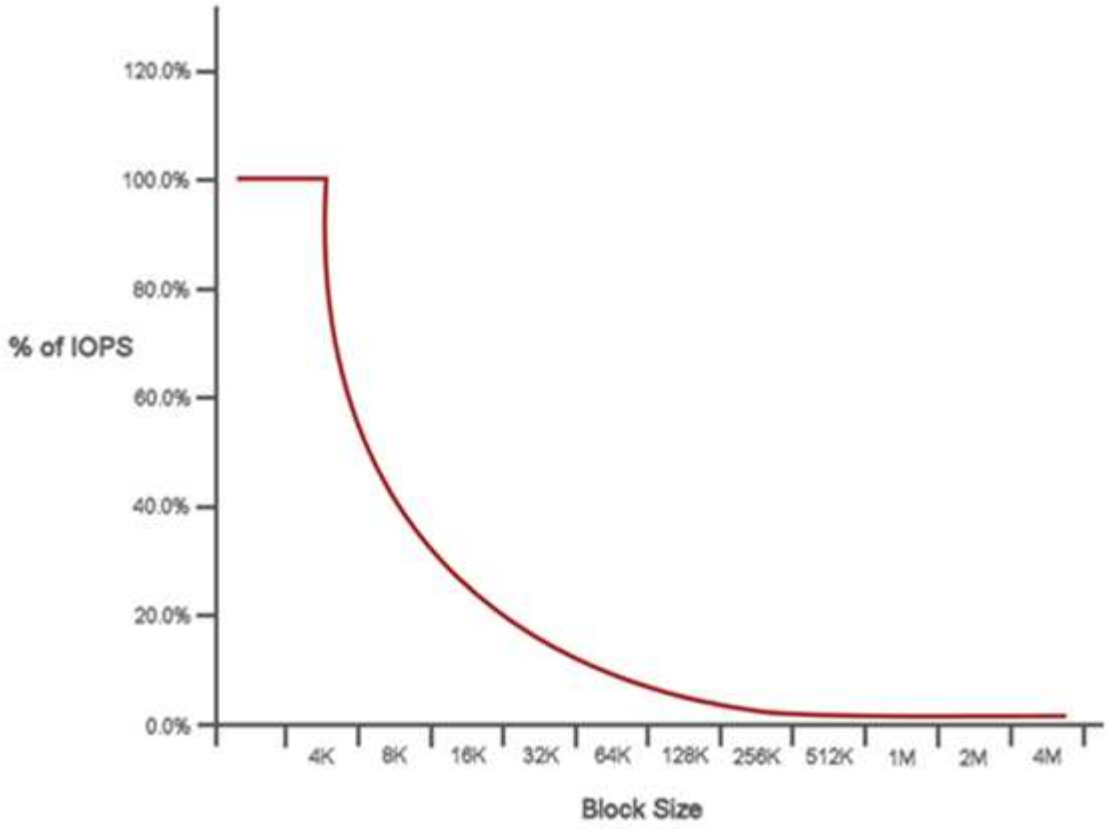
*Ces estimations sont approximatives. **IOPS max et IOPS en rafale peuvent être définis sur 200,000 ; cependant, ce paramètre est uniquement autorisé à uncaréellement les performances d'un volume. Les performances maximales réelles d'un volume sont limitées par l'utilisation du cluster et les performances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

- "Plug-in NetApp Element pour vCenter Server"
- "Page Ressources NetApp HCI"