Administration de VMware vSAN

VMware vSphere 8.0
VMware vSAN 8.0

Vous trouverez la documentation technique la plus récente sur le site Web de VMware, à l'adresse :

https://docs.vmware.com/fr/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Table des matières

À propos de l'administration de VMware vSAN

Administration de VMware vSAN décrit la configuration et la gestion d'un cluster vSAN dans un environnement VMware vSphere®. De plus, l'*Administration de VMware vSAN* explique comment gérer les ressources de stockage physique local servant de périphériques de capacité de stockage dans un cluster vSAN et définir les stratégies de stockage de machines virtuelles déployées vers des banques de données vSAN.

VMware prend l'intégration au sérieux. Afin de promouvoir ce principe pour notre client, nos partenaires et la communauté interne, nous créons du contenu à l'aide du langage inclusif.

Public cible

Ces informations s'adressent à des administrateurs de virtualisation expérimentés qui maîtrisent la technologie de virtualisation, les opérations quotidiennes associées aux centres de données et les concepts vSAN.

Pour plus d'informations sur vSAN et sur comment créer un cluster vSAN, reportez-vous au *Guide de Planification et déploiement de vSAN*.

Pour plus d'informations sur la surveillance d'un vSAN cluster et la résolution de problèmes, reportez-vous au *guide de surveillance et dépannage de vSAN*.

Présentation de vSAN 1

VMware vSAN est une couche distribuée de logiciel qui s'exécute nativement en tant que partie de l'hyperviseur ESXi. vSAN cumule des périphériques de capacité locaux ou à connexion directe d'un cluster hôte et crée un pool de stockage unique partagé sur tous les hôtes du cluster vSAN.

Tout en prenant en charge les fonctionnalités de VMware qui nécessitent un stockage partagé, telles que HA, vMotion et DRS, vSAN élimine la nécessité d'un stockage externe partagé et simplifie la configuration du stockage ainsi que les activités de provisionnement de machine virtuelle.

Ce chapitre contient les rubriques suivantes :

Concepts vSAN

VMware vSAN utilise une approche définie par logiciel pour créer le stockage partagé pour les machines virtuelles. Il virtualise les ressources de stockage physique local des hôtes ESXi et les transforme en pools de stockage pouvant être divisés et attribués à des machines virtuelles et à des applications en fonction de leurs conditions requises en termes de qualité de service. vSAN est mise en œuvre directement dans l'hyperviseur ESXi.

Vous pouvez configurer vSAN pour fonctionner comme un cluster hybride ou intégralement Flash. Dans les cluster hybrides, les périphériques Flash sont utilisés pour la couche de cache et les disques magnétiques sont utilisés pour la couche de capacité de stockage. Dans les clusters intégralement Flash, des périphériques Flash sont utilisés à la fois pour le cache et la capacité.

Vous pouvez activer vSAN sur vos clusters hôtes existants et lors de la création de nouveaux clusters. vSAN agrège tous les périphériques de capacité locaux en une banque de données unique partagée par tous les hôtes du cluster vSAN. Vous pouvez développer la banque de données en ajoutant des périphériques de capacité ou des hôtes avec périphériques de capacité au cluster. vSAN fonctionne mieux lorsque tous les hôtes ESXi dans le cluster partagent des configurations similaires ou identiques avec tous les membres du cluster, y compris des configurations de stockage similaires ou identiques. Cette configuration cohérente équilibre les composants de stockage de machine virtuelle dans tous les périphériques et hôtes du cluster. Les hôtes sans aucun périphérique local peuvent également participer et exécuter leurs machines virtuelles sur la banque de données vSAN.

Dans vSAN Original Storage Architecture, chaque hôte contribuant aux périphériques de stockage de la banque de données vSAN doit fournir au moins un périphérique pour le cache Flash et au moins un périphérique pour la capacité. Les périphériques situés sur l'hôte contributeur forment un ou plusieurs groupes de disques. Chaque groupe de disques contient un périphérique cache Flash ou un ou plusieurs périphériques de capacité pour le stockage permanent. Chaque hôte peut être configuré pour utiliser plusieurs groupes de disques.

Dans vSAN Express Storage Architecture, tous les périphériques de stockage réclamés par vSAN contribuent à la capacité et aux performances. Les périphériques de stockage de chaque hôte réclamés par vSAN forment un pool de stockage. Le pool de stockage représente la quantité de mise en cache et de capacité fournie par l'hôte à la banque de données vSAN.

Pour obtenir des conseils, des informations sur la capacité et des recommandations générales sur la conception et le dimensionnement d'un cluster vSAN, reportez-vous au *Guide de dimensionnement et de conception de VMware vSAN*.

Caractéristiques de vSAN

Cette rubrique récapitule les caractéristiques qui s'appliquent à vSAN, ses clusters et banques de données.

vSAN fournit de nombreux avantages à votre environnement.

Tableau 1-1. Fonctionnalitéss vSAN

Fonctionnalités prises en charge	Description
Prise en charge du stockage partagé	vSAN prend en charge des fonctions VMware qui nécessitent un stockage partagé, telles que HA, vMotion et DRS. Par exemple, si un hôte devient surchargé, DRS peut migrer des machines virtuelles vers d'autres hôtes du cluster.
Format sur disque	Le format de fichier virtuel sur disque de vSAN fournit une prise en charge extrêmement évolutive de la gestion de snapshots et de clones par cluster vSAN. Pour plus d'informations sur le nombre de snapshots et de clones de machine virtuelle pris en charge par cluster vSAN, reportez-vous à la documentation *Configurations maximales*.
Configurations intégralement Flash et hybrides	vSAN peut être configuré pour un cluster intégralement Flash ou hybride.

Tableau 1-1. Fonctionnalitéss vSAN (suite)

Fonctionnalités prises en charge	Description
Domaines de pannes	vSAN prend en charge la configuration des domaines de pannes pour protéger les hôtes des pannes de rack ou de châssis lorsque le cluster vSAN couvre plusieurs racks ou châssis de serveurs lames dans un centre de données.
service cible iSCSI	Le service cible iSCSI vSAN permet aux hôtes et aux charges de travail physiques qui résident en dehors du cluster vSAN d'accéder à la banque de données vSAN.
Cluster étendu	vSAN prend en charge les clusters étendus couvrant deux emplacements géographiques.
Prise en charge des clusters de basculement Windows Server (WSFC)	vSAN 6.7 Update 3 et les versions ultérieures prennent en charge les réservations persistantes SCSI-3 (SCSI3-PR) sur un niveau de disque virtuel requis par le cluster de basculement Windows Server (WSFC) pour arbitrer un accès à un disque partagé entre des nœuds. La prise en charge de des PR SCSI-3 permet la configuration de WSFC avec une ressource de disque partagée entre des machines virtuelles en mode natif sur des banques de données vSAN. Actuellement, les configurations suivantes sont prises en charge : ■ Jusqu'à 6 nœuds d'application par cluster. ■ Jusqu'à 64 disques virtuels partagés par nœud. **Note** Microsoft SQL Server 2012 ou version ultérieure s'exécutant sur Microsoft Windows Server 2012 ou version ultérieure a été qualifié sur vSAN.
service de santé vSAN	Le service de santé vSAN inclut des tests de contrôle de santé préconfigurés pour surveiller, dépanner, diagnostiquer la cause de problèmes de composants de cluster et identifier les risques potentiels.
service de performance vSAN	Le service de performance de vSAN inclut des graphiques statistiques utilisés pour surveiller l'IOPS, le débit, la latence et la congestion. Vous pouvez surveiller les performances d'un cluster, d'un hôte, d'un groupe de disques, d'un disque et de machines virtuelles vSAN.
Intégration avec les fonctionnalités de stockage de vSphere	vSAN s'intègre aux fonctions de gestion de données de vSphere traditionnellement utilisées avec un stockage VMFS et NFS. Ces fonctionnalités incluent les snapshots, les clones liés et vSphere Replication.
Stratégies de stockage de machine virtuelle	vSAN utilise des stratégies de stockage VM pour prendre en charge une approche à la gestion du stockage centrée sur les machines virtuelles. Si vous n'attribuez pas de stratégie de stockage à la machine virtuelle lors du déploiement, la stratégie de stockage vSAN par défaut est automatiquement attribuée à la machine virtuelle.
Provisionnement rapide	vSAN permet le provisionnement rapide du stockage dans vCenter Server® pendant les opérations de création et de déploiement de machine virtuelle.

Tableau 1-1. Fonctionnalitéss vSAN (suite)

Fonctionnalités prises en charge	Description
Déduplication et compression	vSAN effectue une déduplication et une compression au niveau des blocs pour économiser l'espace de stockage. Lorsque vous activez la déduplication et la compression sur un cluster vSAN intégralement Flash, les données redondantes dans chaque groupe de disques sont réduites. La déduplication et la compression sont activées en tant que paramètres à l'échelle du cluster, mais elles sont appliquées au niveau du groupe de disques. Le vSAN de compression seule est appliqué sur une base par disque.
Chiffrement des données au repos	vSAN assure le chiffrement des données au repos. Les données sont chiffrées une fois que tous les autres traitements, tels que la déduplication, ont été effectués. Le chiffrement des données au repos protège les données sur les périphériques de stockage au cas où l'un d'entre eux serait supprimé du cluster.
Prise en charge du SDK	VMware vSAN SDK est une extension de VMware vSphere Management SDK. Ce SDK comprend de la documentation, des bibliothèques et des exemples de code qui permettent aux développeurs d'automatiser l'installation, la configuration, la surveillance et le dépannage de vSAN.

Termes et définitions vSAN

vSAN introduit des termes et définitions spécifiques importants à comprendre.

Avant de commencer avec vSAN, passez en revue les termes et définitions vSAN clés.

Groupe de disques (vSAN Original Storage Architecture)

Un groupe de disques est une unité de capacité et de performances de stockage physique sur un hôte et un groupe de périphériques physiques fournissant des performances et de la capacité au cluster vSAN. Sur chaque hôte ESXi qui met à disposition ses périphériques locaux dans un cluster vSAN, les périphériques sont organisés en groupes de disques.

Chaque groupe de disques doit comporter un périphérique de cache Flash et un ou plusieurs périphériques de capacité. Les périphériques utilisés pour le cache ne peuvent pas être partagés entre groupes de disques, et ne peuvent pas être utilisés à d'autres fins. Un périphérique de mise en cache unique doit être dédié à un groupe de disques unique. Dans les cluster hybrides, les périphériques Flash sont utilisés pour la couche de cache et les disques magnétiques sont utilisés pour la couche de capacité de stockage. Dans un cluster intégralement Flash, des périphériques Flash sont utilisés à la fois pour le cache et la capacité. Pour plus d'informations sur la création et la gestion de groupes de disques, reportez-vous à la section *Administration de VMware vSAN*.

Pool de stockage (vSAN Express Storage Architecture)

Un pool de stockage est une représentation de tous les périphériques de stockage sur un hôte réclamés par vSAN. Chaque hôte contient un pool de stockage. Chaque périphérique du pool de stockage contribue à la fois à la capacité et aux performances. Le nombre de périphériques de stockage autorisés est déterminé par la configuration de l'hôte.

Capacité consommée

La capacité consommée est la quantité de capacité physique consommée par une ou plusieurs machines virtuelles à tout moment. Plusieurs facteurs déterminent la capacité consommée, notamment la taille consommée de vos VMDK, des réplicas de protection, etc. Lors du calcul du dimensionnement du cache, ne tenez pas compte de la capacité utilisée pour les réplicas de protection.

Stockage basé sur un objet

vSAN stocke et gère les données sous la forme de conteneurs de données flexibles nommés objets. Un objet est un volume logique dont les données et métadonnées sont distribuées dans le cluster. Par exemple, chaque VMDK est un objet, tout comme chaque snapshot. Lorsque vous provisionnez une machine virtuelle sur une banque de données vSAN, vSAN crée un jeu d'objets constitué de plusieurs composants pour chaque disque virtuel. Il crée également l'espace de noms de base de la machine virtuelle qui est un objet de conteneur stockant tous les fichiers de métadonnées de votre machine virtuelle. En fonction de la stratégie de stockage de machine virtuelle attribuée, vSAN provisionne et gère chaque objet, individuellement, ce qui peut impliquer également de créer une configuration RAID pour chaque objet.

Note Si vSAN Express Storage Architecture est activé, chaque snapshot n'est pas un nouvel objet. Un VMDK de base et ses snapshots sont contenus dans un objet vSAN. En outre, dans vSAN ESA, le résumé repose sur des objets vSAN.

Lorsque vSAN crée un objet pour un disque virtuel et détermine comment distribuer l'objet dans le cluster, il tient compte des facteurs suivants :

- vSAN vérifie que la configuration requise pour le disque virtuel est appliquée conformément aux paramètres de la stratégie de stockage de la machine virtuelle spécifiée.
- vSAN vérifie que les ressources de cluster adéquates sont utilisées lors du provisionnement. Par exemple, vSAN détermine le nombre de réplicas à créer en fonction de la stratégie de protection. La stratégie de performances détermine la quantité de cache de lecture Flash allouée à chaque réplica, le nombre de bandes à créer pour chacune d'elles et leur emplacement dans le cluster.

- vSAN surveille et crée des rapports en continu sur l'état de conformité de la stratégie du disque virtuel. En cas d'état de non-conformité de la stratégie, vous devez résoudre le problème sous-jacent.

  Note Le cas échéant, vous pouvez modifier les paramètres de la stratégie de stockage de la machine virtuelle. Cela n'affecte en rien l'accès à la machine virtuelle. vSAN limite activement le stockage et les ressources du réseau utilisés pour la reconfiguration afin de minimiser l'impact de la reconfiguration d'objet sur des charges de travail normales. Lorsque vous modifiez les paramètres d'une stratégie de stockage de machine virtuelle, vSAN peut démarrer un processus de recréation d'objets qui est suivi de la resynchronisation. Reportez-vous à la section *Surveillance et dépannage de vSAN*.

- vSAN vérifie que les composants de protection requis, comme les miroirs et les témoins, sont placés sur des hôtes ou des domaines de pannes distincts. Par exemple, pour recréer des composants pendant une panne, vSAN recherche des hôtes ESXi satisfaisant aux règles de placement selon lesquelles les composants de protection d'objets de machine virtuelle doivent être placés sur deux hôtes distincts ou dans des domaines de pannes.

Banque de données vSAN

Une fois que vous activez vSAN sur un cluster, une banque de données vSAN unique est créée. Elle s'affiche comme un autre type de banque de données dans la liste des banques de données susceptibles d'être disponibles, notamment Virtual Volume, VMFS et NFS. Une seule banque de données vSAN fournit différents niveaux de service pour chaque machine virtuelle ou chaque disque virtuel. Dans vCenter Server®, les caractéristiques de stockage de la banque de données vSAN s'affichent sous la forme d'un ensemble de capacités. Vous pouvez référencer ces capacités lors de la définition d'une stratégie de stockage pour machines virtuelles. Lors du déploiement ultérieur des machines virtuelles, vSAN utilise cette stratégie pour placer les machines virtuelles de manière optimale en fonction de la configuration requise de chaque machine virtuelle. Pour plus d'informations sur l'utilisation de stratégies de stockage, reportez-vous à la documentation *Stockage vSphere*.

Une banque de données vSAN a des caractéristiques spécifiques à prendre en compte.

- vSAN fournit une banque de données vSAN unique accessible par tous les hôtes du cluster, qu'ils contribuent ou non au stockage sur le cluster. Chaque hôte peut également monter d'autres banques de données, comme Virtual Volumes, VMFS ou NFS.
- Vous pouvez utiliser Storage vMotion pour déplacer des machines virtuelles entre des banques de données vSAN, NFS et VMFS.
- Seuls les disques magnétiques et les périphériques Flash utilisés pour la capacité peuvent contribuer à la capacité de la banque de données. Les périphériques utilisés pour le cache Flash ne sont pas considérés comme faisant partie de la banque de données.

Objets et composants

Chaque objet est constitué d'un ensemble de composants, déterminé par les capacités utilisées dans la stratégie de stockage de machine virtuelle. Par exemple, lorsque **Pannes tolérées** est configuré sur 1, vSAN vérifie que les composants de protection, comme les réplicas et les témoins, sont placés sur des hôtes distincts dans le cluster vSAN, où chaque réplica est un composant de l'objet. De plus, toujours dans cette stratégie, si **Nombre de bandes de disque par objet** est configuré sur 2 ou plus, vSAN agrège également l'objet par bandes dans divers périphériques de capacité et chaque bande est considérée comme un composant de l'objet spécifié. Au besoin, vSAN peut également partitionner des objets volumineux en plusieurs composants.

Une banque de données vSAN contient les types d'objets suivants :

Espace de noms de base de la VM

Répertoire de base de la machine virtuelle dans lequel sont stockés tous les fichiers de configuration de la machine virtuelle, comme les fichiers `.vmx`, les fichiers de journalisation, les vmdk et les fichiers de description delta de snapshot.

VMDK

Disque de machine virtuelle ou fichier `.vmdk` qui stocke le contenu du lecteur de disque dur d'une machine virtuelle.

Objet de permutation de machine virtuelle

Créé lorsqu'une machine virtuelle est mise sous tension.

VMDK delta de snapshot

Créés lorsque des snapshots de machine virtuelle sont pris. Ces disques delta ne sont pas créés pour vSAN Express Storage Architecture.

Objet de mémoire

Créé lorsque l'option de mémoire de snapshot est sélectionnée au moment de la création ou de l'interruption d'une machine virtuelle.

État de conformité d'une machine virtuelle : Conforme et Non conforme

Une machine virtuelle est considérée comme non conforme lorsqu'un ou plusieurs de ses objets échouent à répondre aux conditions requises de sa stratégie de stockage attribuée. Par exemple, l'état peut devenir non conforme lorsque l'une des copies miroirs est inaccessible. Si vos machines virtuelles sont en conformité avec l'exigence définie dans la stratégie de stockage, l'état de vos machines virtuelles est conforme. Dans l'onglet **Emplacement physique du disque** sur la page **Disques virtuels**, vous pouvez vérifier l'état de conformité de l'objet de la machine virtuelle. Pour plus d'informations sur le dépannage d'un cluster vSAN, reportez-vous à la section *Surveillance et dépannage de vSAN*.

État des composants : états Dégradé et Absent

vSAN reconnaît les états de pannes suivants pour les composants :

- Dégradé. Un composant est Dégradé lorsque vSAN détecte la panne permanente d'un composant et détermine que le composant en panne ne peut pas revenir à son état de fonctionnement d'origine. En conséquence, vSAN commence à recréer les composants dégradés immédiatement. Cet état peut survenir lorsqu'un composant se trouve sur un périphérique en panne.
- Absent. Un composant est Absent lorsque vSAN détecte la panne temporaire d'un composant au cours de laquelle des composants, y compris l'ensemble de leurs données, sont susceptibles de récupérer et de renvoyer vSAN à son état d'origine. Cet état peut survenir lorsque vous redémarrez des hôtes ou si vous débranchez un périphérique d'un hôte vSAN. vSAN commence à recréer les composants se trouvant dans l'état Absent après un délai de 60 minutes.

État d'un objet : Sain et Défectueux

En fonction du type de pannes et de leur nombre dans le cluster, un objet peut être dans l'un des états suivants :

- Intègre. Lorsqu'au moins un miroir RAID 1 complet est disponible ou lorsque le nombre de segments de données minimal requis est disponible, l'objet est considéré comme étant sain.
- Défectueux. Un objet est considéré comme défectueux lorsqu'aucun miroir complet n'est disponible ou que le nombre minimal de segments de données requis n'est pas disponible pour les objets RAID 5 ou RAID 6. Si moins de 50 pour cent des votes d'un objet sont disponibles, l'objet est défectueux. S'il y a plusieurs pannes dans le cluster, les objets peuvent devenir défectueux. Lorsque l'état opérationnel d'un objet est considéré comme défectueux, la disponibilité de la machine virtuelle associée est affectée.

Témoin

Un témoin est un composant contenant uniquement des métadonnées et non des données d'application réelles. Il sert d'arbitre en cas de décision à prendre concernant la disponibilité des composants de banque de données restants, après une panne potentielle. Un témoin consomme environ 2 Mo d'espace pour les métadonnées sur la banque de données vSAN lors de l'utilisation du format sur disque 1.0 et 4 Mo pour le format sur disque version 2.0 et versions ultérieures.

vSAN 6.0 et les versions ultérieures conservent le quorum en utilisant un système de vote asymétrique par lequel chaque composant peut avoir plusieurs votes pour décider de la disponibilité des objets. Plus de 50 pour cent des votes qui constituent un objet de stockage de machine virtuelle doivent être accessibles à tout moment pour que l'objet soit considéré comme étant disponible. Lorsque 50 pour cent des votes ou moins sont accessibles à tous les hôtes, l'objet n'est plus disponible pour la banque de données vSAN. Les objets inaccessibles peuvent avoir un impact sur la disponibilité de la machine virtuelle associée.

Système SPBM (Storage Policy-Based Management)

Lorsque vous utilisez vSAN, vous pouvez définir les besoins en stockage d'une machine virtuelle, par exemple, les performances et la disponibilité, sous la forme d'une stratégie. vSAN s'assure que les machines virtuelles déployées sur les banques de données vSAN se voient attribuer au moins une stratégie de stockage de machine virtuelle. Lorsque vous connaissez les conditions de stockage requises de vos machines virtuelles, vous pouvez définir des stratégies de stockage et les attribuer à vos machines virtuelles. Si vous n'appliquez pas de stratégie de stockage lors du déploiement de machines virtuelles, vSAN attribue automatiquement une stratégie vSAN par défaut avec l'élément **Pannes tolérées** configuré sur 1, une bande de disque unique pour chaque objet et un disque virtuel provisionné dynamiquement. Pour de meilleurs résultats, définissez vos propres stratégies de stockage de machine virtuelle, même si les conditions requises de vos stratégies sont identiques à celles définies dans la stratégie de stockage par défaut. Pour plus d'informations sur l'utilisation de stratégies de stockage vSAN, reportez-vous à la section *Administration de VMware vSAN*.

vSphere PowerCLI

VMware vSphere PowerCLI ajoute la prise en charge du scriptage de la ligne de commande pour vSAN, pour vous aider à automatiser les tâches de configuration et de gestion. vSphere PowerCLI fournit une interface Windows PowerShell avec vSphere API. PowerCLI inclut des cmdlets pour administrer les composants vSAN. Pour plus d'informations sur l'utilisation de vSphere PowerCLI, reportez-vous à la *Documentation de vSphere PowerCLI*.

Différences entre vSAN et le stockage traditionnel

Bien que vSAN partage de nombreuses caractéristiques avec les tableaux de stockage traditionnel, le comportement général et le fonctionnement de vSAN est différent. Par exemple, vSAN peut uniquement gérer des hôtes ESXi et travailler avec ceux-ci, et une instance unique de vSAN ne peut prendre en charge qu'un seul cluster.

vSAN et le stockage traditionnel diffèrent également sur les points suivants :

- vSAN ne requiert pas de stockage en réseau externe pour stocker les fichiers des machines virtuelles à distance, contrairement à Fibre Channel (FC) ou au réseau SAN (Storage Area Network).
- Avec le stockage traditionnel, l'administrateur de stockage préalloue de l'espace de stockage à différents systèmes de stockage. vSAN transforme automatiquement les ressources de stockage local des hôtes ESXi en un pool de stockage unique. Ces pools peuvent être divisés et attribués à des machines virtuelles et à des applications en fonction de leurs exigences en matière de qualité de service.
- vSAN ne se comporte pas comme des volumes de stockage traditionnels basés sur des LUN ou des partages NFS. Le service cible iSCSI utilise les LUN pour activer un initiateur sur un hôte distant afin de transporter les données au niveau bloc vers un périphérique de stockage dans le cluster vSAN.

- Certains protocoles de stockage standard, tels que FCP, ne s'appliquent pas à vSAN.
- vSAN est fortement intégré à vSphere. Vous n'avez pas besoin de plug-ins dédiés ni d'une console de stockage pour vSAN, contrairement au stockage traditionnel. Vous pouvez déployer, gérer et surveiller vSAN à l'aide de vSphere Client.
- Un administrateur de stockage dédié n'a pas besoin de gérer vSAN. Un administrateur vSphere peut toutefois gérer un environnement vSAN.
- Avec vSAN, les stratégies de stockage de VM sont automatiquement affectées lorsque vous déployez de nouvelles machines virtuelles. Les stratégies de stockage peuvent être modifiées dynamiquement, le cas échéant.

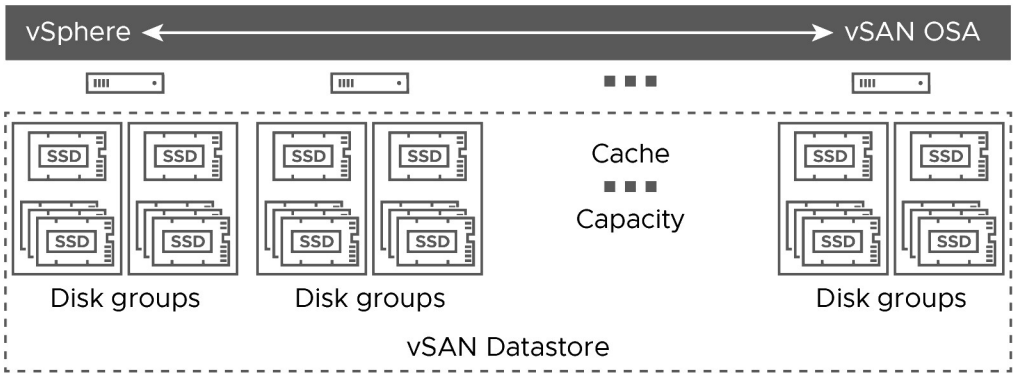
Création d'un cluster vSAN

Vous pouvez choisir l'architecture de stockage et la méthode de configuration lors du déploiement d'un cluster vSAN.

Choisissez l'architecture de stockage vSAN qui convient le mieux à vos ressources et à vos besoins.

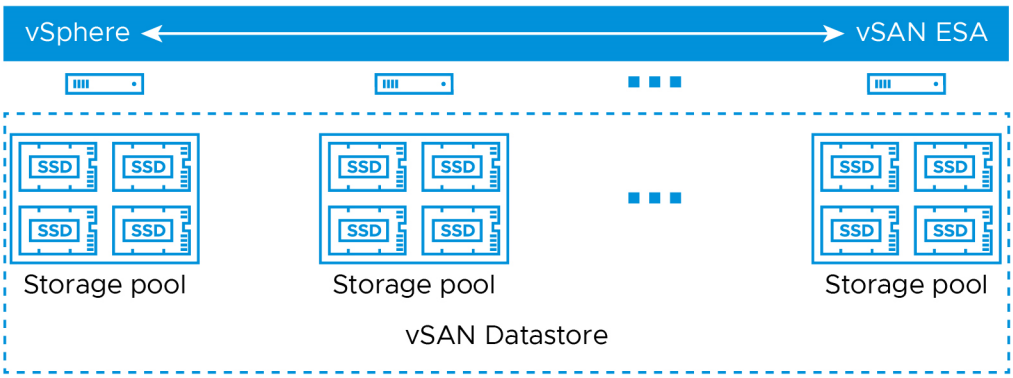
vSAN Original Storage Architecture

vSAN Original Storage Architecture (OSA) est conçu pour une vaste gamme de périphériques de stockage, notamment des disques SSD (Solid State Drive) Flash et des disques magnétiques (HDD). Chaque hôte contribuant au stockage contient un ou plusieurs groupes de disques. Chaque groupe de disques comporte un périphérique de cache Flash et un ou plusieurs périphériques de capacité.



vSAN Express Storage Architecture

vSAN Express Storage Architecture (ESA) est conçue pour les périphériques Flash TLC hautes performances basés sur NVMe et les réseaux hautes performances. Chaque hôte contribuant au stockage contient un pool de stockage unique de quatre périphériques Flash au minimum. Chaque périphérique Flash fournit la mise en cache et la capacité au cluster.



En fonction de vos besoins, vous pouvez déployer vSAN de l'une des manières suivantes.

vSAN ReadyNode

vSAN ReadyNode est une solution préconfigurée du logiciel vSAN fournie par des partenaires VMware, tels que Cisco, Dell, Fujitsu, IBM et Supermicro. Cette solution inclut une configuration validée du serveur dans un format testé et certifié du matériel pour le déploiement de vSAN qui est recommandée par l'OEM des serveurs et VMware. Pour plus d'informations sur la solution vSAN ReadyNode pour un partenaire spécifique, visitez le site Web des partenaires VMware.

Cluster vSAN défini par l'utilisateur

Vous pouvez créer un cluster vSAN en sélectionnant des composants logiciels et matériels individuels, tels que des pilotes, microprogrammes et contrôleurs d'E/S de stockage qui sont répertoriés sur le site Web VCG (vSAN Compatibility Guide, guide de compatibilité) à l'adresse http://www.vmware.com/resources/compatibility/search.php. Vous pouvez choisir tous les serveurs, les contrôleurs d'E/S de stockage, les périphériques de capacité et les périphériques de cache Flash, la mémoire et le nombre de cœurs que vous devez avoir par CPU, tant qu'ils sont certifiés et répertoriés sur le site Web VCG. Consultez les informations de compatibilité sur le site Web VCG avant de choisir les composants matériels et logiciels, les pilotes, les microprogrammes et les contrôleurs d'E/S de stockage qui sont pris en charge par vSAN. Lorsque vous concevez un cluster vSAN, utilisez uniquement les périphériques, les microprogrammes et les pilotes qui sont répertoriés sur le site Web VCG. L'utilisation de versions logicielles et matérielles qui ne sont pas spécifiées sur le site Web du Guide de compatibilité Virtual SAN risque d'entraîner l'échec du cluster ou la perte inattendue de données. Pour plus d'informations sur la conception d'un cluster vSAN, reportez-vous à la section « Conception et dimensionnement d'un cluster vSAN » dans *Planification et déploiement de vSAN*.

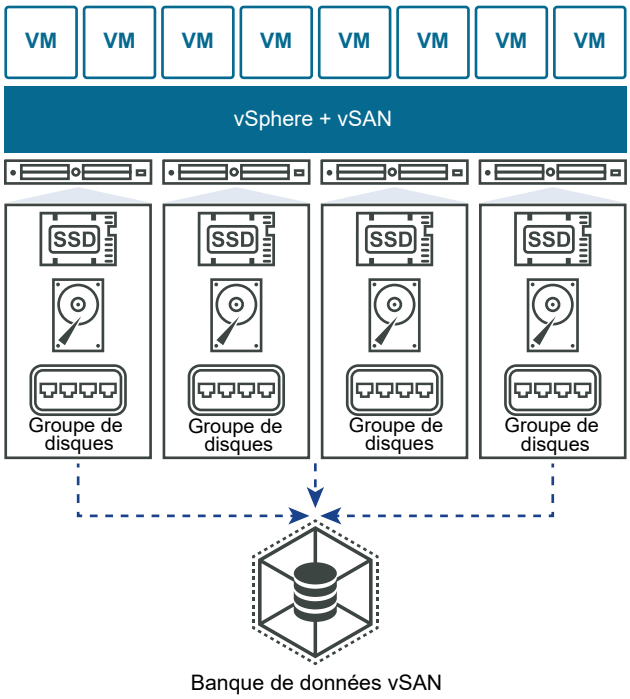
Options de déploiement de vSAN

Cette section présente les différentes options de déploiement prises en charge pour les clusters vSAN.

Cluster vSAN standard

Un cluster vSAN standard est composé d'au moins trois hôtes. En général, tous les hôtes d'un cluster vSAN standard résident dans un site unique et sont connectés sur le même réseau de couche 2. Les configurations intégralement Flash nécessitent des connexions réseau de 10 Go et vSAN Express Storage Architecture requiert des connexions réseau de 25 Go.

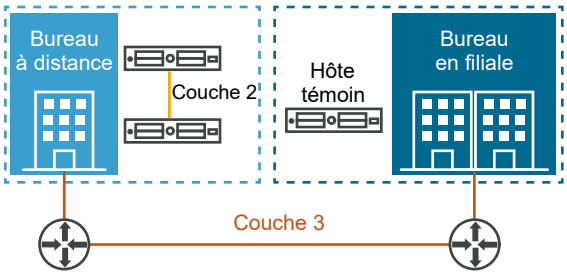
Pour plus d'informations, reportez-vous à la section *Planification et déploiement de vSAN*.



Clusters vSAN à deux nœuds

Les clusters vSAN à deux nœuds sont souvent utilisés pour les environnements de bureau à distance/succursale, qui exécutent généralement un petit nombre de charges de travail nécessitant une haute disponibilité. Un cluster vSAN à deux nœuds se compose de deux hôtes dans le même emplacement, connectés au même commutateur réseau ou entre eux. Vous pouvez configurer un cluster vSAN à deux nœuds afin d'utiliser un troisième hôte comme témoin, qui peut être situé à distance par rapport à la filiale. Le témoin réside généralement sur le site principal, tout comme vCenter Server.

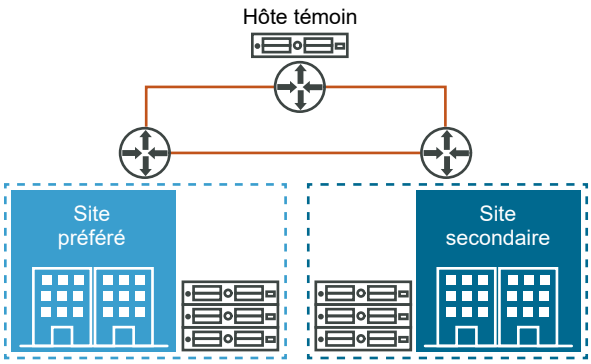
Pour plus d'informations, reportez-vous à la section *Planification et déploiement de vSAN*.



Cluster étendu vSAN

Un cluster étendu vSAN assure une résilience contre la perte d'un site entier. Les hôtes d'un cluster étendu sont répartis uniformément sur les deux sites. Les deux sites doivent avoir une latence réseau maximale de cinq millisecondes (5 ms). Un hôte témoin vSAN se trouve sur un troisième site pour fournir la fonction témoin. Le témoin est également déterminant dans les scénarios où il existe une partition réseau entre les deux sites de données. Seules des métadonnées telles que des composants témoins sont stockées sur le témoin.

Pour plus d'informations, reportez-vous à la section *Planification et déploiement de vSAN*.



Intégrer vSAN à d'autres logiciels VMware

Lorsque vSAN est activé et en cours d'exécution, il est intégré au reste de la pile des logiciels VMware. La plupart des opérations que vous effectuez avec les solutions de stockage traditionnelles peuvent être réalisées avec les composants et fonctionnalités vSphere dont vSphere vMotion, snapshots, clones, Distributed Resource Scheduler (DRS), vSphere High Availability, vCenter Site Recovery Manager, etc.

vSphere HA

Vous pouvez activer vSphere HA et vSAN sur le même cluster. Comme pour les banques de données traditionnelles, vSphere HA fournit le même niveau de protection pour les machines virtuelles qui résident dans des banques de données de vSAN. Ce niveau de protection implique des restrictions spécifiques lorsque vSphere HA et vSAN interagissent. Pour des considérations spécifiques sur la manière d'intégrer vSphere HA et vSAN, reportez-vous à la section #unique_10.

VMware Horizon View

Vous pouvez intégrer vSAN avec VMware Horizon View. Une fois l'intégration terminée, vSAN offre aux environnements de postes de travail virtuels les avantages suivants :

- Stockage haute-performance avec mise en cache automatique
- Gestion du stockage basée sur les stratégies, pour une correction automatique

Pour plus d'informations sur l'intégration de vSAN avec VMware Horizon, reportez-vous à la documentation *VMware avec Horizon View*. Pour obtenir des informations sur la conception et le dimensionnement de VMware Horizon View pour vSAN, reportez-vous à la documentation *Guide de conception et de dimensionnement d'Horizon View*.

Limitations de vSAN

Cette rubrique décrit les limitations de vSAN.

Lorsque vous utilisez vSAN, tenez compte des limitations suivantes :

- vSAN ne prend pas en charge les hôtes participant à plusieurs clusters vSAN. Toutefois, un hôte vSAN peut accéder aux autres ressources de stockage externes partagées par les clusters.
- vSAN ne prend pas en charge vSphere DPM et Storage I/O Control.
- vSAN ne prend pas en charge les disques SE Sparse.
- vSAN ne prend pas en charge RDM, VMFS, la partition de diagnostic et d'autres fonctionnalités d'accès au périphérique.

Configuration et gestion d'un cluster vSAN

2

Vous pouvez configurer et gérer un cluster vSAN à l'aide de vSphere Client, de commandes esxcli et d'autres outils.

Ce chapitre contient les rubriques suivantes :

Configurer un cluster pour vSAN à l'aide de vSphere Client

Vous pouvez utiliser vSphere Client pour configurer vSAN sur un cluster existant.

Note Vous pouvez utiliser le démarrage rapide pour créer et configurer rapidement un cluster vSAN. Pour plus d'informations, reportez-vous à la section « Utilisation du démarrage rapide pour configurer et développer un cluster vSAN » dans *Planification et déploiement de vSAN*.

Conditions préalables

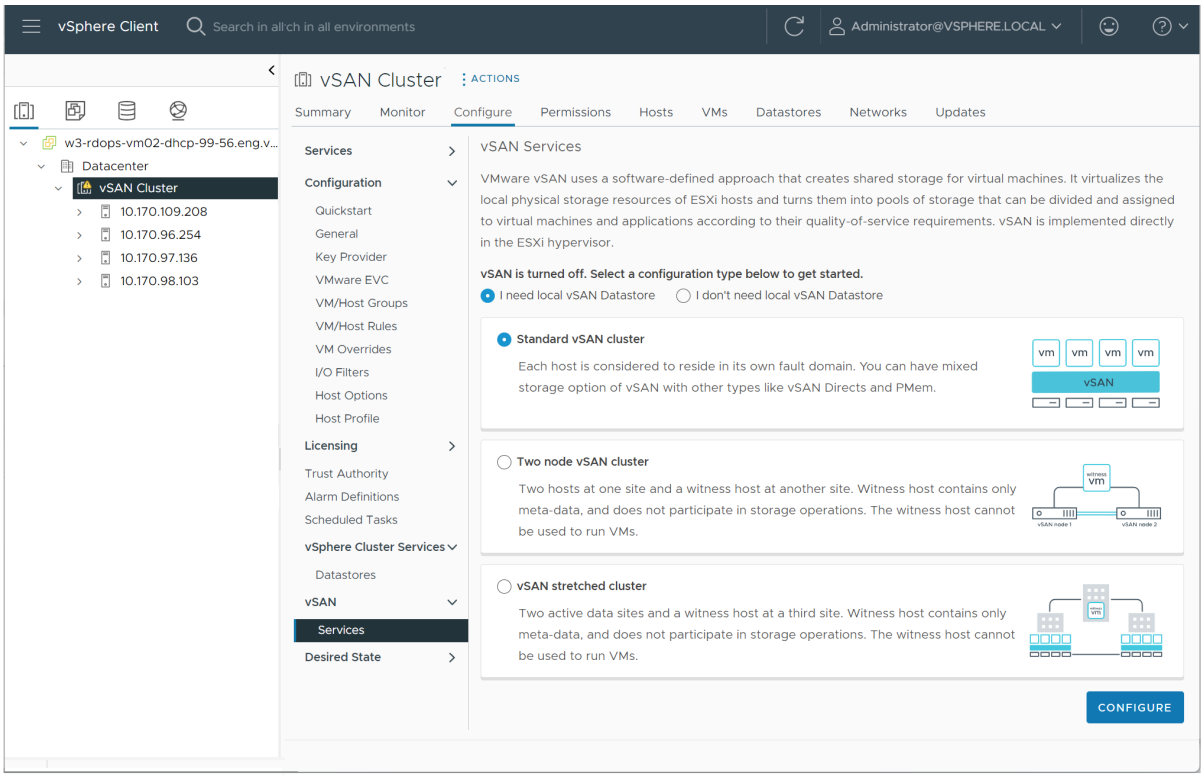
Vérifiez que votre environnement répond à la configuration requise. Reportez-vous à la section « Conditions requises pour l'activation de vSAN » dans *Planification et déploiement de vSAN*.

Créez un cluster et ajoutez à celui-ci des hôtes avant d'activer et de configurer vSAN. Configurez les propriétés de port sur chaque hôte pour ajouter le service vSAN.

Procédure

1. Accédez à un cluster hôte existant.
2. Cliquez sur l'onglet **Configurer**.

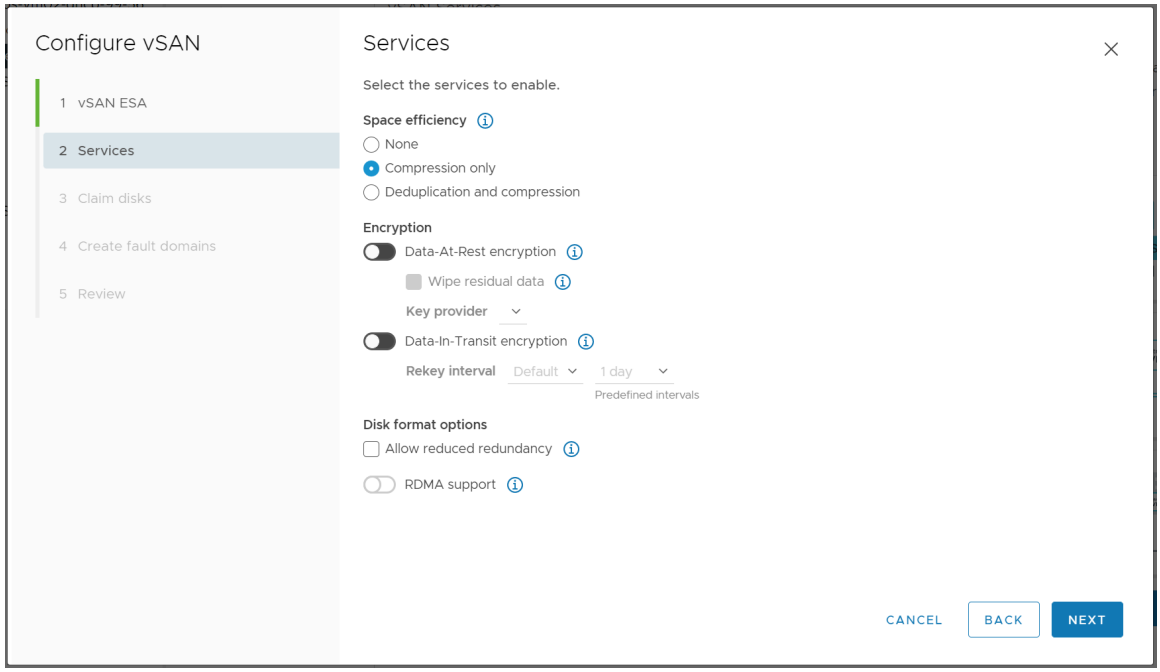
3 Sous vSAN, sélectionnez **Services**.



a Sélectionnez un type de configuration (cluster vSAN standard, cluster vSAN à deux nœuds ou cluster étendu.

b Sélectionnez l'option **J'ai besoin d'une banque de données vSAN locale** si vous prévoyez d'ajouter des groupes de disques ou des pools de stockage aux hôtes du cluster.

c Cliquez sur **Configurer** pour ouvrir l'assistant Configurer vSAN.



4 Sélectionnez vSAN ESA si le cluster est compatible, puis cliquez sur **Suivant**.

5 Configurez les services vSAN à utiliser, puis cliquez sur **Suivant**.

   Configurez les fonctionnalités de gestion des données, notamment la déduplication et la compression, le chiffrement des données au repos et le chiffrement des données en transit. Sélectionnez l'accès direct à distance à la mémoire (RDMA, Remote Direct Memory Access) si le réseau le prend en charge.

6 Réclamez les disques du cluster vSAN, puis cliquez sur **Suivant**.

   Pour vSAN Original Storage Architecture (vSAN OSA), chaque hôte contribuant au stockage nécessite au moins un périphérique Flash pour le cache et un ou plusieurs périphériques pour la capacité. Pour vSAN Express Storage Architecture (vSAN ESA), chaque hôte contribuant au stockage nécessite un ou plusieurs périphériques Flash.

7 Créez des domaines de pannes pour regrouper les hôtes qui peuvent échouer ensemble.

8 Vérifiez la configuration, puis cliquez sur **Terminer**.

Résultats

L'activation de vSAN crée une banque de données vSAN et enregistre le fournisseur de stockage vSAN. Les fournisseurs de stockage vSAN sont des composants logiciels intégrés qui transmettent les capacités de stockage de la banque de données à vCenter Server.

Étape suivante

Vérifiez que la banque de données de vSAN a été créée. Reportez-vous à Afficher la banque de données vSAN.

Vérifiez que le fournisseur de stockage de vSAN est enregistré.

Activer vSAN sur un cluster existant

Vous pouvez configurer un cluster existant pour activer vSAN.

Conditions préalables

Vérifiez que votre environnement répond à la configuration requise. Reportez-vous à la section « Conditions requises pour l'activation de vSAN » dans *Planification et déploiement de vSAN*.

Procédure

1 Accédez à un cluster hôte existant.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, sélectionnez **Services**.

   a Sélectionnez un type de configuration (cluster vSAN standard, cluster vSAN à deux nœuds ou cluster étendu.

   b Sélectionnez l'option **J'ai besoin d'une banque de données vSAN locale** si vous prévoyez d'ajouter des groupes de disques ou des pools de stockage aux hôtes du cluster.

   c Cliquez sur **Configurer** pour ouvrir l'assistant Configurer vSAN.

4 Sélectionnez vSAN ESA si le cluster est compatible, puis cliquez sur **Suivant**.

5 Configurez les services vSAN à utiliser, puis cliquez sur **Suivant**.

   Configurez les fonctionnalités de gestion des données, notamment la déduplication et la compression, le chiffrement des données au repos et le chiffrement des données en transit. Sélectionnez l'accès direct à distance à la mémoire (RDMA, Remote Direct Memory Access) si le réseau le prend en charge.

6 Réclamez les disques du cluster vSAN, puis cliquez sur **Suivant**.

   Pour vSAN Original Storage Architecture (vSAN OSA), chaque hôte contribuant au stockage nécessite au moins un périphérique Flash pour le cache et un ou plusieurs périphériques pour la capacité. Pour vSAN Express Storage Architecture (vSAN ESA), chaque hôte contribuant au stockage nécessite un ou plusieurs périphériques Flash.

7 Créez des domaines de pannes pour regrouper les hôtes qui peuvent échouer ensemble.

8 Vérifiez la configuration, puis cliquez sur **Terminer**.

Désactiver vSAN

Vous pouvez désactiver vSAN d'un cluster d'hôtes.

Lorsque vous désactivez vSAN pour un cluster, toutes les machines virtuelles et les services de données situés sur la banque de données vSAN deviennent inaccessibles. Si vous avez consommé du stockage sur le cluster vSAN à l'aide de vSAN Direct, les services de surveillance vSAN Direct, tels que les contrôles de santé, le rapport sur l'espace et la surveillance des performances, ne sont pas disponibles. Si vous envisagez d'utiliser des machines virtuelles alors que vSAN est désactivé, assurez-vous de migrer les machines virtuelles de la banque de données vSAN vers une autre banque de données avant de désactiver le cluster vSAN.

Conditions préalables

Vérifiez que les hôtes sont en mode de maintenance.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, sélectionnez **Services**.

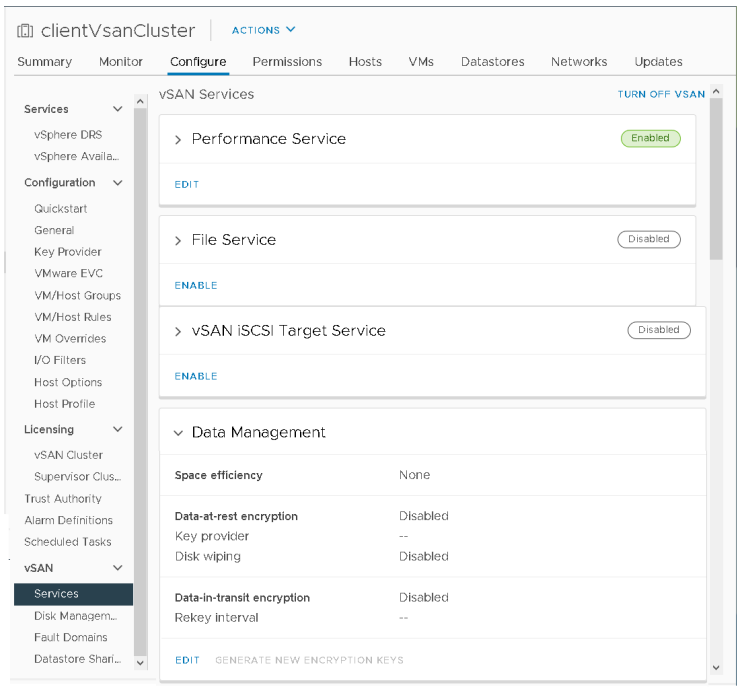
4 Cliquez sur **Désactiver vSAN**.

5 Confirmez votre choix dans la boîte de dialogue Désactiver vSAN.

Modifier les paramètres vSAN

Vous pouvez modifier les paramètres de votre cluster vSAN afin de configurer les fonctionnalités de gestion des données et activer les services fournis par le cluster.

Modifiez les paramètres d'un cluster vSAN existant si vous souhaitez activer la déduplication et la compression, ou activer le chiffrement. Si vous activez la déduplication et la compression, ou si vous activez le chiffrement, le format sur disque du cluster est automatiquement mis à niveau vers la dernière version.



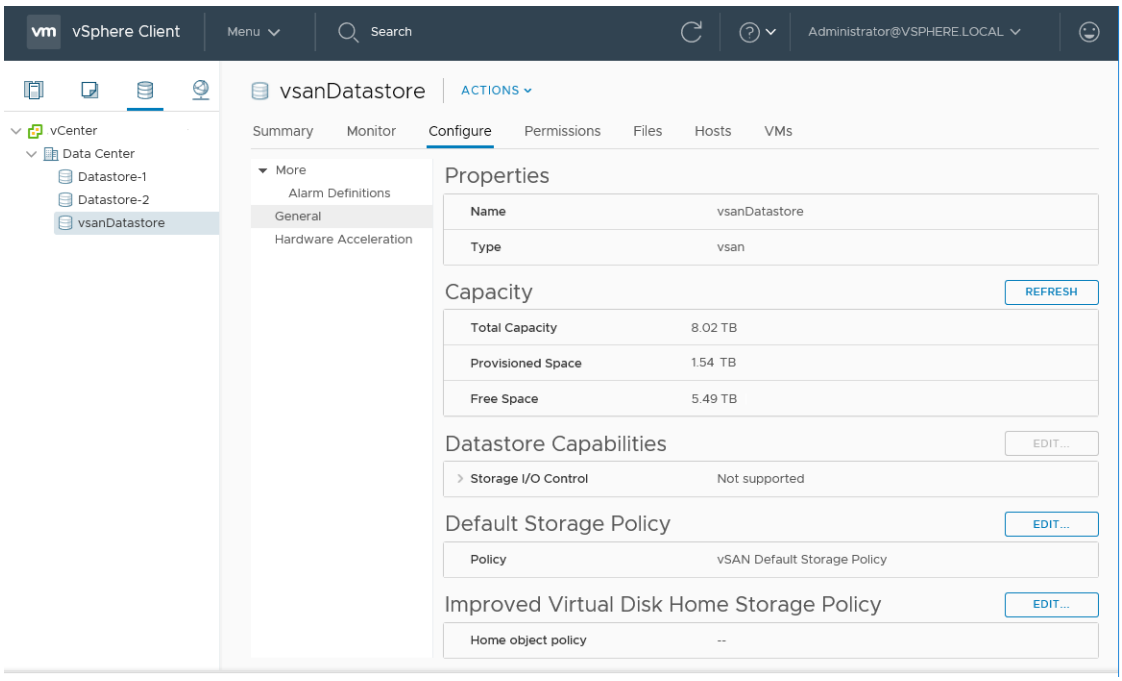
Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.
   a Sous vSAN, sélectionnez **Services**.
   b Cliquez sur le bouton **Modifier** ou **Activer** pour le service que vous souhaitez configurer.
      - Configurez le stockage. Cliquez sur **Monter des banques de données distantes** pour utiliser le stockage d'autres clusters vSAN.
      - Configurez le service de performances vSAN. Pour plus d'informations, reportez-vous à la section Surveillance des performances de vSAN dans *Surveillance et dépannage de vSAN*.
      - Activez le service de fichiers. Pour plus d'informations, reportez-vous à la section « Service de fichiers vSAN » dans *Administration de VMware vSAN*.
      - Configurez les options du réseau vSAN. Pour plus d'informations, reportez-vous à la section Configuration du réseau vSAN dans *Planification et déploiement de vSAN*.
      - Configurez le service cible iSCSI. Pour plus d'informations, reportez-vous à la section « Utilisation du service cible iSCSI vSAN » dans *Administration de VMware vSAN*.
      - Configurez les services de données, notamment la déduplication et la compression, le chiffrement des données au repos et le chiffrement des données en transit.
      - Configurez les alertes et les réservations de capacité. Pour plus d'informations, reportez-vous à la section « À propos de la capacité réservée » dans *Surveillance et dépannage de vSAN*.
      - Configurez les options avancées :
         - Minuteur de réparation d'objet
         - Localité de lecture de site pour les clusters étendus
         - Provisionnement d'échange dynamique
         - Prise en charge de grands clusters pour jusqu'à 64 hôtes
         - Rééquilibrage automatique
      - Configurez le service de santé de l'historique vSAN.
   c Modifiez les paramètres selon vos besoins.
3 Cliquez **Appliquer** pour confirmer vos sélections.

Afficher la banque de données vSAN

Une fois que vSAN est activé, une banque de données unique est créée. Vous pouvez vérifier la capacité de la banque de données de vSAN.



Conditions préalables

Configurez vSAN et des groupes de disques ou des pools de stockage.

Procédure

1 Accédez à Stockage.

2 Sélectionnez la banque de données vSAN.

3 Cliquez sur l'onglet **Configurer**.

4 Vérifiez la capacité de la banque de données vSAN.

La taille de la banque de données vSAN dépend du nombre de périphériques de capacité par hôte ESXi, ainsi que du nombre d'hôtes ESXi dans le cluster. Par exemple, si vous avez sept périphériques de capacité de 2 To chacun et que le cluster inclut huit hôtes, la capacité de stockage sera approximativement de 7 x 2 To x 8 = 112 To. Lorsque vous utilisez la configuration intégralement Flash, des périphériques Flash sont utilisés comme périphériques de capacité. En cas de configuration hybride, des disques magnétiques sont utilisés comme périphériques de capacité.

Une partie de la capacité est allouée aux métadonnées.

- Le format sur disque version 1.0 ajoute environ 1 Go par périphérique de capacité.
- Le format sur disque version 2.0 ajoute une surcharge de capacité, généralement pas plus de 1 à 2 % de capacité par périphérique.

- Le format sur disque version 3.0 et versions ultérieures ajoute une surcharge de capacité, généralement pas plus de 1 à 2 % de capacité par périphérique. La déduplication et la compression pour lesquelles un total de contrôle logiciel est activé nécessite une surcharge d'environ 6,2 pour cent de capacité par périphérique.

Étape suivante

Créez une stratégie de stockage pour les machines virtuelles à l'aide des capacités de stockage de la banque de données vSAN. Pour obtenir plus d'informations, reportez-vous à la documentation *Stockage vSphere*.

Télécharger des fichiers ou des dossiers vers des banques de données vSAN

Vous pouvez télécharger des fichiers VMDK vers une banque de données vSAN. Vous pouvez également télécharger des dossiers vers une banque de données vSAN. Pour plus d'informations sur les banques de données, reportez-vous à *Stockage vSphere*.

Lorsque vous téléchargez un fichier vmdk vers une banque de données vSAN, les considérations suivantes s'appliquent :

- Vous ne pouvez télécharger que des fichiers vmdk optimisés pour la diffusion en continu vers une banque de données vSAN. Le format de fichier VMware optimisé pour la diffusion en continu est un format fragmenté monolithique compressé pour la diffusion en continu. Si vous souhaitez télécharger un fichier vmdk qui n'est pas au format optimisé pour la diffusion en continu, avant de le télécharger, convertissez-le au format optimisé pour la diffusion en continu à l'aide de l'utilitaire de ligne de commande vmware-vdiskmanager. Pour plus d'informations, reportez-vous au *Guide de l'utilisateur de Virtual Disk Manager*.
- Lorsque vous téléchargez un fichier vmdk vers une banque de données vSAN, le fichier vmdk hérite de la stratégie par défaut de cette banque de données. Le vmdk n'hérite pas de la stratégie de la machine virtuelle à partir de laquelle il a été téléchargé. vSAN crée les objets en appliquant la stratégie par défaut vsanDatastore, qui est RAID-1. Vous pouvez modifier la stratégie par défaut de la banque de données. Reportez-vous à la section Modifier la stratégie de stockage par défaut des banques de données vSAN .
- Vous devez charger un fichier vmdk dans le dossier de base de la machine virtuelle.

Procédure

1 Accédez à la banque de données vSAN.

2 Cliquez sur l'onglet **Fichiers**.

Option	Description
Télécharger des fichiers	a Sélectionnez le dossier cible et cliquez sur **Télécharger des fichiers**. Vous voyez un message vous informant que vous pouvez télécharger des fichiers vmdk uniquement au format VMware optimisé pour la diffusion en continu. Si vous essayez de télécharger un fichier vmdk dans un autre format, vous voyez un message d'erreur de serveur interne. b Cliquez sur **Télécharger**. c Localisez l'élément à télécharger sur l'ordinateur local, puis cliquez sur **Ouvrir**.
Télécharger des dossiers	a Sélectionnez le dossier cible et cliquez sur **Télécharger un dossier**. Vous voyez un message vous informant que vous pouvez télécharger des fichiers vmdk uniquement au format VMware optimisé pour la diffusion en continu. b Cliquez sur **Télécharger**. c Localisez l'élément à télécharger sur l'ordinateur local, puis cliquez sur **Ouvrir**.

Télécharger des fichiers ou des dossiers depuis des banques de données vSAN

Vous pouvez télécharger des fichiers et des dossiers à partir d'une banque de données vSAN. Pour plus d'informations sur les banques de données, reportez-vous à *Stockage vSphere*.

Les fichiers VMDK sont téléchargés en tant que fichiers optimisés pour le flux avec le nom de fichier `<vmdkName>_stream.vmdk`. Le format de fichier VMware optimisé pour la diffusion en continu est un format fragmenté monolithique compressé pour la diffusion en continu.

Vous pouvez convertir un fichier vmdk VMware optimisé pour la diffusion en continu en d'autres formats de fichier vmdk à l'aide de l'utilitaire de ligne de commande vmware-vdiskmanager. Pour plus d'informations, reportez-vous au *Guide de l'utilisateur de Virtual Disk Manager*.

Procédure

1 Accédez à la banque de données vSAN.

2 Cliquez sur l'onglet **Fichiers**, puis sur **Télécharger**.

Vous voyez un message vous avertissant que les fichiers vmdk sont téléchargés depuis les banques de données vSAN au format VMware optimisé pour la diffusion en continu avec l'extension de nom de fichier `.stream.vmdk`.

3 Cliquez sur **Télécharger**.

4 Localisez l'élément à télécharger, puis cliquez sur **Télécharger**.

L'utilisation de stratégies vSAN 3

Lorsque vous utilisez vSAN, vous pouvez définir des conditions requises de stockage de machines virtuelles, par exemple la performance et la disponibilité, dans une stratégie. vSAN s'assure que chaque machine virtuelle déployée sur les banques de données vSAN se voient attribuer au moins une stratégie de stockage.

Une fois qu'elles sont attribuées, les conditions requises de la stratégie de stockage sont envoyées à la couche vSAN lors de la création d'une machine virtuelle. Le périphérique virtuel est distribué dans la banque de données vSAN pour répondre aux conditions requises en matière de performances et de disponibilité.

vSAN utilise des fournisseurs de stockage pour fournir des informations sur le stockage sous-jacent à vCenter Server. Ces informations vous aident à prendre des décisions appropriées sur le placement de la machine virtuelle et à surveiller votre environnement de stockage.

Ce chapitre contient les rubriques suivantes :

Présentation des stratégies vSAN

Les stratégies de stockage vSAN définissent les conditions de stockage requises pour vos machines virtuelles. Ces stratégies déterminent comment les objets de stockage de machines virtuelles sont provisionnés et alloués dans la banque de données pour garantir le niveau de service requis.

Lorsque vous activez vSAN sur un cluster hôte, une banque de données vSAN unique est créée et une stratégie de stockage par défaut est attribuée à la banque de données.

Lorsque vous connaissez les conditions de stockage requises de vos machines virtuelles, vous pouvez créer une stratégie de stockage faisant référence aux capacités annoncées par la banque de données. Vous pouvez créer plusieurs stratégies pour capturer différents types ou différentes classes d'exigences.

Chaque machine virtuelle déployée dans les banques de données vSAN se voit attribuer au moins une stratégie de stockage de machine virtuelle. Vous pouvez attribuer des stratégies de stockage lorsque vous créez ou modifiez des machines virtuelles.

Note Si vous n'attribuez pas de stratégie de stockage à une machine virtuelle, vSAN attribue une stratégie par défaut. La stratégie par défaut définit l'option **Pannes tolérées** sur 1 et prévoit une bande de disque par objet ainsi qu'un disque virtuel provisionné dynamiquement.

L'objet de permutation de machine virtuelle et l'objet de mémoire de snapshot de machine virtuelle n'obéissent pas aux stratégies de stockage attribuées à une machine virtuelle. La configuration de ces objets définit **Pannes tolérées** sur 1. Ces objets n'ont pas nécessairement la même disponibilité que d'autres objets auxquels a été attribuée une stratégie dont la valeur de **Pannes tolérées** est différente.

Note Si vSAN Express Storage Architecture est activé, chaque snapshot n'est pas un nouvel objet. Un VMDK de base et ses snapshots sont contenus dans un objet vSAN. En outre, dans vSAN ESA, le résumé repose sur l'objet vSAN. Il diffère en cela de vSAN Original Storage Architecture.

Tableau 3-1. Stratégie de stockage - Disponibilité

Capacité	Description
Pannes tolérées (FTT)	Définit le nombre de pannes d'hôte et de périphérique qu'un objet de machine virtuelle peut tolérer. Pour `n` échecs tolérés, chaque élément de données écrit est stocké à `n+1` endroits, incluant des copies de parité si RAID 5 ou RAID 6 est utilisé. Si des domaines de pannes sont configurés, `2n+1` domaines de pannes avec hôtes contribuant à la capacité sont requis. Un hôte ne faisant pas partie d'un domaine de pannes est considéré comme son propre domaine de pannes à hôte unique. Vous pouvez sélectionner une méthode de réplication des données qui optimise les performances ou la capacité. L'option RAID-1 (mise en miroir) utilise plus d'espace disque pour placer les composants des objets, mais fournit de meilleures performances pour l'accès aux objets. L'option RAID-5/6 (codage d'effacement) utilise moins d'espace disque, mais les performances sont réduites. Vous pouvez sélectionner l'une des options suivantes : ■ **Aucune redondance des données** : spécifiez cette option si vous ne souhaitez pas que vSAN protège une copie miroir unique des objets de machine virtuelle. Cela signifie que vos données ne sont pas protégées et vous risquez d'en perdre si le cluster vSAN subit une panne de périphérique. L'hôte peut rencontrer des retards inhabituels lors du passage en mode de maintenance. Les retards se produisent du fait que vSAN doit supprimer l'objet de l'hôte afin que l'opération de maintenance s'effectue correctement. ■ **Aucune redondance de données avec affinité d'hôte** : spécifiez cette option uniquement si vous souhaitez exécuter des charges de travail vSAN Shared Nothing Architecture (SNA) sur la plate-forme de persistance des données vSAN. ■ **1 panne - RAID-1 (mise en miroir)** : spécifiez cette option si votre objet de machine virtuelle peut tolérer une panne d'hôte ou de périphérique. Pour protéger un objet de machine virtuelle de 100 Go à l'aide de RAID-1 (mise en miroir) avec un FTT de 1, vous consommez 200 Go. ■ **1 panne - RAID-5 (codage d'effacement)** : spécifiez cette option si votre objet de machine virtuelle peut tolérer une panne d'hôte ou de périphérique. Pour protéger un objet de machine virtuelle de 100 Go à l'aide de RAID-5 (codage d'effacement) avec un FTT de 1, vous consommez 133,33 Go. **Note** Si vous utilisez vSAN Express Storage Architecture, vSAN crée un format RAID-5 optimisé en fonction de la taille du cluster. Si le nombre d'hôtes dans le cluster est inférieur à 6, vSAN crée un format RAID-5 (2+1). Si le nombre d'hôtes est supérieur à 6, vSAN crée un format RAID-5 (4+1). Lorsque la taille du cluster s'étend ou diminue, vSAN réajuste automatiquement le format au bout de 24 heures après la modification de la configuration.

Tableau 3-1. Stratégie de stockage - Disponibilité (suite)

Capacité	Description
	■ **2 pannes - RAID-1 (mise en miroir)** : spécifiez cette option si votre objet de machine virtuelle peut tolérer jusqu'à deux pannes de périphérique. Étant donné que vous devez disposer d'un FTT de 2 utilisant RAID-1 (mise en miroir), il y a une surcharge de capacité. Pour protéger un objet de machine virtuelle de 100 Go à l'aide de RAID-1 (mise en miroir) avec un FTT de 2, vous consommez 300 Go. ■ **2 pannes - RAID-6 (codage d'effacement)** : spécifiez cette option si vos objets de machine virtuelle peuvent tolérer jusqu'à deux pannes de périphérique. Pour effectuer la détection d'un objet de machine virtuelle de 100 Go à l'aide de RAID-6 (codage d'effacement) avec un FTT de 2, vous consommez 150 Go. Pour plus d'informations, consultez Utiliser le codage d'effacement RAID 5 ou RAID 6. ■ **3 pannes - RAID-1 (mise en miroir)** : spécifiez cette option si les objets de votre machine virtuelle peuvent tolérer jusqu'à trois pannes de périphérique. Pour protéger un objet de VM de 100 Go à l'aide de RAID-1 (mise en miroir) avec un FTT de 3, vous consommez 400 Go. **Note** Si vous créez une stratégie de stockage et ne spécifiez pas de valeur pour **FTT**, vSAN crée une seule copie miroir des objets de machine virtuelle. Il peut tolérer une panne. Cependant, si plusieurs pannes de composants se produisent, vos données peuvent être menacées.
Tolérance aux pannes du site	Cette règle définit s'il faut utiliser un cluster standard, étendu ou à 2 nœuds. Si vous utilisez un cluster étendu, vous pouvez définir si les données sont mises en miroir sur les deux sites ou sur un seul site. Pour un cluster étendu, vous pouvez choisir de conserver les données sur le site préféré ou secondaire pour l'affinité d'hôte. ■ **Aucun - Cluster standard** est la valeur par défaut. Cela signifie qu'il n'y a pas de tolérance aux pannes du site. ■ **Mise en miroir de l'hôte - cluster à 2 nœuds** : définit le nombre de pannes supplémentaires qu'un objet peut tolérer une fois le nombre de pannes défini par le paramètre FTT atteint. vSAN effectue la mise en miroir d'objets au niveau du groupe de disques. Chaque hôte de données doit disposer d'au moins trois groupes de disques ou de trois disques dans un pool de stockage pour utiliser cette règle. ■ **Mise en miroir du site - cluster étendu** : définit le nombre de pannes d'hôte supplémentaires que l'objet peut tolérer lorsque le nombre de pannes défini par le paramètre FTT est atteint. ■ **Aucun - conserver les données sur le cluster préféré (cluster étendu)**. Utilisez cette option lorsque vous ne souhaitez pas que les objets d'un cluster étendu disposent de la tolérance de panne du site et que vous souhaitez rendre les objets accessibles uniquement sur le site configuré comme Préféré. ■ **Aucun - conserver les données sur le cluster secondaire (cluster étendu)**. Utilisez cette option lorsque vous ne souhaitez pas que les objets d'un cluster étendu disposent de la tolérance de panne du site et que vous souhaitez rendre les objets accessibles uniquement sur le site secondaire. Ces objets ne sont pas affectés par les pannes de liaison intercommutateur (ISL, Inter-Switch Link) ou d'hôte témoin. Ils restent accessibles si le site choisi par la stratégie est accessible.

Tableau 3-1. Stratégie de stockage - Disponibilité (suite)

Capacité	Description
	■ **Aucun - cluster étendu**. Si vous sélectionnez cette option, vSAN ne garantit pas la disponibilité des objets si l'un des sites tombe en panne, et ces objets peuvent consommer trop de bande passante ISL et augmenter la latence pour les objets qui utilisent la stratégie de mise en miroir de sites. N'utilisez cette stratégie que lorsqu'il est impossible d'utiliser les autres stratégies pendant une condition temporaire où il existe une contrainte de capacité (CPU/mémoire/stockage) dans le cluster.

Tableau 3-2. Stratégie de stockage - règles de stockage

Capacité	Description
Services de chiffrement	Définit les options de chiffrement des machines virtuelles que vous déployez sur votre banque de données. Choisissez l'une des options suivantes : ■ **Chiffrement des données au repos** : spécifiez cette option si vous souhaitez appliquer le chiffrement aux données stockées dans votre banque de données. ■ **Aucun chiffrement** : spécifiez cette option si vous ne souhaitez appliquer aucune forme de chiffrement à vos données. ■ **Aucune préférence** : spécifiez cette option si vous ne souhaitez pas appliquer explicitement des règles de chiffrement. Lorsque vous sélectionnez cette option, vSAN applique les deux règles à vos machines virtuelles.
Efficacité de l'utilisation de l'espace	Définit les options d'efficacité de l'utilisation de l'espace pour les machines virtuelles que vous déployez sur votre banque de données. Choisissez l'une des options suivantes : ■ **Déduplication et compression** : spécifiez cette option si vous souhaitez activer et appliquer la déduplication et la compression à vos données. ■ **Compression uniquement** : spécifiez cette option si vous souhaitez appliquer uniquement la compression à vos données. **Note** Pour vSAN Original Storage Architecture, la compression est un paramètre au niveau du cluster. Pour vSAN Express Storage Architecture, la compression s'effectue au niveau de l'objet. Cela signifie que vous pouvez activer la compression pour une machine virtuelle tout en la désactivant pour une autre machine virtuelle dans le même cluster. ■ **Aucune efficacité de l'espace** : spécifiez cette option si vous ne souhaitez pas appliquer de compression à vos objets. Cela signifie que seule la déduplication est appliquée à vos données. ■ **Aucune préférence** : spécifiez cette option si vous ne souhaitez pas appliquer explicitement des règles d'efficacité de l'utilisation de l'espace. Lorsque vous sélectionnez cette option, vSAN applique toutes les règles d'efficacité de l'utilisation de l'espace à vos machines virtuelles.
Niveau de stockage	Spécifiez le niveau de stockage pour toutes les machines virtuelles avec la stratégie de stockage définie. Choisissez l'une des options suivantes : ■ **Intégralement Flash** : spécifiez cette option si vous souhaitez rendre vos machines virtuelles compatibles uniquement avec le niveau Intégralement Flash. ■ **Hybride** : spécifiez cette option si vous souhaitez rendre vos machines virtuelles compatibles avec un environnement hybride uniquement. ■ **Aucune préférence** : spécifiez cette option si vous ne souhaitez pas appliquer explicitement des règles de niveau de stockage. Lorsque vous sélectionnez cette option, vSAN rend les machines virtuelles compatibles avec les environnements hybrides et intégralement Flash.

Tableau 3-3. Stratégie de stockage - Règles de stratégie avancées

Capacité	Description
Nombre de bandes de disque par objet	Nombre minimal de périphériques de capacité sur lesquels chaque réplica d'un objet de machine virtuelle est agrégé par bandes. Une valeur supérieure à 1 peut donner de meilleures performances, mais peut aussi engendrer une plus grande sollicitation des ressources système. La valeur par défaut est 1. La valeur maximale est 12. Ne modifiez pas la valeur d'agrégation de bandes par défaut. Dans un environnement hybride, les bandes de disque sont réparties sur plusieurs disques magnétiques. Pour une configuration intégralement Flash, l'agrégation par bandes est effectuée dans les périphériques Flash constituant la couche de capacité. Assurez-vous que votre environnement vSAN dispose de périphériques de capacité suffisants pour répondre à la demande.
Limite IOPS pour un objet	Définit la limite IOPS pour un objet, tel qu'un VMDK. IOPS sont calculées comme le nombre d'opérations d'E/S, en utilisant une taille pondérée. Si le système utilise la taille de base par défaut de 32 Ko, une E/S de 64 Ko représente deux opérations d'E/S. Lors du calcul d'IOPS, la lecture et l'écriture sont considérées équivalentes, mais le taux de réussite du cache et la séquentialité ne sont pas pris en compte. Si l'IOPS d'un disque dépasse la limite, les opérations d'E/S sont limitées. Si la **Limite IOPS pour un objet** est définie sur 0, les limites IOPS ne sont pas appliquées. vSAN permet à l'objet de doubler le taux de la limite IOPS pendant la première seconde d'une opération ou après une période d'inactivité.
Réservation d'espace de l'objet	Pourcentage de la taille logique de l'objet de disque de machine virtuelle (VMDK) devant être réservé ou provisionné dynamiquement lors du déploiement de machines virtuelles. Les options suivantes sont disponibles : ■ Provisionnement dynamique (par défaut) ■ 25 % de réservation ■ 50 % de réservation ■ 75 % de réservation ■ Provisionnement statique

Tableau 3-3. Stratégie de stockage - Règles de stratégie avancées (suite)

Capacité	Description
Réservation de Flash Read Cache (%)	Capacité de la mémoire flash réservée au cache de lecture pour l'objet de machine virtuelle. Elle est exprimée en pourcentage de la taille logique de l'objet de disque de machine virtuelle (VMDK). La capacité de mémoire flash réservée ne peut pas être utilisée par d'autres objets. La mémoire flash non réservée est partagée équitablement entre tous les objets. Utilisez uniquement cette option pour résoudre des problèmes de performance spécifiques. Vous n'avez pas besoin de définir une réservation pour obtenir le cache. Le fait de définir des réservations pour le cache de lecture peut entraîner des problèmes lorsque vous déplacez l'objet de machine virtuelle, car les paramètres de réservation du cache sont toujours inclus dans l'objet. L'attribut de stratégie de stockage de réservation Flash Read Cache est pris en charge uniquement pour les configurations de stockage hybride. Vous ne devez pas utiliser cet attribut lors de la définition d'une stratégie de stockage de machine virtuelle pour un cluster intégralement Flash. La valeur par défaut est 0 %. La valeur maximale est 100 %. **Note** Par défaut, vSAN alloue dynamiquement un cache de lecture aux objets de stockage à la demande. Cette fonctionnalité garantit une utilisation souple et optimale des ressources. Par conséquent, vous n'avez généralement pas à modifier la valeur par défaut 0 de ce paramètre. Soyez prudent si vous devez augmenter la valeur pour résoudre un problème de performances. Les réservations surprovisionnées entre plusieurs machines virtuelles peuvent entraîner le gaspillage d'espace de périphérique Flash pour des surréservations. Ces réservations de cache ne sont pas disponibles pour servir les charges de travail nécessitant l'espace requis à un moment donné. Ce gaspillage d'espace et cette indisponibilité peuvent compromettre les performances.

Tableau 3-3. Stratégie de stockage - Règles de stratégie avancées (suite)

Capacité	Description
Total de contrôle de l'objet	Si l'option est définie sur **Non**, l'objet calcule les informations de total de contrôle pour garantir l'intégrité de ses données. Si cette option est définie sur **Oui**, l'objet ne calcule pas les informations de total de contrôle. vSAN utilise un total de contrôle de bout en bout pour garantir l'intégrité des données en confirmant que chaque copie d'un fichier est exactement la même que le fichier source. Le système vérifie la validité des données pendant les opérations de lecture/écriture et si une erreur est détectée, vSAN répare les données ou signale l'erreur. Si une non-correspondance de total de contrôle est détectée, vSAN répare automatiquement les données en remplaçant les données incorrectes par les données correctes. Le calcul du total de contrôle et la correction d'erreur sont effectués en arrière-plan. La valeur par défaut pour tous les objets du cluster est **Non**, ce qui signifie que le total de contrôle est activé. **Note** Pour vSAN Express Storage Architecture, le total de contrôle des objets est toujours activé et ne peut pas être désactivé.
Forcer le provisionnement	Si l'option est définie sur **Oui**, l'objet est provisionné, même si les stratégies **Pannes tolérées**, **Nombre de bandes de disque par objet** et **Réservation de Flash Read Cache** spécifiées dans la stratégie de stockage ne peuvent pas être satisfaites par la banque de données. Utilisez ce paramètre dans les scénarios d'amorçage ou lors d'une coupure lorsque le provisionnement standard n'est plus possible. La valeur par défaut **Non** est acceptable pour la plupart des environnements de production. vSAN ne parvient pas à provisionner une machine virtuelle lorsque les conditions requises de la stratégie ne sont pas respectées, mais crée avec succès la stratégie de stockage définie par l'utilisateur.

Si vous utilisez des stratégies de stockage de machine virtuelle, vous devez comprendre comment les différentes possibilités de stockage affectent la consommation de la capacité de stockage du cluster vSAN. Pour plus d'informations sur la conception et le dimensionnement des stratégies de stockage, reportez-vous à la section « Conception et dimensionnement d'un cluster vSAN » dans *Administration de VMware vSAN*.

Gestion des modifications de la stratégie par vSAN

vSAN 6.7 Update 3 et versions ultérieures gère les modifications de stratégie pour réduire la quantité d'espace temporaire consommée dans le cluster.

La capacité transitoire est générée lorsque vSAN reconfigure des objets pour une modification de stratégie.

Lorsque vous modifiez une stratégie, la modification est acceptée mais ne s'applique pas immédiatement. vSAN traite les demandes de modification de stratégie et les exécute de façon asynchrone, afin de conserver une quantité fixe d'espace temporaire.

Les modifications de stratégie sont rejetées immédiatement pour des raisons non liées à la capacité, telles que la modification d'une stratégie RAID5 en RAID6 sur un cluster à cinq nœuds.

Vous pouvez afficher l'utilisation de la capacité transitoire dans le moniteur de capacité vSAN. Pour vérifier l'état d'une modification de stratégie sur un objet, utilisez le service de santé de vSAN pour vérifier la santé de l'objet vSAN.

Afficher les fournisseurs de stockage vSAN

Activer vSAN automatiquement configure et enregistre un fournisseur de stockage pour chaque hôte dans le cluster vSAN.

Les fournisseurs de stockage vSAN sont des composants logiciels intégrés qui fournissent des capacités de banque de données à vCenter Server. Une capacité de stockage est généralement représentée par une paire clé-valeur, dans laquelle la clé est une propriété spécifique offerte par la banque de données. La valeur est un nombre ou une plage que la banque de données peut fournir pour un objet provisionné, par exemple un objet d'espace de noms de base ou un disque virtuel d'une machine virtuelle. Vous pouvez également utiliser des balises pour créer des capacités de stockage définies par l'utilisateur et y faire référence lors de la définition d'une stratégie de stockage pour une machine virtuelle. Pour obtenir des informations sur l'application et l'utilisation de balises avec des banques de données, reportez-vous à la documentation de *Stockage vSphere*.

Les fournisseurs de stockage vSAN signalent un ensemble de capacités de stockage sous-jacent à vCenter Server. Ils communiquent également avec la couche de vSAN pour indiquer les besoins en stockage des machines virtuelles. Pour plus d'informations sur les fournisseurs de stockage, reportez-vous à la documentation *Stockage vSphere*.

vSAN 6.7 et versions ultérieures enregistrent uniquement un seul fournisseur de stockage vSAN pour tous les clusters vSAN gérés par l'instance de vCenter Server à l'aide de l'URL suivante :

```
https://<VC fqdn>:<VC https port>/vsan/vasa/version.xml
```

Vérifiez que les fournisseurs de stockage sont enregistrés.

Procédure

1. Accédez à vCenter Server.
2. Cliquez sur l'onglet **Configurer**, puis cliquez sur **Fournisseurs de stockage**.

Résultats

Le fournisseur de stockage de vSAN figure dans la liste.

Note Il est impossible d'annuler manuellement l'inscription des fournisseurs de stockage utilisés par vSAN. Pour supprimer des fournisseurs de stockage vSAN ou en annuler l'enregistrement, supprimez les hôtes correspondants du cluster vSAN, puis rajoutez-les. Assurez-vous qu'au moins un fournisseur de stockage est actif.

Présentation des stratégies de stockage vSAN par défaut

vSAN requiert que les machines virtuelles déployées sur les banques de données vSAN soient affectées d'au moins une stratégie de stockage. Lors du provisionnement d'une machine virtuelle, si vous n'attribuez pas explicitement de stratégie de stockage à la machine virtuelle, la stratégie de stockage vSAN par défaut est attribuée à la machine virtuelle.

Chaque stratégie de stockage par défaut contient des ensembles de règles vSAN et un ensemble de capacités de stockage de base, généralement utilisés pour le placement de machines virtuelles déployées sur des banques de données vSAN.

Tableau 3-4. vSAN Spécifications de stratégie de stockage par défaut

Spécification	Paramètre
Pannes tolérées	1
Nombre de bandes de disque par objet	1
Réservation de Flash Read Cache ou capacité Flash utilisée pour le cache de lecture	0
Réservation d'espace de l'objet	0 **Note** La définition de Réservation d'espace de l'objet sur 0 signifie que le disque virtuel est provisionné dynamiquement par défaut.
Forcer le provisionnement	Non

Si vous utilisez un cluster vSAN Express Storage Architecture, en fonction de la taille de votre cluster, vous pouvez utiliser l'une des stratégies ESA répertoriées ici.

Tableau 3-5. Spécifications de stratégie de stockage par défaut vSAN ESA - RAID5

Spécification	Paramètre
Pannes tolérées	1
Nombre de bandes de disque par objet	1
Réservation de Flash Read Cache ou capacité Flash utilisée pour le cache de lecture	0
Réservation d'espace de l'objet	Provisionnement dynamique
Forcer le provisionnement	Non

Note Pour utiliser RAID-5, vous devez disposer d'au moins 4 hôtes dans le cluster.

Tableau 3-6. Spécifications de stratégie de stockage par défaut vSAN ESA - RAID6

Spécification	Paramètre
Pannes tolérées	2
Nombre de bandes de disque par objet	1
Réservation de Flash Read Cache ou capacité Flash utilisée pour le cache de lecture	0
Réservation d'espace de l'objet	Provisionnement dynamique
Forcer le provisionnement	Non

Note Pour utiliser RAID-6, vous devez disposer d'au moins 6 hôtes dans le cluster.

Vous pouvez vérifier les paramètres de configuration de la stratégie de stockage de machine virtuelle par défaut lorsque vous accédez à **Stratégie de stockage de VM** > **Ensemble de règles 1 : vSAN**.

Pour de meilleurs résultats, envisagez de créer et d'utiliser vos propres stratégies de stockage de machine virtuelle, même si les conditions requises de la stratégie sont identiques à celles définies dans la stratégie de stockage par défaut. Dans certains cas, lorsque vous augmentez la taille d'un cluster, vous devez modifier la stratégie de stockage par défaut pour assurer la conformité avec les conditions requises par le Contrat de niveau de service pour VMware Cloud on AWS.

Lorsque vous attribuez une stratégie de stockage définie par l'utilisateur à une banque de données, vSAN applique les paramètres de la stratégie définie par l'utilisateur sur la banque de données spécifiée. À tout moment, vous pouvez attribuer une seule stratégie de stockage de machine virtuelle comme stratégie par défaut à la banque de données vSAN.

Spécifications de stratégie de stockage vSAN par défaut

Les spécifications suivantes s'appliquent aux stratégies de stockage vSAN par défaut.

- Une stratégie de stockage vSAN par défaut est attribuée à tous les objets de machine virtuelle si vous n'attribuez aucune autre stratégie vSAN lorsque vous provisionnez une machine virtuelle. La zone de texte **Stratégie de stockage VM** est définie sur **Valeur par défaut de la banque de données** sur la page Sélectionner un stockage. Pour plus d'informations sur l'utilisation des stratégies de stockage, reportez-vous à la documentation *Stockage vSphere*.

  Note Les objets de permutation de machine virtuelle et de mémoire de machine virtuelle reçoivent la stratégie de stockage vSAN par défaut lorsque **Forcer le provisionnement** est défini sur **Oui**.

- Une stratégie par défaut vSAN s'applique uniquement aux banques de données vSAN. Vous ne pouvez pas appliquer une stratégie de stockage par défaut à des banques de données non-vSAN (par exemple, NFS) ou une banque de données VMFS.

- Les objets d'un cluster vSAN Express Storage Architecture avec une configuration RAID 0 ou RAID 1 auront 3 bandes de disque, bien que la stratégie par défaut ne définisse qu'une bande de disque.
- Du fait que la stratégie de stockage de machine virtuelle par défaut est compatible avec toutes les banques de données vSAN de vCenter Server, vous pouvez déplacer vos objets de machine virtuelle provisionnés avec la stratégie par défaut vers n'importe quelle banque de données vSAN de vCenter Server.
- Vous pouvez cloner la stratégie par défaut et l'utiliser comme modèle pour créer une stratégie de stockage définie par l'utilisateur.
- Vous pouvez modifier la stratégie par défaut si vous bénéficiez du privilège StorageProfile.View. Vous devez disposer d'au moins un cluster vSAN qui contient au moins un hôte. En général, vous ne modifiez pas les paramètres de la stratégie de stockage par défaut.
- Vous ne pouvez pas modifier le nom et la description de la stratégie par défaut, ni la spécification du fournisseur de stockage vSAN. Tous les autres paramètres, y compris les règles de stratégie, sont modifiables.
- Vous ne pouvez pas supprimer la stratégie par défaut.
- Une stratégie de stockage par défaut est attribuée si la stratégie que vous attribuez pendant le provisionnement de la machine virtuelle n'inclut pas de règles spécifiques à vSAN.

Modifier la stratégie de stockage par défaut des banques de données vSAN

Vous pouvez modifier la stratégie de stockage par défaut pour une banque de données vSAN sélectionnée.

Conditions préalables

Vérifiez que la stratégie de stockage de machine virtuelle que vous souhaitez attribuer en tant que stratégie par défaut à la banque de données vSAN répond aux conditions requises de vos machines virtuelles dans le cluster vSAN.

Procédure

1. Accédez à la banque de données vSAN.
2. Cliquez sur **Configurer**.
3. Dans **Général**, cliquez sur le bouton **Modifier** de la stratégie de stockage par défaut, puis sélectionnez la stratégie de stockage que vous souhaitez attribuer comme stratégie par défaut à la banque de données vSAN.

   Vous pouvez faire votre choix dans une liste de stratégies de stockage compatibles avec la banque de données vSAN, comme la stratégie de stockage par défaut vSAN et les stratégies de stockage définies par l'utilisateur ayant des ensembles de règles vSAN définies.

4 Sélectionnez une stratégie, puis cliquez sur **OK**.

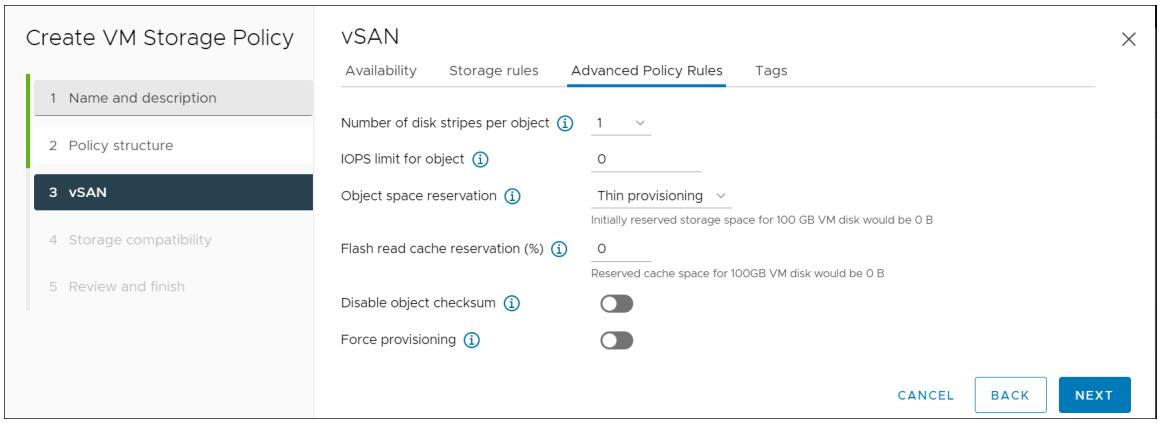
La stratégie de stockage est appliquée en tant que stratégie par défaut lorsque vous provisionnez de nouvelles machines virtuelles sans spécifier explicitement de stratégie de stockage pour une banque de données.

Étape suivante

Vous pouvez définir une nouvelle stratégie de stockage pour les machines virtuelles. Reportez-vous à Définir une stratégie de stockage pour vSAN à l'aide de vSphere Client.

Définir une stratégie de stockage pour vSAN à l'aide de vSphere Client

Vous pouvez créer une stratégie de stockage qui définit des conditions de stockage pour une machine virtuelle et ses disques virtuels. Dans cette stratégie, vous faites référence aux capacités de stockage prises en charge par la banque de données vSAN.



Conditions préalables

- Vérifiez que le fournisseur de stockage de vSAN est disponible. Reportez-vous à Afficher les fournisseurs de stockage vSAN.
- Privilèges requis : **Stockage basé sur le profil.Affichage du stockage basé sur le profi** et **Stockage basé sur le profi.Mise à jour du stockage basé sur le profi**

Procédure

1 Accédez à **Stratégies et profils**, puis cliquez sur **Stratégies de stockage VM**.

2 Cliquez sur **CRÉER**.

3 Sur la page Nom et description, sélectionnez un vCenter Server.

4 Entrez un nom et une description pour la stratégie de stockage et cliquez sur **Suivant**.

5 Sur la page de Structure de la stratégie, sélectionnez Activer les règles de stockage « vSAN », puis cliquez sur **Suivant**.

6 Sur la page vSAN, définissez l'ensemble de règles de la stratégie et cliquez sur **Suivant**.

a Dans l'onglet Disponibilité, définissez les options **Tolérance de sinistre de site** et **Nombre d'échecs tolérés**.

Les options de disponibilité définissent les règles de pannes tolérées, la localité des données et la méthode de tolérance de panne.

- **Tolérance de sinistre de site** définit le type de tolérance de panne de site utilisé pour les objets de machine virtuelle.
- **Nombre d'échecs à tolérer** définit le nombre de pannes d'hôte et de périphérique qu'un objet de machine virtuelle peut tolérer et la méthode de réplication de données.

Par exemple, si vous choisissez **Mise en miroir double site** et **2 pannes - RAID-6 (codage d'effacement)**, vSAN configure les règles de stratégie suivantes :

- Pannes tolérées : 1
- Niveau secondaire de pannes à tolérer : 2
- Localité des données : aucune
- Méthode de tolérance de panne : RAID-5/6 (codage d'effacement) - Capacité

b Dans l'onglet Règles de stockage, définissez les règles de chiffrement, d'efficacité de l'utilisation de l'espace et de niveau de stockage qui peuvent être utilisées avec le maillage HCI pour différencier les banques de données distantes.

- **Services de chiffrement** : définit les règles de chiffrement pour les machines virtuelles que vous déployez à l'aide de cette stratégie. Vous pouvez choisir l'une des options suivantes :
  - **Chiffrement des données au repos** : le chiffrement est activé sur les machines virtuelles.
  - **Aucun chiffrement** : le chiffrement n'est pas activé sur les machines virtuelles.
  - **Aucune préférence** : permet la compatibilité des machines virtuelles avec les options Chiffrement des données au repos et Aucun chiffrement.
- **Efficacité de l'utilisation de l'espace** : définit les règles d'économie de l'espace pour les machines virtuelles que vous déployez à l'aide de cette stratégie. Vous pouvez choisir l'une des options suivantes :
  - **Déduplication et compression** : active la déduplication et la compression sur les machines virtuelles. La déduplication et la compression sont disponibles uniquement sur les groupes de disques intégralement Flash. Pour plus d'informations, consultez Éléments à prendre en compte pour la conception de la déduplication et de la compression.

- **Compression uniquement** : n'active que la compression sur les machines virtuelles. La compression n'est disponible que sur les groupes de disques intégralement Flash. Pour plus d'informations, consultez Éléments à prendre en compte pour la conception de la déduplication et de la compression.
- **Aucune efficacité de l'espace** : les fonctionnalités d'efficacité de l'utilisation de l'espace ne sont pas activées sur les machines virtuelles. Le choix de cette option nécessite des banques de données sans activation des options d'efficacité de l'utilisation de l'espace.
- **Aucune préférence** : permet la compatibilité des machines virtuelles avec toutes les options.

- **Niveau de stockage** : spécifie le niveau de stockage pour les machines virtuelles que vous déployez à l'aide de cette stratégie. Vous pouvez choisir l'une des options suivantes. Le choix de l'option **Aucune préférence** permet la compatibilité des machines virtuelles avec les environnements hybrides et intégralement Flash.
  - **Intégralement Flash**
  - **Hybride**
  - **Aucune préférence**

c Dans l'onglet Règles de stratégie avancées, définissez des règles de stratégie avancées, telles que le nombre de bandes de disque par objet et les limites d'IOPS.

d Dans l'onglet Balises, cliquez sur **Ajouter une règle de balise**, puis définissez les options de règle de balise.

Assurez-vous que les valeurs que vous fournissez sont comprises dans la plage de valeurs annoncée par les capacités de stockage de la banque de données vSAN.

7 Sur la page Compatibilité de stockage, examinez la liste des banques de données sous les onglets **COMPATIBLE** et **INCOMPATIBLE**, puis cliquez sur **Suivant**.

Pour être admissible, une banque de données ne doit pas nécessairement être conforme à tous les ensembles de règles qui constituent la stratégie. Elle doit être conforme à au moins un ensemble de règles et à l'intégralité des règles de cet ensemble. Vérifiez que la banque de données de vSAN répond aux exigences définies dans la stratégie de stockage et qu'elle figure dans la liste de banques de données compatibles.

8 Dans la page Vérifier et terminer, vérifiez les paramètres de la stratégie, puis cliquez sur **Terminer**.

Résultats

La nouvelle stratégie est ajoutée à la liste.

Étape suivante

Attribuez cette stratégie à une machine virtuelle et à ses disques virtuels. vSAN place les objets de machine virtuelle selon les conditions spécifiées dans la stratégie. Pour plus d'informations sur l'application des stratégies de stockage aux objets de machine virtuelle, reportez-vous à la documentation de *Stockage vSphere*.

Développement et gestion d'un clustervSAN

4

Après avoir configuré votre cluster vSAN, vous pouvez ajouter des hôtes et des périphériques de capacité, supprimer des hôtes et des périphériques, et gérer des scénarios de panne.

Ce chapitre contient les rubriques suivantes :

Développement d'un cluster vSAN

Vous pouvez développer un cluster vSAN existant en ajoutant des hôtes ou des périphériques aux hôtes existants, sans interrompre les opérations en cours.

Utilisez l'une des méthodes suivantes pour développer votre cluster de vSAN.

- Ajoutez de nouveaux hôtes ESXi au cluster qui sont configurés à l'aide des périphériques cache et de capacité pris en charge. Reportez-vous à Ajouter un hôte au cluster vSAN.
- Déplacez les hôtes ESXi existants vers le cluster vSAN et configurez-les à l'aide du profil d'hôte. Reportez-vous à Configuation d'hôtes à l'aide du profil d'hôte.
- Ajoutez de nouveaux périphériques de capacité aux hôtes ESXi qui sont des membres du cluster. Reportez-vous à Ajouter des périphériques au groupe de disques.

Développement de vSAN la capacité et des performances du cluster

Si votre cluster vSAN manque de capacité de stockage ou si vous observez une réduction des performances du cluster, vous pouvez augmenter la capacité et les performances du cluster.

- (Uniquement pour vSAN Original Storage Architecture) Augmentez la capacité de stockage de votre cluster en ajoutant des périphériques de stockage aux groupes de disques existants ou en ajoutant des groupes de disques. Les nouveaux groupes de disques nécessitent des périphériques Flash pour le cache. Pour plus d'informations sur l'ajout de périphériques aux groupes de disques, reportez-vous à la section Ajouter des périphériques au groupe de disques. L'ajout de périphériques de capacité sans augmenter le cache risque de diminuer votre rapport cache-capacité à un niveau non pris en charge. Pour plus d'informations reportez-vous à la section *Planification et déploiement de vSAN*.

  Améliorez les performances du cluster en ajoutant au moins un périphérique de cache (Flash) et un périphérique de capacité (disque Flash ou magnétique) à un contrôleur d'E/S de stockage existant ou à un nouvel hôte. Vous pouvez également ajouter un ou plusieurs hôtes avec des groupes de disques, ce qui a les mêmes effets en termes de performances que lorsque vSAN exécute un rééquilibrage proactif du cluster vSAN.

- (Uniquement pour vSAN Express Storage Architecture) Augmentez la capacité de stockage de votre cluster en ajoutant des périphériques Flash aux pools de stockage des hôtes existants ou en ajoutant un ou plusieurs nouveaux hôtes avec des périphériques Flash.

Bien que des hôtes de calcul uniquement peuvent exister dans un cluster vSAN et consommer la capacité d'autres hôtes du cluster, ajoutez des hôtes configurés de manière uniforme pour garantir un bon fonctionnement. Même s'il est préférable d'utiliser des périphériques identiques ou similaires dans les groupes de disques ou les pools de stockage, n'importe quel périphérique répertorié sur la liste HCL vSAN est pris en charge. Tentez de distribuer équitablement la capacité sur les hôtes. Pour plus d'informations sur l'ajout de périphériques aux groupes de disques ou aux pools de stockage, reportez-vous à la section Créer un groupe de disques ou un pool de stockage.

Lorsque vous augmentez la capacité du cluster, effectuez un rééquilibrage manuel pour distribuer équitablement les ressources dans le cluster. Pour plus d'informations, reportez-vous à la section *Surveillance et dépannage de vSAN*.

Utilisez le démarrage rapide pour ajouter des hôtes à un cluster vSAN

Si vous avez configuré votre cluster vSAN avec le démarrage rapide, vous pouvez utiliser le workflow de démarrage rapide pour ajouter des hôtes et des périphériques de stockage au cluster.

Lorsque vous ajoutez de nouveaux hôtes au cluster vSAN, vous pouvez également utiliser l'assistant Configuration de cluster pour terminer la configuration de l'hôte. Pour plus d'informations sur le démarrage rapide, reportez-vous à « Utilisation du démarrage rapide pour configurer et développer un cluster vSAN » dans *Planification et déploiement de vSAN*.

Note Si vous exécutez vCenter Server sur un hôte, l'hôte ne peut pas être placé en mode de maintenance lorsque vous l'ajoutez à un cluster à l'aide du workflow de démarrage rapide. Le même hôte peut également exécuter une instance de Platform Services Controller. Toutes les autres machines virtuelles sur l'hôte doivent être hors tension.

Conditions préalables

- Le workflow de démarrage rapide doit être disponible pour votre cluster vSAN.
- Aucune configuration réseau effectuée via le workflow de démarrage rapide n'a été modifiée en dehors du workflow de démarrage rapide.

Procédure

1. Accédez au cluster dans vSphere Client.
2. Cliquez sur l'onglet Configurer, puis sélectionnez **Configuration > Démarrage rapide**.
3. Sur la fiche Ajouter des hôtes, cliquez sur **Lancer** pour ouvrir l'assistant Ajouter des hôtes.
   a. Sur la page Ajouter des hôtes, entrez les informations des nouveaux hôtes ou cliquez sur Hôtes existants et sélectionnez des hôtes répertoriés dans l'inventaire.
   b. Sur la page Résumé hôte, vérifiez les paramètres de l'hôte.
   c. Sur la page Prêt à terminer, cliquez sur **Terminer**.
4. Sur la fiche Configuration du cluster, cliquez sur **Lancer** pour ouvrir l'assistant Configuration de cluster.
   a. Sur la page Configurer des Distributed Switches, entrez les paramètres de mise en réseau pour les nouveaux hôtes.
   b. (Facultatif) Sur la page Réclamer des disques, sélectionnez des disques sur chaque nouvel hôte.
   c. (Facultatif) Sur la page Créer des domaines de pannes, déplacez les nouveaux hôtes dans leur domaine de pannes correspondant.

      Pour plus informations sur les domaines de pannes, reportez-vous à la section Gestion des domaines de pannes dans les clusters vSAN.
   d. Dans la page Prêt à terminer, vérifiez les paramètres du cluster, puis cliquez sur **Terminer**.

Ajouter un hôte au cluster vSAN

Vous pouvez ajouter des hôtes ESXi à un cluster vSAN en cours d'exécution, sans interrompre les opérations en cours. Les nouvelles ressources de l'hôte sont alors associées à ce cluster.

Conditions préalables

- Vérifiez que les ressources (notamment les pilotes, microprogrammes et contrôleurs d'E/S de stockage) sont répertoriées dans le Guide de compatibilité VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php.
- VMware vous recommande de créer des hôtes avec une configuration uniforme dans le cluster vSAN afin que les composants et les objets soient uniformément répartis entre les périphériques du cluster. Néanmoins, il peut y avoir des situations au cours desquelles le cluster se retrouve déséquilibré, en particulier pendant la maintenance ou si vous surchargez la capacité de la banque de données vSAN avec des déploiements de machines virtuelles excessifs.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez avec le bouton droit de la souris sur le cluster et sélectionnez **Ajouter des hôtes**. L'assistant Ajouter des hôtes s'ouvre.

Option	Description
Nouveaux hôtes	a Entrez le nom d'hôte ou l'adresse IP. b Entrez le nom d'utilisateur et le mot de passe associés à l'hôte.
Hôtes existants	a Sélectionnez les hôtes que vous avez précédemment ajoutés à vCenter Server.

3. Cliquez sur **Suivant**.
4. Lisez les informations récapitulatives et cliquez sur **Suivant**.
5. Vérifiez les paramètres et cliquez sur **Terminer**.

   L'hôte est ajouté au cluster.

Étape suivante

Vérifiez que le contrôle de santé Équilibre des disques vSAN est vert.

Pour plus d'informations sur la configuration du cluster vSAN et la résolution des problèmes, reportez-vous à la section « Problèmes de configuration du cluster vSAN » dans *Surveillance et dépannage de vSAN*.

Configuation d'hôtes à l'aide du profil d'hôte

Lorsque vous avez plusieurs hôtes dans le cluster vSAN, vous pouvez réutiliser le profil d'un hôte vSAN existant afin de configurer les autres hôtes du cluster vSAN.

Le profil d'un hôte contient des informations sur la configuration du stockage, la configuration du réseau ou d'autres caractéristiques de l'hôte. Si vous prévoyez de créer un cluster avec un grand nombre d'hôtes, par exemple 8, 16, 32 ou 64 hôtes, utilisez la fonctionnalité de profil d'hôte. Les profils d'hôte vous permettent d'ajouter plusieurs hôtes à la fois au cluster vSAN.

Conditions préalables

- Vérifiez que l'hôte est en mode maintenance.
- Vérifiez que les composants matériels, pilotes, microprogrammes et contrôleurs d'E/S de stockage sont répertoriés dans le Guide de compatibilité de VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php.

Procédure

1 Créez un profil d'hôte.
   a Accédez à la vue Profils d'hôtes.
   b Cliquez sur l'icône **Extraire un profil depuis un hôte** (✚).
   c Sélectionnez l'hôte que vous souhaitez utiliser comme hôte de référence et cliquez sur **Suivant**.

      L'hôte sélectionné doit être un hôte actif.
   d Tapez un nom et une description pour le nouveau profil, puis cliquez sur **Suivant**.
   e Vérifiez les informations récapitulatives pour le nouveau profil d'hôte et cliquez sur **Terminer**.

      Le nouveau profil figure dans la liste Profils d'hôte.
2 Attachez l'hôte au profil d'hôte.
   a Dans la liste des profils de la vue Profils d'hôte, sélectionnez le profil d'hôte à appliquer à l'hôte vSAN.
   b Cliquez sur l'icône **Attacher/Détacher des hôtes et des clusters à/d'un profil d'hôte** ( ).
   c Sélectionnez l'hôte dans la liste qui est développée, puis cliquez sur **Attacher** pour l'attacher au profil.

      L'hôte est ajouté à la liste Entités attachées.
   d Cliquez sur **Suivant**.
   e Cliquez sur **Terminer** pour terminer le détachement de l'hôte du profil.
3 Détachez l'hôte vSAN référencé du profil d'hôte.

   Lorsqu'un profil d'hôte est attaché à un cluster, l'hôte ou les hôtes du cluster sont également attachés au profil d'hôte. Toutefois, lorsque le profil d'hôte est détaché du cluster, l'association entre l'hôte ou les hôtes du cluster et ce profil d'hôte est maintenue.
   a Dans la liste de profils de la vue Profils d'hôte, sélectionnez le profil d'hôte à détacher d'un hôte ou d'un cluster.
   b Cliquez sur l'icône **Attacher/Détacher des hôtes et des clusters à/d'un profil d'hôte** ( ).
   c Sélectionnez l'hôte ou le cluster dans la liste étendue et cliquez sur **Détacher**.
   d Cliquez sur **Détacher tout** pour détacher du profil tous les hôtes et clusters répertoriés.

e Cliquez sur **Suivant**.

f Cliquez sur **Terminer** pour terminer le détachement de l'hôte du profil d'hôte.

4 Vérifiez si l'hôte vSAN est conforme au profil d'hôte qui lui est associé et déterminez quels sont les paramètres de configuration de l'hôte qui sont différents de ceux du profil, le cas échéant.

a Accédez à un profil d'hôte.

L'onglet **Objets** affiche la liste des profils d'hôte, le nombre d'hôtes associés à chaque profil, ainsi que le résumé des résultats de la dernière vérification de conformité.

b Cliquez sur l'icône **Vérifier la conformité d'un profil d'hôte** ( ).

Pour connaître en détail les paramètres qui diffèrent entre l'hôte non conforme et le profil d'hôte, cliquez sur l'onglet **Surveiller**, puis sélectionnez la vue Conformité. Développez la hiérarchie de l'objet et sélectionnez l'hôte non conforme. Les paramètres qui varient s'affichent dans la fenêtre Conformité, en-dessous de la hiérarchie.

En cas d'échec de la conformité, utilisez la fonction Corriger pour appliquer les paramètres du profil d'hôte à l'hôte. Cette action remplace les valeurs de tous les paramètres de profil d'hôte gérés par celles du profil d'hôte associé à l'hôte.

c Pour connaître en détail les paramètres qui diffèrent entre l'hôte non conforme et le profil d'hôte, cliquez sur l'onglet **Surveiller**, puis sélectionnez la vue Conformité.

d Développez la hiérarchie de l'objet et sélectionnez l'hôte défaillant.

Les paramètres qui varient s'affichent dans la fenêtre Conformité, en-dessous de la hiérarchie.

5 Corrigez l'hôte pour corriger les erreurs de conformité.

a Sélectionnez l'onglet **Surveiller**, puis cliquez sur **Conformité**.

b Cliquez avec le bouton droit sur l'hôte ou les hôtes à corriger, puis sélectionnez **Toutes les actions vCenter > Profils d'hôtes > Corriger**.

Vous pouvez mettre à jour ou modifier les paramètres d'entrée utilisateur des règles des profils d'hôtes en personnalisant l'hôte.

c Cliquez sur **Suivant**.

d Vérifiez les tâches qui sont nécessaires pour corriger le profil d'hôte et cliquez sur **Terminer**.

L'hôte fait partie du cluster vSAN et le cluster vSAN peut accéder aux ressources de cet hôte. L'hôte peut également accéder à toutes les stratégies d'E/S de stockage vSAN existant sur le cluster vSAN.

Partage de banques de données distantes avec le maillage HCI

Les clusters vSAN peuvent partager leurs banques de données avec d'autres clusters vSAN. Vous pouvez provisionner des machines virtuelles exécutées sur le cluster local pour utiliser l'espace de stockage sur la banque de données distante.

Note Si vSAN Express Storage Architecture est activé dans votre cluster, vous ne pouvez pas utiliser le cluster pour une configuration de maillage HCI.

Utilisez la vue Partage de banque de données pour surveiller et gérer des banques de données distantes montées sur le cluster vSAN local. Chaque cluster vSAN client peut monter des banques de données distantes à partir de clusters vSAN de serveurs situés dans le même centre de données géré par vCenter Server. Chaque cluster vSAN compatible peut également agir comme serveur et permettre à d'autres clusters vSAN de monter ses banques de données locales.

Le montage d'une banque de données distante avec le maillage HCI est une configuration à l'échelle du cluster. Vous pouvez monter une banque de données distante sur un cluster vSAN, qui est ensuite monté sur tous les hôtes du cluster.

Lorsque vous provisionnez une nouvelle machine virtuelle, vous pouvez sélectionner une banque de données distante montée sur le cluster client. Attribuez les stratégies de stockage compatibles configurées pour la banque de données.

Les vues de surveillance de la capacité, des performances, de la santé et du placement d'objets virtuels indiquent l'état des banques de données et des objets distants.

L'instance de vSAN du maillage HCI prend en compte les éléments suivants pour la conception :

- Les clusters doivent être gérés par le même serveur vCenter Server et se trouver dans le même centre de données.
- Les clusters doivent exécuter la version 7.0 Update 1 ou une version ultérieure.
- Un cluster vSAN peut desservir sa banque de données locale vers 10 clusters vSAN clients maximum.
- Un cluster client peut monter jusqu'à cinq banques de données distantes à partir d'un ou de plusieurs clusters de serveurs vSAN.
- Vous pouvez monter une banque de données distante unique sur 128 hôtes vSAN au maximum, y compris ceux dans le cluster de serveurs vSAN.
- Tous les objets qui constituent une machine virtuelle doivent résider sur la même banque de données.
- Pour que vSphere HA fonctionne avec le maillage HCI, configurez la réponse aux pannes suivante pour la banque de données avec APD : Mettre hors tension et redémarrer les machines virtuelles.

- Les hôtes clients qui ne font pas partie d'un cluster ne sont pas pris en charge. Vous pouvez configurer un cluster de calcul d'hôte unique, mais vSphere HA ne fonctionne pas, sauf si vous ajoutez un deuxième hôte au cluster.

Les fonctionnalités suivantes ne sont pas prises en charge avec le maillage HCI :

- Chiffrement des données en transit vSAN
- Clusters étendus vSAN
- Clusters à 2 nœuds vSAN

Les configurations suivantes ne sont pas prises en charge avec le maillage HCI :

- Provisionnement distant du partage de fichiers, des volumes iSCSI ou des volumes CNS persistants vSAN. Vous pouvez les provisionner sur la banque de données vSAN locale, mais pas sur une banque de données vSAN distante.
- Réseaux ou clusters vSAN isolés utilisant plusieurs ports VMkernel vSAN
- Communication de vSAN sur RDMA

Client de calcul uniquement de maillage HCI

vSAN 7.0 Update 2 et versions ultérieures permettent de configurer un cluster non-vSAN comme client de maillage HCI. Les hôtes d'un cluster client de calcul uniquement de maillage HCI ne nécessitent aucun stockage local. Ils peuvent monter des banques de données distantes à partir d'un cluster vSAN situé dans le même centre de données.

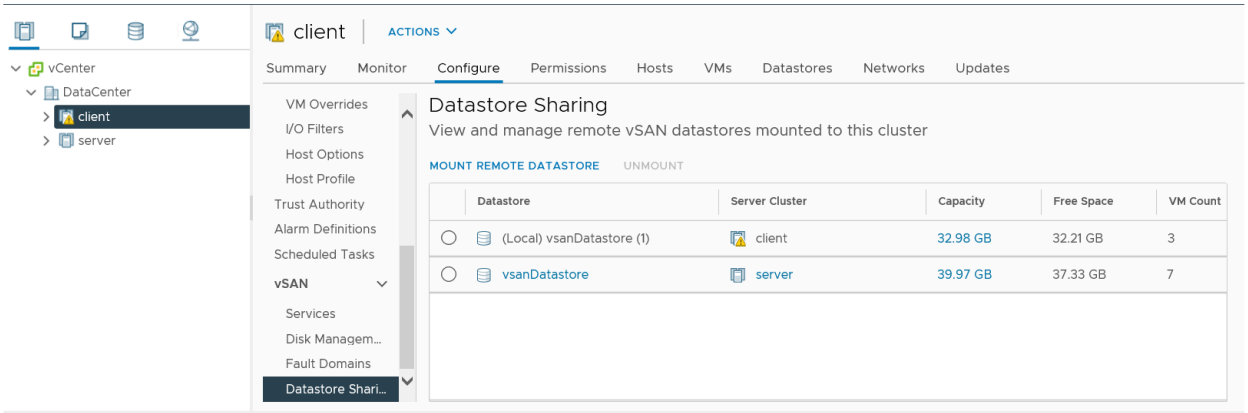
Les clusters de calcul uniquement de maillage HCI présentent les éléments à prendre en compte pour la conception :

- Vous devez configurer la mise en réseau vSAN sur les hôtes clients.
- Aucun groupe de disques ne peut être présent sur hôtes de calcul uniquement vSAN.
- Vous ne pouvez configurer aucune fonctionnalité de gestion des données vSAN sur le cluster de calcul uniquement.

Lorsque vous configurez un cluster vSphere pour vSAN, vous pouvez le spécifier en tant que cluster de calcul de maillage HCI. Vous pouvez monter une banque de données distante et surveiller la capacité, la santé et les performances de la banque de données vSAN distante.

Afficher les banques de données distantes

Utilisez la page Partage de banque de données pour afficher les banques de données distantes montées sur le cluster vSAN local et les clusters clients partageant la banque de données locale.



Procédure

1 Accédez au cluster vSAN local.

2 Cliquez sur l'onglet Configurer.

3 Sous vSAN, cliquez sur **Partage de banque de données**.

Résultats

Cette vue répertorie les informations sur chaque banque de données montée sur le cluster local.

- Cluster de serveurs qui héberge la banque de données
- Capacité de la banque de données
- Espace libre disponible
- Nombre de machines virtuelles utilisant la banque de données (nombre de machines virtuelles utilisant les ressources de calcul du cluster local, mais les ressources de stockage du cluster de serveurs)
- Clusters clients qui ont monté la banque de données.

Étape suivante

Vous pouvez monter ou démonter des banques de données distantes sur cette page.

Monter la banque de données distante

Vous pouvez monter une ou plusieurs banques de données à partir d'autres clusters vSAN gérés par le même serveur vCenter Server.

Procédure

1 Accédez au cluster vSAN local.

2 Cliquez sur l'onglet Configurer.

3 Sous vSAN, cliquez sur **Partage de banque de données**.

4 Cliquez sur **Monter la banque de données distante**.

5 Sélectionnez une banque de données et cliquez sur **Suivant**.

6 Vérifiez la compatibilité de la banque de données, puis cliquez sur **Terminer**.

Résultats

La banque de données distante est montée sur le cluster vSAN local.

Étape suivante

Lorsque vous provisionnez une machine virtuelle, vous pouvez sélectionner la banque de données distante en tant que ressource de stockage. Attribuez une stratégie de stockage prise en charge par la banque de données distante.

Démonter une banque de données distante

Vous pouvez démonter une banque de données distante d'un cluster vSAN.

Si aucune machine virtuelle du cluster local n'utilise la banque de données vSAN distante, vous pouvez démonter la banque de données de votre cluster vSAN local.

Procédure

1 Accédez au cluster vSAN local.

2 Cliquez sur l'onglet Configurer.

3 Sous vSAN, cliquez sur **Partage de banque de données**.

4 Sélectionnez une banque de données et cliquez sur **Démonter**.

5 Cliquez sur **Démonter** pour confirmer.

Résultats

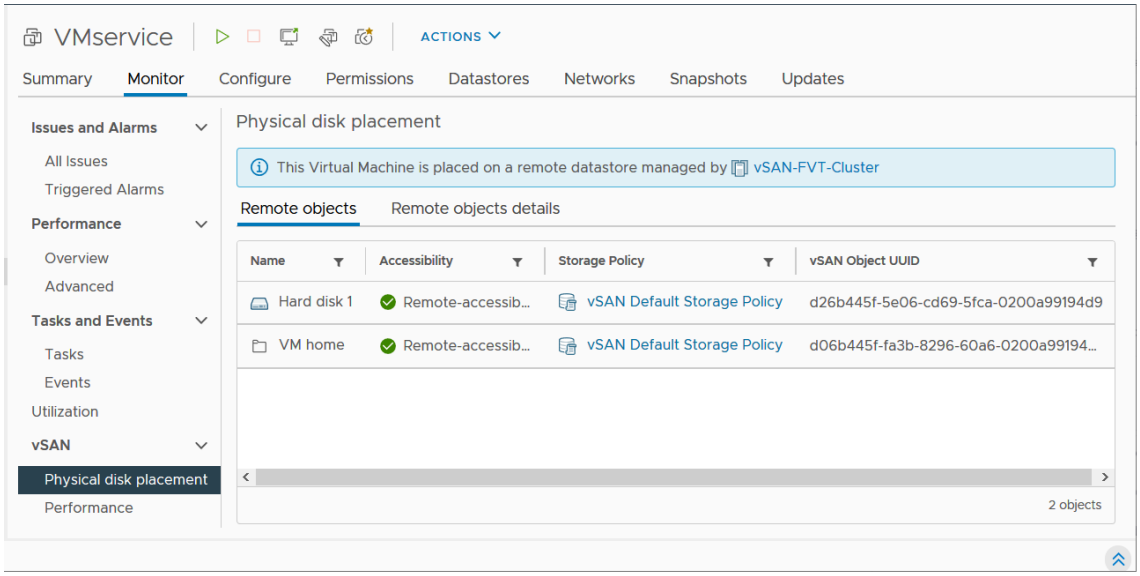
La banque de données sélectionnée est démontée du cluster local.

Surveiller le maillage HCI

Vous pouvez utiliser vSphere Client pour surveiller l'état des opérations de maillage HCI.

Le moniteur de capacité vSAN vous avertit lorsque des banques de données distantes sont montées sur le cluster. Vous pouvez sélectionner la banque de données distante pour afficher les informations sur sa capacité.

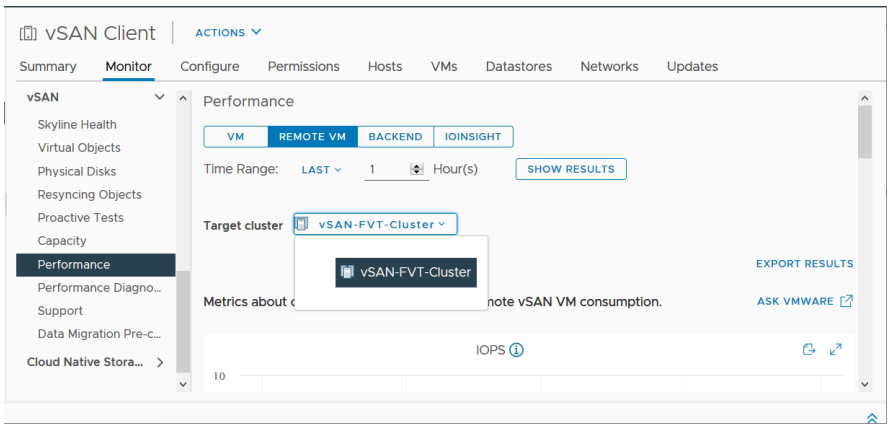
La vue Objets virtuels affiche la banque de données dans laquelle résident les objets virtuels. La vue Emplacement physique du disque d'une machine virtuelle située sur une banque de données distante affiche des informations sur son emplacement distant.



Les contrôles de santé vSAN informent sur l'état des fonctions HCI.

- Données > Contrôle de santé de l'objet vSAN affiche les informations sur l'accessibilité des objets distants.
- Réseau > Contrôle de partition du cluster de serveurs signale les partitions réseau entre les hôtes du cluster client et du cluster de serveurs.
- Réseau > Latence contrôle la latence entre les hôtes du cluster client et du cluster de serveurs.

Les vues Performances du cluster vSAN incluent des diagrammes de performances de machine virtuelle qui affichent les performances au niveau de la machine virtuelle du cluster client du point de vue du cluster distant. Vous pouvez sélectionner une banque de données distante pour afficher les performances.



Vous pouvez exécuter des tests proactifs sur des banques de données distantes pour vérifier la création de machines virtuelles et les performances du réseau. Le test de création de VM crée une VM sur la banque de données distante. Le test de performances réseau vérifie les performances du réseau entre tous les hôtes du cluster client et tous les hôtes des clusters de serveurs.

Utilisation du mode de maintenance

Avant de pouvoir arrêter, redémarrer ou déconnecter un hôte faisant partie d'un cluster vSAN, vous devez le placer en mode de maintenance.

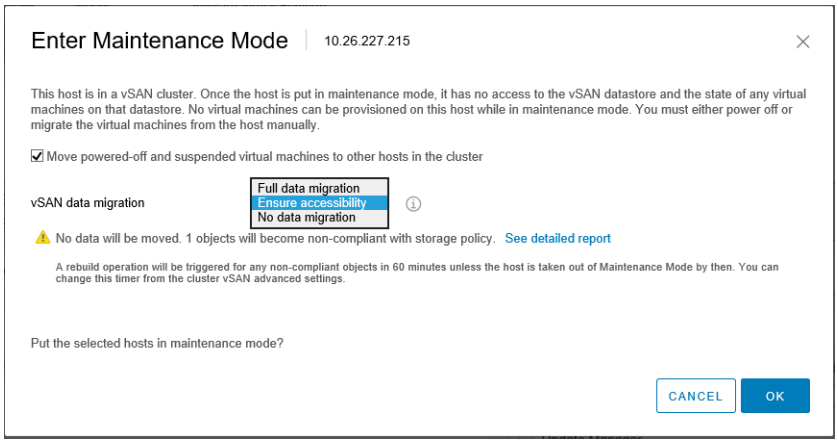
Lors de l'utilisation du mode de maintenance, tenez compte des directives suivantes :

- Lorsque vous placez un hôte ESXi en mode de maintenance, vous devez sélectionner un mode de suppression de données, tel que **Assurer l'accessibilité** ou **Migration intégrale des données**.
- Lorsqu'un hôte membre d'un cluster vSAN entre en mode de maintenance, la capacité du cluster est automatiquement réduite du fait que l'hôte membre ne contribue plus au stockage du cluster.
- Les ressources de calcul d'une machine virtuelle peuvent ne pas résider sur l'hôte qui est placé en mode de maintenance, et les ressources de stockage des machines virtuelles peuvent se trouver n'importe où dans le cluster.
- Le mode **Assurer l'accessibilité** est plus rapide que le mode **Migration intégrale des données**, car le mode **Assurer l'accessibilité** migre uniquement les composants des hôtes qui sont essentiels à l'exécution des machines virtuelles. Dans ce mode, lorsque vous rencontrez une panne, la disponibilité de votre machine virtuelle est affectée. La sélection du mode **Assurer l'accessibilité** ne reprotège pas vos données pendant une panne et une perte de données inattendue risque de se produire.
- Lorsque vous sélectionnez le mode **Migration intégrale des données**, vos données sont automatiquement reprotégées en cas de panne, si les ressources sont disponibles et que le paramètre **Pannes tolérées** est défini sur 1 ou plus. Dans ce mode, tous les composants de l'hôte sont migrés et, en fonction du volume des données qui se trouvent sur l'hôte, la migration pourrait être plus longue. Avec le mode **Migration intégrale des données**, vos machines virtuelles peuvent tolérer des pannes, même au cours d'une maintenance planifiée.
- Lors de l'utilisation d'un cluster à trois hôtes, vous ne pouvez pas placer un serveur en mode de maintenance avec **Migration intégrale des données**. Envisagez de concevoir un cluster avec quatre hôtes ou plus pour une disponibilité maximale.

Avant de placer un hôte en mode de maintenance, vous devez vérifier les éléments suivants :

- Si vous utilisez le mode **Migration intégrale des données**, vérifiez que le cluster dispose de suffisamment d'hôtes et de capacité pour répondre aux conditions requises de la stratégie **Pannes tolérées**.
- Vérifiez qu'une capacité Flash suffisante existe sur les hôtes restants afin de pouvoir traiter les réservations de Flash Read Cache. Pour analyser la capacité actuelle utilisée par hôte et déterminer si une panne d'hôte unique peut entraîner un manque d'espace sur le cluster et affecter la capacité, la réservation de cache et les composants du cluster, exécutez la commande RVC suivante : `vsan.whatif_host_failures`. Pour plus d'informations sur les commandes de RVC, reportez-vous au *Guide de référence des commandes de l'outil RVC*.

- Vérifiez que vous disposez de suffisamment de périphériques de capacité dans les hôtes restants afin de répondre aux conditions relatives à la largeur des bandes, le cas échéant.
- Assurez-vous de disposer d'une capacité libre suffisante sur les hôtes restants afin de pouvoir traiter le volume de données à migrer depuis l'hôte entrant en mode de maintenance.



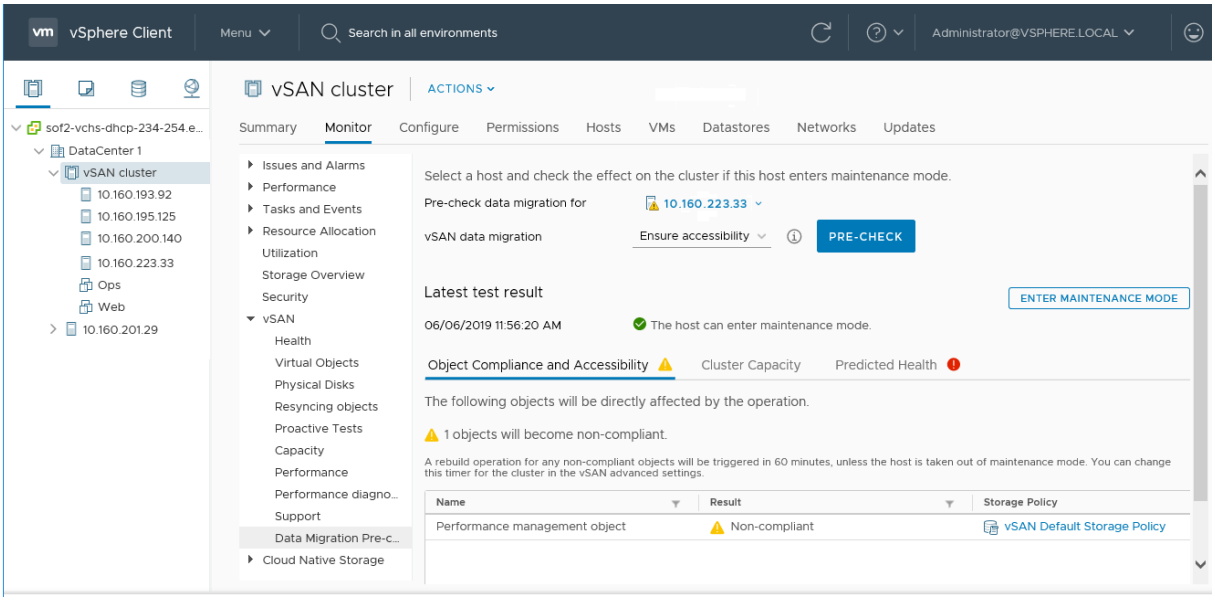
La boîte de dialogue Confirmer le mode maintenance fournit des informations pour guider vos activités de maintenance. Vous pouvez afficher l'incidence de chaque option d'évacuation de données.

- Si la capacité disponible est suffisante pour effectuer l'opération.
- La quantité de données qui seront déplacées.
- Le nombre d'objets qui deviendront non conformes.
- Le nombre d'objets qui deviendront inaccessibles.

Vérifier les capacités de migration des données d'un hôte

Utilisez la prévérification de la migration des données pour déterminer l'effet des options de migration des données lorsque vous placez un hôte en mode de maintenance ou que vous le supprimez du cluster.

Avant de placer un hôte vSAN en mode de maintenance, exécutez la prévérification de la migration des données. Les résultats des tests fournissent des informations pour vous aider à déterminer l'impact sur la capacité du cluster, les contrôles de santé prévus et tous les objets qui seront incompatibles. Si l'opération échoue, la prévérification fournit des informations sur les ressources nécessaires.



Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet Surveiller.

3 Sous vSAN, cliquez sur **Prévérification de la migration des données**.

4 Sélectionnez un hôte, une option de migration de données et cliquez sur **Prévérification**.

vSAN exécute les tests de prévérification de migration des données.

5 Affichez les résultats du test.

Les résultats de la prévérification indiquent si l'hôte peut passer en mode de maintenance en toute sécurité.

- L'onglet Conformité et accessibilité des objets affiche les objets susceptibles de présenter des problèmes après la migration des données.
- L'onglet Capacité du cluster affiche l'impact de la migration des données sur le cluster vSAN avant et après l'exécution de l'opération.
- L'onglet Santé prévue affiche les contrôles de santé qui peuvent être affectés par la migration des données.

Étape suivante

Si la prévérification indique que vous pouvez placer l'hôte en mode de maintenance, vous pouvez cliquer sur **Entrer en mode de maintenance** pour migrer les données et placer l'hôte en mode de maintenance.

Placer un membre de cluster vSAN en mode de maintenance

Avant de pouvoir arrêter, redémarrer ou déconnecter un hôte faisant partie d'un cluster de vSAN, vous devez le placer en mode de maintenance. Lorsque vous placez un hôte en mode de maintenance, vous devez sélectionner un mode de suppression de données, tel que **Assurer l'accessibilité** ou **Migration intégrale des données**.

Lorsqu'un hôte membre d'un cluster vSAN passe en mode de maintenance, la capacité du cluster est automatiquement réduite, car l'hôte membre ne contribue plus à la capacité du cluster.

Toutes les cibles iSCSI vSAN servies par cet hôte sont transférées vers d'autres hôtes du cluster, et par conséquent, l'initiateur iSCSI est redirigé vers le nouveau propriétaire de la cible.

Conditions préalables

Vérifiez que votre environnement dispose des capacités requises par l'option sélectionnée.

Procédure

1. Cliquez avec le bouton droit sur l'hôte et sélectionnez **Mode maintenance > Passer en mode maintenance**.

2 Sélectionnez un mode de suppression des données, puis cliquez sur **OK**.

Option	Description
Assurer l'accessibilité	Il s'agit de l'option par défaut. Lorsque vous mettez l'hôte hors tension ou que vous le supprimez du cluster, vSAN veille à ce que toutes les machines virtuelles accessibles sur cet hôte le restent. Sélectionnez cette option si vous souhaitez retirez l'hôte du cluster de manière provisoire (par exemple, pour installer des mises à niveau) et que vous prévoyez de l'intégrer de nouveau au cluster. Cette option n'est pas appropriée si vous souhaitez supprimer définitivement l'hôte du cluster. En général, seule l'évacuation partielle des données est requise. Toutefois, la machine virtuelle peut ne plus être entièrement conforme à une stratégie de stockage de VM lors de l'évacuation. Par conséquent, elle peut ne pas avoir accès à toutes ses répliques. Si une panne se produit lorsque l'hôte est en mode de maintenance et que l'option **Pannes tolérées** est définie sur 1, vous risquez de perdre des données du cluster. **Note** Il s'agit du seul mode d'évacuation disponible si vous travaillez avec un cluster à trois hôtes ou un cluster vSAN configuré avec trois domaines de pannes.
Migration intégrale des données	vSAN évacue toutes les données vers les autres hôtes du cluster et maintient l'état actuel de conformité des objets. Sélectionnez-la si vous prévoyez de migrer l'hôte définitivement. Lorsque vous évacuez des données du dernier hôte du cluster, assurez-vous de migrer les machines virtuelles vers une autre banque de données, puis placez l'hôte en mode de maintenance. Ce mode de suppression entraîne le plus gros transfert de données et consomme le plus de temps et de ressources. Tous les composants sur le stockage local de l'hôte sélectionné sont migrés ailleurs dans le cluster. Lorsque l'hôte entre en mode de maintenance, toutes les machines virtuelles ont accès à leurs composants de stockage et sont toujours conformes aux stratégies de stockage attribuées. **Note** S'il existe des objets dans l'état de disponibilité réduite, ce mode maintient cet état de conformité et ne garantit pas la conformité des objets. Si un objet de la machine virtuelle dont l'hôte comporte des données n'est pas accessible et n'est pas entièrement évacué, l'hôte ne peut pas passer en mode de maintenance.
Aucune migration de données	vSAN ne supprime aucune données de cet hôte. Si vous mettez hors tension ou supprimez l'hôte du cluster, certaines machines virtuelles peuvent devenir inaccessibles.

Un cluster avec trois domaines de pannes a les mêmes restrictions qu'un cluster à trois hôtes, comme l'incapacité d'utiliser le mode **Migration intégrale des données** et de reprotéger les données après une panne.

Vous pouvez également placer un hôte en mode de maintenance à l'aide d'ESXCLI. Avant de placer un hôte dans ce mode, veillez à mettre hors tension les VM qui s'exécutent sur l'hôte.

Pour passer en mode de maintenance, exécutez la commande suivante sur l'hôte :

```
esxcli system maintenanceMode set --enable 1
```

Pour vérifier l'état de l'hôte, exécutez la commande suivante :

```
esxcli system maintenanceMode get
```

Pour quitter le mode de maintenance, exécutez la commande suivante :

```
esxcli system maintenanceMode set --enable 0
```

Étape suivante

Vous pouvez suivre l'état d'avancement de la migration des données dans le cluster. Pour plus d'informations, reportez-vous à la section *Surveillance et dépannage de vSAN*.

Gestion des domaines de pannes dans les clusters vSAN

Les domaines de pannes vous permettent de vous protéger contre une panne du rack ou du châssis si votre cluster vSAN s'étend sur plusieurs racks ou châssis de serveur lame. Vous pouvez créer des domaines de pannes et ajouter un ou plusieurs hôtes à chaque domaine de pannes.

Un domaine de pannes comprend un ou plusieurs hôtes vSAN regroupés en fonction de leur emplacement physique dans le centre de données. Une fois configurés, les domaines de pannes permettent à vSAN de tolérer les échecs de l'intégralité des racks physiques ainsi que les échecs d'un hôte, d'un périphérique de capacité, d'une liaison réseau ou d'un commutateur réseau unique dédié à un domaine de pannes.

La stratégie **Pannes tolérées** pour le cluster dépend du nombre de pannes qu'une machine virtuelle peut tolérer selon son provisionnement. Lorsqu'une machine virtuelle est configurée avec l'option **Pannes tolérées** définie sur 1 `(FTT=1)`, vSAN peut tolérer une panne unique de n'importe quel type et de n'importe quel composant d'un domaine de pannes, y compris la panne d'un rack entier.

Lorsque vous configurez des domaines de pannes sur un rack et que vous provisionnez une nouvelle machine virtuelle, vSAN s'assure que les objets de protection, comme les réplicas et les témoins, sont placés dans différents domaines de pannes. Par exemple, si la stratégie de stockage d'une machine virtuelle définit **Pannes tolérées** sur N `(FTT=n)`, vSAN nécessite un minimum de `2*n+1` domaines de pannes dans le cluster. Lorsque des machines virtuelles sont provisionnées dans un cluster avec des domaines de pannes utilisant cette stratégie, les copies des objets de machine virtuelle associés sont stockées sur des racks distincts.

Un minimum de trois domaines de pannes est requis pour prendre en charge l'option FTT=1. Pour de meilleurs résultats, configurez quatre domaines de pannes ou plus dans le cluster. Un cluster avec trois domaines de pannes a les mêmes restrictions qu'un cluster à trois hôtes, comme l'incapacité de reprotéger les données après une panne et d'utiliser le mode **Migration intégrale des données**. Pour plus d'informations sur la conception et le dimensionnement de domaines de pannes, reportez-vous à la section « Conception et dimensionnement de domaines de pannes vSAN » dans *Planification et déploiement de vSAN*.

Envisagez un scénario dans lequel vous avez un cluster vSAN avec 16 hôtes. Les hôtes sont répartis sur quatre racks, chaque rack contenant quatre hôtes. Afin de tolérer al panne de l'intégralité d'un rack, vous devez créer un domaine de pannes pour chaque rack. Vous pouvez configurer un cluster de cette capacité lorsque l'option **Pannes tolérées** est définie sur 1. Si vous voulez que l'option **Pannes tolérées** soit définie sur 2, configurez cinq domaines de pannes dans le cluster.

Lorsqu'un rack est défaillant, toutes les ressources comprenant le CPU et la mémoire dans le rack deviennent inaccessible au cluster. Pour réduire l'impact d'une panne potentielle du rack, vous devez configurer des domaines de pannes de taille inférieure. L'augmentation du nombre de domaines de pannes augmente la disponibilité totale des ressources dans le cluster après une panne du rack.

Lorsque vous utilisez des domaines de pannes, suivez ces recommandations.

- Configurez un minimum de trois domaines de pannes dans le cluster vSAN. Pour de meilleurs résultats, configurez quatre domaines de pannes ou plus.
- Un hôte non inclus dans un domaine de pannes est considéré résider dans son propre domaine de pannes à hôte unique.
- Vous n'avez pas besoin d'attribuer chaque hôte vSAN à un domaine de pannes. Si vous décidez d'utiliser des domaines de pannes pour protéger l'environnement vSAN, pensez à créer des domaines de pannes de taille identique.
- Lorsque des hôtes vSAN sont déplacés vers un autre cluster, ils conservent les domaines de pannes qui leur sont attribués.
- Lorsque vous concevez un domaine de pannes, placez un nombre uniforme d'hôtes dans chaque domaine de pannes.

  Pour obtenir des instructions sur la conception des domaines de pannes, reportez-vous à la section « Conception et dimensionnement de domaines de pannes vSAN » dans *Planification et le déploiement de vSAN*.
- Vous pouvez ajouter n'importe quel nombre d'hôtes à un domaine de pannes. Chaque domaine de pannes doit contenir au moins un hôte.

Créer un nouveau domaine de pannes dans le cluster vSAN

Pour s'assurer que les objets de machine virtuelle continuent de s'exécuter sans encombre en cas de panne de rack, vous pouvez regrouper les hôtes dans différents domaines de pannes.

Lorsque vous provisionnez une machine virtuelle sur le cluster comportant des domaines de pannes, vSAN distribue des composants de protection, comme des témoins et des répliques des objets de machine virtuelle, dans les différents domaines de pannes. En conséquence, l'environnement vSAN devient capable de tolérer des pannes dans l'ensemble d'un rack en plus d'une panne d'hôte, de disque de stockage ou de réseau unique.

Conditions préalables

- Choisissez un nom de domaine de pannes unique. vSAN ne prend pas en charge les noms de domaine de pannes en double dans un cluster.
- Vérifiez la version de vos hôtes ESXi. Vous ne pouvez inclure que des hôtes de la version 6.0 ou ultérieure dans des domaines de pannes.
- Vérifiez que vos hôtes vSAN sont en ligne. Vous ne pouvez pas attribuer des hôtes à un domaine de pannes hors ligne ou indisponible en raison d'un problème de configuration matérielle.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, cliquez sur **Domaines de pannes**.
4. Cliquez sur l'icône plus. L'assistant Nouveau domaine de pannes s'ouvre.
5. Entrez le nom du domaine de pannes.
6. Sélectionnez un ou plusieurs hôtes à ajouter au domaine de pannes.

   Un domaine de pannes ne peut pas être vide. Vous devez sélectionner au moins un hôte à inclure dans le domaine de pannes.
7. Cliquez sur **Créer**.

   Les hôtes sélectionnés s'affichent dans le domaine de pannes. Chaque domaine de pannes affiche les informations de capacité utilisée et réservée. Cela vous permet d'afficher la répartition de capacité dans le domaine de pannes.

Déplacer des hôtes vers un domaine de pannes

Vous pouvez déplacer un hôte vers un domaine de pannes sélectionné dans le cluster vSAN.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, cliquez sur **Domaines de pannes**.
4. Cliquez sur l'hôte que vous souhaitez ajouter sur un domaine de pannes existant et faites-le glisser.

   L'hôte sélectionné s'affiche dans le domaine de pannes.

Retirer des hôtes d'un domaine de pannes

Selon vos conditions requises, vous pouvez retirer des hôtes d'un domaine de pannes.

Conditions préalables

Vérifiez que l'hôte est en ligne. Vous ne pouvez pas déplacer des hôtes qui sont hors ligne ou non disponibles d'un domaine de pannes.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, cliquez sur **Domaines de pannes**.

   a Cliquez sur l'hôte et faites-le glisser du domaine de pannes vers la zone Hôtes autonomes.

   b Cliquez sur **Déplacer** pour confirmer.

Résultats

L'hôte sélectionné ne fait plus partie du domaine de pannes. Tout hôte qui ne fait pas partie d'un domaine de pannes est considéré résider dans son propre domaine de pannes à hôte unique.

Étape suivante

Vous pouvez ajouter des hôtes à des domaines de pannes. Reportez-vous à Déplacer des hôtes vers un domaine de pannes.

Renommer un domaine de pannes

Vous pouvez modifier le nom d'un domaine de pannes existant dans votre cluster vSAN.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, cliquez sur **Domaines de pannes**.

   a Cliquez sur l'icône Actions sur le côté droit du domaine de pannes et sélectionnez **Modifier**.

   b Entrez le nouveau nom du domaine de pannes.

4 Cliquez sur **Appliquer** ou **OK**.

   Le nouveau nom apparaît dans la liste des domaines de pannes.

Supprimer les domaines de pannes sélectionnés

Lorsque vous n'avez plus besoin d'un domaine de pannes, vous pouvez le supprimer du cluster vSAN.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, cliquez sur **Domaines de pannes**.

4 Cliquez sur l'icône Actions sur le côté droit du domaine de pannes et sélectionnez **Supprimer**.

5 Cliquez sur **Supprimer** pour confirmer.

Résultats

Tous les hôtes du domaine de pannes sont supprimés et le domaine de pannes sélectionné est supprimé du cluster vSAN. Chaque hôte qui ne fait pas partie d'un domaine de pannes est considéré résider dans son propre domaine de pannes à hôte unique.

Tolérer des pannes supplémentaires avec le domaine de pannes

Les domaines de pannes dans un cluster vSAN fournissent la résilience et garantissent la disponibilité des données, même en cas de pannes basées sur la stratégie. Si le nombre de pannes à tolérer (FTT) est défini sur 1, l'objet peut tolérer une panne. Cependant, une panne temporaire suivie d'une panne permanente dans un cluster peut entraîner une perte de données.

Un domaine de pannes supplémentaire permet à vSAN de créer un composant de durabilité sans disposer d'autres FTT pour l'objet. vSAN déclenche ce composant supplémentaire lors de pannes prévues et imprévues. Les pannes imprévues comprennent la déconnexion du réseau, les pannes de disques et les pannes d'hôtes. Les pannes prévues comprennent la tâche Entrer en mode de maintenance (EMM, Entering Maintenance Mode). Par exemple, un cluster à 6 hôtes avec un objet RAID 6 ne peut créer aucun composant de durabilité en cas de panne d'hôte.

vSAN garantit la disponibilité des données des objets lorsque les composants sont hors ligne et qu'ils reviennent en ligne de manière inattendue en fonction des FTT spécifiées dans la stratégie de stockage. En cas de panne, les opérations d'écriture du composant en panne sont redirigées vers le composant de durabilité. Lorsque le composant récupère suite à la panne temporaire et revient en ligne, le composant de durabilité ne s'affiche plus et entraîne la resynchronisation du composant.

Sans le composant de durabilité en place, si une deuxième panne permanente se produit dans le cluster et que l'objet miroir est concerné, les données de l'objet sont définitivement perdues, même en cas de résolution de la panne.

Utilisation du service cible iSCSI vSAN

Utilisez le service cible iSCSI pour activer les hôtes et les charges de travail physiques qui résident en dehors du cluster vSAN et accéder à la banque de données vSAN.

Cette fonctionnalité active un initiateur iSCSI sur un hôte distant afin de transporter les données de niveau bloc vers une cible iSCSI sur un périphérique de stockage d'un cluster vSAN. vSAN 6.7 et versions ultérieures prennent en charge la fonctionnalité WSFC (clustering de basculement Windows Server), pour que les nœuds WSFC puissent accéder aux cibles iSCSI vSAN.

Après avoir configuré le service cible iSCSI vSAN, vous pouvez détecter les cibles iSCSI vSAN d'un hôte distant. Pour détecter les cibles iSCSI vSAN, utilisez l'adresse IP de chaque hôte dans le cluster vSAN et le port TCP de la cible iSCSI. Pour garantir une haute disponibilité pour la cible iSCSI vSAN, configurez la prise en charge de chemins multiples pour votre application iSCSI. Vous pouvez utiliser les adresses IP de plusieurs hôtes pour configurer les chemins multiples.

Note Le service cible iSCSI vSAN ne prend pas en charge les autres initiateurs ou clients vSphere ou ESXi, les hyperviseurs tiers, ni les migrations qui utilisent le mappage de périphériques bruts (RDM).

Le service cible iSCSI vSAN prend en charge les méthodes d'authentification CHAP suivantes :

CHAP

En authentification CHAP, la cible authentifie l'initiateur, mais l'initiateur n'authentifie pas la cible.

CHAP mutuel

Dans l'authentification CHAP mutuelle, un niveau de sécurité supplémentaire permet à l'initiateur d'authentifier la cible.

Pour plus d'informations sur l'utilisation du service cible iSCSI vSAN, reportez-vous au *Guide d'utilisation de la cible iSCSI vSAN*.

Cibles iSCSI

Vous pouvez ajouter une ou plusieurs cibles iSCSI pour fournir des blocs de stockage comme numéros d'unité logique (LUN). vSAN identifie chaque cible iSCSI en fonction de son nom qualifié iSCSI (IQN) unique. Vous pouvez utiliser l'IQN pour présenter la cible iSCSI à un initiateur iSCSI distant afin que l'initiateur puisse accéder au LUN de la cible.

Chaque cible iSCSI contient un ou plusieurs LUN. Vous pouvez définir la taille chaque LUN, attribuer une stratégie de stockage vSAN à chaque LUN et activer le service cible iSCSI sur un cluster vSAN. Vous pouvez configurer une stratégie de stockage à utiliser par défaut pour l'objet de base du service cible iSCSI vSAN.

Groupes d'initiateurs iSCSI

Vous pouvez définir un groupe d'initiateurs iSCSI ayant accès à une cible iSCSI donnée. Le groupe d'initiateurs iSCSI limite l'accès aux initiateurs membres du groupe uniquement. Si vous ne définissez pas d'initiateur iSCSI ou de groupe d'initiateurs, alors chaque cible est accessible par tous les initiateurs iSCSI.

Un nom unique identifie chaque groupe d'initiateurs iSCSI. Vous pouvez ajouter un ou plusieurs initiateurs iSCSI comme membres du groupe. Utilisez l'IQN de l'initiateur comme nom d'initiateur membre.

Activer le service cible iSCSI

Avant de pouvoir créer des cibles iSCSI ou des LUN et définir des groupes d'initiateurs iSCSI, vous devez activer le service cible iSCSI sur le cluster vSAN.

Procédure

1. Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Services**.
2. Sur la ligne Service cible iSCSI vSAN, cliquez sur **ACTIVER**.

   L'assistant Modifier le service cible iSCSI vSAN s'ouvre.
3. Modifiez la configuration du service cible iSCSI vSAN.

   Vous pouvez sélectionner le réseau par défaut, le port TCP et la méthode d'authentification à ce moment. Vous pouvez également sélectionner une stratégie de stockage vSAN.
4. Cliquez sur le curseur **Activer le service cible iSCSI vSAN** pour l'activer, puis cliquez sur **APPLIQUER**.

Résultats

Le service cible iSCSI vSAN est activé.

Étape suivante

Après avoir activé le service cible iSCSI, vous pouvez créer des cibles iSCSI ou des LUN et définir des groupes d'initiateurs iSCSI.

Créer une cible iSCSI

Vous pouvez créer ou modifier une cible iSCSI et le LUN qui y est associé.

Conditions préalables

Vérifiez que le service cible iSCSI est activé.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
   a. Sous vSAN, cliquez sur **Service cible iSCSI**.
   b. Cliquez sur l'onglet Cibles iSCSI.
   c. Cliquez sur **Ajouter**. La boîte de dialogue **Nouvelle cible iSCSI** s'affiche. Si vous laissez le champ IQN cible vide, le nom IQN sera généré automatiquement.
   d. Saisissez un **alias** cible.

e Sélectionnez une **Stratégie de stockage**, un **Réseau**, un **Port TCP** et une méthode d'**authentification**.

f Sélectionnez l'**emplacement du propriétaire d'E/S**. Cette fonctionnalité n'est disponible que si vous avez configuré un cluster vSAN en tant que cluster étendu. Elle vous permet de spécifier l'emplacement du site pour l'hébergement du service cible iSCSI pour une cible. Cela permet d'éviter le trafic iSCSI entre sites. Si vous avez défini la stratégie sur HFT>=1, en cas de défaillance du site, l'emplacement du propriétaire d'E/S devient le site secondaire. Après la récupération de la défaillance du site, l'emplacement du propriétaire d'E/S est automatiquement remplacé par l'emplacement du propriétaire d'E/S d'origine conformément à la configuration. Vous pouvez sélectionner l'une des options suivantes pour définir l'emplacement du site :

- **L'un ou l'autre** : héberge le service cible iSCSI sur un site Préféré ou Secondaire.
- **Préféré** : héberge le service cible iSCSI sur le site préféré.
- **Secondaire** : héberge le service cible iSCSI sur le site secondaire.

3 Cliquez sur **OK**.

Résultats

La cible iSCSI est créée et répertoriée dans la section des cibles iSCSI vSAN avec les informations telles que IQN, l'hôte du propriétaire d'E/S, etc.

Étape suivante

Définissez une liste d'initiateurs iSCSI pouvant accéder à cette cible.

Ajouter un LUN à une cible iSCSI

Vous pouvez ajouter un ou plusieurs LUN à une cible iSCSI ou modifier un LUN existant.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

a Sous vSAN, cliquez sur **Service cible iSCSI**.

b Cliquez sur l'onglet Cibles iSCSI, puis sélectionnez une cible.

c Dans la section LUN iSCSI vSAN, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un LUN à la cible** s'affiche.

d Saisissez la taille du LUN. La stratégie de stockage vSAN configurée pour le service cible iSCSI est attribuée de manière automatique. Vous pouvez attribuer une stratégie différente pour chaque LUN.

3 Cliquez sur **Ajouter**.

Redimensionner un LUN sur une cible iSCSI

En fonction de vos besoins, vous pouvez augmenter la taille d'un LUN en ligne. Le redimensionnement en ligne du LUN est activé uniquement si tous les hôtes du cluster sont mis à niveau vers vSAN 6.7 Update 3 ou version ultérieure.

Procédure

1. Dans vSphere Client, accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, cliquez sur **Service cible iSCSI**.
4. Cliquez sur l'onglet **Cibles iSCSI**, puis sélectionnez une cible.
5. Dans la section LUN iSCSI vSAN, sélectionnez un LUN et cliquez sur **Modifier**. La boîte de dialogue Modifier le LUN s'affiche.
6. Augmentez la taille du LUN en fonction de vos besoins.
7. Cliquez sur **OK**.

Créer un groupe d'initiateurs iSCSI

Vous pouvez créer un groupe d'initiateurs iSCSI pour fournir un contrôle d'accès aux cibles iSCSI. Seuls les initiateurs iSCSI membres du groupe d'initiateurs peuvent accéder aux cibles iSCSI.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
   a. Sous vSAN, cliquez sur **Service cible iSCSI**.
   b. Cliquez sur l'onglet Groupes d'initiateurs et cliquez sur l'icône **Ajouter un nouveau groupe d'initiateurs iSCSI** (✚). La boîte de dialogue **Nouveau groupe d'initiateurs** s'affiche.
   c. Entrez un nom pour le groupe d'initiateurs iSCSI.
   d. (Facultatif) Pour ajouter des membres au groupe d'initiateurs, saisissez l'IQN de chaque membre. Utilisez le format suivant pour saisir l'IQN des membres :

      iqn.AAAA-MM.domaine:nom

      Où :

      - AAAA = année. Par exemple, 2016
      - MM = mois. Par exemple, 09
      - domaine = domaine dans lequel réside l'initiateur
      - nom = nom du membre (facultatif)
3. Cliquez sur **OK** ou **Créer**.

Étape suivante

Ajoutez des membres au groupe d'initiateurs iSCSI.

Attribuer une cible à un groupe d'initiateurs iSCSI

Vous pouvez attribuer une cible iSCSI à un groupe d'initiateurs iSCSI. Seuls les initiateurs membres du groupe d'initiateurs peuvent accéder aux cibles attribuées.

Conditions préalables

Vérifiez que vous possédez un groupe d'initiateurs iSCSI existant.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
   a. Sous vSAN, cliquez sur **Service cible iSCSI**.
   b. Sélectionnez l'onglet **Groupes d'initiateurs**.
   c. Dans la section Cibles accessibles, cliquez sur l'icône **Ajouter une nouvelle cible accessible pour le groupe d'initiateurs iSCSI** (+). La boîte de dialogue **Ajouter des cibles accessibles** s'affiche.
   d. Sélectionnez une cible de la liste des cibles disponibles.
3. Cliquez sur **Ajouter**.

Désactiver le service cible iSCSI

Vous pouvez désactiver le service cible iSCSI vSAN. La désactivation du service cible iSCSI vSAN ne supprime pas les LUN/cibles. Si vous souhaitez récupérer l'espace, supprimez manuellement les LUN/cibles avant de désactiver le service cible iSCSI vSAN.

Conditions préalables

Les charges de travail s'exécutant sur des LUN iSCSI sont arrêtées lorsque vous désactivez le service cible iSCSI. Avant de le désactiver, assurez-vous qu'aucune charge de travail n'est en cours d'exécution sur les LUN iSCSI.

Procédure

1. Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Services**.
2. Sur la ligne Service cible iSCSI vSAN, cliquez sur **MODIFIER**.

   L'assistant Modifier le service cible iSCSI vSAN s'ouvre.
3. Cliquez sur le curseur **Activer le service cible iSCSI vSAN** pour le désactiver et cliquez sur **Appliquer**.

Résultats

Le service cible iSCSI vSAN n'est pas activé.

Étape suivante

Surveiller le Service cible iSCSI vSAN

Vous pouvez surveiller le service cible iSCSI pour afficher l'emplacement physique des composants de la cible iSCSI et rechercher des composants défaillants. Vous pouvez également surveiller l'était de santé du service cible iSCSI.

Conditions préalables

Vérifiez que vous avez activé le service cible iSCSI vSAN et créé des cibles et des LUN.

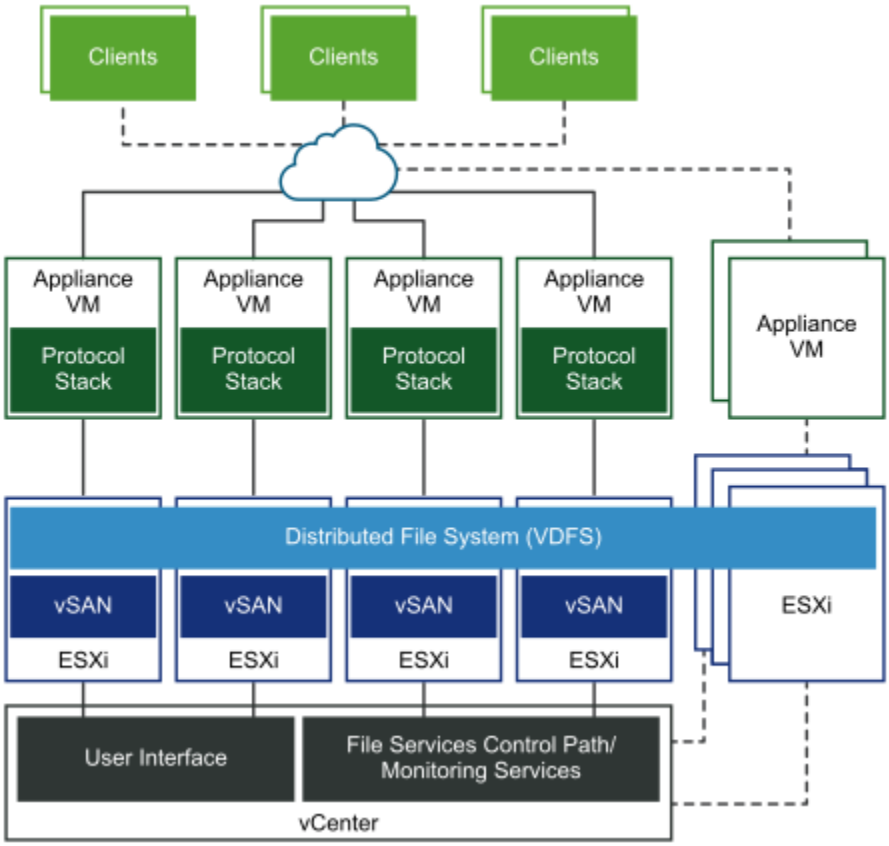
Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur **Surveiller** et sélectionnez **Objets virtuels**. Les cibles iSCSI sont répertoriées sur la page.
3. Sélectionnez une cible, puis cliquez sur **Afficher les détails du placement**. L'emplacement physique indique où se situent les composants de données de la cible.
4. Cliquez sur **Composants de groupe par placement d'hôte** pour afficher les hôtes associés aux composants de données iSCSI.

Service de fichiers vSAN

Utilisez le service de fichiers vSAN pour créer des partages de fichiers dans la banque de données vSAN à laquelle les stations de travail ou les machines virtuelles clientes peuvent accéder. Les données stockées dans un partage de fichiers sont accessibles depuis n'importe quel périphérique disposant de droits d'accès.

Le service de fichiers vSAN est une couche qui se trouve au-dessus de vSAN pour fournir des partages de fichiers. Il prend actuellement en charge les partages de fichiers SMB, NFSv3 et NFSv4.1. Le service de fichiers vSAN se compose de vSAN Distributed File System (vDFS) qui fournit le système de fichiers évolutif sous-jacent en agrégeant des objets vSAN, une plate-forme de services de stockage qui fournit des points de terminaison de serveur de fichiers résilients et un plan de contrôle pour le déploiement, la gestion et la surveillance. Les partages de fichiers sont intégrés à la gestion basée sur des stratégies de stockage vSAN existante et répartis par partage. Le service de fichiers vSAN permet d'héberger des partages de fichiers directement sur le cluster vSAN.



Lorsque vous configurez le service de fichiers vSAN, vSAN crée un seul système de fichiers distribués VDFS pour le cluster utilisé en interne à des fins de gestion. Une machine virtuelle de service de fichiers (FSVM, File Service VM) est placée sur chaque hôte. Les FSVM gèrent les partages de fichiers dans la banque de données vSAN. Chaque FSVM contient un serveur de fichiers qui fournit les services NFS et SMB.

Un pool d'adresses IP statiques doit être fourni en tant qu'entrée lors de l'activation du workflow de service de fichiers. L'une des adresses IP est désignée en tant qu'adresse IP principale. Vous pouvez utiliser l'adresse IP principale pour accéder à tous les partages du cluster des services de fichiers à l'aide des références SMB et NFSv4.1. Un serveur de fichiers est démarré pour chaque adresse IP fournie dans le pool d'adresses IP. Un partage de fichiers est exporté par un seul serveur de fichiers. Toutefois, les partages de fichiers sont répartis uniformément sur tous les serveurs de fichiers. Pour fournir des ressources de calcul qui aident à gérer les demandes d'accès, le nombre d'adresses IP doit être égal au nombre d'hôtes dans le cluster vSAN.

Le service de fichiers vSAN prend en charge les clusters étendus et les clusters à deux nœuds. Le cluster à deux nœuds doit comporter deux serveurs de nœuds de données dans le même emplacement ou le même bureau, et le témoin dans un emplacement distant ou partagé.

Pour plus d'informations sur les volumes de fichiers de stockage cloud natif (CNS), reportez-vous à la documentation de *Plug-in VMware vSphere Container Storage* et à la documentation de *Configuration et gestion de vSphere with Tanzu*.

Limitations et considérations

Tenez compte des éléments suivants lors de la configuration du service de fichiers vSAN :

- Avec vSAN 8.0, les machines virtuelles de service de fichiers sont hors tension, mais ne sont plus supprimées lorsque le cluster vSAN entre en mode de maintenance.
- vSAN 8.0 prend en charge les configurations à deux nœuds et les clusters étendus.
- vSAN 8.0 prend en charge 64 serveurs de fichiers dans une configuration à 64 hôtes.
- vSAN 8.0 prend en charge 100 partages de fichiers.
- Le service de fichiers ne prend pas en charge vSAN Express Storage Architecture.
- Les services de fichiers vSAN ne prennent pas en charge les éléments suivants :
  - Les contrôleurs de domaine en lecture seule (RODC) pour joindre des domaines, car le RODC ne peut pas créer de comptes de machine. En tant que meilleure pratique de sécurité, il est recommandé de créer au préalable une unité d'organisation dédiée dans Active Directory, et le nom d'utilisateur mentionné ici doit contrôler cette organisation.
  - Espace de noms disjoint.
  - Espaces dans les noms des unités d'organisation.
  - Environnements à plusieurs domaines et à forêt Active Directory unique.
- Dans les versions antérieures à vSAN 7.0 Update 3, lorsqu'un hôte entre en mode de maintenance, le conteneur de la pile de protocoles se déplace vers un autre FSVM. Le FSVM sur l'hôte qui est entré en mode de maintenance est supprimé. Une fois que l'hôte a quitté le mode de maintenance, un nouveau FSVM est provisionné.

  Les machines virtuelles de service de fichiers sont mises hors tension et supprimées lorsque le cluster vSAN entre en mode de maintenance, et sont recréées lorsque l'hôte quitte le mode de maintenance.
- Le réseau interne de Docker de la VM de services de fichiers (FSVM) vSAN peut chevaucher le réseau client sans avertissement ni reconfiguration.

  Il existe un problème de conflit connu si le réseau de service de fichiers spécifié chevauche le réseau interne de Docker (172.17.0.0/16). Cela provoque un problème de routage pour le trafic vers le point de terminaison adéquat.

  Comme solution de contournement, spécifiez un réseau de service de fichiers différent afin qu'il ne chevauche pas le réseau interne de Docker (172.17.0.0/16).

Activer le service de fichiers vSAN

Vous pouvez activer des services de fichiers vSAN sur un cluster vSAN standard, un cluster étendu vSAN ou un cluster ROBO vSAN.

Conditions préalables

Assurez-vous que les éléments suivants sont configurés avant d'activer les services de fichiers vSAN :

- La configuration matérielle minimale requise de chaque hôte ESXi du cluster vSAN doit être la suivante :
  - CPU à 4 cœurs
  - 16 Go de mémoire physique
- Veillez à préparer le réseau comme réseau de services de fichiers vSAN :
  - Si vous utilisez le réseau standard basé sur commutateur, le mode promiscuité et les fausses transmissions sont activés dans le cadre du processus d'activation des services de fichiers vSAN.
  - Si vous utilisez un réseau basé sur DVS, les services de fichiers vSAN sont pris en charge sur DVS version 6.6.0 ou ultérieure. Créez un groupe de ports dédié pour les services de fichiers vSAN dans DVS. MacLearning et les fausses transmissions sont activés dans le cadre du processus d'activation des services de fichiers vSAN pour un groupe de ports DVS fourni.
  - **Important** En cas d'utilisation d'un réseau basé sur NSX, veillez à activer MacLearning pour l'entité réseau fournie dans la console d'administration de NSX et à connecter tous les hôtes et les nœuds des services de fichiers au réseau NSX-T souhaité.

Procédure

1. Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Services**.
2. Sur la ligne Service de fichiers, cliquez sur **Activer**.

   L'assistant Activer le service de fichiers s'ouvre.
3. Dans le menu déroulant **Sélectionner**, sélectionnez un réseau.

4 Dans l'agent de service de fichiers, sélectionnez l'une des options suivantes pour télécharger le fichier OVF.

Option	Description
Charger automatiquement le dernier fichier OVF	Cette option permet au système de rechercher et de télécharger le fichier OVF. **Note** ■ Assurez-vous d'avoir configuré le proxy et le pare-feu afin que vCenter puisse accéder au site Web suivant et télécharger le fichier JSON approprié. https://download3.vmware.com/software/VSANOVF/FsOvfMapping.json Pour plus d'informations sur la configuration des paramètres DNS, d'adresse IP et de proxy de vCenter, reportez-vous à la section *Configuration de vCenter Server Appliance*. ■ **Utiliser le fichier OVF actuel** : vous permet d'utiliser le fichier OVF qui est déjà disponible. ■ **Charger automatiquement le dernier fichier OVF** : permet au système de rechercher et de télécharger le dernier fichier OVF.
Charger manuellement le dernier fichier OVF	Cette option vous permet de parcourir et de sélectionner un fichier OVF déjà disponible sur votre système local. **Note** Si vous sélectionnez cette option, vous devez télécharger tous les fichiers suivants : ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.mf` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x_OVF10.cert` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x-system.vmdk` ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-cloud-components.vmdk ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-log.vmdk ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x_OVF10.ovf

5 Cliquez sur **Activer**.

Résultats

- Le fichier OVF est téléchargé et déployé.
- Les services de fichiers vSAN sont activés.

- Une machine virtuelle des services de fichiers (FSVM, File Service VM) est placée sur chaque hôte.

  Note Les FSVM sont gérées par les services de fichiers vSAN. N'effectuez aucune opération sur les FSVM.

Configurer les services de fichiers vSAN

Vous pouvez configurer les services de fichiers, ce qui vous permet de créer des partages de fichiers sur votre banque de données vSAN.

Conditions préalables

Assurez-vous que les conditions suivantes sont remplies avant de configurer les services de fichiers vSAN :

- Activez les services de fichiers vSAN.
- Allouez des adresses IP statiques comme adresses IP de serveur de fichiers à partir du réseau de services de fichiers vSAN. Chaque adresse IP représente un accès à point unique aux partages de fichiers vSAN.
  - Pour des performances optimales, le nombre d'adresses IP doit être égal au nombre d'hôtes dans le cluster vSAN.
  - Toutes les adresses IP statiques doivent provenir du même sous-réseau.
  - Un nom de domaine complet doit correspondre à chaque adresse IP statique, qui doit faire partie des zones de recherche directe et de recherche inversée du serveur DNS.
- Si vous prévoyez de créer un partage de fichiers SMB basé sur Kerberos ou un partage de fichiers NFS basé sur Kerberos, vous avez besoin des éléments suivants :
  - Domaine Microsoft Active Directory (AD) à des fins d'authentification pour créer un partage de fichiers SMB ou un partage de fichiers NFS avec la sécurité Kerberos.
  - (Facultatif) Unité d'organisation Active Directory pour créer tous les objets ordinateur du serveur de fichiers.
  - Utilisateur de domaine dans le service d'annuaire disposant des privilèges suffisants pour créer et supprimer des objets ordinateur.

Procédure

1. Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Services**.
2. Cliquez sur **Configurer le domaine**.

   L'assistant Domaine de services de fichiers s'ouvre.
3. Sur la page Domaine de services de fichiers, entrez l'espace de noms unique, puis cliquez sur **Suivant**. Le nom de domaine doit comporter au moins deux caractères. Le premier caractère doit être une lettre ou un chiffre. Les autres caractères peuvent inclure une lettre, un chiffre, un trait de soulignement (_), un point (.) ou un trait d'union (-).

4 Sur la page Mise en réseau, entrez les informations suivantes, puis cliquez sur **Suivant** :

- **Protocole** : vous pouvez sélectionner IPv4 ou IPv6. Le service de fichiers vSAN prend uniquement en charge la pile IPv4 ou IPv6. La reconfiguration entre IPv4 et IPv6 n'est pas prise en charge.
- **Serveurs DNS** : entrez un serveur DNS valide pour garantir une configuration correcte des services de fichiers.
- **Suffixes DNS** : fournissez le suffixe DNS utilisé avec les services de fichiers. Tous les autres suffixes DNS à partir desquels les clients peuvent accéder à ces serveurs de fichiers doivent également être inclus. Les services de fichiers ne prennent pas en charge le domaine DNS avec une seule étiquette, telle que « app », « wiz », « com », etc.
  Un nom de domaine donné aux services de fichiers doit être au format thisdomain. registerdrootdnsname. Le nom et le suffixe DNS doivent respecter les meilleures pratiques exposées dans https://docs.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/selecting-the-forest-root-domain.
- **Masque de sous-réseau** : entrez un masque de sous-réseau valide. Cette zone de texte s'affiche lorsque vous sélectionnez IPv4.
- **Longueur du préfixe** : entrez un nombre compris entre 1 et 128. Cette zone de texte s'affiche lorsque vous sélectionnez IPv6.
- **Passerelle** : entrez une passerelle valide.
- **Pool d'adresses IP** : entrez l'adresse IP principale et le nom DNS.

L'option Site d'affinité est disponible si vous configurez le service de fichiers vSAN sur un cluster étendu. Cette option vous permet de configurer le placement du serveur de fichiers sur votre site **préféré** ou **secondaire**. Cela permet de réduire la latence du trafic entre les sites. La valeur par défaut est **L'un ou l'autre**, ce qui indique qu'aucune règle d'affinité de site n'est appliquée au serveur de fichiers.

Note Si votre cluster est un cluster ROBO, assurez-vous que la valeur du site d'affinité est définie sur **L'un ou l'autre**.

Dans un événement de panne de site, le serveur de fichiers affilié à ce site bascule vers l'autre site. Le serveur de fichiers est restauré automatiquement vers le site affilié lors de la récupération. Configurez des serveurs de fichiers supplémentaires sur un site si des charges de travail supplémentaires peuvent être attendues sur un site spécifique.

Note Si le serveur de fichiers contient des partages de fichiers SMB, il ne se restaure pas automatiquement même si la panne du site est résolue.

Tenez compte des éléments suivants lors de la configuration des adresses IP et des noms DNS :

- Pour garantir une configuration correcte des services de fichiers, les adresses IP que vous entrez sur la page Mise en réseau doivent être des adresses statiques et le serveur DNS doit avoir des enregistrements pour ces adresses IP. Pour des performances optimales, le nombre d'adresses IP doit être égal au nombre d'hôtes dans le cluster vSAN.
- Vous pouvez disposer d'un maximum de 64 hôtes dans le cluster. Si la prise en charge de cluster à grande échelle est configurée, vous pouvez entrer jusqu'à 64 adresses IP.
- Vous pouvez utiliser les options suivantes pour renseigner automatiquement les zones de texte Adresse IP et Nom du serveur DNS :

  REMPLISSAGE AUTOMATIQUE : cette option s'affiche lorsque vous entrez la première adresse IP dans la zone de texte Adresse IP. Cliquez sur l'option REMPLISSAGE AUTOMATIQUE pour remplir automatiquement les champs restants avec des adresses IP séquentielles, en fonction du masque de sous-réseau et de l'adresse de la passerelle de l'adresse IP que vous avez fournie dans la première ligne. Vous pouvez modifier les adresses IP remplies automatiquement.

  RECHERCHE DE DNS : cette option s'affiche lorsque vous entrez la première adresse IP dans la zone de texte Adresse IP. Cliquez sur l'option RECHERCHE DE DNS pour récupérer automatiquement le nom de domaine complet correspondant aux adresses IP dans la colonne Adresse IP.

  Note

  - Toutes les règles valides s'appliquent aux noms de domaine complets. Pour plus d'informations, reportez-vous à la page https://tools.ietf.org/html/rfc953.
  - La première partie du nom de domaine complet, également nommée nom NetBIOS, ne doit pas comporter plus de 15 caractères.

  Les noms de domaine complets sont automatiquement récupérés dans les conditions suivantes :

  - Vous devez avoir entré un serveur DNS valide dans la page Domaine.
  - Les adresses IP entrées dans la page Pool d'adresses IP doivent être des adresses statiques et le serveur DNS doit avoir des enregistrements pour ces adresses IP.

5 Sur la page Service d'annuaire, entrez les informations suivantes, puis cliquez sur **Suivant**.

Option	Description
Active Directory	Configurez un domaine Active Directory pour les services de fichiers vSAN à des fins d'authentification. Si vous prévoyez de créer un partage de fichiers SMB ou un partage de fichiers NFSv4.1 avec l'authentification Kerberos, vous devez configurer un domaine AD pour les services de fichiers vSAN.
Domaine AD	Nom de domaine complet joint par le serveur de fichiers.
Unité d'organisation (facultative)	Contient le compte d'ordinateur que les services de fichiers vSAN créent. Dans une organisation avec des hiérarchies complexes, créez le compte d'ordinateur dans un conteneur spécifié à l'aide d'une barre oblique pour indiquer les hiérarchies (par exemple, organizational_unit/inner_organizational_unit). **Note** Par défaut, les services de fichiers vSAN créent le compte d'ordinateur dans le conteneur Ordinateurs.
Nom d'utilisateur AD	Nom d'utilisateur à utiliser pour se connecter au service Active Directory et le configurer. Ce nom d'utilisateur authentifie l'annuaire Active Directory sur le domaine. Un utilisateur de domaine authentifie le contrôleur de domaine et crée des comptes d'ordinateur des services de fichiers vSAN, les entrées SPN associées et les entrées DNS des fichiers (lors de l'utilisation de Microsoft DNS). Nous vous recommandons de créer un compte de service dédié pour les services de fichiers. Utilisateur de domaine dans le service d'annuaire disposant des privilèges suffisants suivants pour créer et supprimer des objets ordinateur : ■ (Facultatif) Ajout/Mise à jour des entrées DNS
Mot de passe	Mot de passe du nom d'utilisateur de l'annuaire Active Directory sur le domaine. Les services de fichiers vSAN utilisent le mot de passe pour s'authentifier auprès d'AD et pour créer le compte d'ordinateur des services de fichiers vSAN.

Note

- Les services de fichiers vSAN ne prennent pas en charge les éléments suivants :
  - Les contrôleurs de domaine en lecture seule (RODC) pour joindre des domaines, car le RODC ne peut pas créer de comptes de machine. En tant que meilleure pratique de sécurité, il est recommandé de créer au préalable une unité d'organisation dédiée dans Active Directory, et le nom d'utilisateur mentionné ici doit contrôler cette organisation.
  - Espace de noms disjoint.
  - Espaces dans les noms des unités d'organisation.
  - Environnements à plusieurs domaines et à forêt Active Directory unique.
- Seuls les caractères anglais sont pris en charge pour le nom d'utilisateur Active Directory.
- Seule la configuration de domaine AD unique est prise en charge. Cependant, les serveurs de fichiers peuvent être placés sur un sous-domaine DNS valide. Par exemple, un domaine AD portant le nom `example.com` peut avoir `name1.eng.example.com` comme nom de domaine complet du serveur de fichiers.
- Les objets ordinateur précréés pour les serveurs de fichiers ne sont pas pris en charge. Assurez-vous que l'utilisateur fourni ici dispose de privilèges suffisants sur l'unité d'organisation.
- Les services de fichiers vSAN mettent à jour les enregistrements DNS des serveurs de fichiers si l'annuaire Active Directory est également utilisé comme serveur DNS et si l'utilisateur dispose des autorisations suffisantes pour mettre à jour les enregistrements DNS. Les services de fichiers vSAN disposent également d'un contrôle de santé pour indiquer si les recherches directes et inversées des serveurs de fichiers fonctionnent correctement. Cependant, s'il existe d'autres solutions propriétaires utilisées en tant que serveurs DNS, l'administrateur Vi doit mettre à jour ces enregistrements DNS.

6 Vérifiez les paramètres et cliquez sur **Terminer**.

Résultats

Le domaine des services de fichiers est configuré. Les serveurs de fichiers sont démarrés avec les adresses IP attribuées lors du processus de configuration des services de fichiers vSAN.

Modifier le service de fichiers vSAN

Vous pouvez modifier et reconfigurer les paramètres d'un service de fichiers vSAN.

Conditions préalables

- Si vous effectuez une mise à niveau de vSAN 7.0 vers la version 7.0 Update 1, vous pouvez créer des partages de fichiers SMB et NFS Kerberos. Cela nécessite la configuration du domaine Active Directory pour le service de fichiers vSAN.

- S'il existe des partages actifs, la modification du domaine Active Directory n'est pas autorisée, car cette action peut perturber les autorisations de l'utilisateur sur les partages actifs.
- Si votre mot de passe Active Directory a été modifié, vous pouvez modifier les paramètres de configuration d'Active Directory et fournir le nouveau mot de passe.

  Note Cette action peut entraîner une interruption mineure des E/S en vol sur les partages de fichiers.

Procédure

1. Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Services**.
2. Sur la ligne Service de fichiers, cliquez sur **Modifier** > **Modifier le domaine**.

   L'assistant Domaine de services de fichiers s'ouvre.
3. Sur la page Domaine de services de fichiers, modifiez le nom de domaine du service de fichiers et cliquez sur **Suivant**.
4. Sur la page Mise en réseau, effectuez les modifications appropriées, puis cliquez sur **Suivant**. Vous pouvez modifier les adresses IP principales, les adresses IP statiques et les noms DNS. Vous pouvez ajouter ou supprimer les adresses IP principales ou les adresses IP statiques. Vous ne pouvez pas modifier le nom DNS sans modifier l'adresse IP.

   Note La modification des informations de domaine est une action perturbatrice. Il peut être nécessaire que tous les clients utilisent de nouvelles URL pour se reconnecter aux partages de fichiers.
5. Sur la page Service d'annuaire, effectuez les modifications appropriées relatives à l'annuaire, puis cliquez sur **Suivant**.

   Note Vous ne pouvez pas modifier le domaine AD, l'unité d'organisation et le nom d'utilisateur après la configuration initiale des services de fichiers vSAN.
6. Sur la page Vérifier, cliquez sur **Terminer** après avoir apporté les modifications nécessaires.

Résultats

Les modifications sont appliquées à la configuration du service de fichiers vSAN.

Créer un partage de fichiers

Lorsque le service de fichiers vSAN est activé, vous pouvez créer un ou plusieurs partages de fichiers sur la banque de données vSAN. Le service de fichiers vSAN ne prend pas en charge l'utilisation de ces partages de fichiers NFS sur ESXi.

Conditions préalables

Si vous créez un partage de fichiers SMB ou un partage de fichiers NFSv4.1 avec la sécurité Kerberos, assurez-vous que vous avez configuré le service de fichiers vSAN sur un domaine AD.

Éléments à prendre en compte pour le nom et l'utilisation de partage

- Les noms d'utilisateurs comportant des caractères non-ASCII peuvent être utilisés pour accéder aux données de partage.
- Les noms de partage ne peuvent pas dépasser 80 caractères et peuvent contenir des caractères anglais, des nombres et des traits d'union. Chaque trait d'union doit être précédé et suivi d'un chiffre ou d'une lettre. Les traits d'union consécutifs ne sont pas autorisés.
- Pour les partages de type SMB, les fichiers et les répertoires peuvent contenir toute chaîne compatible Unicode.
- Pour les partages de type NFSv4 purs, le fichier et les répertoires peuvent contenir toute chaîne compatible UTF-8.
- Pour les partages NFSv3 et NFSv3+NFSv4 purs, les fichiers et les répertoires peuvent uniquement contenir des chaînes compatibles ASCII.
- La migration de données de partage d'une version antérieure de NFSv3 vers de nouveaux partages de service de fichiers vSAN avec NFSv4 requiert uniquement la conversion de tous les noms de fichiers et de répertoires en codage UTF-8. Il existe des outils tiers qui permettent d'obtenir le même résultat.

Procédure

1. Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Partages de fichiers**.
2. Cliquez sur **Ajouter**.

   L'assistant Créer un partage de fichiers s'ouvre.
3. Sur la page Général, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - **Nom** : entrez un nom de fichier pour le partage de fichiers.
   - **Protocole** : sélectionnez un protocole approprié. Le service de fichiers vSAN prend en charge les protocoles de système de fichiers SMB et NFS.

     Si vous sélectionnez le protocole **SMB**, vous pouvez également configurer le partage de fichiers SMB pour qu'il accepte uniquement les données chiffrées à l'aide de l'option de **chiffrement de protocole**.

     Si vous sélectionnez le protocole **NFS**, vous pouvez configurer le partage de fichiers pour qu'il prenne en charge **NFS 3**, **NFS 4** ou les deux versions de **NFS 3 et NFS 4**. Si vous sélectionnez la version **NFS 4**, vous pouvez définir la sécurité **AUTH_SYS** ou **Kerberos**.

     Note Le protocole SMB et la sécurité Kerberos pour le protocole NFS ne peuvent être configurés que si le service de fichiers vSAN est configuré avec Active Directory. Pour plus d'informations, consultez Configurer les services de fichiers vSAN.
   - Avec le protocole SMB, vous pouvez masquer les fichiers et les dossiers auxquels l'utilisateur du client de partage n'est pas autorisé à accéder à l'aide de l'option **Énumération basée sur l'accès**.

- **Stratégie de stockage** : sélectionnez une stratégie de stockage appropriée.
- **Site d'affinité** : cette option est disponible si vous créez un partage de fichiers sur un cluster étendu. Cette option vous permet de placer le partage de fichiers sur un serveur de fichiers qui appartient au site de votre choix. Utilisez cette option lorsque vous préférez une faible latence lors de l'accès au partage de fichiers. La valeur par défaut est **L'un ou l'autre**, ce qui indique que le partage de fichiers est placé sur un site avec moins de trafic sur le site préféré ou sur le site secondaire.
- **Quotas d'espace de stockage** : vous pouvez définir les valeurs suivantes :
  - **Seuil d'avertissement du partage** : lorsque le partage atteint ce seuil, un message d'avertissement s'affiche.
  - **Quota de partage inconditionnel** : lorsque le partage atteint ce seuil, les nouvelles allocations de blocs sont refusées.
- **Étiquettes** : une étiquette est une paire clé-valeur qui vous permet d'organiser les partages de fichiers. Vous pouvez joindre des étiquettes à chaque partage de fichiers, puis filtrer les partages en fonction de celles-ci. Une clé d'étiquette est une chaîne comportant entre 1 et 250 caractères. Une valeur d'étiquette est une chaîne et sa longueur doit être inférieure à 1 Ko. Le service de fichiers vSAN prend en charge jusqu'à 5 étiquettes par partage.

4 La page Contrôle d'accès au réseau fournit des options pour définir l'accès au partage de fichiers. Les options de contrôle d'accès au réseau ne sont disponibles que pour les partages NFS. Sélectionnez une des options suivantes, puis cliquez sur **Suivant**.

- **Aucun accès** : sélectionnez cette option pour rendre le partage de fichiers inaccessible à partir de n'importe quelle adresse IP.
- **Autoriser l'accès à partir de n'importe quelle adresse IP** : sélectionnez cette option pour rendre le partage de fichiers accessible à partir de toutes les adresses IP.
- **Personnaliser l'accès au réseau** : sélectionnez cette option pour définir des autorisations pour des adresses IP spécifiques. Cette option vous permet de spécifier si une adresse IP spécifique peut accéder au partage de fichiers, apporter des modifications ou le lire uniquement. Vous pouvez également activer **Réduire les droits du compte racine** pour chaque adresse IP. Vous pouvez entrer les adresses IP dans les formats suivants :
  - Une adresse IP unique. Par exemple, 123.23.23.123
  - Une adresse IP avec un masque de sous-réseau. Par exemple, 123.23.23.0/8
  - Une plage en spécifiant une adresse IP de début et une adresse IP de fin séparées par un trait d'union (-). Par exemple, 123.23.23.123-123.23.23.128
  - Astérisque (*) pour impliquer tous les clients.

5 Sur la page Vérifier, vérifiez les paramètres, puis cliquez sur **Terminer**.

Un nouveau partage de fichiers est créé sur la banque de données vSAN.

Afficher les partages de fichiers

Vous pouvez afficher la liste des partages de fichiers vSAN.

Pour afficher la liste des partages de fichiers vSAN, accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Partages de services de fichiers**.

Une liste des partages de fichiers vSAN s'affiche. Pour chaque partage de fichiers, vous pouvez afficher des informations telles que la stratégie de stockage, le quota inconditionnel, l'utilisation au-delà du quota, l'utilisation réelle, etc.

Accéder à des partages de fichiers

Vous pouvez accéder à un partage de fichiers à partir d'un client hôte.

Accéder à un partage de fichiers NFS

Vous pouvez accéder à un partage de fichiers à partir d'un client hôte, à l'aide d'un système d'exploitation qui communique avec des systèmes de fichiers NFS. Pour les distributions Linux basées sur RHEL, la prise en charge de NFS 4.1 est disponible dans RHEL 7.3 et CentOS 7.3-1611 exécutant le noyau 3.10.0-514 ou version ultérieure. Pour les distributions Linux basées sur Debian, la prise en charge de NFS 4.1 est disponible dans le noyau Linux version 4.0.0 ou ultérieure. Tous les clients NFS doivent disposer de noms d'hôte uniques pour que NFS 4.1 fonctionne. Vous pouvez utiliser la commande mount de Linux avec l'adresse IP principale pour monter un partage de fichiers vSAN sur le client. Par exemple : `mount -t nfs4 -o minorversion=1,sec=sys <primary ip>:/vsanfs/<share name>`. La prise en charge de NFSv3 est disponible pour les distributions Linux basées sur RHEL et Debian. Vous pouvez utiliser la commande mount de Linux pour monter un partage de fichiers vSAN sur le client. Par exemple, montez `-t nfs vers=3 <nfsv3_access_point> <localmount_point>`.

Exemple

Exemples de commandes de la version 41 permettant de vérifier le partage de fichiers NFS à partir d'un client hôte :

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=sys <primary ip address>:/vsanfs/
TestShare-0 /mnt/TestShare-0
[root@localhost ~]# cd /mnt/TestShare-0/
[root@localhost TestShare-0]# mkdir bar
[root@localhost TestShare-0]# touch foo
[root@localhost TestShare-0]# ls -l
total 0
drwxr-xr-x. 1 root root 0 Feb 19 18:35 bar
-rw-r--r--. 1 root root 0 Feb 19 18:35 foo
```

Accès au partage de fichiers NFS Kerberos

Un client Linux accédant à un partage NFS Kerberos doit disposer d'un ticket Kerberos valide.

Exemples de commandes de la version 41 permettant de vérifier le partage de fichiers NFS Kerberos à partir d'un client hôte :

Un partage NFS Kerberos peut être monté à l'aide de la commande de montage suivante :

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=krb5/krb5i/krb5p <primary ip
address>:/vsanfs/TestShare-0 /mnt/TestShare-0
[root@localhost ~]# cd /mnt/TestShare-0/
[root@localhost TestShare-0]# mkdir bar
[root@localhost TestShare-0]# touch foo
[root@localhost TestShare-0]# ls -l
total 0
drwxr-xr-x. 1 root root 0 Feb 19 18:35 bar
-rw-r--r--. 1 root root 0 Feb 19 18:35 foo
```

Modification de la propriété d'un partage NFS Kerberos

Vous devez vous connecter à l'aide du nom d'utilisateur de domaine AD pour modifier la propriété d'un partage. Le nom d'utilisateur de domaine AD indiqué dans la configuration du service de fichiers agit en tant qu'utilisateur sudo pour le partage de fichiers Kerberos.

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=sys <primary ip address>:/vsanfs/
TestShare-0 /mnt/TestShare-0
[fsadmin@ocalhost ~]# chown user1 /mnt/TestShare-0
[user1@localhost ~]# ls -l /mnt/TestShare-0
total 0
drwxr-xr-x. 1 user1 domain  users 0 Feb 19 18:35 bar
-rw-r--r--. 1 user1 domain users 0 Feb 19 18:35 foo
```

Accéder à un partage de fichiers SMB

Vous pouvez accéder à un partage de fichiers SMB à partir d'un client Windows.

Conditions préalables

Assurez-vous que le client Windows est joint au domaine Active Directory configuré avec le service de fichiers vSAN.

Procédure

1. Copiez le chemin de partage de fichiers SMB à l'aide de la procédure suivante :
   a. Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Partages de services de fichiers**.

      La liste de tous les partages de fichiers vSAN s'affiche.

   b. Sélectionnez le partage de fichiers SMB auquel vous souhaitez accéder à partir du client Windows.

   c. Cliquez sur **COPIER LE CHEMIN D'ACCÈS** > **SMB**.

      Le chemin du partage de fichiers SMB est copié dans le Presse-papiers.
2. Connectez-vous au client Windows en tant qu'utilisateur de domaine Active Directory normal.

3 Accédez au partage de fichiers SMB en utilisant le chemin que vous avez copié.

Modifier un partage de fichiers

Vous pouvez modifier les paramètres d'un partage de fichiers vSAN.

Procédure

1 Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Partages de services de fichiers**.

La liste de tous les partages de fichiers vSAN s'affiche.

2 Sélectionnez le partage de fichiers à modifier, puis cliquez sur **MODIFIER**.

3 Sur la page Modifier un partage de fichiers, apportez les modifications appropriées aux paramètres du partage de fichiers, puis cliquez sur **Terminer**.

Résultats

Les paramètres de partage de fichiers sont mis à jour.

Note vSAN n'autorise pas le remplacement du protocole de partage de fichiers SMB par NFS.

Gérer le partage de fichiers SMB

Le service de fichiers vSAN prend en charge le composant logiciel enfichable des dossiers partagés pour MMC (Microsoft Management Console) afin de gérer les partages SMB sur le cluster vSAN.

Vous pouvez effectuer les tâches suivantes sur les partages SMB du système de fichiers vSAN à l'aide de l'outil MMC :

- gérer la liste de contrôles d'accès (ACL) ;
- fermer les fichiers ouverts ;
- consulter les sessions actives ;
- afficher les fichiers ouverts ;
- fermer les connexions client.

Procédure

1 Copiez la commande MMC à l'aide de la procédure suivante :

a Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Partages de services de fichiers**.

La liste de tous les partages de fichiers vSAN s'affiche.

b Sélectionnez le partage de fichiers SMB que vous souhaitez gérer à partir du client Windows à l'aide de l'outil MMC.

c Cliquez sur **COPIER LA COMMANDE MMC**.

La commande MMC est copiée dans votre Presse-papiers.

2 Connectez-vous au client Windows en tant qu'utilisateur Admin du service de fichiers. L'utilisateur Admin du service de fichiers est configuré lorsque vous créez le domaine de services de fichiers. Un utilisateur Admin du service de fichiers dispose de tous les privilèges sur le serveur de fichiers.

3 Dans la zone de recherche de la barre des tâches, tapez Exécuter, puis sélectionnez **Exécuter**.

4 Dans la zone Exécuter, exécutez la commande MMC que vous avez copiée pour accéder au partage SMB et le gérer à l'aide de l'outil MMC.

Supprimer un partage de fichiers

Vous pouvez supprimer un partage de fichiers lorsqu'il n'est plus utile. Lorsque vous supprimez un partage de fichiers, tous les snapshots qui lui sont associés sont également supprimés.

Procédure

1 Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Partages de services de fichiers**.

La liste de tous les partages de fichiers vSAN s'affiche.

2 Sélectionnez le partage de fichiers à modifier, puis cliquez sur **SUPPRIMER**.

3 Dans la boîte de dialogue Supprimer des partages de fichiers, cliquez sur **SUPPRIMER**.

Snapshot du système vSAN Distributed File System

Un snapshot fournit une archive temporelle et peu volumineuse des données. Elle permet de récupérer les données d'un fichier ou d'un ensemble de fichiers en cas de suppression accidentelle d'un fichier. Un snapshot de niveau système de fichiers fournit des informations sur les fichiers qui ont été modifiés et les modifications apportées au fichier. Il fournit un service de récupération de fichiers automatisé qui est plus efficace que la méthode de sauvegarde basée sur les bandes traditionnelle. Un snapshot seul n'offre pas de solution complète de récupération d'urgence, mais il peut être utilisé par les fournisseurs de systèmes de sauvegarde tiers pour copier les fichiers modifiés (sauvegarde incrémentielle) vers un emplacement physique différent.

Les services de fichiers vSAN disposent d'une fonctionnalité intégrée qui permet de créer une image ponctuelle du partage de fichiers vSAN. Lorsque le service de fichiers vSAN est activé, vous pouvez créer jusqu'à 32 snapshots par partage. Un snapshot de partage de fichiers vSAN est un snapshot de système de fichiers qui fournit une image ponctuelle d'un partage de fichiers vSAN.

Créer un snapshot

Lorsque le service de fichiers vSAN est activé, vous pouvez créer un ou plusieurs snapshots qui fournissent une image ponctuelle du partage de fichiers vSAN. Vous pouvez créer un maximum de 32 snapshots par partage de fichiers.

Conditions préalables

Vous devez avoir créé un partage de fichiers vSAN.

Procédure

1. Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Partages de services de fichiers**.

   Une liste des partages de fichiers vSAN s'affiche.
2. Sélectionnez le partage de fichiers pour lequel vous souhaitez créer un snapshot, puis cliquez sur **SNAPSHOTS** > **NOUVEAU SNAPSHOT**.

   La boîte de dialogue Créer un snapshot s'affiche.
3. Dans la boîte de dialogue Créer un snapshot, indiquez un nom pour le snapshot, puis cliquez sur **Créer**.

Résultats

Un snapshot ponctuel du partage de fichiers sélectionné est créé.

Afficher un snapshot

Vous pouvez afficher la liste des snapshots ainsi que des informations telles que la date et l'heure de création du snapshot, et sa taille.

Procédure

1. Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Partages de services de fichiers**.

   Une liste des partages de fichiers vSAN s'affiche.
2. Sélectionnez un partage de fichiers et cliquez sur **SNAPSHOTS**.

Résultats

Une liste de snapshots pour ce partage de fichiers s'affiche. Vous pouvez afficher des informations telles que la date et l'heure de création du snapshot et sa taille.

Supprimer un snapshot

Vous pouvez supprimer un snapshot lorsqu'il n'est plus utile.

Procédure

1. Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Partages de services de fichiers**.

   Une liste des partages de fichiers vSAN s'affiche.

2 Sélectionnez un partage de fichiers et cliquez sur **SNAPSHOTS**.

Une liste des snapshots appartenant au partage de fichiers que vous avez sélectionné s'affiche.

3 Sélectionnez le snapshot que vous voulez supprimer, puis cliquez sur **DELETE**.

Rééquilibrer la charge de travail sur les hôtes de service de fichiers vSAN

Santé de Skyline affiche l'état de santé de l'équilibrage de la charge de travail pour tous les hôtes qui font partie de l'infrastructure du service de fichiers vSAN.

S'il existe un déséquilibre dans la charge de travail d'un hôte, vous pouvez le corriger en rééquilibrant la charge de travail.

Conditions préalables

Procédure

1 Accédez au cluster vSAN, puis cliquez sur **Surveiller** > **vSAN** > **Santé de Skyline**.

2 Sous Santé de Skyline, développez **Service de fichiers**, puis cliquez sur **Santé de l'infrastructure**.

L'onglet Santé de l'infrastructure affiche la liste de tous les hôtes qui font partie de l'infrastructure du service de fichiers vSAN. Pour chaque hôte, l'état de l'équilibrage de la charge de travail s'affiche. En cas de déséquilibre de la charge de travail d'un hôte, une alerte s'affiche dans la colonne **Description**.

3 Cliquez sur **Rééquilibrer le déséquilibre**, puis **Rééquilibrer** pour corriger le déséquilibre.

Avant de procéder au rééquilibrage, prenez en compte les éléments suivants :

- Lors du rééquilibrage, les conteneurs dans les hôtes avec une charge de travail déséquilibrée peuvent être déplacés vers d'autres hôtes. L'activité de rééquilibrage peut également avoir un effet sur les autres hôtes du cluster.
- Pendant le processus de rééquilibrage, les charges de travail s'exécutant sur des partages NFS ne sont pas interrompues. Cependant, les E/S vers les partages SMB situés dans les conteneurs qui ont été déplacés sont perturbées.

Résultats

La charge de travail de l'hôte est équilibrée et l'état d'équilibrage de la charge de travail passe à vert.

Réclamation d'espace à l'aide de la commande unmap

vSAN 6.7 Update 2 et versions ultérieures prend en charge les commandes UNMAP qui vous permettent de récupérer l'espace de stockage qui est mappé à des fichiers supprimés du système vSAN Distributed File System (VDFS) créé par l'invité sur l'objet vSAN.

La suppression de fichiers et de snapshots libère de l'espace dans le système de fichiers. Cet espace libre est mappé sur un périphérique de stockage jusqu'à ce que le système de fichiers le libère ou le démappe. vSAN prend en charge la récupération d'espace libre, qui est également appelée opération unmap. Vous pouvez libérer de l'espace de stockage dans le système VDFS notamment lorsque vous supprimez et consolidez des partages de fichiers et des snapshots. Vous pouvez supprimer le mappage de l'espace de stockage lorsque vous supprimez des fichiers ou des snapshots.

La capacité de démappage n'est pas activée par défaut. Pour activer la commande unmap sur un cluster vSAN, utilisez la commande RVC suivante :

```
vsan.unmap_support –enable
```

Lorsque vous activez la commande unmap sur un cluster vSAN, vous devez mettre hors tension, puis remettre sous tension toutes les machines virtuelles. Les machines virtuelles doivent utiliser le matériel virtuel version 13 ou supérieure pour effectuer des opérations UNMAP.

Mettre à niveau le service de fichiers

Lorsque vous mettez à niveau le service de fichiers, la mise à niveau est effectuée de manière continue. Pendant la mise à niveau, les conteneurs de serveur de fichiers exécutés sur les machines virtuelles en cours de mise à niveau basculent vers d'autres machines virtuelles. Les partages de fichiers restent accessibles pendant la mise à niveau. Pendant la mise à niveau, des interruptions peuvent se produire lors de l'accès aux partages de fichiers.

Conditions préalables

Assurez-vous que les éléments suivants sont mis à niveau :

- Hôtes ESXi
- vCenter Server
- format de disque vSAN

Procédure

1. Accédez au cluster vSAN, puis cliquez sur **Configurer** > **vSAN** > **Services**.
2. Sous Services vSAN, sur la ligne Service de fichiers, cliquez sur **VÉRIFIER LA MISE À NIVEAU**.

3 Dans la boîte de dialogue Mettre à niveau le service de fichiers, sélectionnez l'une des options de déploiement suivantes, puis cliquez sur **METTRE À NIVEAU**.

Option	Action
Méthode automatique	Il s'agit de l'option par défaut. Cette option permet au système de rechercher et de télécharger le fichier OVF. Une fois la mise à niveau lancée, vous ne pouvez pas annuler la tâche. **Note** vSAN nécessite une connectivité Internet pour cette option.
Méthode manuelle	Cette option vous permet de parcourir et de sélectionner un fichier OVF déjà disponible sur votre système local. Une fois la mise à niveau lancée, vous ne pouvez pas annuler la tâche. **Note** Si vous sélectionnez cette option, vous devez télécharger tous les fichiers suivants : ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.mf` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x_OVF10.cert` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x-system.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-cloud-components.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-log.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.ovf`

Surveiller les performances

Vous pouvez surveiller les performances des partages de fichiers NFS et SMB.

Conditions préalables

Assurez-vous que le service de performance vSAN est activé. Si vous utilisez le service de performance de vSAN pour la première fois, vous voyez un message vous avertissant de l'activer. Pour plus d'informations sur le service de performance vSAN, reportez-vous au *Guide de surveillance et de dépannage de vSAN*.

Procédure

1 Accédez au cluster vSAN, puis cliquez sur **Surveiller** > **vSAN** > **Performances**.

2 Cliquez sur l'onglet **PARTAGE DE FICHIERS**.

3 Sélectionnez l'une des options suivantes :

Option	Action
Intervalle de temps	■ Sélectionnez **Dernière** pour sélectionner le nombre d'heures pendant lesquelles vous souhaitez afficher le rapport de performances. ■ Sélectionnez **PERSONNALISÉ** pour sélectionner la date et l'heure auxquelles vous souhaitez afficher le rapport de performances. ■ Sélectionnez **ENREGISTRER** pour ajouter le paramètre actuel comme option à la liste Intervalle de temps.
Partage de fichiers	Sélectionnez le partage de fichiers pour lequel vous souhaitez générer et afficher le rapport de performances.

4 Cliquez sur **AFFICHER LES RÉSULTATS**.

Résultats

Les mesures de débit, d'IOPS et de latence du service de fichiers vSAN pour la période sélectionnée s'affichent.

Pour plus d'informations sur les graphiques de performances vSAN, reportez-vous à l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/2144493.

Surveiller la capacité

Vous pouvez surveiller la capacité des partages de fichiers natifs et des partages de fichiers gérés par CNS.

Procédure

1 Accédez au cluster vSAN, puis cliquez sur **Surveiller** > **vSAN** > **Capacité**.

2 Cliquez sur l'onglet **UTILISATION DE LA CAPACITÉ**.

3 Dans la section Répartition de l'utilisation avant la déduplication et la compression, développez le menu **Objets d'utilisateur**.

Résultats

Les informations de capacité de partage de fichiers s'affichent.

Pour plus d'informations sur la surveillance de la capacité de vSAN, reportez-vous au *Guide de surveillance et de dépannage de vSAN*.

Surveiller la santé

Vous pouvez surveiller la santé du service de fichiers vSAN et des objets de partage de fichiers.

Afficher la santé du service de fichiers vSAN

Vous pouvez surveiller l'état de santé du service de fichiers vSAN.

Conditions préalables

Assurez-vous que le service de performances de vSAN est activé.

Procédure

1 Accédez au cluster vSAN, puis cliquez sur **Surveiller** > **vSAN**.

2 Dans la section Santé de Skyline, développez **Service de fichiers**.

3 Cliquez sur les paramètres de santé du service de fichiers suivants pour afficher l'état.

Option	Action
Santé de l'infrastructure	Affiche l'état de santé de l'infrastructure du service de fichiers par hôte ESXi. Pour plus d'informations, cliquez sur l'onglet **Info**.
Santé du serveur de fichiers	Affiche l'état de santé du serveur de fichiers. Pour plus d'informations, cliquez sur l'onglet **Info**.
Santé du partage	Affiche la santé du partage de services de fichiers. Pour plus d'informations, cliquez sur l'onglet **Info**.

Surveiller la santé des objets de partage de fichiers

Vous pouvez surveiller la santé des objets de partage de fichiers.

Pour afficher l'état de santé d'un objet de partage de fichiers, accédez au cluster vSAN, puis cliquez sur **Surveiller** > **vSAN** > **Objets virtuels**.

Les informations sur le périphérique, telles que le nom, l'identifiant ou l'UUID, le nombre de périphériques utilisés pour chaque machine virtuelle et la manière dont ils sont mis en miroir sur les hôtes s'affichent dans la section AFFICHER LES DÉTAILS DU PLACEMENT.

Migrer un cluster vSAN hybride vers un cluster intégralement Flash

Vous pouvez migrer les groupes de disques d'un cluster vSAN hybride vers des groupes de disques intégralement Flash.

Le cluster hybride vSAN utilise des disques magnétiques pour la couche de capacité et des périphériques Flash pour la couche de cache. Vous pouvez modifier la configuration des groupes de disques du cluster afin qu'il utilise des périphériques Flash pour la couche de cache et la couche de capacité.

Procédure

1 Accédez au cluster vSAN.

2 Supprimez les groupes de disques hybrides pour chaque hôte du cluster.

   a Cliquez sur l'onglet **Configurer**.

   b Sous vSAN, cliquez sur **Gestion de disques**.

c Sous Groupes de disques, sélectionnez le groupe de disques à supprimer, cliquez sur **...**, puis sur **Supprimer**.

d Sélectionnez **Migration intégrale des données** comme mode de migration, puis cliquez sur **Oui**.

3 Supprimez les disques HDD physiques de l'hôte.

4 Ajoutez les périphériques Flash à l'hôte.

Vérifiez qu'aucune partition n'existe sur les périphériques Flash.

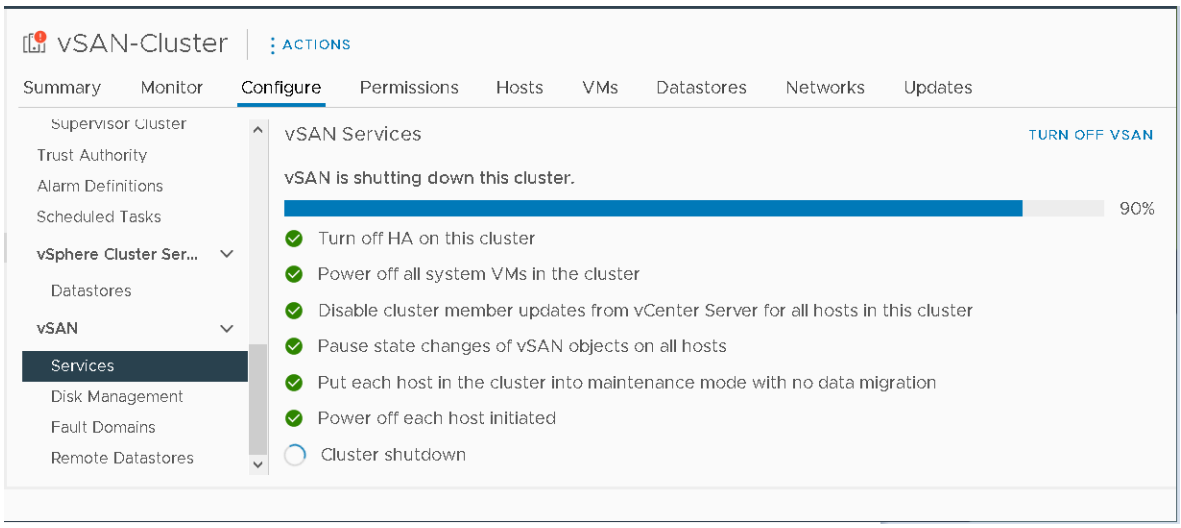
5 Créez les groupes de disques 100 % Flash sur chaque hôte.

Arrêt et redémarrage du cluster vSAN

Vous pouvez arrêter l'intégralité du cluster vSAN pour effectuer la maintenance ou le dépannage.

Utilisez l'assistant Arrêter le cluster pour arrêter le cluster vSAN. L'assistant effectue les étapes nécessaires et vous avertit lorsqu'il nécessite une action de l'utilisateur. Vous pouvez également arrêter manuellement le cluster, si nécessaire.

Note Lorsque vous arrêtez un cluster étendu, l'hôte témoin reste actif.



Arrêter le cluster vSAN à l'aide de l'assistant Arrêter le cluster

Utilisez l'assistant Arrêter le cluster pour arrêter normalement le cluster vSAN à des fins de maintenance ou de dépannage. L'assistant Arrêter le cluster est disponible avec vSAN 7.0 Update 3 et versions ultérieures.

Note Si vous disposez d'un environnement vSphere with Tanzu, vous devez suivre l'ordre spécifié lors de l'arrêt ou du démarrage des composants. Pour plus d'informations, reportez-vous à la section « Arrêt et démarrage de VMware Cloud Foundation » du *Guide des opérations de VMware Cloud Foundation*.

Procédure

1 Préparez le cluster vSAN pour l'arrêt.

   a Vérifiez le service de santé de vSAN pour confirmer que le cluster est sain.

   b Mettez hors tension toutes les machines virtuelles (VM) stockées dans le cluster vSAN, à l'exception des VM vCenter Server, des VM vCLS et des VM du service de fichiers. Si vCenter Server est hébergé sur le cluster vSAN, ne mettez pas hors tension la VM vCenter Server ou les VM de service (telles que DNS, Active Directory) utilisées par vCenter Server.

   c S'il s'agit d'un cluster de serveurs de maillage HCI, mettez hors tension toutes les machines virtuelles clientes stockées sur le cluster. Si la VM vCenter Server du cluster client est stockée sur ce cluster, migrez la VM ou mettez-la hors tension. Une fois ce cluster de serveurs arrêté, la banque de données partagée est inaccessible aux clients.

   d Vérifiez que toutes les tâches de resynchronisation sont terminées.

      Cliquez sur l'onglet **Surveiller**, puis sélectionnez **vSAN** > **Resynchronisation des objets**.

   Note Si des hôtes membres sont en mode de verrouillage, ajoutez le compte racine de l'hôte à la liste Utilisateurs exceptionnels du profil de sécurité. Pour plus d'informations, reportez-vous à la section Mode de verrouillage dans *Sécurité vSphere*.

2 Dans vSphere Client, cliquez avec le bouton droit sur le cluster vSAN, puis sélectionnez **Arrêter le cluster**.

   Vous pouvez également cliquer sur **Arrêter le cluster** sur la page Services vSAN.

3 Dans l'assistant Arrêter le cluster, vérifiez que les vérifications préalables à l'arrêt ont des coches vertes. Résolvez les problèmes indiqués par des points d'exclamation rouges. Cliquez sur **Suivant**.

   Si le dispositif vCenter Server est déployé sur le cluster vSAN, l'assistant Arrêter le cluster affiche la notification vCenter Server. Notez l'adresse IP de l'hôte d'orchestration, si vous en avez besoin lors du redémarrage du cluster. Si vCenter Server utilise des VM de service telles que DNS ou Active Directory, notez-les comme des VM exceptionnelles dans l'assistant Arrêter le cluster.

4 Entrez le motif de l'arrêt, puis cliquez sur **Arrêter**.

   La page Services vSAN s'actualise pour afficher des informations sur le processus d'arrêt.

5 Surveillez le processus d'arrêt.

   vSAN exécute les étapes d'arrêt du cluster, met hors tension les machines virtuelles du système, puis met hors tension les hôtes.

Étape suivante

Redémarrez le cluster vSAN. Reportez-vous à la section Redémarrez le cluster vSAN.

Redémarrez le cluster vSAN

Vous pouvez redémarrer un cluster vSAN arrêté pour maintenance ou dépannage.

Procédure

1. Mettez sous tension les hôtes du cluster.

   Si l'instance de vCenter Server est hébergée sur le cluster vSAN, attendez qu'elle redémarre.
2. Dans vSphere Client, cliquez avec le bouton droit sur le cluster vSAN, puis sélectionnez **Redémarrer le cluster**.

   Vous pouvez également cliquer sur **Redémarrer le cluster** sur la page Services vSAN.
3. Dans la boîte de dialogue Redémarrer le cluster, cliquez sur **Redémarrer**.

   La page Services vSAN s'actualise pour afficher des informations sur le processus de redémarrage.
4. Une fois le cluster redémarré, vérifiez le service de santé vSAN et résolvez les problèmes en attente.

Arrêter et redémarrer manuellement le cluster vSAN

Vous pouvez arrêter manuellement l'intégralité du cluster vSAN pour effectuer des opérations de maintenance ou de dépannage.

Utilisez l'assistant Arrêter le cluster, sauf si un arrêt manuel est requis dans votre workflow. Lorsque vous arrêtez manuellement le cluster vSAN, ne désactivez pas vSAN dans le cluster.

Note Si vous disposez d'un environnement vSphere with Tanzu, vous devez suivre l'ordre spécifié lors de l'arrêt ou du démarrage des composants. Pour plus d'informations, reportez-vous à la section « Arrêt et démarrage de VMware Cloud Foundation » du *Guide des opérations de VMware Cloud Foundation*.

Procédure

1. Arrêtez le cluster vSAN.
   a. Vérifiez le service de santé de vSAN pour confirmer que le cluster est sain.
   b. Mettez hors tension toutes les machines virtuelles (VM) en cours d'exécution dans le cluster vSAN si vCenter Server n'est pas hébergé sur le cluster. Si vCenter Server est hébergé dans le cluster vSAN, ne mettez pas hors tension la VM vCenter Server ou les VM de service (telles que DNS, Active Directory) utilisées par vCenter Server.
   c. Cliquez sur l'onglet **Configurer** et désactivez HA. Ainsi, le cluster n'enregistre pas les arrêts de l'hôte en tant qu'échecs.

      Pour vSphere 7.0 U1 et versions ultérieures, activez le mode de retraitement vCLS. Pour plus d'informations, reportez-vous à l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/80472.

d Vérifiez que toutes les tâches de resynchronisation sont terminées.

Cliquez sur l'onglet **Surveiller**, puis sélectionnez **vSAN** > **Resynchronisation des objets**.

e Si vCenter Server est hébergé dans le cluster vSAN, mettez la machine virtuelle vCenter Server hors tension.

Notez l'hôte qui exécute la machine virtuelle vCenter Server. Il s'agit de l'hôte sur lequel vous devez redémarrer la machine virtuelle vCenter Server.

f Désactivez les mises à jour des membres du cluster à partir de vCenter Server en exécutant la commande suivante sur les hôtes ESXi dans le cluster. Assurez-vous d'exécuter la commande suivante sur tous les hôtes.

```
esxcfg-advcfg -s 1 /VSAN/IgnoreClusterMemberListUpdates
```

g Connectez-vous à n'importe quel hôte du cluster autre que l'hôte témoin.

h Exécutez la commande suivante uniquement sur cet hôte. Si vous exécutez la commande sur plusieurs hôtes simultanément, cela peut entraîner une condition de concurrence entraînant des résultats inattendus.

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py prepare
```

Cette commande renvoie et imprime les éléments suivants :

```
La préparation du cluster est terminée.
```

Note

- Le cluster est entièrement partitionné après l'exécution réussie de la commande.
- Si vous rencontrez une erreur, résolvez le problème en fonction du message d'erreur et réessayez d'activer le mode de retraitement vCLS.
- S'il existe des hôtes défectueux ou déconnectés dans le cluster, supprimez ces hôtes et réessayez d'exécuter la commande.

i Placez tous les hôtes en mode de maintenance avec le mode **Aucune action**. Si l'instance de vCenter Server est hors tension, utilisez la commande suivante pour placer les hôtes ESXi en mode de maintenance avec le mode **Aucune action**.

```
esxcli system maintenanceMode set -e true -m noAction
```

Effectuez cette opération sur tous les hôtes.

Pour éviter le risque d'indisponibilité des données lors de l'utilisation du mode **Aucune action** en même temps sur plusieurs hôtes, suivie d'un redémarrage de plusieurs hôtes, reportez-vous à l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/60424. Pour effectuer un redémarrage simultané de tous les hôtes du cluster à l'aide d'un outil intégré, reportez-vous à l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/70650.

j Une fois que tous les hôtes sont passés en mode de maintenance, effectuez les tâches de maintenance nécessaires et mettez les hôtes hors tension.

2 Redémarrez le cluster vSAN.

a Mettez les hôtes ESXi sous tension.

Mettez sous tension la boîte physique dans laquelle ESXi est installé. L'hôte ESXi démarre, localise ses machines virtuelles et fonctionne normalement.

Si un ou plusieurs hôtes ne parviennent pas à redémarrer, vous devez récupérer manuellement ces hôtes défectueux ou les retirer du cluster vSAN.

b Lorsque tous les hôtes sont de nouveau actifs après la mise sous tension, sortez tous les hôtes du mode de maintenance. Si l'instance de vCenter Server est hors tension, utilisez la commande suivante sur les hôtes ESXi pour quitter le mode de maintenance.

```
esxcli system maintenanceMode set -e false
```

Effectuez cette opération sur tous les hôtes.

c Connectez-vous à l'un des hôtes du cluster autre que l'hôte témoin.

d Exécutez la commande suivante uniquement sur cet hôte. Si vous exécutez la commande sur plusieurs hôtes simultanément, cela peut entraîner une condition de concurrence entraînant des résultats inattendus.

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py recover
```

Cette commande renvoie et imprime les éléments suivants :

```
Le redémarrage/la mise sous tension du cluster s'est terminé
correctement.
```

e Vérifiez que tous les hôtes sont disponibles dans le cluster en exécutant la commande suivante sur chaque hôte.

```
esxcli vsan cluster get
```

f Activez les mises à jour des membres du cluster à partir de vCenter Server en exécutant la commande suivante sur les hôtes ESXi dans le cluster. Assurez-vous d'exécuter la commande suivante sur tous les hôtes.

```
esxcfg-advcfg -s 0 /VSAN/IgnoreClusterMemberListUpdates
```

g Redémarrez la machine virtuelle vCenter Server si elle est hors tension. Attendez que la machine virtuelle vCenter Server soit sous tension et en cours d'exécution. Pour désactiver le mode de retraitement vCLS, reportez-vous à l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/80472.

h Vérifiez à nouveau que tous les hôtes participent dans le cluster vSAN en exécutant la commande suivante sur chaque hôte.

```
esxcli vsan cluster get
```

i Redémarrez les machines virtuelles restantes via vCenter Server.

j Vérifiez le service de santé de vSAN et résolvez les problèmes éventuels en attente.

k (Facultatif) Si Disponibilité vSphere est activé sur le cluster vSAN, vous devez redémarrer manuellement Disponibilité vSphere pour éviter l'erreur suivante : `L'agent maître de vSphere HA est introuvable.`

Pour redémarrer manuellement Disponibilité vSphere, sélectionnez le cluster vSAN et accédez à :

1 **Configurer** > **Services** > **Disponibilité vSphere** > **MODIFIER** > **Désactiver vSphere HA**

2 **Configurer** > **Services** > **Disponibilité vSphere** > **MODIFIER** > **Activer vSphere HA**

3 S'il existe des hôtes défectueux ou déconnectés dans le cluster, récupérez ou supprimez ces hôtes du cluster vSAN. Si vCenter Server utilise des VM de service telles que DNS ou Active Directory, notez-les comme des VM exceptionnelles dans l'assistant Arrêter le cluster.

Essayez d'exécuter à nouveau les commandes ci-dessus uniquement après que le service de santé de vSAN affiche tous les hôtes disponibles avec l'état vert.

Si vous disposez d'un cluster vSAN à trois nœuds, la commande `reboot_helper.py recover` ne peut pas fonctionner en cas de panne d'un hôte. En tant qu'administrateur, procédez comme suit :

a Supprimez temporairement les informations de l'hôte en échec de la liste des agents de monodiffusion.

b Ajoutez l'hôte après l'exécution de la commande suivante.

```
reboot_helper.py recover
```

Les commandes suivantes permettent de supprimer et d'ajouter l'hôte à un cluster vSAN :

```
#esxcli vsan cluster unicastagent remove -a <IP Address> -t node -u <NodeUuid>
```

```
#esxcli vsan cluster unicastagent add -t node -u <NodeUuid> -U true -a <IP Address> -p
12321
```

Étape suivante

Redémarrez le cluster vSAN. Reportez-vous à la section Redémarrez le cluster vSAN.

Gestion de périphériques dans un cluster vSAN

5

Vous pouvez effectuer diverses tâches de gestion des périphériques dans un cluster vSAN. Vous pouvez créer des groupes de disques hybrides ou intégralement Flash, permettre à vSAN de réclamer des périphériques pour de la capacité et du cache, activer ou désactiver les voyants, marquer des périphériques comme périphériques Flash, marquer des périphériques distants comme locaux, etc.

Note Le marquage de périphériques comme périphériques Flash et le marquage de périphériques distants comme périphériques locaux ne sont pas pris en charge dans un cluster vSAN Express Storage Architecture.

Ce chapitre contient les rubriques suivantes :

Gestion des périphériques de stockage

Lorsque vous configurez vSAN sur un cluster, réclamez des périphériques de stockage sur chaque hôte pour créer la banque de données vSAN.

Le cluster vSAN contient initialement une seule banque de données vSAN. Lorsque vous réclamez des disques pour des groupes de disques ou un pool de stockage sur chaque hôte. La taille de la banque de données augmente en fonction de la capacité physique ajoutée par ces terminaux.

vSAN dispose d'un workflow uniforme pour réclamer des disques dans tous les scénarios. Vous pouvez répertorier tous les disques disponibles par modèle et taille, ou par hôte.

Ajouter un groupe de disques (vSAN Original Storage Architecture)

Lorsque vous ajoutez un groupe de disques vous devez spécifier l'hôte et les terminaux à réclamer. Chaque groupe de disques comporte un périphérique de cache Flash et un ou plusieurs périphériques de capacité. Vous pouvez créer plusieurs groupes de disques sur chaque hôte et réclamer un périphérique de cache pour chaque groupe de disques.

Lorsque vous ajoutez un groupe de disques, tenez compte du rapport entre cache Flash et capacité consommée. Le rapport varie en fonction de la configuration requise et de la charge de travail du cluster. Pour un cluster hybride, envisagez d'utiliser au moins 10 % du cache flash pour le taux de capacité consommée (sans inclure les répliques comme les miroirs).

Note Si un nouvel hôte ESXi est ajouté au cluster vSAN, le stockage local de cet hôte n'est pas ajouté automatiquement à la banque de données vSAN. Vous devez ajouter un groupe de disques pour utiliser le stockage à partir du nouvel hôte.

Ajouter un pool de stockage (vSAN Express Storage Architecture)

Chaque hôte contribuant au stockage contient un pool de stockage unique de périphériques Flash. Chaque périphérique Flash fournit la mise en cache et la capacité au cluster. Vous pouvez ajouter un pool de stockage à l'aide de n'importe quel terminal compatible. vSAN crée un seul pool de stockage par hôte, quel que soit le nombre de disques de stockage auxquels l'hôte est associé.

Réclamer des disques pour vSAN Direct

Utilisez vSAN Direct pour permettre aux services avec état d'accéder à un stockage local brut non-vSAN via un chemin direct.

Vous pouvez réclamer des périphériques locaux au niveau de l'hôte pour vSAN Direct et utiliser vSAN pour gérer et surveiller ces périphériques. Sur chaque périphérique local, vSAN Direct crée une banque de données VMFS indépendante et la met à disposition de votre application avec état.

Chaque banque de données vSAN Direct locale s'affiche comme banque de données vSAN-D.

Note Si vSAN Express Storage Architecture est activé pour le cluster, vous ne pouvez pas réclamer de disques pour vSAN Direct.

Créer un groupe de disques ou un pool de stockage

Selon l'architecture de stockage que vous utilisez dans le cluster, vous pouvez décider de créer un groupe de disques ou un pool de stockage.

Créer un groupe de disques sur un hôte (vSAN Original Storage Architecture)

Vous pouvez réclamer des périphériques de cache et de capacité pour définir des groupes de disques sur un hôte vSAN. Sélectionnez un périphérique de cache et un ou plusieurs périphériques de capacité pour créer le groupe de disques.

1 Naviguer vers le cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, cliquez sur **Gestion de disques**, sélectionnez un hôte dans le tableau, puis cliquez sur **AFFICHER LES DISQUES**.

4 Cliquez sur **CRÉER UN GROUPE DE DISQUES**.

5 Sélectionnez les disques à réclamer.

a Sélectionnez le périphérique Flash à utiliser pour le niveau de cache.

b Sélectionnez les disques à utiliser pour le niveau de capacité.

7. Cliquez sur **Créer** pour confirmer vos sélections.

Note Le nouveau groupe de disques figure dans la liste.

Créer un pool de stockage sur un hôte (vSAN Express Storage Architecture)

Vous pouvez réclamer des disques pour définir un pool de stockage sur un hôte vSAN. Chaque hôte contribuant au stockage contient un pool de stockage unique de périphériques Flash. Chaque périphérique Flash fournit la mise en cache et la capacité au cluster. Vous pouvez créer un pool de stockage avec n'importe quel périphérique compatible avec ESA. vSAN crée un seul pool de stockage par hôte.

Dans un pool de stockage, chaque périphérique fournit la mise en cache et la capacité dans un niveau unique. Cela est différent d'un groupe de disques qui dispose de périphériques dédiés dans différents niveaux de cache et de capacité.

Utilisez la réclamation de disques gérés vSAN pour réclamer automatiquement tous les disques compatibles sur les hôtes du cluster. Lorsque vous ajoutez de nouveaux hôtes, vSAN réclame également des disques compatibles sur ces hôtes. Les disques ajoutés manuellement ne sont pas affectés par ce paramètre. Vous pouvez ajouter manuellement ces disques au pool de stockage.

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, cliquez sur **Gestion de disques**.

4 Cliquez sur **Réclamer des disques inutilisés**.

Note Vous pouvez modifier le mode de réclamation de disques pour utiliser l'option **Réclamation de disques gérés vSAN**. vSAN réclame automatiquement tous les périphériques compatibles sur les hôtes du cluster.

5 Groupez par hôte.

6 Sélectionnez les disques compatibles à réclamer.

7 Cliquez sur **Créer** pour confirmer vos sélections.

Note La page de gestion des disques s'affiche avec les hôtes répertoriés. Elle contient une mention indiquant que les disques sont réclamés sur les hôtes dans la colonne « Disques en cours d'utilisation » et mentionnant le nombre de disques mis à jour par hôte. Pour afficher les disques réclamés pour l'hôte, cliquez sur le bouton « Afficher les disques ».

Réclamer des périphériques de stockage pour le cluster vSAN Original Storage Architecture

Vous pouvez sélectionner un groupe de périphériques de cache et de capacité, et vSAN les organise en groupes de disques par défaut.

Dans cette méthode, vous sélectionnez les périphériques pour créer des groupes de disques pour le cluster vSAN. Il vous faut un périphérique de cache et au moins un périphérique de capacité pour chaque groupe de disques.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, cliquez sur **Gestion de disques**.
4. Cliquez sur **Réclamer des disques inutilisés**.
5. Sélectionnez les périphériques à ajouter au groupe de disques.
   - Pour les groupes de disques hybrides, chaque hôte contribuant au stockage doit contribuer avec un périphérique de cache Flash et un ou plusieurs périphériques de capacité HDD. Vous pouvez ajouter un seul périphérique de cache Flash par groupe de disques.
     - Sélectionnez des périphériques Flash à utiliser comme cache, puis cliquez sur **Réclamer pour le niveau du cache**.
     - Sélectionnez un ou plusieurs périphériques HDD à utiliser comme capacité et cliquez sur **Réclamer pour le niveau de la capacité** pour chacun d'eux.
     - Cliquez sur **Créer** ou sur **OK**.
   - Pour les groupes de disques intégralement Flash, chaque hôte contribuant au stockage doit fournir un périphérique de cache Flash, et un ou plusieurs périphériques de capacité Flash. Vous pouvez ajouter un seul périphérique de cache Flash par groupe de disques.
     - Sélectionnez un ou plusieurs périphériques Flash à utiliser comme cache et cliquez sur **Réclamer pour le niveau du cache** pour chaque périphérique.
     - Sélectionnez un périphérique Flash à utiliser pour la capacité, puis cliquez sur **Réclamer pour le niveau de la capacité**.
     - Cliquez sur **Créer** ou sur **OK**.

   vSAN réclame les périphériques que vous avez sélectionnés et les classe en groupes de disques par défaut qui contribuent à la banque de données vSAN.

Pour vérifier le rôle de chaque périphérique ajouté au groupe de disques intégralement Flash, accédez à la colonne « Réclamé comme » pour un hôte donné sur la page Gestion de disques. Le tableau affiche la liste de périphériques et leur fonction dans un groupe de disques. Pour les groupes de disques intégralement Flash et hybrides, le disque de cache est toujours affiché en premier dans la grille du groupe de disques.

Réclamer des périphériques de stockage pour le cluster vSAN Express Storage Architecture

Vous pouvez sélectionner un groupe de périphériques d'un hôte et vSAN les organise en pools de stockage.

Une fois vSAN ESA activé, vous pouvez réclamer des disques manuellement ou automatiquement. Dans la méthode manuelle, vous pouvez sélectionner un groupe de périphériques de stockage à réclamer.

Dans la réclamation automatique de disques, vSAN sélectionne automatiquement tous les disques compatibles à partir des hôtes. Lorsque de nouveaux hôtes sont ajoutés au cluster, vSAN réclame automatiquement les disques compatibles disponibles dans ces hôtes et ajoute le stockage à la banque de données vSAN.

Vous pouvez choisir des périphériques qui ne sont pas signalés comme certifiés pour vSAN ESA. Ces périphériques seront pris en compte dans le pool de stockage, mais cette configuration n'est pas recommandée et peut affecter les performances.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, cliquez sur **Gestion de disques**.
4. Pour réclamer manuellement des disques, cliquez sur **Réclamer des disques inutilisés**.
   a. Sélectionnez les périphériques à réclamer.
   b. Cliquez sur **Créer**.
5. Pour réclamer automatiquement des disques, cliquez sur **MODIFIER LE MODE DE RÉCLAMATION DE DISQUES**, puis cliquez sur le bouton bascule **Réclamation de disques gérés vSAN**.

   Note Si vous choisissez d'utiliser la réclamation de disques géré vSAN lors de la configuration du cluster, le bouton bascule est déjà activé.

   vSAN réclame les périphériques que vous avez sélectionnés et les classe en pools de stockage qui prennent en charge la banque de données vSAN. Par défaut, vSAN crée un pool de stockage pour chaque hôte ESXi contribuant au stockage du cluster. Si les périphériques sélectionnés ne sont pas certifiés pour vSAN ESA, ils ne sont pas pris en compte pour la création de pools de stockage.

Réclamer des disques pour vSAN Direct

Vous pouvez réclamer des périphériques de stockage local en tant que vSAN Direct pour une utilisation avec la plate-forme de persistance des données vSAN.

Note Seule la plate-forme de persistance des données vSAN peut consommer le stockage vSAN Direct. La plate-forme de persistance des données vSAN fournit une structure aux partenaires de technologies logicielles pour l'intégration à VMware Infrastructure. Chaque partenaire doit développer son propre plug-in pour les clients VMware qui bénéficient des avantages de la plate-forme de persistance des données vSAN. La plate-forme n'est opérationnelle que lorsque la solution partenaire exécutée au-dessus est opérationnelle. Pour plus d'informations, reportez-vous à la section *Configuration et gestion de vSphere avec Tanzu*.

Procédure

1. Dans vSphere Client, accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, cliquez sur **Gestion de disques**.
4. Cliquez sur **Réclamer des disques inutilisés**.
5. Dans l'assistant Réclamer des disques inutilisés, sélectionnez l'onglet vSAN Direct.
6. Sélectionnez un périphérique à réclamer en cochant la case correspondante dans la colonne **Réclamer pour vSAN Direct**.

   Note Les périphériques réclamés pour votre cluster vSAN ne s'affichent pas dans l'onglet vSAN Direct.
7. Cliquez sur **Créer**.

Résultats

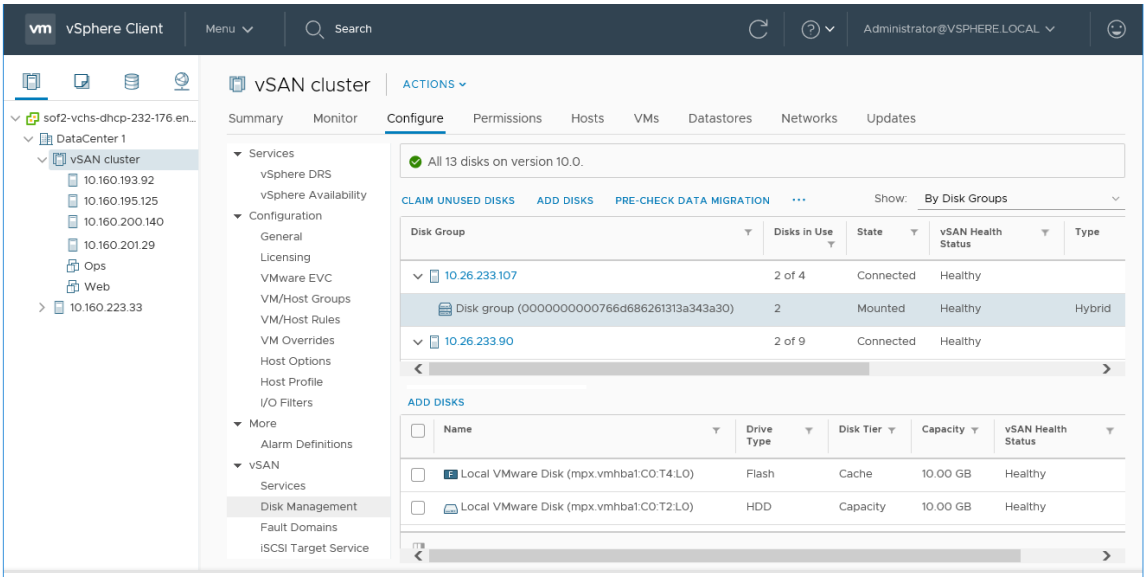
Pour chaque périphérique que vous réclamez, vSAN crée une banque de données vSAN Direct.

Étape suivante

Vous pouvez cliquer sur l'onglet Banques de données pour afficher les banques de données vSAN Direct dans votre cluster.

Utilisation de périphériques individuels

Vous pouvez effectuer diverses tâches de gestion de périphériques dans le cluster vSAN, comme ajouter des périphériques à un groupe de disques, supprimer des périphériques d'un groupe de disques, activer ou désactiver des voyants de localisateur, et marquer des périphériques. Vous pouvez également ajouter ou supprimer des disques réclamés à l'aide de vSAN Direct.



Ajouter des périphériques au groupe de disques

Lorsque vous configurez vSAN pour réclamer des disques en mode manuel, vous pouvez ajouter des périphériques locaux supplémentaires aux groupes de disques existants.

Les périphériques doivent être du même type que les périphériques existants dans les groupes de disques, par exemple un SSD ou des disques magnétiques.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, cliquez sur **Gestion de disques**.
4. Sélectionnez le groupe de disques, puis cliquez sur **Ajouter des disques**.
5. Sélectionnez le périphérique à ajouter, puis cliquez sur **Ajouter**.

   Si vous ajoutez un périphérique utilisé qui contient des données résiduelles ou des informations de partition, vous devez nettoyer le périphérique. Pour plus d'informations sur la suppression d'informations de partition des périphériques, reportez-vous à la section Supprimer une partition de périphériques. Vous pouvez également exécuter la commande RVC `host_wipe_vsan_disks` pour formater le périphérique.

Étape suivante

Vérifiez que le contrôle de santé Équilibre des disques vSAN est vert. Si le contrôle de santé Équilibre des disques émet un avertissement, procédez à une opération de rééquilibrage manuelle pendant les heures de faible activité. Pour plus d'informations, reportez-vous à la section « Rééquilibrage manuel » dans *Surveillance et dépannage de vSAN*.

Vérifier les capacités de migration des données d'un disque ou d'un groupe de disques

Utilisez la prévérification de la migration des données pour déterminer l'effet des options de migration des données lorsque vous démontez un disque ou un groupe de disques ou que vous le supprimez du cluster vSAN.

Exécutez la prévérification de la migration des données avant de démonter ou de supprimer un disque ou un groupe de disques du cluster vSAN. Les résultats des tests fournissent des informations pour vous aider à déterminer l'impact sur la capacité du cluster, les contrôles de santé prévus et tous les objets qui seront incompatibles. Si l'opération échoue, la prévérification fournit des informations sur les ressources nécessaires.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet Surveiller.
3. Sous vSAN, cliquez sur **Prévérification de la migration des données**.
4. Sélectionnez un disque ou un groupe de disques, choisissez une option de migration des données, puis cliquez sur **Prévérifier**.

   vSAN exécute les tests de prévérification de migration des données.
5. Affichez les résultats du test.

   Les résultats de la prévérification indiquent si vous pouvez démonter ou supprimer en toute sécurité le disque ou le groupe de disques.

   - L'onglet Conformité et accessibilité des objets affiche les objets susceptibles de présenter des problèmes après la migration des données.
   - L'onglet Capacité du cluster affiche l'impact de la migration des données sur le cluster vSAN avant et après l'exécution de l'opération.
   - L'onglet Santé prévue affiche les contrôles de santé qui peuvent être affectés par la migration des données.

Étape suivante

Si la prévérification indique que vous pouvez démonter ou supprimer le périphérique, cliquez sur l'option pour poursuivre l'opération.

Supprimer des groupes de disques ou des périphériques de vSAN

Vous pouvez supprimer des périphériques sélectionnés du groupe de disques ou l'intégralité d'un groupe de disques.

Du fait que la suppression des périphériques non protégés peut être un événement perturbateur pour la banque de données vSAN ainsi que pour les machines virtuelles dans la banque de données, évitez de supprimer des périphériques ou des groupes de disques.

Généralement, vous supprimez des périphériques ou des groupes de disques de vSAN lorsque vous mettez à niveau un périphérique ou que vous remplacez un périphérique en panne, ou lorsque vous devez supprimer un périphérique cache. D'autres fonctionnalités de stockage de vSphere peuvent utiliser un périphérique Flash quelconque que vous supprimez du cluster vSAN.

La suppression définitive d'un groupe de disques supprime l'appartenance au disque ainsi que les données stockées sur les périphériques.

Note La suppression d'un périphérique de mémoire cache Flash ou de tous les périphériques de capacité d'un groupe de disques supprime l'intégralité du groupe de disques.

La suppression des données de périphériques ou de groupes de disques risque de générer une non-conformité temporaire des stratégies de stockage de machine virtuelle.

Conditions préalables

Exécutez la prévérification de la migration des données sur le périphérique ou le groupe de disques avant de le supprimer du cluster. Pour plus d'informations, consultez

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, cliquez sur **Gestion de disques**.
4. Supprimez un groupe de disques ou les périphériques sélectionnés.

Option	Description
Supprimer le groupe de disques	a Sous Groupes de disques, sélectionnez le groupe de disques à supprimer, puis cliquez sur **...**, puis sur **Supprimer**. b Sélectionnez un mode de suppression des données.
Supprimer le périphérique sélectionné	a Sous Groupes de disques, sélectionnez le groupe de disques qui contient le périphérique que vous supprimez. b Sous Disques, sélectionnez le périphérique à supprimer, puis cliquez sur **Supprimer un ou plusieurs disques**. c Sélectionnez un mode de suppression des données.

5. Cliquez sur **Oui** ou **Supprimer** pour confirmer.

   Les données sont évacuées des périphériques sélectionnés ou d'un groupe de disques.

Recréer un groupe de disques

Lorsque vous recréez un groupe de disques dans le cluster vSAN, les disques existants sont supprimés du groupe de disques et le groupe de disques est supprimé. vSAN recrée le groupe de disques avec les mêmes disques.

Lorsque vous recréez un groupe de disques sur un cluster vSAN, vSAN gère le processus pour vous. vSAN supprime les données de tous les disques du groupe de disques, supprime le groupe de disques et crée le groupe de disques avec les mêmes disques.

Procédure

1 Accédez au cluster vSAN dans vSphere Client.
2 Cliquez sur l'onglet **Configurer**.
3 Sous vSAN, cliquez sur **Gestion de disques**.
4 Sous Groupes de disques, sélectionnez le groupe de disques à recréer.
5 Cliquez sur **...**, puis cliquez sur **Recréer**.

   La boîte de dialogue Recréer le groupe de disques s'affiche.
6 Sélectionnez un mode de migration des données, puis cliquez sur **Recréer**.

Résultats

Toutes les données enregistrées sur les disques sont supprimées. Le groupe de disques est supprimé du cluster et recréé.

Utilisation des voyants de localisation

Vous pouvez utiliser les voyants de localisation pour identifier l'emplacement des périphériques de stockage.

vSAN peut allumer le voyant de localisateur sur un périphérique en panne pour vous permettre de l'identifier plus facilement. Cette option est particulièrement utile lorsque vous utilisez plusieurs scénarios de connexion à chaud et d'échange d'hôte.

Envisagez l'utilisation de contrôleurs de stockage d'E/S en mode relais, car les contrôleurs en mode RAID 0 nécessitent des étapes supplémentaires pour leur permettre de reconnaître les voyants de localisateur.

Pour plus d'informations sur la configuration des contrôleurs de stockage en mode RAID 0, reportez-vous à la documentation du fournisseur.

Voyants de localisateur

Vous pouvez activer ou désactiver les voyants de localisateur sur les périphériques de stockage vSAN. Lorsque vous activez le voyant de localisateur, vous pouvez identifier l'emplacement d'un périphérique de stockage spécifique.

Lorsque vous n'avez plus besoin d'alerte visuelle concernant vos périphériques vSAN, vous pouvez désactiver les voyants de localisateur sur les périphériques sélectionnés.

Conditions préalables

- Vérifiez que vous avez installé les pilotes pris en charge pour les contrôleurs d'E/S de stockage qui activent cette fonctionnalité. Pour plus d'informations sur les pilotes certifiés par VMware, reportez-vous au *Guide de compatibilité VMware* à l'adresse http://www.vmware.com/resources/compatibility/search.php.
- Dans certains cas, vous pouvez avoir besoin d'utilitaires tiers pour configurer la fonctionnalité des voyants de localisateur sur vos contrôleurs d'E/S de stockage. Par exemple, lorsque vous utilisez HP, vous devez vérifier que l'interface de ligne de commande SSA HP est installée.

Pour plus d'informations sur l'installation de VIB tiers, reportez-vous à la documentation *Mise à niveau vSphere*.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, cliquez sur **Gestion de disques**.
4. Sélectionnez un hôte pour consulter la liste des périphériques.
5. Au bas de la page, sélectionnez un ou plusieurs périphériques de stockage dans la liste et effectuez l'action souhaitée pour les voyants de localisateur.

Option	Action
Activer la LED	Active le voyant de localisateur sur le périphérique de stockage sélectionné. Vous pouvez également utiliser l'onglet **Gérer** et cliquer sur **Stockage > Périphériques de stockage**.
Désactiver la LED	Désactive le voyant de localisateur sur le périphérique de stockage sélectionné. Vous pouvez également utiliser l'onglet **Gérer** et cliquer sur **Stockage > Périphériques de stockage**.

Marquer des périphériques comme Flash

Lorsque des périphériques Flash ne sont pas identifiés automatiquement en tant que Flash par les hôtes ESXi, vous pouvez les marquer manuellement comme périphériques Flash locaux.

Les périphériques Flash peuvent ne pas être reconnus en tant que tels lorsqu'ils sont activés pour le mode RAID 0 mode au lieu du mode relais. Lorsque des périphériques ne sont pas reconnus comme périphériques Flash locaux, ils sont exclus de la liste de périphériques proposés pour vSAN et vous ne pouvez pas les utiliser dans le cluster vSAN. Le marquage de ces périphériques en tant que périphériques Flash locaux les rend disponibles pour vSAN.

Conditions préalables

- Vérifiez que le périphérique est local pour votre hôte.
- Vérifiez que le périphérique n'est pas utilisé.

- Vérifiez que les machines virtuelles accédant au périphérique sont hors tension et que la banque de données est démontée.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, cliquez sur **Gestion de disques**.
4. Sélectionnez l'hôte pour afficher la liste des périphériques disponibles.
5. Dans le menu déroulant **Afficher** situé en bas de la page, sélectionnez **Pas en cours d'utilisation**.
6. Sélectionnez un ou plusieurs périphériques Flash dans la liste et cliquez sur **Marquer en tant que disque Flash**.
7. Cliquez sur **Oui** pour enregistrer vos modifications.

   Le type de lecteur des périphériques sélectionnés s'affiche en tant que Flash.

Marquer des périphériques comme HDD

Lorsque des disques magnétiques locaux ne sont pas automatiquement définis comme périphériques HDD par les hôtes ESXi, vous pouvez les marquer manuellement comme périphériques HDD locaux.

Si vous avez marqué un disque magnétique en tant que périphérique Flash, vous pouvez modifier manuellement le type de disque du périphérique en le marquant comme disque magnétique.

Conditions préalables

- Vérifiez que le disque magnétique est en local sur votre hôte.
- Vérifiez que le disque magnétique n'est pas utilisé et qu'il n'est pas vide.
- Vérifiez que les machines virtuelles qui accèdent au périphérique sont sous tension.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, cliquez sur **Gestion de disques**.
4. Sélectionnez un hôte pour afficher la liste des disques magnétiques disponibles.
5. Dans le menu déroulant **Afficher** situé en bas de la page, sélectionnez **Pas en cours d'utilisation**.
6. Sélectionnez un ou plusieurs disques magnétiques dans la liste et cliquez sur **Marquer en tant que disque dur**.

7 Cliquez sur **Oui** pour enregistrer.

Le type de lecteur pour les disques magnétiques sélectionnés s'affiche en tant que lecteur HDD.

Marquer des périphériques comme locaux

Lorsque des hôtes SAS utilisent des encadrements SAS externes, vSAN peut reconnaître certains périphériques comme distants et ne pas pouvoir les réclamer automatiquement comme locaux.

En pareils cas, vous pouvez marquer ces périphériques comme étant locaux.

Conditions préalables

Assurez-vous que le périphérique de stockage n'est pas partagé.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, cliquez sur **Gestion de disques**.

4 Sélectionnez un hôte pour consulter la liste des périphériques.

5 Dans le menu déroulant **Afficher** situé en bas de la page, sélectionnez **Pas en cours d'utilisation**.

6 Dans la liste des périphériques, sélectionnez un ou plusieurs périphériques distants que vous souhaitez marquer comme locaux, puis cliquez sur **Marquer en tant que disque local**.

7 Cliquez sur **Oui** pour enregistrer vos modifications.

Marquer des périphériques comme distants

Les hôtes qui utilisent des contrôleurs SAS externes peuvent partager des périphériques. Vous pouvez marquer manuellement ces périphériques comme distants, de sorte que vSAN ne les réclame pas lors de la création de groupes de disques.

Dans vSAN, vous ne pouvez pas ajouter de périphériques partagés à un groupe de disques.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, cliquez sur **Gestion de disques**.

4 Sélectionnez un hôte pour consulter la liste des périphériques.

5 Dans le menu déroulant **Afficher** situé en bas de la page, sélectionnez **Pas en cours d'utilisation**.

6 Sélectionnez un ou plusieurs périphériques que vous souhaitez marquer comme distants, puis cliquez sur **Marquer en tant que disque distant**.

7 Cliquez sur **Oui** pour confirmer.

Ajouter un périphérique de capacité

Vous pouvez ajouter un périphérique de capacité à un groupe de disques vSAN existant.

Vous ne pouvez pas ajouter un périphérique partagé à un groupe de disques.

Conditions préalables

Vérifiez que le périphérique est formaté et n'est pas utilisé.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, cliquez sur **Gestion de disques**.

4 Sélectionnez un groupe de disques.

5 Cliquez sur **Ajouter des disques** en bas de la page.

6 Sélectionnez le périphérique de capacité que vous souhaitez ajouter au groupe de disques.

7 Cliquez sur **OK** ou sur **Ajouter**.

Le périphérique est ajouté au groupe de disques.

Supprimer une partition de périphériques

Vous pouvez supprimer les informations d'une partition d'un périphérique afin que vSAN puissent réclamer le périphérique pour utilisation.

Si vous avez ajouté un périphérique qui contient des données résiduelles ou des informations de partition, vous devez supprimer toutes les informations de partition préexistantes du périphérique avant de pouvoir le réclamer pour une utilisation par vSAN. VMware recommande d'ajouter des périphériques propres aux groupes de disques.

Lorsque vous supprimez les informations de partition d'un périphérique, vSAN supprime la partition principale qui inclut les informations de formatage de disque et les partitions logiques du périphérique.

Conditions préalables

Vérifiez que le périphérique n'est pas utilisé par ESXi comme disque de démarrage, banque de données VMFS ou vSAN.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, cliquez sur **Gestion de disques**.

4 Sélectionnez un hôte pour afficher la liste des périphériques disponibles.

5 Dans le menu déroulant **Afficher**, sélectionnez **Inéligible**.

6 Sélectionnez un périphérique dans la liste, puis cliquez sur **Effacer les partitions**.

7 Cliquez sur **OK** pour confirmer.

Le périphérique est propre et n'inclut pas d'informations de partition.

Augmenter l'efficacité d'utilisation de l'espace dans un cluster vSAN

6

Vous pouvez utiliser des techniques d'efficacité d'utilisation de l'espace pour réduire la quantité d'espace requise pour stocker des données. Ces techniques réduisent l'espace de stockage total requis pour répondre à vos besoins.

Ce chapitre contient les rubriques suivantes :

Présentation de l'efficacité d'utilisation de l'espace vSAN

Vous pouvez utiliser des techniques d'efficacité d'utilisation de l'espace pour réduire la quantité d'espace requise pour stocker des données. Ces techniques réduisent la capacité de stockage totale requise pour répondre à vos besoins.

vSAN 6.7 Update 1 et versions ultérieures prend en charge des commandes SCSI unmap vous permettant de récupérer l'espace de stockage mappé à un objet vSAN supprimé.

Vous pouvez utiliser la déduplication et la compression sur un cluster vSAN pour éliminer les données en double et réduire la quantité d'espace requise pour stocker les données. Vous pouvez également utiliser le vSAN de compression seule pour réduire les exigences de stockage sans compromettre les performances du serveur.

Vous pouvez définir l'attribut de stratégie **Méthode de tolérance de panne** sur les machines virtuelles pour utiliser le codage d'effacement RAID 5 ou RAID 6. Le codage d'effacement peut protéger vos données tout en utilisant moins d'espace de stockage que la mise en miroir RAID 1 par défaut.

Vous pouvez utiliser la déduplication et la compression, ainsi que le codage d'effacement RAID 5 ou RAID 6 pour favoriser les économies d'espace de stockage. RAID 5 ou RAID 6 permettent chacun des économies d'espace clairement définies par rapport à RAID 1. La déduplication et la compression peuvent apporter des économies supplémentaires.

Réclamation d'espace à l'aide de la commande SCSI unmap

vSAN 6.7 Update 1 et versions ultérieures prend en charge les commandes SCSI UNMAP qui vous permettent de récupérer l'espace de stockage qui est mappé à des fichiers supprimés dans le système de fichiers créé par l'invité sur l'objet vSAN.

La suppression de fichiers libère de l'espace dans le système de fichiers. Cet espace libre est mappé sur un périphérique de stockage jusqu'à ce que le système de fichiers le libère ou le démappe. vSAN prend en charge la récupération d'espace libre, qui est également appelée opération UNMAP. Vous pouvez libérer de l'espace de stockage dans la banque de données vSAN lorsque vous supprimez ou migrez une machine virtuelle, consolidez un snapshot, etc.

La récupération de l'espace de stockage peut fournir un débit d'E/S hôte-à-Flash plus élevé et améliorer l'endurance Flash.

vSAN prend également en charge les commandes SCSI UNMAP soumises directement depuis un système d'exploitation invité pour récupérer de l'espace de stockage. vSAN prend en charge les opérations UNMAP hors ligne et en ligne. Sur les systèmes d'exploitation Linux, les demandes UNMAP hors ligne sont exécutées avec la commande **`fstrim(8)`**, et les demandes UNMAP en ligne sont effectuées lorsque la commande **`mount -o discard`** est utilisée. Sur le système d'exploitation Windows, NTFS effectue des demandes UNMAP en ligne par défaut.

La capacité de démappage n'est pas activée par défaut. Pour activer UNMAP sur un cluster vSAN, utilisez la commande RVC suivante : **`vsan.unmap_support –enable`**

Lorsque vous activez UNMAP sur un cluster vSAN, vous devez mettre hors tension puis remettre sous tension toutes les machines virtuelles. Les machines virtuelles doivent utiliser le matériel virtuel version 13 ou supérieure pour effectuer des opérations UNMAP.

Utiliser la déduplication et la compression

vSAN peut effectuer une déduplication et une compression au niveau des blocs pour économiser l'espace de stockage. Lorsque vous activez la déduplication et la compression sur un cluster vSAN intégralement Flash, les données redondantes dans chaque groupe de disques ou pool de stockage sont réduites.

La déduplication supprime les blocs de données redondants, tandis que la compression supprime les données redondantes supplémentaires au sein de chaque bloc de données. Ces techniques fonctionnent en synergie pour réduire la quantité d'espace requise pour stocker les données. vSAN applique la déduplication, puis la compression lorsqu'il déplace les données du niveau cache au niveau capacité. Utilisez le vSAN de compression uniquement pour les charges de travail qui ne bénéficient pas de la déduplication, par exemple le traitement transactionnel en ligne.

La déduplication s'effectue en ligne lors de la réécriture des données du niveau de cache au niveau de capacité. L'algorithme de déduplication utilise une taille de bloc fixe et est appliqué dans chaque groupe de disques. Les copies redondantes d'un bloc dans le même groupe de disques sont dédupliquées.

Pour vSAN Original Storage Architecture, la déduplication et la compression sont activées en tant que paramètres à l'échelle du cluster, mais elles sont appliquées au niveau du groupe de disques. En outre, vous ne pouvez pas activer la compression sur des charges de travail spécifiques, car les paramètres ne peuvent pas être modifiés via des stratégies vSAN. Lorsque vous activez la déduplication et la compression sur un cluster vSAN, les données redondantes au sein d'un groupe de disques particulier sont réduites à une seule copie.

Note Le vSAN de compression seule est appliqué sur une base par disque.

Pour vSAN Express Storage Architecture, la compression est activée par défaut sur le cluster. Si vous ne souhaitez pas activer la compression sur certaines charges de travail de machine virtuelle. Vous pouvez le faire en créant une stratégie de stockage personnalisée et en appliquant la stratégie aux machines virtuelles. En outre, la compression pour vSAN Express Storage Architecture s'applique uniquement aux nouvelles écritures. Les anciens blocs restent non compressés même après l'activation de la compression pour un objet.

Vous pouvez activer la déduplication et la compression lorsque vous créez un cluster vSAN intégralement Flash ou lorsque vous modifiez un cluster vSAN intégralement Flash existant. Pour plus d'informations, consultez Activer la déduplication et la compression sur un cluster vSAN existant.

Lorsque vous activez ou désactivez la déduplication et la compression, vSAN effectue un reformatage de chaque groupe de disques ou pool de stockage sur chaque hôte. Selon les données stockées sur la banque de données vSAN, ce processus peut être long. N'effectuez pas ces opérations fréquemment. Si vous prévoyez de désactiver la déduplication et la compression, vous devez d'abord vérifier que suffisamment de capacité physique est disponible pour recevoir vos données.

Note La déduplication et la compression peuvent être inefficaces pour les machines virtuelles chiffrées, car le chiffrement des VM chiffre les données sur l'hôte avant leur écriture vers le stockage. Des compromis en matière de stockage pourraient être nécessaires lors de l'utilisation du chiffrement des machines virtuelles.

Gérer les disques dans un cluster avec la déduplication et la compression

Note Cette rubrique s'applique uniquement au cluster vSAN Original Storage Architecture.

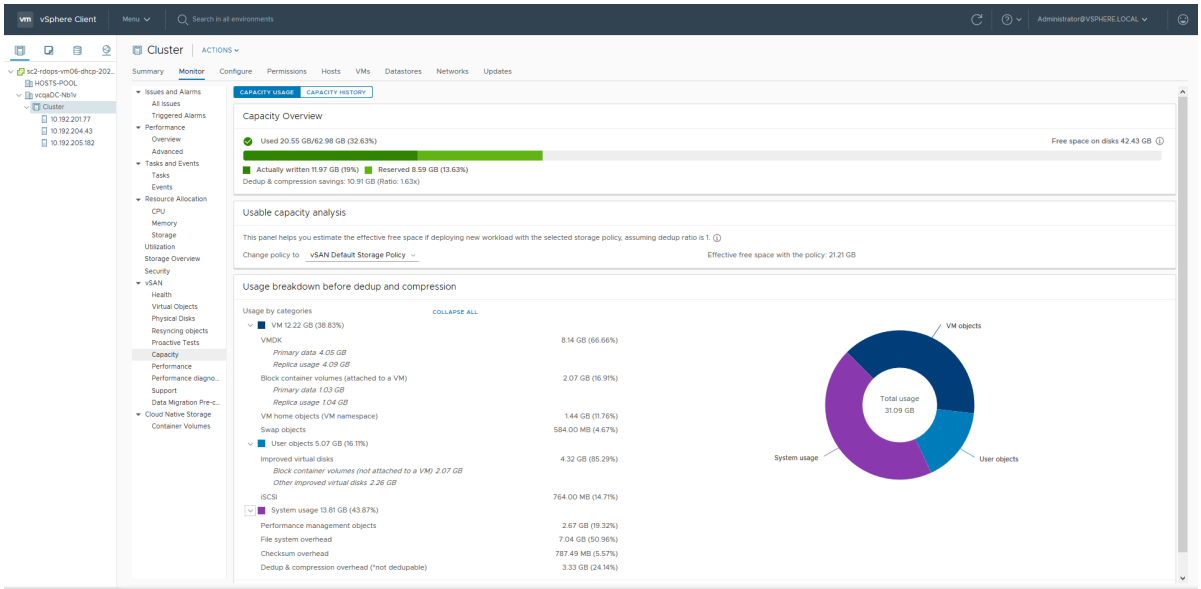
Tenez compte des directives suivantes lors de la gestion de disques dans un cluster sur lequel la déduplication et la compression sont activées. Ces directives ne s'appliquent pas au vSAN de compression seule.

- Évitez d'ajouter des disques à un groupe de disques de façon incrémentielle. Pour une déduplication et une compression plus efficaces, envisagez d'ajouter un groupe de disques pour augmenter la capacité de stockage du cluster.
- Lorsque vous ajoutez un groupe de disques manuellement, ajoutez tous les disques de capacité en même temps.

- Vous ne pouvez pas supprimer un disque spécifique d'un groupe de disques. Vous devez supprimer l'intégralité du groupe de disques pour apporter des modifications.
- Une panne d'un seul disque provoque la panne de tout le groupe de disques.

Vérification des économies d'espace réalisées par la déduplication et la compression

Le niveau de réduction de l'espace de stockage lié à la déduplication et la compression dépend de nombreux facteurs, notamment le type de données stockées et le nombre de blocs en double. Les grands groupes de disques ont tendance à offrir un taux de déduplication plus élevé. Vous pouvez vérifier les résultats de la déduplication et de la compression en affichant Répartition de l'utilisation avant déduplication et compression dans le moniteur de capacité vSAN.



Vous pouvez afficher Répartition de l'utilisation avant déduplication et compression lorsque vous surveillez la capacité de vSAN dans vSphere Client. Elle affiche des informations sur les résultats de la déduplication et de la compression. L'espace Utilisé avant indique l'espace logique requis avant d'appliquer la déduplication et la compression, tandis que l'espace Utilisé après indique l'espace physique utilisé après l'application de la déduplication et de la compression. L'espace Utilisé après affiche également une vue d'ensemble de la quantité d'espace économisée, et le taux de déduplication et de compression.

Le taux de déduplication et de compression est basé sur l'espace logique (Utilisé avant) requis pour stocker les données avant d'appliquer la déduplication et la compression, en relation avec l'espace physique (Utilisé après) requis après l'application de la déduplication et de la compression. Spécifiquement, le taux correspond à l'espace Utilisé avant divisé par l'espace Utilisé après. Par exemple, si l'espace Utilisé avant est de 3 Go, alors que l'espace physique Utilisé après est de 1 Go, le taux de déduplication et de compression est de 3x.

Lorsque la déduplication et la compression sont activées sur le cluster vSAN, vous devrez éventuellement attendre plusieurs minutes avant que les mises à jour de capacité se reflètent dans le Moniteur de capacité pendant que l'espace disque est réclamé et réaffecté.

Éléments à prendre en compte pour la conception de la déduplication et de la compression

Tenez compte de ces directives lorsque vous configurez la déduplication et la compression dans un cluster vSAN.

- La déduplication et la compression sont disponibles uniquement sur les groupes de disques intégralement Flash.
- Le format sur disque version 3.0 ou version ultérieure est requis pour prendre en charge la déduplication et la compression.
- Vous devez détenir une licence valide pour la déduplication et la compression sur un cluster.
- Lorsque vous activez la déduplication et la compression sur un cluster vSAN, tous les groupes de disques participent à la réduction des données par la déduplication et la compression.
- vSAN peut éliminer les blocs de données en double dans chaque groupe de disques, mais pas entre les groupes de disques (applicable uniquement à vSAN Original Storage Architecture).
- La surcharge de capacité pour la déduplication et la compression est d'environ 5 % de la capacité brute totale.
- Les stratégies doivent disposer de réservations d'espace d'objet de 0 ou de 100 %. Les stratégies avec réservations d'espace d'objet de 100 % sont toujours honorées, mais peuvent rendre la déduplication et la compression moins efficaces.

Activer la déduplication et la compression sur un nouveau cluster vSAN

Vous pouvez activer la déduplication et la compression lorsque vous configurez un nouveau cluster vSAN intégralement Flash.

Procédure

1. Accédez à un nouveau cluster vSAN intégralement Flash.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, sélectionnez **Services**.
   a. Cliquez sur **Modifier** sous **Services de données**.
   b. Sélectionnez une option d'efficacité de l'utilisation de l'espace : déduplication et compression, ou compression uniquement.

c Sous **Chiffrement**, activez le chiffrement des données au repos à l'aide du bouton bascule.

Note Si vous utilisez un cluster vSAN Express Storage Architecture, vous ne pouvez pas modifier ce paramètre après avoir réclamé des disques.

d (Facultatif) Sélectionnez **Autoriser la redondance réduite**. Si nécessaire, vSAN permet de réduire le niveau de protection de vos machines virtuelles tout en activant la déduplication et la compression. Pour plus de détails, reportez-vous à Réduction de la redondance des machines virtuelles pour le cluster vSAN.

4 Terminez la configuration de votre cluster.

Activer la déduplication et la compression sur un cluster vSAN existant

Vous pouvez activer la déduplication et la compression en modifiant les paramètres de configuration sur un cluster vSAN existant intégralement Flash.

Pour activer ces fonctionnalités sur un cluster vSAN Original Storage Architecture :

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, sélectionnez **Services**.

a Cliquez ici pour modifier l'efficacité de l'utilisation de l'espace.

b Sélectionnez une option d'efficacité de l'utilisation de l'espace : déduplication et compression, ou compression uniquement.

c (Facultatif) Sélectionnez **Autoriser la redondance réduite**. Si nécessaire, vSAN permet de réduire le niveau de protection de vos machines virtuelles tout en activant la déduplication et la compression. Pour plus de détails, reportez-vous à Réduction de la redondance des machines virtuelles pour le cluster vSAN.

4 Cliquez sur **Appliquer** pour enregistrer les modifications de la configuration.

Pour activer ces fonctionnalités sur un cluster vSAN Express Storage Architecture :

1 Accédez au cluster.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, sélectionnez **Services**.

4 Sous Services de données, cliquez sur **Modifier**.

a Sous **Chiffrement**, activez le chiffrement des données au repos à l'aide du bouton bascule.

Note Vous ne pouvez pas modifier ce paramètre après avoir réclamé des disques.

b Activez le chiffrement des données en transit à l'aide du bouton bascule Chiffrement des données en transit et spécifiez l'intervalle de renouvellement de clés.

c (Facultatif) Sélectionnez **Autoriser la redondance réduite**. Si nécessaire, vSAN permet de réduire le niveau de protection de vos machines virtuelles tout en activant la déduplication et la compression. Pour plus de détails, reportez-vous à Réduction de la redondance des machines virtuelles pour le cluster vSAN.

5 Cliquez sur **Appliquer** pour enregistrer les modifications de la configuration.

Lors de l'activation de la déduplication et de la compression, vSAN met à jour le format de disque de chaque groupe de disques du cluster. Pour effectuer cette modification, vSAN supprime les données du groupe de disques, supprime le groupe de disques, puis le recrée sous un nouveau format qui prend en charge la déduplication et la compression.

Cette opération d'activation ne nécessite ni migration de machine virtuelle, ni DRS. Le temps requis pour cette opération dépend du nombre d'hôtes dans le cluster et de la quantité de données. Vous pouvez surveiller la progression dans l'onglet **Tâches et événements**.

Désactiver la déduplication et la compression

Vous pouvez désactiver la déduplication et la compression sur votre cluster vSAN.

Lorsque la déduplication et la compression sont désactivées sur le cluster vSAN, la taille de la capacité utilisée dans le cluster peut être étendue (en fonction du taux de déduplication). Avant de désactiver la déduplication et la compression, vérifiez que la capacité du cluster est suffisante pour gérer la taille des données étendues.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

a Sous vSAN, sélectionnez **Services**.

b Cliquez sur **Modifier**.

c Désactivez la déduplication et la compression.

d (Facultatif) Sélectionnez **Autoriser la redondance réduite**. Si nécessaire, vSAN permet de réduire le niveau de protection de vos machines virtuelles tout en désactivant Déduplication et compression. Reportez-vous à Réduction de la redondance des machines virtuelles pour le cluster vSAN.

3 Cliquez sur **Appliquer** ou sur **OK** pour enregistrer vos modifications de configuration.

Résultats

Lors de la désactivation de la déduplication et de la compression, vSAN modifie le format de disque sur chaque groupe de disques du cluster. Il supprime les données du groupe de disques, supprime le groupe de disques, puis le recrée sous un format qui ne prend pas en charge la déduplication et la compression.

Le temps requis pour cette opération dépend du nombre d'hôtes dans le cluster et de la quantité de données. Vous pouvez surveiller la progression dans l'onglet **Tâches et événements**.

Réduction de la redondance des machines virtuelles pour le cluster vSAN

Lorsque vous activez la déduplication et la compression, vous devrez dans certains cas réduire le niveau de protection de vos machines virtuelles.

L'activation de la déduplication et de la compression nécessite une modification du format des groupes de disques. Pour effectuer cette modification, vSAN supprime les données du groupe de disques, supprime le groupe de disques, puis le recrée sous un nouveau format qui prend en charge la déduplication et la compression.

Dans certains environnements, votre cluster vSAN peut ne pas avoir les ressources nécessaires pour procéder à l'évacuation complète du groupe de disques. Les exemples de tels déploiements incluent un cluster à trois nœuds sans ressources afin d'évacuer le réplica ou le témoin tout en maintenant une protection totale. Ou encore un cluster à quatre nœuds avec des objets RAID-5 déjà déployés. Dans ce dernier cas, vous n'avez pas la place de déplacer une partie de la bande RAID-5, étant donné que les objets RAID-5 nécessitent un minimum de quatre nœuds.

Vous pouvez également activer la déduplication et la compression et utiliser l'option Autoriser la redondance réduite. Cette option maintient les machines virtuelles en cours d'exécution, mais il est possible qu'elles ne puissent pas tolérer le nombre total d'échecs défini dans la stratégie de stockage de machine virtuelle. Ainsi, de manière temporaire au cours de la modification du format pour la déduplication et la compression, des pertes de données risquent de se produire sur vos machines virtuelles. vSAN restaure la conformité totale et la redondance une fois la conversion du format terminée.

Ajout ou suppression de disques lorsque la déduplication et la compression sont activées

Lors de l'ajout de disques à un cluster vSAN sur lequel la déduplication et la compression sont activées, des considérations spécifiques s'appliquent.

- Vous pouvez ajouter un disque de capacité à un groupe de disques pour lequel la déduplication et la compression sont activées. Toutefois, pour une déduplication et une compression plus efficaces, créez un nouveau groupe de disques pour augmenter la capacité de stockage du cluster (plutôt que d'ajouter des disques de capacité).
- Lorsque vous supprimez un disque d'un niveau de cache, l'intégralité du groupe de disques est supprimée. Supprimer un disque au niveau du cache lorsque la déduplication et la compression sont activées déclenche l'évacuation des données.
- La déduplication et la compression sont mises en œuvre au niveau du groupe de disques. Il est impossible de supprimer un disque de capacité du cluster lorsque la déduplication et la compression sont activées. Vous devez supprimer l'intégralité du groupe de disques.
- Si un disque de capacité échoue, l'intégralité du groupe de disques devient indisponible. Pour résoudre ce problème, identifiez et remplacez immédiatement le composant défaillant. Utilisez l'option Aucune migration de données lors de la suppression du groupe de disques défaillant.

Utiliser le codage d'effacement RAID 5 ou RAID 6

Vous pouvez utiliser le codage d'effacement RAID 5 ou RAID 6 pour protéger le système contre la perte de données et pour augmenter l'efficacité de stockage. Le codage d'effacement peut offrir le même niveau de protection des données que la mise en miroir (RAID 1) tout en utilisant moins de capacité de stockage.

Le codage d'effacement RAID 5 ou RAID 6 permet à vSAN de tolérer la panne de maximum deux périphériques de capacité dans la banque de données. Vous pouvez configurer RAID 5 sur des clusters intégralement Flash incluant quatre domaines de pannes ou plus. Vous pouvez configurer RAID 5 ou RAID 6 sur des clusters intégralement Flash incluant six domaines de pannes ou plus.

Le codage d'effacement RAID 5 ou RAID 6 nécessite moins de capacité de stockage supplémentaire pour protéger vos données que la mise en miroir RAID 1. Par exemple, une machine virtuelle protégée par un paramètre **Pannes tolérées** de 1 avec RAID 1 nécessite deux fois la taille de disque virtuel, tandis qu'avec RAID 5 elle nécessite 1,33 fois la taille de disque virtuel. Le tableau suivant présente une comparaison générale entre RAID 1 et RAID 5 ou RAID 6.

Tableau 6-1. Capacité requise pour stocker et protéger les données à différents niveaux RAID

Configuration RAID	Pannes tolérées	Taille des données	Capacité requise
RAID 1 (mise en miroir)	1	100 Go	200 Go
RAID 5 ou RAID 6 (codage d'effacement) avec quatre domaines de pannes	1	100 Go	133 Go
RAID 1 (mise en miroir)	2	100 Go	300 Go
RAID 5 ou RAID 6 (codage d'effacement) avec six domaines de pannes	2	100 Go	150 Go

Le codage d'effacement RAID 5 ou RAID 6 est un attribut de stratégie que vous pouvez appliquer aux composants de machines virtuelles. Pour utiliser RAID 5, définissez **Méthode de tolérance de panne** sur **RAID-5/6 (codage d'effacement)** et **Pannes tolérées** sur 1. Pour utiliser RAID 6, définissez **Méthode de tolérance de panne** sur **RAID-5/6 (codage d'effacement)** et **Pannes tolérées** sur 2. Le codage d'effacement RAID 5 ou RAID 6 ne prend pas en charge un paramètre **Pannes tolérées** de 3.

Pour utiliser RAID 1, définissez **Méthode de tolérance de panne** sur **RAID-1 (Mise en miroir)**. La mise en miroir RAID 1 nécessite moins d'opérations d'E/S sur les périphériques de stockage et peut donc offrir de meilleures performances. Par exemple, une resynchronisation de cluster est plus rapide avec RAID 1.

Note Dans un cluster étendu vSAN, la **Méthode de tolérance de panne RAID-5/6 (codage d'effacement)** s'applique uniquement au paramètre **Tolérance aux pannes du site**.

Note Pour un cluster vSAN Express Storage Architecture, selon le nombre de domaines de pannes que vous utilisez, le nombre de composants répertoriés sous **RAID 5** (**Surveiller** > **vSAN** > **Objets virtuels** > testVM > **Afficher les détails du placement**) varie. Si six domaines de pannes ou plus sont disponibles dans le cluster, cinq composants seront répertoriés sous **RAID 5**. Si cinq domaines de pannes ou moins sont disponibles, trois composants seront répertoriés.

Pour plus d'informations sur la configuration de stratégies, reportez-vous à la section Chapitre 3 L'utilisation de stratégies vSAN.

Éléments à prendre en compte pour la conception de RAID 5 ou RAID 6

Tenez compte de ces directives lorsque vous configurez le codage d'effacement RAID 5 ou RAID 6 dans un cluster vSAN.

- Le codage d'effacement RAID 5 ou RAID 6 est disponible uniquement sur les groupes de disques intégralement Flash.
- Le format sur disque version 3.0 ou version ultérieure est requis pour prendre en charge RAID 5 ou RAID 6.
- Vous devez avoir une licence valide pour activer RAID 5/6 sur un cluster.
- Vous pouvez réaliser des économies d'espace supplémentaires en activant la déduplication et la compression sur le cluster vSAN.

Utilisation du chiffrement dans un cluster vSAN 7

Vous pouvez chiffrer les données en transit dans votre cluster vSAN et chiffrer les données au repos dans votre banque de données vSAN.

vSAN peut chiffrer les données en transit à travers les hôtes du cluster vSAN. Le chiffrement des données en transit protège les données au fur et à mesure qu'elles se déplacent dans le cluster vSAN.

vSAN peut chiffrer des données au repos dans votre banque de données vSAN. Le chiffrement des données au repos protège les données sur les périphériques de stockage en cas de suppression de l'un d'entre eux du cluster.

Ce chapitre contient les rubriques suivantes :

Chiffrement des données vSAN en transit

vSAN peut chiffrer les données en transit lorsqu'elles se déplacent à travers les hôtes de votre cluster vSAN.

vSAN peut chiffrer les données en transit à travers les hôtes du cluster. Lorsque vous activez le chiffrement des données en transit, vSAN chiffre l'ensemble du trafic de données et de métadonnées entre les hôtes.

Le chiffrement des données vSAN en transit présente les caractéristiques suivantes :

- vSAN utilise le chiffrement AES-256 bits sur les données en transit.
- Le chiffrement des données en transit de vSAN n'est pas lié au chiffrement des données au repos. Vous pouvez activer ou désactiver chacun d'eux séparément.
- La confidentialité persistante est appliquée pour le chiffrement des données vSAN en transit.
- Le trafic entre les hôtes de données et les hôtes témoins est chiffré.
- Le trafic de données du service de fichiers entre le proxy VDFS et le serveur VDFS est chiffré.
- Les connexions entre les hôtes de services de fichiers vSAN sont chiffrées.

vSAN utilise des clés symétriques générées dynamiquement et partagées entre les hôtes. Les hôtes génèrent dynamiquement une clé de chiffrement lorsqu'ils établissent une connexion et qu'ils utilisent la clé pour chiffrer tout le trafic entre les hôtes. Vous n'avez pas besoin d'un serveur de gestion des clés pour effectuer un chiffrement des données en transit.

Chaque hôte est authentifié lorsqu'il rejoint le cluster, garantissant ainsi que les connexions uniquement aux hôtes approuvés soient autorisées. La suppression d'un hôte du cluster entraîne celle de son certificat d'authentification.

Le chiffrement des données vSAN en transit est un paramètre à l'échelle du cluster. Lorsque vous l'activez, l'ensemble du trafic de données et de métadonnées est chiffré lors de son transit à travers les hôtes.

Activer le chiffrement des données en transit sur un cluster vSAN

Vous pouvez activer le chiffrement des données en transit en modifiant les paramètres de configuration d'un cluster vSAN.

Procédure

1. Accédez à un cluster existant.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, sélectionnez **Services** et cliquez sur le bouton **Modifier** pour le chiffrement des données en transit.
4. Cliquez pour activer **Chiffrement des données en transit**, puis sélectionnez un intervalle de renouvellement de clés.
5. Cliquez sur **Appliquer**.

Résultats

Le chiffrement des données en transit est activé sur le cluster vSAN. vSAN chiffre toutes les données circulant entre les hôtes et les connexions entre hôtes de service de fichiers du cluster.

Chiffrement des données vSAN au repos

vSAN peut chiffrer des données au repos dans votre banque de données vSAN.

vSAN peut effectuer un chiffrement des données stockées. Les données sont chiffrées une fois que tous les autres traitements, tels que la déduplication, ont été effectués. Le chiffrement des données au repos protège les données sur les périphériques de stockage au cas où l'un d'entre eux serait supprimé du cluster.

L'utilisation du chiffrement sur votre banque de données vSAN nécessite un minimum de préparation. Après la configuration de votre environnement, vous pouvez activer le chiffrement des données au repos sur votre cluster vSAN.

Le chiffrement des données au repos nécessite un serveur de gestion des clés (KMS) externe ou une instance de vSphere Native Key Provider. Pour plus d'informations sur le chiffrement vSphere, reportez-vous à *Sécurité vSphere*.

Vous pouvez utiliser un serveur de gestion des clés (KMS) externe, le système vCenter Server et vos hôtes ESXi pour chiffrer les données dans votre cluster vSAN. vCenter Server demande des clés de chiffrement auprès d'un KMS externe. Le KMS génère et stocke les clés, et vCenter Server obtient les ID de clés du KMS et les distribue aux hôtes ESXi.

vCenter Server ne stocke pas les clés KMS mais conserve une liste des ID de clé.

Fonctionnement du chiffrement des données au repos

Lorsque vous activez le chiffrement des données au repos, vSAN chiffre tout le contenu de la banque de données vSAN. Tous les fichiers sont chiffrés, de telle sorte que toutes les machines virtuelles et leurs données correspondantes sont protégées. Seuls les administrateurs disposant de privilèges de chiffrement peuvent effectuer des tâches de chiffrement et de déchiffrement.

vSAN utilise des clés de chiffrement comme suit :

- vCenter Server demande une clé de chiffrement (KEK) AES-256 à partir du serveur KMS. vCenter Server stocke uniquement l'ID de la clé KEK, mais pas la clé proprement dite.
- L'hôte ESXi chiffre les données du disque en utilisant le mode standard AES-256 XTS. Chaque disque possède une clé DEK (Data Encryption Key) différente générée de façon aléatoire.
- Chaque hôte ESXi utilise la clé pour chiffrer ses clés DEK et stocke les clés DEK chiffrées sur disque. L'hôte ne stocke pas la clé KEK sur disque. Si un hôte redémarre, il demande la clé KEK avec l'ID correspondant au serveur KMS. L'hôte déchiffre ensuite ses clés DEK si nécessaire.
- Une clé d'hôte est utilisée pour chiffrer les vidages de mémoire, pas les données. Tous les hôtes d'un même cluster utilisent la même clé d'hôte. Lors de la collecte de bundles de support, une clé aléatoire est générée pour rechiffrer les vidages de mémoire. Vous pouvez spécifier un mot de passe pour chiffrer la clé aléatoire.

Lorsqu'un hôte redémarre, il ne monte pas ses groupes de disques tant qu'il n'a pas reçu la clé KEK. Ce processus peut durer plusieurs minutes, voire davantage. Vous pouvez surveiller l'état des groupes de disques dans vSAN Health Service, sous **Disques physiques > Santé de l'état du logiciel**.

Persistance de la clé de chiffrement

Dans vSAN 7.0 Update 3 et versions ultérieures, le chiffrement des données au repos peut continuer à fonctionner même lorsque le serveur de clés est temporairement hors ligne ou inaccessible. Lorsque la persistance des clés est activée, les hôtes ESXi peuvent conserver les clés de chiffrement, même après un redémarrage.

Chaque hôte ESXi obtient initialement les clés de chiffrement et les conserve dans son cache de clés. Si l'hôte ESXi dispose d'un module TPM (Trusted Platform Module, module de plate-forme sécurisée), les clés de chiffrement sont persistantes sur le module TPM lors des redémarrages. L'hôte n'a pas besoin de demander des clés de chiffrement. Les opérations de chiffrement peuvent se poursuivre lorsque le serveur de clés n'est pas disponible, car les clés sont persistantes dans le TPM.

Utilisez les commandes suivantes pour activer la persistance de clé sur un hôte de cluster.

```
esxcli system settings encryption set --mode=TPM
```

```
esxcli system security keypersistence enable
```

Pour plus d'informations sur la persistance des clés de chiffrement, reportez-vous à la section « Présentation de la persistance des clés » dans *Sécurité vSphere*.

Utilisation de vSphere Native Key Provider

vSAN 7.0 Update 2 prend en charge vSphere Native Key Provider. Si votre environnement est configuré pour vSphere Native Key Provider, vous pouvez l'utiliser pour chiffrer les machines virtuelles dans votre cluster vSAN. Pour plus d'informations, reportez-vous à la section « Configuration et gestion de vSphere Native Key Provider » dans *Sécurité vSphere*.

vSphere Native Key Provider ne nécessite aucun serveur de gestion de clés (KMS) externe. vCenter Server génère la clé de chiffrement des clés et la transfère vers les hôtes ESXi. Les hôtes ESXi peuvent générer ensuite des clés de chiffrement de données.

vSphere Native Key Provider peut coexister avec une infrastructure de serveur de clés existante.

Éléments à prendre en compte pour la conception du chiffrement des données au repos

Tenez compte de ces directives lors de l'utilisation d'un chiffrement des données au repos.

- Ne déployez pas votre serveur KMS sur la banque de données vSAN que vous prévoyez de chiffrer.
- Le chiffrement nécessite une utilisation importante du CPU. AES-NI améliore de manière significative les performances du chiffrement. Activez AES-NI dans votre BIOS.
- L'hôte témoin dans un cluster étendu ne participe pas au chiffrement vSAN. L'hôte témoin ne stocke pas les données client, uniquement les métadonnées, telles que la taille et l'UUID de l'objet et des composants vSAN.

  Note Si l'hôte témoin est un dispositif exécuté sur un autre cluster, vous pouvez chiffrer les métadonnées qui y sont stockées. Activez le chiffrement des données au repos sur le cluster qui contient l'hôte témoin.

- Établissez une stratégie concernant les vidages de mémoire. Les vidages de noyau sont chiffrés, car ils peuvent contenir des informations sensibles. Si vous déchiffrez un vidage de mémoire, traitez avec précaution ses informations sensibles. Les vidages de mémoire ESXi peuvent contenir des clés pour l'hôte ESXi et pour les données qui s'y trouvent.
  - Utilisez toujours un mot de passe lorsque vous collectez un bundle `vm-support`. Vous pouvez spécifier le mot de passe lorsque vous générez le bundle de support à partir de vSphere Client ou à l'aide de la commande `vm-support`.

    Le mot de passe rechiffre les vidages de mémoire utilisant des clés internes de façon à utiliser les clés reposant sur le mot de passe. Vous pouvez utiliser ultérieurement le mot de passe pour déchiffrer les vidages de mémoire chiffrés susceptibles d'être intégrés dans le bundle de support. Les vidages de mémoire ou les journaux non chiffrés ne sont pas concernés.
  - Le mot de passe que vous spécifiez pendant la création du bundle `vm-support` n'est pas conservé dans les composants vSphere. Vous êtes responsable du suivi des mots de passe pour les bundles de support.

Configurer le fournisseur de clés standard

Utilisez un fournisseur de clés standard pour distribuer les clés qui chiffrent la banque de données vSAN.

Avant de chiffrer la banque de données vSAN, vous devez configurer un fournisseur de clés standard afin qu'il prenne en charge le chiffrement. Cette opération implique d'ajouter le KMS à vCenter Serveret d'établir une relation de confiance avec celui-ci. vCenter Server provisionne les clés de chiffrement depuis le fournisseur de clés.

Le serveur KMS doit prendre en charge la norme KMIP (Key Management Interoperability Protocol) 1.1. Pour plus d'informations, reportez-vous aux *Matrices de compatibilité vSphere*.

Ajouter un serveur KMS à vCenter Server

Vous ajoutez un serveur de gestion des clés (KMS) à votre système vCenter Server à partir de vSphere Client.

vCenter Server crée un fournisseur de clés standard lorsque vous ajoutez la première instance du serveur KMS. Si vous configurez le fournisseur de clés sur au moins deux instances de vCenter Server, veillez à utiliser le même nom de fournisseur de clés.

Note Ne déployez pas vos serveurs KMS sur le cluster vSAN que vous prévoyez de chiffrer. Si une panne se produit, les hôtes dans le cluster vSAN doivent communiquer avec le serveur KMS.

- Lorsque vous ajoutez le serveur KMS, vous êtes invité à définir par défaut ce fournisseur de clés. Vous pouvez ensuite modifier le paramètre par défaut.

- Une fois que vCenter Server crée le premier fournisseur de clés, vous pouvez ajouter des instances du serveur KMS du même fournisseur au fournisseur de clés et configurer toutes les instances du serveur KMS pour synchroniser les clés entre elles. Utilisez la méthode documentée par votre fournisseur de serveur KMS.
- Vous ne pouvez configurer le fournisseur de clés qu'avec une seule instance du serveur KMS.
- Si votre environnement prend en charge des solutions du serveur KMS de différents fournisseurs, vous pouvez ajouter plusieurs fournisseurs de clés.

Conditions préalables

- Vérifiez que le serveur de gestion de clés se trouve dans *Matrices de compatibilité vSphere* et est conforme à KMIP 1.1.
- Vérifiez que vous avez les privilèges requis : **Cryptographer.ManageKeyServers**
- La connexion à un serveur de gestion des clés à l'aide d'une adresse IPv6 uniquement n'est pas prise en charge.
- La connexion à un serveur KMS au moyen d'un serveur proxy qui nécessite un nom d'utilisateur ou un mot de passe n'est pas prise en charge.

Procédure

1. Connectez-vous à vCenter Server.
2. Parcourez la liste d'inventaire et sélectionnez l'instance de vCenter Server.
3. Cliquez sur **Configurer** et, sous Sécurité, cliquez sur **Fournisseurs de clés**.
4. Cliquez sur **Ajouter un fournisseur de clés standard**, entrez les informations du fournisseur de clés, puis cliquez sur **Ajouter un fournisseur de clés**.

   Vous pouvez cliquer sur **Ajouter un KMS** pour ajouter d'autres serveurs de gestion de clés.
5. Cliquez sur **Approuver**.

   vCenter Server ajoute le fournisseur de clés et affiche l'état Connecté.

Établissement d'une connexion approuvée de fournisseur de clés standard en échangeant des certificats

Après avoir ajouté le fournisseur de clés standard au système vCenter Server, vous pouvez établir une connexion approuvée. Le processus exact dépend des certificats acceptés par le fournisseur de clés, et de la stratégie de votre entreprise.

Conditions préalables

Ajoutez le fournisseur de clés standard.

Procédure

1. Accédez à l'instance de vCenter Server.
2. Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.

3 Sélectionnez le fournisseur de clés.

Le serveur KMS du fournisseur de clés s'affiche.

4 Sélectionnez le KMS.

5 Dans le menu déroulant **Établir une approbation**, sélectionnez **Établir une relation de confiance entre le KMS et l'instance de vCenter**.

6 Sélectionnez l'option correspondant à votre serveur et suivez la procédure.

Option	Reportez-vous au
Certificat d'autorité de certification racine vCenter Server	Utiliser l'option Certificat d'autorité de certification racine pour établir une connexion de confiance avec le fournisseur de clés standard.
Certificat vCenter Server	Utiliser l'option de certificat pour établir une connexion de confiance avec le fournisseur de clés standard.
Télécharger le certificat et la clé privée	Utiliser l'option Télécharger le certificat et la clé privée pour établir une connexion de confiance avec le fournisseur de clés standard.
Demande de signature du nouveau certificat	Utiliser l'option Nouvelle demande de signature de certificat pour établir une connexion de confiance avec un fournisseur de clés standard.

Utiliser l'option Certificat d'autorité de certification racine pour établir une connexion de confiance avec le fournisseur de clés standard

Certains fournisseurs de serveurs de gestion de clés (KMS) imposent le téléchargement du certificat d'autorité de certification racine sur le serveur KMS. Tous les certificats qui sont signés par votre autorité de certification racine sont alors approuvés par ce KMS.

Le certificat d'autorité de certification racine que le chiffrement de machines virtuelles vSphere utilise est un certificat autosigné qui est stocké dans un magasin distinct du VECS (VMware Endpoint Certificate Store) sur le système vCenter Server.

Note Générez un certificat d'autorité de certification uniquement si vous souhaitez remplacer des certificats existants. Si vous le faites en effet, les autres certificats signés par cette autorité de certification racine deviennent non valides. Vous pouvez générer un nouveau certificat d'autorité de certification racine dans le cadre de ce workflow.

Procédure

1 Accédez à l'instance de vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.

3 Sélectionnez le fournisseur de clés auquel vous souhaitez établir une connexion approuvée.

Le serveur KMS du fournisseur de clés s'affiche.

4 Dans le menu déroulant **Établir une approbation**, sélectionnez **Établir une relation de confiance entre le KMS et l'instance de vCenter**.

5 Sélectionnez **Certificat d'autorité de certification racine vCenter** et cliquez sur **Suivant**.

La boîte de dialogue Télécharger un certificat d'autorité de certification est renseignée avec le certificat racine utilisé par vCenter Server pour le chiffrement. Ce certificat est stocké dans VECS.

6 Copiez le certificat dans le presse-papiers ou téléchargez-le comme un fichier.

7 Suivez les instructions de votre fournisseur de KMS pour télécharger le certificat sur son système.

Note Certains fournisseurs de KMS exigent que le fournisseur de KMS redémarre le KMS pour détecter le certificat racine que vous téléchargez.

Étape suivante

Finalisez l'échange de certificat. Reportez-vous à la section Terminer la configuration de l'approbation pour un fournisseur de clés standard.

Utiliser l'option de certificat pour établir une connexion de confiance avec le fournisseur de clés standard

Certains fournisseurs de serveurs de gestion de clés (KMS) imposent le téléchargement du certificat de vCenter Server sur le serveur KMS. Une fois le téléchargement effectué, le KMS accepte le trafic provenant d'un système avec ce certificat.

vCenter Server génère un certificat pour protéger les connexions avec le KMS. Le certificat est stocké dans un magasin de clés distinct dans VECS (VMware Endpoint Certificate Store) sur le système vCenter Server.

Procédure

1 Accédez à l'instance de vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.

3 Sélectionnez le fournisseur de clés auquel vous souhaitez établir une connexion approuvée.

Le serveur KMS du fournisseur de clés s'affiche.

4 Dans le menu déroulant **Établir une approbation**, sélectionnez **Établir une relation de confiance entre le KMS et l'instance de vCenter**.

5 Sélectionnez **Certificat vCenter** et cliquez sur **Suivant**.

La boîte de dialogue Télécharger le certificat est renseignée avec le certificat racine utilisé par vCenter Server pour le chiffrement. Ce certificat est stocké dans VECS.

Note Ne générez pas de nouveau certificat sauf si vous souhaitez remplacer des certificats existants.

6 Copiez le certificat dans le presse-papier ou téléchargez-le comme un fichier.

7 Suivez les instructions de votre fournisseur de KMS pour mettre à jour le certificat sur le KMS.

Étape suivante

Finalisez la relation de confiance. Reportez-vous à la section Terminer la configuration de l'approbation pour un fournisseur de clés standard.

Utiliser l'option Nouvelle demande de signature de certificat pour établir une connexion de confiance avec un fournisseur de clés standard

Certains fournisseurs de serveur de gestion de clés (KMS) exigent que vCenter Server génère une demande de signature de certificat (CSR) et envoie cette demande CSR au KMS. Le KMS signe le CSR et renvoie le certificat signé. Vous pouvez télécharger le certificat signé sur vCenter Server.

L'utilisation de l'option **Demande de signature du nouveau certificat** se fait en deux étapes. Dans un premier temps, vous générez le CSR et vous l'envoyez au fournisseur de KMS. Vous téléchargez ensuite le certificat signé que vous avez reçu du fournisseur de KMS sur vCenter Server.

Procédure

1. Accédez à l'instance de vCenter Server.
2. Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.
3. Sélectionnez le fournisseur de clés auquel vous souhaitez établir une connexion approuvée.

   Le serveur KMS du fournisseur de clés s'affiche.
4. Dans le menu déroulant **Établir une approbation**, sélectionnez **Établir une relation de confiance entre le KMS et l'instance de vCenter**.
5. Sélectionnez **Nouvelle demande de signature de certificat (CSR)**, puis cliquez sur **Suivant**.
6. Dans la boîte de dialogue, copiez dans le Presse-papiers le certificat complet contenu dans la zone de texte ou téléchargez-le sous la forme d'un fichier.

   Utilisez le bouton **Générer un nouveau CSR** dans la zone de dialogue uniquement si vous souhaitez générer explicitement un CSR.
7. Suivez les instructions fournies par votre fournisseur de KMS pour envoyer le CSR.
8. Lorsque vous recevez le certificat signé du fournisseur de KMS, cliquez de nouveau sur **Fournisseurs de clés**, sélectionnez le fournisseur de clés et, dans le menu déroulant **Établir une relation de confiance**, sélectionnez **Télécharger le certificat CSR signé**.
9. Collez le certificat signé dans la zone de texte du bas ou cliquez sur **Télécharger le fichier** et télécharger le fichier, puis cliquez sur **Télécharger**.

Étape suivante

Finalisez la relation de confiance. Reportez-vous à Terminer la configuration de l'approbation pour un fournisseur de clés standard.

Utiliser l'option Télécharger le certificat et la clé privée pour établir une connexion de confiance avec le fournisseur de clés standard

Certains fournisseurs de serveur de gestion de clés (KMS) exigent que vous téléchargiez le certificat et la clé privée du serveur KMS sur le système vCenter Server.

Certains fournisseurs de KMS génèrent un certificat et une clé privée pour la connexion et les mettent à votre disposition. Après le téléchargement des fichiers, le KMS approuve votre instance de vCenter Server.

Conditions préalables

- Demandez un certificat et une clé privée au fournisseur de KMS. Les fichiers sont des fichiers X509 au format PEM.

Procédure

1. Accédez à l'instance de vCenter Server.
2. Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.
3. Sélectionnez le fournisseur de clés auquel vous souhaitez établir une connexion approuvée.

   Le serveur KMS du fournisseur de clés s'affiche.
4. Dans le menu déroulant **Établir une approbation**, sélectionnez **Établir une relation de confiance entre le KMS et l'instance de vCenter**.
5. Sélectionnez **Certificat KMS et clé privée** et cliquez sur **Suivant**.
6. Collez le certificat que vous avez reçu du fournisseur KMS dans la zone de texte supérieure ou cliquez sur **Télécharger un fichier** pour télécharger le fichier de certificat.
7. Collez le fichier de clé dans la zone de texte supérieure ou cliquez sur **Télécharger un fichier** pour télécharger le fichier de clé.
8. Cliquez sur **établir la confiance**.

Étape suivante

Finalisez la relation de confiance. Reportez-vous à la section Terminer la configuration de l'approbation pour un fournisseur de clés standard.

Définir le fournisseur de clés par défaut à l'aide de vSphere Client

Vous devez définir le fournisseur de clés par défaut si vous ne configurez pas le premier cluster comme fournisseur de clés par défaut, ou si votre environnement utilise plusieurs fournisseurs de clés et que vous supprimez le fournisseur par défaut. Vous pouvez utiliser vSphere Client pour définir le fournisseur de clés par défaut au niveau de vCenter Server.

Conditions préalables

Nous vous recommandons de vérifier que l'état de la connexion dans l'onglet Fournisseurs de clés indique Actif et présente une coche verte.

Procédure

1. Connectez-vous à l'aide de vSphere Client.
2. Accédez à l'instance de vCenter Server.

3 Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.

4 Sélectionnez le fournisseur de clés.

5 Cliquez sur **Définir comme valeur par défaut**.

Une boîte de dialogue de confirmation apparaît.

6 Cliquez sur **Définir comme valeur par défaut**.

Le fournisseur de clés s'affiche en tant que valeur par défaut actuelle.

Terminer la configuration de l'approbation pour un fournisseur de clés standard

À moins que la boîte de dialogue **Ajouter un serveur de clés standard** ne vous ait invité à approuver le KMS, vous devez explicitement établir la confiance une fois l'échange de certificats terminé.

Vous pouvez terminer la configuration de la confiance, c'est-à-dire indiquer à vCenter Server de faire confiance au certificat KMS, soit en faisant confiance au KMS, soit en téléchargeant un certificat KMS. Deux options s'offrent à vous :

- Faire explicitement confiance au certificat en utilisant l'option **Télécharger un certificat KMS**.
- Télécharger un certificat KMS feuille ou le certificat KMS de l'autorité de certification sur vCenter Server à l'aide de l'option **Établir une relation de confiance entre l'instance de vCenter et le KMS**.

Note Si vous téléchargez le certificat de l'autorité de certification racine ou le certificat de l'autorité de certification intermédiaire, vCenter Server fait confiance à tous les certificats signés par cette autorité de certification. Pour une sécurité renforcée, téléchargez un certificat feuille ou un certificat d'autorité de certification intermédiaire contrôlé par le fournisseur KMS.

Procédure

1 Accédez à l'instance de vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.

3 Sélectionnez le fournisseur de clés auquel vous souhaitez établir une connexion approuvée.

Le serveur KMS du fournisseur de clés s'affiche.

4 Sélectionnez le KMS.

5 Sélectionnez une des options suivantes à partir du menu déroulant **Établir une relation de confiance**.

Option	Action
Établir une relation de confiance entre l'instance de vCenter et le KMS	Dans la boîte de dialogue qui apparaît, cliquez sur **Faire confiance**.
Télécharger un certificat KMS	a Dans la boîte de dialogue qui s'affiche, collez le certificat ou cliquez sur **Télécharger un fichier** et accédez au fichier de certificat. b Cliquez sur **Télécharger**.

Activer le chiffrement des données au repos sur un nouveau cluster vSAN

Vous pouvez activer le chiffrement des données au repos lorsque vous configurez un nouveau cluster vSAN.

Conditions préalables

Note Si vous utilisez un cluster vSAN Express Storage Architecture, vous ne pouvez pas activer le chiffrement des données au repos dans vSphere 8.0.

- Privilèges requis :
  - **Host.Inventory.EditCluster**
  - **Cryptographer.ManageEncryptionPolicy**
  - **Cryptographer.ManageKMS**
  - **Cryptographer.ManageKeys**
- Vous devez avoir configuré un fournisseur de clés standard et établi une connexion approuvée entre vCenter Server et le serveur KMS.

Procédure

1 Accédez à un cluster existant.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, sélectionnez **Services** et cliquez sur le bouton **Modifier** pour le chiffrement.

4 Dans la boîte de dialogue **Services vSAN**, activez l'option **Chiffrement**, puis sélectionnez un cluster KMS ou un fournisseur de clés.

Note Utilisez la case à cocher **Effacer les données résiduelles** pour effacer les données résiduelles des périphériques avant d'activer le chiffrement vSAN. Assurez-vous de décocher cette case, sauf si vous souhaitez effacer les données existantes des périphériques de stockage lors du chiffrement d'un cluster qui contient des données de machine virtuelle. Cela permet de garantir que les données non chiffrées ne résident plus sur les périphériques après l'activation du chiffrement vSAN. Ce paramètre n'est pas nécessaire pour les nouvelles installations qui n'ont pas de données de machine virtuelle sur les périphériques de stockage.

5 Terminez la configuration de votre cluster.

Résultats

Le chiffrement des données stockées est activé sur le cluster vSAN. vSAN chiffre toutes les données ajoutées à la banque de données vSAN.

Générer de nouvelles clés de clé de chiffrement des données au repos

Vous pouvez générer de nouvelles clés de chiffrement pour les données au repos si une clé expire ou devient compromise.

Les options suivantes sont disponibles lorsque vous générez de nouvelles clés de chiffrement pour votre cluster vSAN.

- Si vous générez une nouvelle clé KEK, tous les hôtes dans le cluster vSAN reçoivent la nouvelle clé KEK du serveur KMS. La clé DEK de chaque hôte est rechiffrée avec la nouvelle clé KEK.
- Si vous choisissez de rechiffrer toutes les données en utilisant de nouvelles clés, de nouvelles clés KEK et DEK sont générées. Un reformatage de disque successif est requis pour rechiffrer les données.

Conditions préalables

- Privilèges requis :
  - **Host.Inventory.EditCluster**
  - **Cryptographer.ManageKeys**
- Vous devez avoir configuré un fournisseur de clés et établi une connexion approuvée entre vCenter Server et le serveur KMS.

Procédure

1 Accédez au cluster hôte vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, sélectionnez **Services**.

4 Cliquez sur **Générer de nouvelles clés de chiffrement**.

5 Pour générer une nouvelle clé KEK, cliquez sur **Appliquer**. Les clés DEK sont rechiffrées avec la nouvelle clé KEK.

- Pour générer une nouvelle clé KEK et plusieurs nouvelles clés DEK, et rechiffrer toutes les données dans le cluster vSAN, cochez la case suivante : **Rechiffrer également toutes les données du stockage avec de nouvelles clés**.

  Note Ce renouvellement de clés en profondeur n'est pas pris en charge dans vSphere 8.0 si vSAN Express Storage Architecture est activé dans le cluster.

  .

- Si votre cluster vSAN dispose de ressources limitées, cochez la case **Autoriser la redondance réduite**. Si vous autorisez une redondance réduite, vos données peuvent être menacées pendant une opération de reformatage du disque.

Activer le chiffrement des données au repos sur un cluster vSAN existant

Vous pouvez activer le chiffrement des données au repos en modifiant les paramètres de configuration d'un cluster vSAN existant.

Conditions préalables

- Privilèges requis :
  - **Host.Inventory.EditCluster**
  - **Cryptographer.ManageEncryptionPolicy**
  - **Cryptographer.ManageKMS**
  - **Cryptographer.ManageKeys**
- Vous devez avoir configuré un fournisseur de clés standard et établi une connexion approuvée entre vCenter Server et le serveur KMS.
- Le mode de réclamation de disques du cluster doit être défini sur manuel.

Procédure

1 Accédez au cluster hôte vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, sélectionnez **Services**.

4 Cliquez sur le bouton **Modifier** pour le chiffrement.

5 Dans la boîte de dialogue Services vSAN, activez l'option **Chiffrement**, puis sélectionnez un cluster KMS ou un fournisseur de clés.

6 (Facultatif) Si les périphériques de stockage dans le cluster contiennent des données sensibles, sélectionnez l'option **Effacer les données résiduelles**.

   Ce paramètre demande à vSAN d'effacer les données existantes des périphériques de stockage pendant leur chiffrement. Cette option peut augmenter le temps de traitement de chaque disque. Par conséquent, ne le choisissez pas sauf si vous possédez des données indésirables sur les disques.

7 Cliquez sur **Appliquer**.

Résultats

Un reformatage successif de tous les groupes de disques est effectué pendant que vSAN chiffre toutes les données dans la banque de données vSAN.

Chiffrement et vidages de mémoire vSAN

Si votre cluster vSAN utilise le chiffrement des données au repos et si une erreur se produit sur l'hôte ESXi, le vidage de mémoire qui en résulte est chiffré pour protéger les données client. Les vidages de mémoire qui sont inclus dans le module `vm-support` sont également chiffrés.

Note Les vidages de mémoire peuvent contenir des informations sensibles. Suivez la stratégie de votre organisation en matière de sécurité et de confidentialité lorsque vous gérez des vidages de mémoire.

Vidages de mémoire sur hôtes ESXi

Lorsqu'un hôte ESXi se bloque, un vidage de mémoire chiffré est généré et l'hôte redémarre. Le vidage de mémoire est chiffré avec la clé de l'hôte qui se trouve dans le cache de la clé ESXi. Ce que vous pouvez faire ensuite dépend de plusieurs facteurs.

- Dans la plupart des cas, vCenter Server récupère la clé de l'hôte à partir du KMS et tente de transmettre la clé à l'hôte ESXi après le redémarrage. Si l'opération réussit, vous pouvez générer le module `vm-support` et vous pouvez déchiffrer ou rechiffrer le vidage de mémoire.
- Si vCenter Server ne peut pas se connecter à l'hôte ESXi, vous devriez pouvoir récupérer la clé du KMS.
- Si l'hôte a utilisé une clé personnalisée et que cette clé diffère de la clé que vCenter Server transmet à l'hôte, vous ne pouvez pas manipuler le vidage de mémoire. Évitez d'utiliser des clés personnalisées.

Vidages de mémoire et modules vm-support

Lorsque vous contactez le support technique de VMware pour une erreur grave, le représentant du support vous demande généralement de générer un module `vm-support`. Le module inclut des fichiers journaux et d'autres informations, notamment les vidages de mémoire. Si les représentants du support ne parviennent pas à résoudre les problèmes en examinant les fichiers journaux et les autres informations, vous pouvez déchiffrer les vidages de mémoire afin de leur transmettre les informations pertinentes. Suivez la stratégie de votre organisation en matière de sécurité et de confidentialité pour protéger les informations sensibles comme les clés des hôtes.

Vidages de mémoire sur systèmes vCenter Server

Un vidage de mémoire sur un système vCenter Server n'est pas chiffré. vCenter Server contient déjà des informations potentiellement sensibles. Assurez-vous au minimum que le vCenter Server est protégé. Il peut également s'avérer utile de désactiver les vidages de mémoire pour le système vCenter Server. Les autres informations contenues dans les fichiers journaux peuvent aider à déterminer le problème.

Collecter un module vm-support pour un hôte ESXi dans une banque de données vSAN chiffrée

Si le chiffrement des données au repos est activé sur un cluster vSAN, tous les vidages de mémoire dans le module `vm-support` sont chiffrés. Vous pouvez collecter le module et également spécifier un mot de passe si vous prévoyez de déchiffrer le vidage de mémoire à une date ultérieure.

Le module `vm-support` inclut des fichiers journaux, des fichiers de vidage de mémoire, etc.

Conditions préalables

Informez votre représentant de l'assistance technique que le chiffrement des données au repos est activé pour la banque de données vSAN. Votre représentant de l'assistance technique vous demandera éventuellement de déchiffrer les vidages de mémoire pour extraire les informations appropriées.

Note Les vidages de mémoire peuvent contenir des informations sensibles. Suivez la stratégie de votre organisation en matière de sécurité et de confidentialité pour protéger les informations sensibles comme les clés des hôtes.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Cliquez sur **Hôtes et clusters**, puis cliquez avec le bouton droit de la souris sur l'hôte ESXi.
3. Sélectionnez l'option **Exporter les journaux système**.
4. Dans la boîte de dialogue, sélectionnez l'option **Mot de passe pour les vidages de mémoire chiffrés**, puis indiquez un mot de passe et confirmez-le.

5 Pour les autres options, conservez les paramètres par défaut ou effectuez des modifications si l'assistance technique VMware vous y invite, puis cliquez sur **Terminer**.

6 Indiquez l'emplacement du fichier.

7 Si votre représentant de l'assistance technique vous a demandé de déchiffrer le vidage de mémoire dans le module `vm-support`, connectez-vous à n'importe quel hôte ESXi et procédez comme suit.

   a Connectez-vous à l'hôte ESXi, puis au répertoire dans lequel se trouve le module `vm-support`.

   Le nom de fichier est de type **`esx.date_and_time.tgz`**.

   b Assurez-vous que le répertoire dispose de suffisamment d'espace pour le module, le module décompressé et le module recompressé, ou déplacez le module.

   c Procédez à l'extraction du module dans le répertoire local.

```
vm-support -x *.tgz .
```

   La hiérarchie de fichiers qui en résulte peut contenir des fichiers de vidage de mémoire pour l'hôte ESXi, en général dans `/var/core`. Elle peut contenir plusieurs fichiers de vidage de mémoire pour des machines virtuelles.

   d Déchiffrez individuellement chaque fichier de vidage de mémoire chiffré.

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

   vm-support-incident-key-file est le fichier de clé d'incident se trouvant au niveau supérieur du répertoire.

   encryptedZdump est le nom du fichier de vidage de mémoire chiffré.

   decryptedZdump est le nom du fichier généré par la commande. Choisissez un nom semblable à celui du fichier *encryptedZdump*.

   e Fournissez le mot de passe que vous avez spécifié lors de la création du module `vm-support`.

   f Supprimez les vidages de mémoire chiffrés et compressez à nouveau le module.

```
vm-support --reconstruct
```

8 Supprimez tout fichier contenant des informations confidentielles.

Déchiffrer ou chiffrer à nouveau un vidage de mémoire chiffré

Vous pouvez déchiffrer ou chiffrer à nouveau un vidage de mémoire chiffré sur votre hôte ESXi à l'aide de l'interface de ligne de commande `crypto-util`.

Vous pouvez vous-même déchiffrer et examiner les vidages de mémoire dans le module `vm-support`. Les vidages de mémoire peuvent contenir des informations sensibles. Suivez la stratégie de votre organisation en matière de sécurité et de confidentialité pour protéger les informations sensibles comme les clés des hôtes.

Pour plus de détails sur le rechiffrement d'un vidage de mémoire et sur d'autres fonctionnalités de `crypto-util`, consultez l'aide de la ligne de commande.

Note `crypto-util` est destinée à des utilisateurs expérimentés.

Conditions préalables

La clé d'hôte ESXi ayant servi à chiffrer le vidage de mémoire doit être disponible sur l'hôte ESXi qui a généré le vidage de mémoire.

Procédure

1 Connectez-vous directement à l'hôte ESXi sur lequel le vidage de mémoire s'est produit.

Si l'hôte ESXi est en mode de verrouillage ou si l'accès SSH n'est pas activée, vous devrez peut-être commencer par activer l'accès.

2 Déterminez si le vidage de mémoire est chiffré.

Option	Description
Surveiller le vidage de mémoire	`crypto-util envelope describe vmmcores.ve`
fichier zdump	`crypto-util envelope describe --offset 4096 zdumpFile`

3 Déchiffrez le vidage de mémoire, selon son type.

Option	Description
Surveiller le vidage de mémoire	`crypto-util envelope extract vmmcores.ve vmmcores`
fichier zdump	`crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted`

Mise à niveau du Cluster vSAN

8

La mise à niveau de vSAN s'effectue en plusieurs étapes au cours desquelles vous devez exécuter les procédures dans l'ordre décrit dans ce chapitre.

Note Vous ne pouvez pas mettre à niveau un cluster vSAN Original Storage Architecture vers un cluster vSAN Express Storage Architecture à l'aide de vSphere Client ou de Ruby vSphere Console (RVC).

Avant de faire une tentative de mise à niveau, assurez-vous de comprendre le processus connexe complet pour être sûr d'effectuer cette tâche sans problème et sans interruption. Si vous n'êtes pas familiarisé avec la procédure de mise à niveau de vSphere, reportez-vous d'abord à la documentation *Mise à niveau vSphere*.

Note En cas de non-respect de la séquence des tâches de mise à niveau décrite ici, vous risquez de perdre des données et de provoquer la panne du cluster.

La mise à niveau du cluster vSAN s'effectue selon la séquence de tâches suivante.

1. Mettez à niveau vCenter Server. Reportez-vous à la documentation de *Mise à niveau vSphere*.
2. Mettez à niveau les hôtes ESXi. Reportez-vous à Mettre à niveau les hôtes ESXi. Pour plus d'informations sur la migration et la préparation de vos hôtes ESXi à des fins de mise à niveau, reportez-vous à la documentation *Mise à niveau vSphere*.
3. Mettez à niveau le format de disque vSAN. La mise à niveau du format de disque est facultative, mais pour de meilleurs résultats, mettez à niveau les objets pour utiliser la toute dernière version. Le format sur disque expose votre environnement au jeu de fonctionnalités complet de vSAN. Reportez-vous à Mise à niveau du format de disque vSAN à l'aide de RVC.

Ce chapitre contient les rubriques suivantes :

- Utiliser les options de commande de mise à niveau RVC
- Recommandations de build vSAN pour vSphere Lifecycle Manager

Avant de procéder à la mise à niveau de vSAN

Planifiez et concevez votre mise à niveau de sorte qu'elle se produise sans défaillance. Avant de tenter de mettre à niveau vSAN, vérifiez que votre environnement répond à la configuration matérielle et logicielle requise de vSphere.

Conditions préalables à la mise à niveau

Tenez compte des différents aspects susceptibles de retarder le processus global de mise à niveau. Pour obtenir des directives et des recommandations, reportez-vous à la documentation *Mise à niveau vSphere*.

Passez en revue les principales exigences avant de procéder à la mise à niveau du cluster.

Tableau 8-1. Conditions préalables à la mise à niveau

Conditions préalables à la mise à niveau	Description
Logiciel, matériel, pilotes, microprogramme et contrôleurs d'E/S de stockage	Vérifiez que la nouvelle version de vSAN prend en charge les composants logiciels et matériels, les pilotes, le microprogramme et les contrôleurs d'E/S de stockage que vous prévoyez d'utiliser. Les éléments pris en charge sont répertoriés sur le site Web Guide de compatibilité VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php.
Version de vSAN	Vérifiez que vous utilisez la version la plus récente de vSAN. Vous ne pouvez pas effectuer une mise à niveau à partir d'une version bêta vers la nouvelle instance de vSAN. Lorsque vous procédez à une mise à niveau à partir d'une version bêta, vous devez effectuer un déploiement récent de vSAN.
Espace disque	Vérifiez que vous disposez de suffisamment d'espace pour terminer la mise à niveau de la version logicielle. La quantité de stockage sur disque nécessaire pour l'installation de vCenter Server dépend de la configuration de vCenter Server. Pour obtenir des directives sur l'espace disque requis pour la mise à niveau de vSphere, reportez-vous à la documentation *Mise à niveau vSphere*.

Tableau 8-1. Conditions préalables à la mise à niveau (suite)

Conditions préalables à la mise à niveau	Description
format de disque vSAN	Vérifiez que vous disposez d'une capacité disponible suffisante pour mettre à niveau le format de disque. Si vous ne disposez pas d'un espace libre égal à la capacité utilisée du plus grand groupe de disques, avec de l'espace disponible sur des groupes de disques différents des groupes de disques qui sont en cours de conversion, vous devez choisir **Autoriser la redondance réduite** comme option de migration des données. Par exemple, le groupe de disques le plus grand d'un cluster dispose de 10 To de capacité physique, mais seuls 5 To sont consommés. Un supplément de capacité de 5 To est requis ailleurs dans le cluster, à l'exception des groupes de disques en cours de migration. Lors de la mise à niveau du format de disque vSAN, vérifiez que les hôtes ne sont pas en mode de maintenance. Quand l'un des hôtes membres d'un cluster vSAN entre en mode de maintenance, la capacité du cluster est automatiquement réduite. L'hôte membre ne contribue plus au stockage du cluster et la capacité de l'hôte est indisponible pour les données. Pour plus d'informations sur les différents modes d'évacuation, reportez-vous à la documentation *Administration de VMware vSAN*.
hôtes vSAN	Vérifiez que vous avez placé les hôtes vSAN en mode de maintenance et que vous avez sélectionné le mode **Assurer l'accessibilité aux données** ou l'option **Évacuer toutes les données**. Vous pouvez utiliser vSphere Lifecycle Manager pour l'automatisation et le test du processus de mise à niveau. Néanmoins, quand vous utilisez vSphere Lifecycle Manager pour mettre à niveau vSAN, le mode d'évacuation par défaut est **Assurer l'accessibilité aux données**. Lorsque vous utilisez le mode **Assurer l'accessibilité aux données**, vos données ne sont pas protégées et si une panne survient pendant la mise à niveau de vSAN, il se peut que vous perdiez des données. Toutefois, le mode **Assurer l'accessibilité aux données** est plus rapide que le mode **Évacuer toutes les données**, car vous n'avez pas besoin de déplacer toutes les données vers un autre hôte du cluster. Pour plus d'informations sur les différents modes d'évacuation, reportez-vous à la documentation *Administration de VMware vSAN*.
Machines virtuelles	Vérifiez que vous avez sauvegardé vos machines virtuelles.

Recommandations

Tenez compte des recommandations suivantes lors du déploiement d'hôtes ESXi à utiliser avec vSAN :

- Si les hôtes ESXi sont configurés avec une capacité de mémoire de 512 Go ou inférieure, utilisez les périphériques SATADOM, SD, USB ou disque dur comme support d'installation.
- Si les hôtes ESXi sont configurés avec une capacité de mémoire supérieure à 512 Go, utilisez un périphérique disque magnétique ou Flash séparé comme périphérique d'installation. Si vous utilisez un périphérique distinct, vérifiez que vSAN ne réclame pas le périphérique.

- Lorsque vous démarrez un hôte vSAN depuis un périphérique SATADOM, vous devez utiliser un périphérique SLC (single-level cell) et la taille du périphérique de démarrage doit être d'au moins 16 Go.
- Pour garantir que votre matériel répond à la configuration requise pour vSAN, reportez-vous à la section *Planification et déploiement de vSAN*.

vSAN 6.5 et version ultérieure vous permettent d'ajuster les conditions requises de taille de démarrage pour un hôte ESXi dans un cluster vSAN. Pour plus d'informations, reportez-vous à l'article de la base de connaissances VMware à l'adresse http://kb.vmware.com/kb/2147881.

Mise à niveau de l'hôte témoin dans un cluster à deux hôtes ou un cluster étendu

L'hôte témoin d'un cluster à deux hôtes ou d'un cluster étendu se situe à l'extérieur du cluster vSAN, mais est géré par le même système vCenter Server. Vous pouvez utiliser le même processus pour mettre à niveau l'hôte témoin que celui utilisé pour un hôte de données vSAN.

Ne mettez pas à niveau l'hôte témoin tant que tous les hôtes de données n'ont pas été mis à niveau et n'ont pas quitté le mode de maintenance.

L'utilisation de vSphere Lifecycle Manager pour mettre à niveau des hôtes en parallèle peut entraîner la mise à niveau de l'hôte témoin en parallèle avec l'un des hôtes de données. Pour éviter les problèmes de mise à niveau, configurez vSphere Lifecycle Manager de manière qu'il ne mette pas à niveau l'hôte témoin en parallèle avec les hôtes de données.

Mettre à niveau vCenter Server

La première étape à effectuer au cours d'une mise à niveau de vSAN consiste à procéder à la mise à niveau générale de vSphere. Cette opération consiste à mettre à niveau vCenter Server et les hôtes ESXi.

VMware prend en charge les mises à niveau sur place de systèmes 64 bits à partir de vCenter Server 4.x, vCenter Server 5.0.x, vCenter Server 5.1.x et vCenter Server 5.5 vers vCenter Server 6.0 versions ultérieures. La mise à niveau de vCenter Server implique une mise à niveau du schéma de base de données et une mise à niveau du système vCenter Server.

Les détails et le niveau de prise en charge d'une mise à niveau vers ESXi 7.0 dépendent de l'hôte à mettre à niveau et de la méthode de mise à niveau utilisée. Assurez-vous de la prise en charge du chemin de mise à niveau depuis votre version actuelle d'ESXi jusqu'à la version vers laquelle vous procédez à la mise à niveau. Pour plus d'informations, reportez-vous aux matrices d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Plutôt que d'effectuer une mise à niveau sur place du système vCenter Server, vous pouvez utiliser une autre machine pour réaliser cette opération. Pour obtenir des instructions détaillées et connaître les options de mise à niveau, reportez-vous à la documentation *Mise à niveau de vCenter Server*.

Mettre à niveau les hôtes ESXi

Après avoir mis à niveau vCenter Server, la tâche suivante pour la mise à niveau du cluster vSAN consiste à mettre à niveau les hôtes ESXi pour utiliser la version actuelle.

Vous pouvez mettre à niveau les hôtes ESXi dans le cluster vSAN à l'aide de :

- vSphere Lifecycle Manager : en utilisant des images ou des lignes de base, vSphere Lifecycle Manager vous permet de mettre à niveau des hôtes ESXi dans le cluster vSAN. Le mode d'évacuation par défaut est **Assurer l'accessibilité aux données**. Si vous utilisez ce mode et que, lors de la mise à niveau de vSAN vous rencontrez un problème, les données peuvent devenir inaccessibles jusqu'à ce que l'un des hôtes soit à nouveau en ligne. Pour obtenir des informations sur l'utilisation des modes d'évacuation et de maintenance, reportez-vous à la section Utilisation du mode de maintenance. Pour plus d'informations sur les mises à niveau et les mises à jour, consultez la documentation *Gestion du cycle de vie de l'hôte et du cluster*.
- Commande Esxcli : vous pouvez utiliser des composants, des images de base et des modules complémentaires comme nouveaux éléments logiciels pour mettre à jour ou corriger les hôtes ESXi 7.0 à l'aide de la mise à niveau manuelle.

Lorsque vous mettez à niveau un cluster vSAN avec des domaines de pannes configurés, vSphere Lifecycle Manager met à niveau un hôte dans un domaine de pannes unique, puis passe à l'hôte suivant. Cela garantit que le cluster dispose des mêmes versions de vSphere en cours d'exécution sur tous les hôtes. Lorsque vous mettez à niveau un cluster étendu, vSphere Lifecycle Manager met à niveau tous les hôtes à partir du site préféré, puis passe à l'hôte sur le site secondaire. Cela garantit que le cluster dispose des mêmes versions de vSphere en cours d'exécution sur tous les hôtes. Pour plus d'informations sur la mise à niveau d'un cluster étendu, reportez-vous à la documentation *Gestion du cycle de vie des hôtes et des clusters*.

Avant de tenter de mettre à niveau les hôtes ESXi, examinez les recommandations présentées dans la documentation intitulée *Mise à niveau vSphere*. VMware fournit plusieurs options de mise à niveau d'ESXi. Choisissez l'option de mise à niveau la plus adaptée au type d'hôte que vous mettez à niveau. Pour obtenir des instructions détaillées et connaître les options de mise à niveau, reportez-vous à la documentation *Mise à niveau de VMware ESXi*.

Étape suivante

1. (Facultatif) Mettez à niveau le format de disque vSAN. Reportez-vous à Mise à niveau du format de disque vSAN à l'aide de RVC.
2. Vérifiez la licence de l'hôte. Dans la plupart des cas, vous devez appliquer à nouveau votre licence d'hôte. Pour plus d'informations sur l'application des licences d'hôtes, reportez-vous à la documentation *vCenter Server et gestion des hôtes*.
3. (Facultatif) Mettez à niveau les machines virtuelles sur les hôtes à l'aide de vSphere Client ou de vSphere Lifecycle Manager.

À propos du format de disque vSAN

La mise à niveau du format de disque est facultative. Votre cluster vSAN continue à s'exécuter sans encombres si vous utilisez une version précédente du format de disque.

Pour obtenir de meilleurs résultats, mettez à niveau les objets de façon à utiliser le format sur disque le plus récent. Le format sur disque le plus récent offre l'intégralité des fonctionnalités de vSAN.

En fonction de la taille des groupes de disques, le processus de mise à niveau du format de disque peut être long, car les groupes de disques sont mis à niveau un à la fois. Pour chaque mise à niveau d'un groupe de disques, toutes les données de chaque périphérique sont évacuées et le groupe de disques est supprimé du cluster vSAN. Le groupe de disques est ensuite rajouté à vSAN avec le nouveau format sur disque.

Note Une fois que vous avez mis à niveau le format sur disque, vous ne pouvez plus restaurer le logiciel sur les hôtes ni ajouter d'hôtes plus anciens au cluster.

Lorsque vous lancez une mise à niveau du format sur disque, vSAN effectue plusieurs opérations que vous pouvez surveiller sur la page Resynchronisation des composants. Le tableau résume chaque processus exécuté pendant la mise à niveau du format de disque.

Tableau 8-2. Avancement de la mise à niveau

Pourcentage d'achèvement	Description
0 %-5 %	Vérification du cluster. Les composants du cluster sont vérifiés et préparés pour la mise à niveau. Ce processus dure quelques minutes. vSAN vérifie qu'aucun problème en suspens n'existe qui pourrait empêcher la mise à niveau. ■ Tous les hôtes sont connectés. ■ La version du logiciel appropriée est installée sur tous les hôtes. ■ Tous les disques sont sains. ■ Tous les objets sont accessibles.
5 %-10 %	Mise à niveau d'un groupe de disques. vSAN effectue la mise à niveau initiale du disque sans migration de données. Ce processus dure quelques minutes.
10 %-15 %	Réalignement des objets. vSAN modifie la disposition de tous les objets pour s'assurer qu'ils sont correctement alignés. Le processus peut prendre plusieurs minutes pour un petit système composé de quelques snapshots. Il peut prendre de nombreuses heures, voir plusieurs jours, pour un système plus vaste comprenant beaucoup de snapshots, d'enregistrements fragmentés et d'objets non alignés.

Tableau 8-2. Avancement de la mise à niveau (suite)

Pourcentage d'achèvement	Description
15 %-95 %	Suppression et reformatage des groupes de disques lorsque vous mettez à niveau des versions de vSAN antérieures à la version 3.0. Chaque groupe de disques est supprimé du cluster, reformaté, puis rajouté au cluster. Le temps requis pour ce processus est variable, selon les méga-octets alloués et le chargement du système. Un système qui se trouve à sa capacité d'E/S ou qui s'en approche procède plus lentement aux transferts.
95 %-100 %	Mise à niveau vers la version finale des objets. Conversion des objets au nouveau format sur disque et achèvement de la resynchronisation. Le temps requis pour ce processus est variable, selon la quantité d'espace utilisée et l'éventuelle sélection de l'option **Autoriser la redondance réduite**.

Pendant la mise à niveau, vous pouvez surveiller le processus de mise à niveau à partir de la page Resynchronisation des composants. Reportez-vous à la section *Surveillance et dépannage de vSAN*. Vous pouvez également utiliser la commande RVC `vsan.upgrade_status <cluster>` pour surveiller la mise à niveau. Utilisez l'indicateur facultatif `-r <seconds>` pour actualiser l'état de mise à niveau périodiquement jusqu'à ce que vous appuyiez sur Ctrl+C. Le nombre minimal de secondes autorisé entre chaque actualisation est de 60.

Vous pouvez surveiller d'autres tâches de mise à niveau, telles que la suppression et la mise à niveau des périphériques dans le volet Tâches récentes de la barre d'état.

Les considérations suivantes s'appliquent lorsque vous mettez à niveau le format de disque :

- Si vous mettez à niveau un cluster contenant trois hôtes et que vous voulez effectuer une évacuation complète, l'évacuation échoue pour les objets dont le paramètre **Pannes tolérées** est supérieur ou égal à 0 (zéro). Un cluster à trois hôtes ne peut pas reprotéger un groupe de disques qui est en train d'être complètement évacué à l'aide de ressources de seulement deux disques. Par exemple, lorsque le paramètre **Pannes tolérées** est défini sur 1, vSAN requiert trois composants de protection (deux miroirs et un témoin), chacun étant placé sur un hôte séparé.

  Pour un cluster à trois hôtes, vous devez choisir le mode de suppression **Assurer l'accessibilité des données**. Dans ce mode, toute panne matérielle risque d'entraîner la perte de données.

  Vous devez également vous assurer que suffisamment d'espace libre est disponible. L'espace doit être égal à la capacité logique consommée du plus grand groupe de disques. Cette capacité doit être disponible sur un groupe de disques séparé de l'hôte en cours de migration.

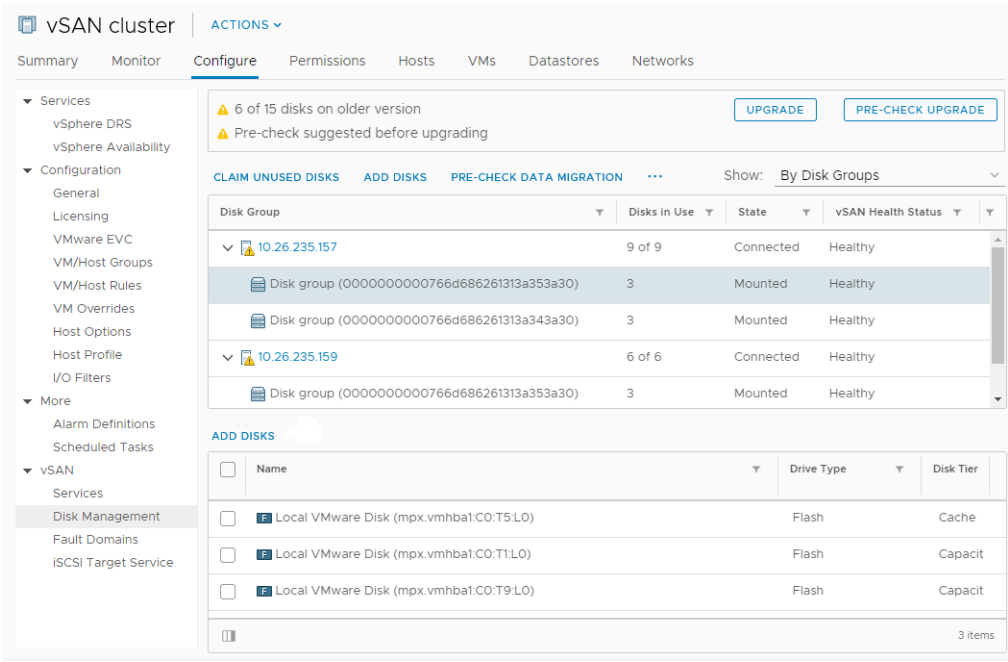
- Lorsque vous mettez à niveau un cluster à trois hôtes ou ayant des ressources limitées, autorisez les machines virtuelles à fonctionner en mode de redondance réduit. Exécutez la commande RVC avec l'option `vsan.ondisk_upgrade --allow-reduced-redundancy`.

- L'utilisation de l'option de commande `--allow-reduced-redundancy` implique que certaines machines virtuelles risquent de ne pas pouvoir tolérer d'échecs lors de la migration. Cette diminution de la tolérance aux échecs peut aussi entraîner une perte de données. vSAN restaure la conformité et la redondance complètes une fois la mise à niveau terminée. Pendant la mise à niveau, l'état de conformité des machines virtuelles et leur redondance sont temporairement non conformes. Une fois la mise à niveau et les tâches de reconstruction terminées, les machines virtuelles deviennent conformes.
- Pendant le déroulement de la mise à niveau, ne supprimez pas ou ne déconnectez pas d'hôtes, et ne placez pas un hôte en mode de maintenance. Ces actions peuvent entraîner l'échec de la mise à niveau.

Pour plus d'informations sur les commandes RVC et les options de commande, reportez-vous à la documentation *Guide de référence des commandes de l'outil RVC*.

Mise à niveau du format de disque vSAN à l'aide de vSphere Client

Après avoir procédé à la mise à niveau des hôtes vSAN, vous pouvez effectuer la mise à niveau du format de disque.



Note Si vous activez le chiffrement ou la déduplication et la compression sur un cluster vSAN existant, le format sur disque est automatiquement mis à niveau vers la dernière version. Cette procédure n'est pas requise. Reportez-vous à Modifier les paramètres vSAN.

Conditions préalables

- Vérifiez que vous utilisez la version mise à jour de vCenter Server.
- Vérifiez que vous utilisez la dernière version des hôtes ESXi.
- Vérifiez que les disques sont dans un état sain. Accédez à la page Gestion de disques pour vérifier l'état de l'objet.

- Vérifiez que le matériel et le logiciel que vous prévoyez d'utiliser sont certifiés et qu'ils figurent dans le site Web du Guide de compatibilité de VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php.
- Vérifiez que vous disposez de suffisamment d'espace libre pour effectuer la mise à niveau du format de disque. Exécutez la commande RVC `vsan.whatif_host_failures` afin de déterminer si vous disposez d'une capacité suffisante pour terminer la mise à niveau ou pour reconstruire des composants en cas de panne pendant l'opération de mise à niveau.
- Vérifiez que vos hôtes ne sont pas en mode de maintenance. Lors de la mise à niveau du format de disque, ne placez pas les hôtes en mode de maintenance. Lorsqu'un hôte membre d'un cluster vSAN entre en mode de maintenance, l'hôte membre ne contribue plus à la capacité du cluster. La capacité du cluster est réduite et la mise à niveau du cluster peut échouer.
- Vérifiez qu'aucune tâche de reconstruction de composants n'est actuellement en cours dans le cluster vSAN. Pour plus d'informations sur la resynchronisation vSAN, reportez-vous à la section *Surveillance et performances de vSphere*.

Procédure

1. Accédez au cluster vSAN.
2. Cliquez sur l'onglet **Configurer**.
3. Sous vSAN, sélectionnez **Gestion de disques**.
4. (Facultatif) Cliquez sur **Prévérifier la mise à niveau**.

   La prévérification analyse le cluster à la recherche de tout problème qui pourrait empêcher la réussite de la mise à niveau. L'état de l'hôte, l'état du disque, l'état du réseau et l'état de l'objet sont notamment vérifiés. Les problèmes de mise à niveau s'affichent dans le champ de texte **État de la prévérification du disque**.
5. Cliquez sur **Mettre à niveau**.
6. Cliquez sur **Oui** dans la boîte de dialogue Mettre à niveau pour effectuer la mise à niveau du format sur disque.

Résultats

vSAN met à niveau le format sur disque. La colonne Version du format sur disque affiche la version du format de disque des périphériques de stockage du cluster.

Si une panne se produit pendant la mise à niveau, vous pouvez consulter la page Objets de resynchronisation. Attendez la fin de toutes les resynchronisations, puis relancez la mise à niveau. Vous pouvez également vérifier la santé du cluster à l'aide du service de santé. Une fois que vous avez résolu les éventuels problèmes détectés par les contrôles de santé, vous pouvez relancer la mise à niveau.

Mise à niveau du format de disque vSAN à l'aide de RVC

Une fois que vous avez terminé la mise à niveau des hôtes vSAN, vous pouvez utiliser la console RVC (Ruby vSphere Console) pour poursuivre la mise à niveau du format de disque.

Conditions préalables

- Vérifiez que vous utilisez la version mise à jour de vCenter Server.
- Vérifiez que la version que les hôtes ESXi exécutent dans le cluster vSAN est la version 6.5 ou ultérieure.
- Vérifiez que les disques sont dans un état sain sur la page Gestion de disques. Vous pouvez également exécuter la commande RVC `vsan.disks_stats` pour vérifier l'état du disque.
- Vérifiez que le matériel et le logiciel que vous prévoyez d'utiliser sont certifiés et qu'ils figurent dans le site Web du Guide de compatibilité de VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php.
- Vérifiez que vous disposez de suffisamment d'espace libre pour effectuer la mise à niveau du format de disque. Exécutez la commande RVC `vsan.whatif_host_failures` afin de déterminer si vous disposez d'une capacité suffisante pour terminer la mise à niveau ou pour reconstruire des composants en cas de panne pendant la mise à niveau.
- Vérifiez que vous avez installé PuTTY ou un client SSH similaire pour l'accès à RVC.

  Pour plus d'informations sur le téléchargement de l'outil RVC et sur l'utilisation des commandes RVC, reportez-vous au *Guide de référence des commandes de l'outil RVC*.
- Vérifiez que vos hôtes ne sont pas en mode de maintenance. Lors de la mise à niveau du format sur disque, ne placez pas vos hôtes en mode de maintenance. Lorsqu'un hôte membre d'un cluster vSAN passe en mode de maintenance, la capacité des ressources disponible dans le cluster est réduite, car l'hôte membre ne contribue plus à la capacité du cluster. La mise à niveau du cluster risque d'échouer.
- Vérifiez qu'aucune tâche de reconstruction de composants n'est en cours dans le cluster vSAN en exécutant la commande RVC `vsan.resync_dashboard`.

Procédure

1. Connectez-vous à vCenter Server à l'aide de RVC.
2. Exécutez la commande RVC suivante pour afficher l'état du disque : `vsan.disks_stats /<vCenter IP address or hostname>/<data center name>/computers/<cluster name>`

   Par exemple :`vsan.disks_stats /192.168.0.1/BetaDC/computers/VSANCluster`

   Cette commande affiche le nom de tous les périphériques et hôtes du cluster vSAN. Elle affiche également le format de disque actuel et son état de santé. De plus, vous pouvez vérifier l'état de santé actuel des périphériques dans la colonne **État de santé** à la page **Gestion de disques**. Par exemple, l'état du périphérique indique qu'il est défectueux dans la colonne **État de santé** des hôtes ou groupes de disques ayant des périphériques défectueux.

3 Exécutez la commande RVC suivante : `vsan.ondisk_upgrade <path to vsan cluster>`

   Par exemple :`vsan.ondisk_upgrade /192.168.0.1/BetaDC/computers/VSANCluster`

4 Contrôler l'état d'avancement dans RVC.

   RVC met à jour un groupe de disques à la fois.

   Une fois que la mise à niveau du format de disque a abouti, le message suivant s'affiche.

```
Mise à niveau du format de disque réalisée
```

```
n objets v1 requièrent une mise à niveau État d'avancement de mise à niveau des objets : n mis à niveau, 0 restant
```

```
Mise à niveau des objets terminée : n mis à niveau
```

```
Mise à niveau de VSAN réalisée
```

5 Exécutez la commande RVC suivante pour vérifier que les versions des objets sont mises à niveau vers le nouveau format sur disque : `vsan.obj_status_report`

Vérifier la mise à niveau du format de disque vSAN

Après avoir procédé à la mise à niveau du format de disque, vous devez vérifier si le cluster vSAN utilise le nouveau format sur disque.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer**.

3 Sous vSAN, cliquez sur **Gestion de disques**.

   La version du format de disque actuel s'affiche dans la colonne Version du format de disque.

À propos du format d'objet vSAN

L'espace requis par vSAN pour effectuer une modification de stratégie ou d'autres opérations sur un objet créé par vSAN 7.0 ou version antérieure est l'espace utilisé par un objet le plus grand du cluster. Cela est généralement difficile à prévoir et, par conséquent, il est recommandé d'utiliser 30 % d'espace libre dans le cluster, en partant du principe qu'il est peu probable que le plus grand objet du cluster consomme plus de 25 % de l'espace et que 5 % de l'espace sont réservés pour s'assurer que le cluster ne devient pas plein en raison de modifications de stratégie. Dans vSAN 7.0 U1 et versions ultérieures, tous les objets sont créés dans un nouveau format qui offre à vSAN l'espace nécessaire pour effectuer une modification de stratégie sur un objet s'il y a 255 Go par hôte pour les objets inférieurs à 8 To et 765 Go par hôte pour les objets de 8 To ou plus.

Après la mise à niveau d'un cluster vers vSAN 7.0 U1 ou version ultérieure à partir de vSAN 7.0 ou version antérieure, les objets supérieurs à 255 Go créés avec l'ancienne version doivent être réécrits dans le nouveau format avant que vSAN puisse offrir l'avantage d'effectuer des opérations sur un objet avec les nouvelles exigences relatives à l'espace libre. Une nouvelle alerte de santé du format d'objet s'affiche après une mise à niveau, s'il existe des objets qui doivent être corrigés sur le nouveau format d'objet et permet de corriger l'état de santé en lançant une tâche de réorganisation pour corriger ces objets. L'alerte de santé fournit des informations sur le nombre d'objets qui doivent être corrigés et la quantité de données qui seront réécrites. Le cluster peut enregistrer une diminution d'environ 20 % des performances alors que la tâche de réorganisation est en cours. Le tableau de bord de resynchronisation fournit des informations plus précises sur la durée d'exécution de cette opération.

Vérifier la mise à niveau du cluster vSAN

La mise à niveau d'un cluster vSAN n'est pas terminée tant que vous n'avez pas vérifié que vous utilisez la version la plus récente de vSphere et que vSAN est disponible.

Procédure

1 Accédez au cluster vSAN.

2 Cliquez sur l'onglet **Configurer** et vérifiez que vSAN est répertorié.

- Vous pouvez également accéder à l'hôte ESXi et sélectionner **Résumé** > **Configuration**, puis vérifiez que vous utilisez la dernière version de l'hôte ESXi.

Utiliser les options de commande de mise à niveau RVC

La commande `vsan.ondisk_upgrade` offre différentes options de commandes vous permettant de contrôler et de gérer la mise à niveau du cluster vSAN. Par exemple, vous pouvez autoriser une redondance réduite pour effectuer la mise à niveau lorsque vous n'avez que peu d'espace libre disponible.

Exécutez la commande `vsan.ondisk_upgrade --help` pour afficher la liste des options des commandes RVC.

Utilisez ces options de commande avec la commande `vsan.ondisk_upgrade`.

Tableau 8-3. Options de commande de mise à niveau

Options	Description
`--hosts_and_clusters`	Utilisez cette option pour spécifier des chemins vers tous les systèmes hôtes dans le cluster ou les ressources de calcul du cluster.
`--ignore-objects, -i`	Utilisez cette option pour ignorer vSAN la mise à niveau des objets. Vous pouvez également utiliser cette option de commande pour éliminer la mise à niveau de la version de l'objet. Lorsque vous utilisez cette option de commande, les objets continuent à utiliser la version de format sur disque actuelle.

Tableau 8-3. Options de commande de mise à niveau (suite)

Options	Description
`--allow-reduced-redundancy, -a`	Utilisez cette option pour supprimer les conditions requises d'espace disponible égal à un groupe de disques au cours de la mise à niveau de disque. Avec cette option, les machines virtuelles fonctionnent dans un mode de redondance réduite pendant la mise à niveau ce qui signifie que certaines machines virtuelles peuvent être incapables de tolérer des pannes temporaires et que cette incapacité peut entraîner la perte de données. vSAN restaure la conformité et la redondance complètes une fois la mise à niveau terminée.
`--force, -f`	Utilisez cette option pour activer l'exécution de force et répondre automatiquement à toutes les questions de confirmation.
`--help, -h`	Utilisez cette option pour afficher les options d'aide.

Pour plus d'informations sur les commandes RVC, reportez-vous au *Guide de référence des commandes de l'outil RVC*.

Recommandations de build vSAN pour vSphere Lifecycle Manager

vSAN génère des lignes de base de système et des groupes de lignes de base que vous pouvez utiliser avec vSphere Lifecycle Manager. vSphere Lifecycle Manager dans vSphere 7.0 comporte des lignes de base de système qu'Update Manager fournies dans les versions précédentes de vSphere. Il contient également de nouvelles fonctionnalités de gestion d'images pour les hôtes exécutant ESXi 7.0 et versions ultérieures.

vSAN 6.6.1 et versions ultérieures génèrent des recommandations de build automatisées pour les clusters vSAN. vSAN combine les informations du Guide de compatibilité VMware et du catalogue de version de vSAN avec des informations sur les versions d'ESXi installées. Ces mises à jour recommandées fournissent la meilleure version disponible pour conserver votre matériel dans un état pris en charge.

Les lignes de base de système de vSAN 6.7.1 sur vSAN 7.0 peuvent également inclure des mises à jour de pilote de périphérique et de microprogramme. Ces mises à jour prennent en charge le logiciel ESXi recommandé pour votre cluster.

Dans vSAN 6.7.3 et versions ultérieures, vous pouvez fournir des recommandations de build uniquement pour la version actuelle d'ESXi ou pour la version la plus récente d'ESXi prise en charge. Une recommandation de build pour la version actuelle inclut tous les correctifs et les mises à jour de pilotes pour la version.

Dans vSAN 7.0 et versions ultérieures, les recommandations de build vSAN incluent des mises à jour de correctifs et des mises à jour de pilotes applicables. Pour mettre à jour le microprogramme sur les clusters vSAN 7.0, vous devez utiliser une image via vSphere Lifecycle Manager.

Lignes de base de système vSAN

Les recommandations de build vSAN sont fournies à l'aide de lignes de base de système vSAN pour vSphere Lifecycle Manager. Ces lignes de base de système sont gérées par vSAN. Elles sont en lecture seule et ne peuvent pas être personnalisées.

vSAN génère un groupe de lignes de base pour chaque cluster vSAN. Les lignes de base de système vSAN sont répertoriées dans le volet **Lignes de base** de l'onglet Lignes de base et groupes. Vous pouvez continuer à créer et à corriger vos propres lignes de base.

Les lignes de base système vSAN peuvent inclure des images ISO personnalisées fournies par les fournisseurs certifiés. Si les hôtes dans votre cluster vSAN possèdent des images ISO personnalisées spécifiques OEM, les lignes de base de système recommandées vSAN peuvent inclure des images ISO personnalisées à partir du même fournisseur. vSphere Lifecycle Manager ne peut pas générer de recommandation pour les images ISO personnalisées non prises en charge par vSAN. Si vous exécutez une image du logiciel personnalisée qui remplace le nom du fournisseur dans le profil d'image de l'hôte, vSphere Lifecycle Manager ne peut pas recommander une ligne de base de système.

vSphere Lifecycle Manager analyse automatiquement chaque cluster vSAN pour vérifier la conformité par rapport au groupe de lignes de base. Pour mettre à niveau le cluster, vous devez corriger manuellement la ligne de base de système via vSphere Lifecycle Manager. Vous pouvez corriger une ligne de base de système vSAN sur un hôte unique ou sur l'intégralité du cluster.

Catalogue de version de vSAN

Le catalogue de version de vSAN contient des informations sur les versions disponibles, sur l'ordre de préférence des versions et sur les correctifs critiques nécessaire pour chaque version. Le catalogue de version de vSAN est hébergé sur VMware Cloud.

vSAN nécessite une connexion à Internet pour accéder au catalogue de version. La participation au Programme d'amélioration du produit (CEIP) n'est pas obligatoire pour permettre à vSAN d'accéder au catalogue de version.

Si vous ne disposez pas d'une connexion Internet, vous pouvez télécharger le catalogue de version vSAN directement sur vCenter Server. Dans vSphere Client, cliquez sur **Configurer > vSAN > Mise à jour**, puis cliquez sur **Télécharger à partir d'un fichier** dans la section Catalogue de version. Vous pouvez télécharger le dernier vSAN catalogue de version.

vSphere Lifecycle Manager vous permet d'importer les pilotes de contrôleur de stockage recommandés pour votre cluster vSAN. Certains fournisseurs de contrôleurs de stockage proposent un outil de gestion de logiciel que vSAN peut utiliser pour mettre à jour les pilotes de contrôleur. Si l'outil de gestion n'est pas présent sur les hôtes ESXi, vous pouvez le télécharger.

Utilisation des recommandations de build vSAN

vSphere Lifecycle Manager vérifie les versions d'ESXi installées par rapport aux informations de la liste de compatibilité matérielle (HCL) du Guide de compatibilité VMware. Il détermine le chemin de mise à niveau correct pour chaque cluster vSAN, en fonction du catalogue de version de vSAN actuel. vSAN inclut également les pilotes et les mises à jour de correctif nécessaires pour la version recommandée dans sa ligne de base de système.

Les recommandations de build vSAN permettent de garantir que chaque cluster vSAN reste à l'état actuel ou supérieur de la compatibilité matérielle. Si le matériel du cluster vSAN n'est pas inclus dans la liste HCL, vSAN peut recommander une mise à niveau vers la dernière version, car elle ne suppose aucune détérioration par rapport à l'état actuel.

Note vSphere Lifecycle Manager utilise vSAN Health Service lors de l'exécution de la prévérification de la correction des hôtes dans un cluster vSAN. vSANHealth Service n'est pas disponible sur les hôtes exécutant ESXi 6. 0 Update 1 ou version antérieure. Lorsque vSphere Lifecycle Manager met à niveau des hôtes exécutant ESXi 6.0 Update 1 ou version antérieure, la mise à niveau du dernier hôte dans le cluster vSAN risque d'échouer. Si la correction a échoué en raison de problèmes de santé de vSAN, vous pouvez toujours effectuer la mise à niveau. Utilisez vSAN Health Service pour résoudre les problèmes de santé sur l'hôte, puis retirez cet hôte du mode de maintenance pour terminer le workflow de mise à niveau.

Les exemples suivants décrivent la logique derrière les recommandations de build vSAN.

Exemple 1

Un cluster vSAN exécute la version 6.0 Update 2 et le matériel est inclus dans la liste HCL de la version 6.0 Update 2. La liste HCL répertorie le matériel comme pris en charge jusqu'à la version 6.0 Update 3, mais comme non pris en charge pour la version 6.5 et les versions ultérieures. vSAN recommande une mise à niveau vers la version 6.0 Update 3, y compris les correctifs critiques nécessaires pour la version.

Exemple 2

Un cluster vSAN exécute la version 6.7 Update 2 et le matériel est inclus dans la liste HCL de la version 6.7 Update 2. Le matériel est également pris en charge sur la liste HCL de la version 7.0 Update 3. vSAN recommande une mise à niveau vers la version 7.0 Update 3.

Exemple 3

Un cluster vSAN exécute la version 6.7 Update 2 et son matériel n'est pas répertorié dans la liste HCL de cette version. vSAN recommande une mise à niveau vers la version 7.0 Update 3, même si le matériel n'est pas répertorié sur la liste HCL de la version 7.0 Update 3. vSAN recommande la mise à niveau, car le nouvel état ne suppose aucune détérioration par rapport à l'état actuel.

Exemple 4

Un cluster vSAN exécute la version 6.7 Update 2 et le matériel est inclus dans la liste HCL de la version 6.7 Update 2. Le matériel est également pris en charge dans la liste HCL pour la version 7.0 Update 3 et la préférence de ligne de base sélectionnée est correctif uniquement. vSAN recommande une mise à niveau vers la version 7.0 Update 3, y compris les correctifs critiques nécessaires pour la version.

Le moteur de recommandation s'exécute régulièrement (une fois par jour) ou lorsque les événements suivants se produisent.

- Modification de l'appartenance au cluster. Par exemple, lorsque vous ajoutez ou supprimez un hôte.
- Le service de gestion vSAN redémarre.
- Un utilisateur se connecte à VMware Customer Connect à l'aide d'un navigateur Web ou RVC.
- Le Guide de compatibilité de VMware ou le catalogue de version de vSAN est mis à jour.

Le contrôle de santé de la recommandation de build vSAN affiche la build actuelle recommandée pour le cluster vSAN. Il vous prévient également des problèmes potentiels de la fonctionnalité.

Configuration système requise

vSphere Lifecycle Manager est un service d'extension dans vCenter Server 7.0 et versions ultérieures.

vSAN nécessite un accès à Internet pour mettre à jour les métadonnées de version, consulter le Guide de compatibilité de VMware et télécharger des images ISO à partir de VMware Customer Connect.

vSAN nécessite des informations d'authentification valides pour télécharger les images ISO correspondant aux mises à niveau depuis VMware Customer Connect. Pour les hôtes qui exécutent la version 6.0 Update 1 ou les versions antérieures, vous devez utiliser RVC pour entrer les informations d'identification **VMware Customer Connect**. Pour les hôtes exécutant une version ultérieure, vous pouvez vous connecter à partir du contrôle de santé de recommandation de build ESX.

Pour entrer les informations d'identification **VMware Customer Connect** à partir de RVC, exécutez la commande suivante : **`vsan.login_iso_depot -u`** *<username>* **`-p`** *<password>*