

Stockage vSphere

Update 1

VMware vSphere 8.0

VMware ESXi 8.0

vCenter Server 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

Copyright © 2009-2023 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

À propos de vSphere Storage	13
1 Présentation du stockage dans l'environnement vSphere	14
Modèles de virtualisation du stockage traditionnel dans un environnement vSphere	14
Modèles de stockage à définition logicielle	16
API de stockage vSphere	17
2 Démarrage avec un modèle de stockage traditionnel dans un environnement vSphere	19
Types de stockage physique pris en charge par ESXi	19
Stockage local	19
Stockage en réseau	21
Comparaison des types de stockage	25
Représentations de périphériques et de cibles	26
Accès des machines virtuelles au stockage	27
Affichage des périphériques de stockage disponibles pour un hôte ESXi	28
Affichage des périphériques de stockage d'un hôte ESXi	30
Affichage des périphériques de stockage d'un adaptateur	30
Adaptateurs de stockage disponibles sur un hôte ESXi	31
Caractéristiques des banques de données ESXi	33
Afficher les informations relatives aux banques de données	35
Utilisation de périphériques à mémoire persistante avec ESXi	36
Surveiller les statistiques de la banque de données PMem	38
Utilisation d'ESXi avec un SAN	39
Cas d'utilisation d'ESXi et du SAN	40
Informations détaillées sur l'utilisation du stockage SAN avec l'ESXi	41
Prendre des décisions LUN	41
Sélection de l'emplacement des machines virtuelles	43
Applications de gestion tierces	43
Considérations sur la sauvegarde de stockage SAN	44
3 Utilisation d'ESXi avec un SAN Fibre Channel	46
Configuration de l'environnement ESXi Fibre Channel	49
Restrictions de SAN Fibre Channel ESXi	50
Définition des allocations de LUN	50
Configuration des HBA Fibre Channel	51
Configuration de Fibre Channel over Ethernet	52
Workflow de configuration	52

Démarrage ESXi à partir du SAN Fibre Channel	52
Avantages du démarrage à partir d'un SAN	53
Exigences et considérations lors du démarrage à partir du SAN Fibre Channel	53
Préparation pour le démarrage ESXi à partir du SAN	54
Meilleures pratiques pour le stockage Fibre Channel	56
Prévention des problèmes de SAN Fibre Channel	57
Désactiver l'enregistrement automatique de l'hôte ESXi	57
Optimisation des performances du stockage SAN Fibre Channel	58
Utilisation de Fibre Channel NPIV avec des machines virtuelles vSphere	60
Comment fonctionne l'accès à un LUN par NPIV	60
Conditions nécessaires pour l'utilisation de NPIV	60
Capacités et limitations NPIV	61
Configurer ou modifier des attributions WWN	62
4 Utilisation d'ESXi avec un SAN iSCSI	63
Démarrage à partir du SAN iSCSI	72
Recommandations générales pour le démarrage à partir du SAN iSCSI	72
Préparation du SAN iSCSI	73
Configurer l'adaptateur iSCSI matériel indépendant pour le démarrage à partir du SAN	74
Meilleures pratiques pour le stockage iSCSI	75
Prévention des problèmes de iSCSI SAN	76
Optimisation des performances du stockage SAN iSCSI	77
Consultation des statistiques des commutateurs Ethernet	81
5 Configuration des adaptateurs iSCSI et iSER et du stockage	82
Configurer des adaptateurs iSCSI matériel indépendants	85
Afficher des adaptateurs de matériel iSCSI dépendants	85
Modifier des paramètres réseau pour du matériel iSCSI	86
Configurer des adaptateurs iSCSI matériel dépendants	87
Considérations sur l'iSCSI matériel dépendant	88
Affichage des adaptateurs iSCSI matériel dépendants	89
Déterminer l'association entre les adaptateurs iSCSI et les adaptateurs réseau	90
Configurer l'adaptateur iSCSI logiciel	90
Ajouter ou supprimer l'adaptateur iSCSI logiciel	91
Configurer iSER avec ESXi	92
Installer et afficher un adaptateur réseau prenant en charge RDMA	93
Activer l'adaptateur iSER VMware	94
Modifier les propriétés générales des adaptateurs iSCSI ou iSER	97
Configuration du réseau pour iSCSI et iSER	98
Multiples adaptateurs réseau dans une configuration iSCSI ou iSER	99
Recommandations pour la configuration de la mise en réseau avec un iSCSI logiciel	100

Gestion du réseau iSCSI	105
Dépannage du réseau iSCSI	105
Configurer la liaison de port pour les protocoles iSCSI ou iSER	106
Créer un adaptateur VMkernel unique pour iSCSI ou iSER	106
Lier des adaptateurs iSCSI ou iSER à des adaptateurs VMkernel	108
Vérifier les détails de liaison de port sur l'hôte ESXi	109
Utilisation de trames Jumbo avec iSCSI et iSER	110
Activer les trames Jumbo pour la mise en réseau	110
Activer les trames Jumbo pour l'iSCSI matériel indépendant	111
Configurer la découverte dynamique ou statique pour iSCSI et iSER sur l'hôte ESXi	111
Supprimer des cibles iSCSI dynamiques ou statiques	113
Configuration des paramètres CHAP pour les adaptateurs de stockage iSCSI ou iSER	114
Sélection de la méthode d'authentification CHAP	114
Configurer CHAP pour un adaptateur de stockage iSCSI ou iSER	115
Configurer CHAP pour une cible	117
Configuration des paramètres avancés iSCSI	118
Configurer les paramètres avancés pour iSCSI sur un hôte ESXi	120
Gestion des sessions iSCSI	120
Passer en revue les sessions iSCSI	121
Ajout de sessions iSCSI	122
Supprimer des sessions iSCSI	122
6 Gestion des périphériques de stockage	124
Noms et identifiants de périphérique de stockage ESXi	124
Périphériques NVMe avec identifiants de périphérique NGUID	126
Renommer des périphériques de stockage	126
Réanalyser les opérations de stockage ESXi	127
Réanalyse du stockage	127
Effectuer une réanalyse d'adaptateur	128
Modifier le nombre de périphériques de stockage analysés	128
Identification des problèmes de connectivité de stockage ESXi	129
Détection des états PDL	130
Effectuer un retrait de périphérique de stockage prévu	131
Récupération à partir des états PDL	133
Traitement des conditions APD passagères	134
Vérifier l'état de la connexion d'un périphérique de stockage sur un hôte ESXi	136
Utiliser le voyant de localisation sur les périphériques de stockage ESXi	136
Effacer des périphériques de stockage	137
Modifier les paramètres de réservation perpétuelle	137
7 Utilisation de périphériques Flash avec les hôtes ESXi	139

Meilleures pratiques pour les périphériques Flash sur les hôtes ESXi	140
Surveiller les périphériques Flash	141
Estimer la durée de vie des périphériques Flash	141
Garder les disques Flash sans formatage VMFS	142
Marquage de périphériques de stockage sur des hôtes ESXi	143
Marquer les périphériques de stockage en tant que Flash	143
Marquer des périphériques de stockage comme locaux	144
À propos des ressources Virtual Flash dans l'environnement vSphere	144
Considérations relatives aux ressources Virtual Flash	145
Configurer une ressource Virtual Flash	145
Supprimer une ressource Virtual Flash	146
Définir une alarme pour l'utilisation de Virtual Flash	147
Configurer le cache d'échange d'hôte avec une banque de données VMFS	147

8 À propos du stockage VMware NVMe 149

Concepts de VMware NVMe	149
Architecture et composants de base de VMware NVMe	151
Conditions requises et limitations du stockage VMware NVMe	154
Configuration de la technologie Ethernet sans perte pour NVMe sur RDMA	156
Configuration d'adaptateurs pour le stockage NVMe over RDMA (RoCE v2)	158
Voir les adaptateurs réseau RDMA	159
Configurer la liaison VMkernel pour l'adaptateur RDMA	159
Configuration des adaptateurs pour le stockage NVMe over TCP	166
Configurer la liaison VMkernel pour l'adaptateur NVMe over TCP	166
Ajout d'adaptateurs logiciels NVMe	172
Ajouter des contrôleurs pour NVMe over Fabrics	173
Supprimer des adaptateurs NVMe logiciels	175

9 Utilisation des banques de données 176

Concepts de banque de données VMFS	177
Création de banques de données	183
Créer une banque de données VMFS	184
Créer une banque de données NFS	186
Créer une banque de données Virtual Volumes	187
Opérations administratives de base pour les banques de données	188
Modifier le nom d'une banque de données	188
Démontage des banques de données	189
Monter des banques de données	190
Supprimer des banques de données VMFS	191
Utilisation du navigateur de banque de données	191
Accéder au navigateur de banque de données	191

Télécharger des fichiers ou des dossiers vers des banques de données	192
Télécharger des fichiers à partir de banques de données	194
Renommer les fichiers de banque de données	194
Déplacer ou copier des dossiers de banque de données ou des fichiers	195
Gonfler les disques virtuels dynamiques	195
Gestion des banques de données VMFS	196
Mécanismes de verrouillage VMFS	196
Administration des banques de données VMFS dupliquées	202
Augmenter la capacité d'une banque de données VMFS	204
Configurer les paramètres des disques virtuels en cluster sur la banque de données VMFS6	
206	
Désactivation des filtres de stockage	207
Configuration de la mise en miroir des disques dynamiques	208
Collecte d'informations de diagnostic pour les hôtes ESXi sur une banque de données VMFS	
209	
Vérification de la cohérence des métadonnées avec VOMA	212
Configuration du cache de blocs de pointage VMFS	216
Concepts et opérations de banque de données NFS	218
Directives et configuration requise du stockage NFS	221
Configurations de pare-feu pour le stockage NFS	225
Utiliser des connexions routées L3 pour accéder à un stockage NFS	227
Utilisation de Kerberos pour NFS 4.1	227
Configurer un environnement de stockage NFS	228
Configurer les hôtes ESXi pour l'authentification Kerberos	229
Configurer la liaison VMkernel pour la banque de données NFS 3	232
Collecte d'informations statistiques pour le stockage NFS	234
10 Présentation de la gestion multivoie et du basculement	235
Basculements avec Fibre Channel	235
Basculement basé sur hôte avec iSCSI	236
Basculement à base de baie avec iSCSI	238
Basculement de chemin et machines virtuelles	239
Définir le délai d'expiration du SE invité Windows	240
Architecture de stockage enfichable et gestion des chemins	240
À propos de l'architecture de stockage enfichable	242
VMware Native Multipathing Plug-In	243
Path Selection Plug-Ins et règles	245
SATP de VMware	247
VMware High Performance Plug-In et Path Selection Schemes	249
Affichage et gestion des chemins	256
Affichage des chemins d'accès aux périphériques de stockage	256
Affichage des chemins d'accès aux banques de données	257

Modification de la stratégie de sélection de chemin d'accès	258
Modifier les paramètres par défaut pour la latence circulaire	259
Désactiver les chemins de stockage	260
Utilisation des règles de réclamation	261
Considérations concernant la gestion multivoie	261
Liste de règles de réclamation de gestion multivoie pour l'hôte	262
Ajout de règles de réclamation de gestion multivoie	264
Suppression de règles de réclamation de gestion multivoie	268
Masquage des chemins	269
Démasquage des chemins	270
Définition des règles SATP de NMP	271
Files d'attente de planification pour les E/S de machines virtuelles	273
Modifier la planification des E/S par fichier dans vSphere Client	273
Utiliser les commandes esxcli pour modifier la planification des E/S par fichier	274

11 Mappage de périphérique brut 275

À propos du mappage de périphérique brut	275
Avantages du mappage de périphérique brut	276
Considérations et Limitations des RDM	279
Caractéristiques du mappage de périphérique brut	279
Modes de compatibilité physique et virtuel du RDM	280
Résolution dynamique de nom	280
Mappage de périphérique brut sur des clusters de machine virtuelle	280
Comparaison des modes d'accès disponibles du périphérique SCSI	281
Création de machines virtuelles avec des RDM	281
Gérer les chemins pour un LUN mappé	283
Les machines virtuelles dotées de RDM doivent ignorer le cache SCSI INQUIRY	284

12 Gestion basée sur des stratégies de stockage (SPBM, Storage Policy Based Management) 286

Stratégies de stockage de machine virtuelle	287
Workflow pour les stratégies de stockage de machine virtuelle	287
Remplissage de l'interface des stratégies de stockage de machine virtuelle	288
Utiliser des fournisseurs de stockage pour remplir l'interface des stratégies de stockage de machine virtuelle	289
Affecter des balises à des banques de données	290
À propos des règles et groupes de règles	292
Création et gestion de stratégies de stockage de machine virtuelle	295
Créer une stratégie de stockage de machine virtuelle pour les services de données basés sur l'hôte	295
Créer une stratégie de stockage de machine virtuelle pour Virtual Volumes	297
Créer une stratégie de stockage de machines virtuelles pour le placement basé sur des balises	300

Modifier ou cloner une stratégie de stockage de machine virtuelle	301
À propos des composants de stratégie de stockage	302
Créer des composants de stratégie de stockage	303
Modifier ou cloner les composants d'une stratégie de stockage	304
Stratégies de stockage et machines virtuelles	305
Attribuer des stratégies de stockage à des machines virtuelles	305
Modifier l'attribution d'une stratégie de stockage pour des fichiers et des disques de machine virtuelle	307
Vérifier la conformité d'une stratégie de stockage de machine virtuelle	308
Rechercher des ressources de stockage compatibles pour une machine virtuelle non conforme	309
Réappliquer une stratégie de stockage de machine virtuelle	310
Stratégies de stockage par défaut	311
Modifier la stratégie de stockage par défaut d'une banque de données	312

13 Utilisation de fournisseurs de stockage 313

Gestion des fournisseurs de stockage	316
Enregistrement des fournisseurs de stockage	316
Afficher des informations sur le fournisseur de stockage	316
Gérer les fournisseurs de stockage	317

14 Utilisation de VMware vSphere Virtual Volumes 320

Concepts et architecture de Virtual Volumes	320
Objets de volume virtuel	321
Fournisseurs de stockage Virtual Volumes	322
Conteneurs de stockage Virtual Volumes	323
Points de terminaison de protocole	324
Liaison et annulation de liaison de Virtual Volumes	325
Banques de données Virtual Volumes	325
Virtual Volumes et stratégies de stockage de machine virtuelle	326
Virtual Volumes et protocoles de stockage	327
Architecture de Virtual Volumes	329
Virtual VolumesSécurité	330
Snapshots de volume virtuel	333
Avant d'activer Virtual Volumes	334
Synchroniser l'environnement vSphere Storage avec un serveur de temps réseau	335
Configurer Virtual Volumes	335
Enregistrer des fournisseurs de stockage pour Virtual Volumes	335
Créer une banque de données Virtual Volumes	336
Vérifier et gérer des points de terminaison de protocole	337
Modifier la stratégie de sélection de chemin d'accès pour un point de terminaison de protocole	338

Provisionner des machines virtuelles sur des banques de données Virtual Volumes	339
Gérer les fournisseurs de stockage pour Virtual Volumes	340
NVMe et Virtual Volumes	341
Configurer NVMe avec Virtual Volumes	343
Virtual Volumes et réPLICATION	345
Conditions requises en matière de réPLICATION avec Virtual Volumes	346
Virtual Volumes et groupes de réPLICATION	347
Virtual Volumes et domaines de pannes	347
Workflow de réPLICATION de Virtual Volumes	349
Directives et considérations relatives à la réPLICATION	350
Meilleures pratiques d'utilisation de Virtual Volumes	351
Directives et limitations lors de l'utilisation de Virtual Volumes	351
Meilleures pratiques pour le provisionnement de conteneurs de stockage	352
Meilleures pratiques pour les performances de Virtual Volumes	354
Dépannage de Virtual Volumes	355
Virtual Volumes et commandes esxcli	356
Collecte d'informations statistiques pour les Virtual Volumes	356
La banque de données Virtual Volumes est inaccessible	357
Erreurs lors de la migration de machines virtuelles ou du déploiement d'environnements OVF de machine virtuelle vers des banques de données Virtual Volumes	358

15 Filtrage des E/S de machines virtuelles 360

À propos des filtres d'E/S	360
Types de filtres d'E/S	361
Composants de filtrage d'E/S	362
Fournisseurs de stockage pour filtres d'E/S	363
Utilisation de périphériques de stockage Flash avec des filtres d'E/S de cache	364
Configuration système requise pour les filtres d'E/S	365
Configurer des filtres d'E/S dans l'environnement vSphere	365
Installer des filtres d'E/S dans un cluster	366
Afficher les filtres d'E/S et les fournisseurs de stockage	366
Activer les services de données de filtre d'E/S sur des disques virtuels	367
Attribuer la stratégie de filtre d'E/S à des machines virtuelles	368
Gestion des filtres d'E/S	369
Désinstaller des filtres d'E/S d'un cluster	370
Mettre à niveau les filtres d'E/S d'un cluster	370
Directives et meilleures pratiques applicables aux filtres d'E/S	371
Migration de machines virtuelles avec des filtres d'E/S	372
Gestion des incidents d'installation des filtres d'E/S	372
Installer les filtres d'E/S sur un hôte ESXi unique	373

16 Accélération matérielle du stockage 374

Avantages de l'accélération matérielle	374
Conditions requises pour l'accélération matérielle	375
État de la prise en charge de l'accélération matérielle	375
Accélération pour les périphériques de stockage de blocs	375
Désactiver l'accélération matérielle des périphériques de stockage des blocs	376
Gestion de l'accélération matérielle sur les périphériques de stockage des blocs	377
Accélération matérielle sur les périphériques NAS	384
Activer les snapshots natifs NAS sur des machines virtuelles	386
Considérations sur l'accélération matérielle	386
17 Provisionnement de stockage et récupération d'espace	388
Provisionnement dynamique du disque virtuel	388
À propos des règles de provisionnement des disques virtuels	389
Création de disques virtuels alloués dynamiquement	390
Affichage des ressources de stockage des machines virtuelles	391
Déterminer le format de disque d'une machine virtuelle	392
Gonfler les disques virtuels dynamiques	392
Traitement du sur-abonnement de banque de données	393
ESXi et provisionnement dynamique de la baie	394
Surveillance de l'utilisation de l'espace	394
Identifier les périphériques de stockage à provisionnement dynamique	395
Récupération d'espace de stockage	396
Récupération d'espace sur les banques de données VMFS	398
Demandes de récupération d'espace provenant de systèmes d'exploitation invités	404
18 Démarrage avec Stockage cloud natif	406
Concepts et terminologie du Stockage cloud natif	406
Composants Stockage cloud natif	409
Utilisation du service de fichiers vSAN pour provisionner des volumes de fichiers	412
Utilisateurs de Stockage cloud natif	414
Stockage natif sur le cloud pour les administrateurs vSphere	415
Configuration requise de Stockage cloud natif	415
Rôles et priviléges de Stockage cloud natif	419
Créer une stratégie de stockage pour Kubernetes	420
Configurer des machines virtuelles de cluster Kubernetes	422
Surveiller les volumes de conteneur entre les clusters Kubernetes	423
Utilisation du chiffrement avec le stockage cloud natif	424
19 Utilisation de vmkfstools	426
Syntaxe des commandes vmkfstools	426
Options de la commande vmkfstools	427

- Sous-option -v 428
- Options de système de fichiers 428
- Options de disque virtuel 431
- Options de périphérique de stockage 438

À propos de vSphere Storage

vSphere Storage décrit les technologies de stockage définies par logiciel et virtualisées que VMware ESXi™ et VMware vCenter Server® offrent et explique comment configurer et utiliser ces technologies.

VMware prend l'intégration au sérieux. Pour promouvoir ce principe au sein de notre communauté de clients, de partenaires et interne, nous créons du contenu à l'aide d'une langue inclusive.

Public cible

Ces informations s'adressent aux administrateurs système expérimentés qui maîtrisent les technologies de machine virtuelle et de virtualisation de stockage, les opérations associées aux centres de données et les concepts de stockage SAN.

Présentation du stockage dans l'environnement vSphere

vSphere prend en charge diverses fonctionnalités et options de stockage dans des environnements de stockage traditionnels et logiciels. Une présentation de haut niveau des éléments et aspects du stockage vSphere vous permet de planifier une stratégie de stockage appropriée pour votre centre de données virtuel.

Ce chapitre contient les rubriques suivantes :

- [Modèles de virtualisation du stockage traditionnel dans un environnement vSphere](#)
- [Modèles de stockage à définition logicielle](#)
- [API de stockage vSphere](#)

Modèles de virtualisation du stockage traditionnel dans un environnement vSphere

En règle générale, la virtualisation de stockage se rapporte à une abstraction logique de ressources de stockage physique et de capacités à partir des machines virtuelles et de leurs applications. ESXi offre la virtualisation de stockage au niveau de l'hôte.

Dans l'environnement vSphere , un modèle traditionnel repose sur les technologies de stockage ainsi que sur les fonctionnalités de virtualisation ESXi et vCenter Server suivantes.

Stockage local et en réseau

Dans les environnements de stockage traditionnels, le processus de gestion de stockage d'ESXi débute avec l'espace de stockage préalloué par votre administrateur stockage sur différents systèmes de stockage. ESXi prend en charge le stockage local et en réseau.

Reportez-vous à la section [Types de stockage physique pris en charge par ESXi](#).

Réseaux de zone de stockage

Un réseau de zone de stockage (SAN) est un réseau à haute vitesse spécialisé qui connecte des systèmes informatiques, ou des hôtes ESXi, à des systèmes de stockage à hautes performances. L'ESXi peut utiliser les protocoles Fibre Channel ou iSCSI pour se connecter aux systèmes de stockage.

Reportez-vous à la section [Utilisation d'ESXi avec un SAN](#).

Fibre Channel

Fibre Channel (FC) est un protocole de stockage que le SAN utilise pour transférer le trafic de données des serveurs d'hôtes ESXi au stockage partagé. Le protocole conditionne les commandes SCSI en trames FC. Pour se connecter au SAN FC, votre hôte utilise des adaptateurs de bus hôte (HBA) Fibre Channel.

Reportez-vous à la section [Chapitre 3 Utilisation d'ESXi avec un SAN Fibre Channel](#).

Internet SCSI

Internet iSCSI (iSCSI) est un protocole de transport SAN qui peut utiliser des connexions Ethernet entre les systèmes informatiques, ou les hôtes ESXi, et les systèmes de stockage à hautes performances. Pour vous connecter aux systèmes de stockage, vos hôtes utilisent des adaptateurs iSCSI matériels ou des initiateurs iSCSI logiciels avec des adaptateurs réseau standard.

Reportez-vous à la section [Chapitre 4 Utilisation d'ESXi avec un SAN iSCSI](#).

Périphérique de stockage ou LUN

Dans le contexte ESXi, les termes « périphérique de stockage » et « LUN » sont utilisés de manière interchangeable. En général, les deux termes signifient un volume de stockage qui est présenté à l'hôte à partir d'un système de stockage des blocs et qui est disponible pour le formatage.

Reportez-vous aux sections [Représentations de périphériques et de cibles](#) et [Chapitre 6 Gestion des périphériques de stockage](#).

Disques virtuels

Une machine virtuelle sur un hôte ESXi utilise un disque virtuel pour stocker son système d'exploitation, les fichiers d'applications et d'autres données liées à ses activités. Les disques virtuels sont des fichiers physiques volumineux, ou des ensembles de fichiers, qui peuvent être copiés, déplacés, archivés et sauvegardés comme n'importe quel autre fichier. Vous pouvez configurer les machines virtuelles avec plusieurs disques virtuels.

Pour accéder aux disques virtuels, une machine virtuelle utilise des contrôleurs virtuels NVMe ou SCSI. Ces contrôleurs virtuels incluent BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, VMware Paravirtual, NVMe, etc.

Chaque disque virtuel réside sur une banque de données qui est déployée sur un stockage physique. Du point de vue de la machine virtuelle, chaque disque virtuel apparaît comme un lecteur SCSI ou NVMe connecté à un contrôleur SCSI ou NVMe. Que le stockage physique soit accessible via des adaptateurs de stockage ou des adaptateurs réseau sur l'hôte, il est généralement transparent pour le système d'exploitation invité et les applications sur la machine virtuelle.

Pour plus d'informations sur la configuration des contrôleurs pour les machines virtuelles, reportez-vous à la section [Conditions, limitations et compatibilité des contrôleurs de stockage SCSI, SATA et NVMe](#).

VMware vSphere® VMFS

Les banques de données que vous déployez sur des périphériques de stockage des blocs utilise le format VMFS (vSphere Virtual Machine File System) natif. Il s'agit d'un format de système de fichiers haute performance qui est optimisé pour stocker les machines virtuelles.

Reportez-vous à la section [Concepts de banque de données VMFS](#).

NFS

Un client NFS intégré dans ESXi utilise le protocole NFS (Network File System) sur TCP/IP pour accéder à un volume NFS qui se trouve sur un serveur NAS. L'hôte ESXi peut monter le volume et l'utiliser comme une banque de données NFS.

Reportez-vous à la section [Concepts et opérations de banque de données NFS](#).

Mappage de périphérique brut

En plus des disques virtuels, vSphere propose un mécanisme appelé mappage de périphérique brut (RDM). Le RDM est utile lorsqu'un système d'exploitation invité dans une machine virtuelle requiert un accès direct à un périphérique de stockage. Pour plus d'informations sur les RDM, consultez [Chapitre 11 Mappage de périphérique brut](#).

Modèles de stockage à définition logicielle

Outre l'abstraction des capacités de stockage sous-jacentes des machines virtuelles, à l'instar des modèles de stockage traditionnels, le stockage défini par le logiciel crée une abstraction des capacités de stockage.

Avec le modèle de stockage à définition logicielle, une machine virtuelle devient une unité de provisionnement de stockage et peut être gérée au moyen d'un mécanisme flexible basé sur la stratégie. Le modèle implique les technologies vSphere suivantes.

VMware vSphere® Virtual Volumes™ (vVols)

La fonctionnalité Virtual Volumes modifie le paradigme de gestion du stockage de la gestion de l'espace au sein de banques de données à la gestion d'objets de stockage abstraits par des baies de stockage. Avec Virtual Volumes, une machine virtuelle individuelle, pas la banque de données, devient une unité de gestion de stockage. Par ailleurs, le matériel de stockage possède le contrôle complet sur le contenu, l'architecture et la gestion des disques virtuels.

Reportez-vous à la section [Chapitre 14 Utilisation de VMware vSphere Virtual Volumes](#).

VMware vSAN

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

Reportez-vous à la section [Administration de VMware vSAN](#).

Gestion basée sur une stratégie de stockage (SPBM, Storage Policy Based Management)

SPBM est une infrastructure qui fournit un panneau de commande unique pour les différents services de données et différentes solutions de stockage, notamment vSAN et Virtual Volumes. À l'aide des stratégies de stockage, l'infrastructure aligne les demandes d'applications de vos machines virtuelles avec les fonctionnalités proposées par les entités de stockage.

Reportez-vous à la section [Chapitre 12 Gestion basée sur des stratégies de stockage \(SPBM, Storage Policy Based Management\)](#).

Filtres d'E/S

Les filtres d'E/S sont des composants logiciels pouvant être installés sur les hôtes ESXi et offrir des services de données supplémentaires aux machines virtuelles. En fonction de la mise en œuvre, les services peuvent inclure la réplication, le chiffrement, la mise en cache, etc.

Reportez-vous à la section [Chapitre 15 Filtrage des E/S de machines virtuelles](#).

API de stockage vSphere

Les API de stockage représentent une famille d'API utilisée par des fournisseurs tiers de matériels, de logiciels et de stockage pour développer des composants qui améliorent plusieurs fonctionnalités et solutions de vSphere.

Cette publication de stockage décrit plusieurs API de stockage qui constituent votre environnement de stockage. Pour plus d'informations sur d'autres API de cette famille, notamment vSphere APIs - Data Protection, rendez-vous sur le site Web de VMware.

VASA (vSphere APIs for Storage Awareness)

Les API VASA, proposées par des distributeurs tiers ou par VMware, permettent les communications entre vCenter Server et le stockage sous-jacent. Via VASA, les entités de stockage peuvent indiquer à vCenter Server leurs configurations, leurs capacités, ainsi que des informations concernant la santé et les événements de stockage. En retour, VASA peut transmettre des conditions requises de stockage de machine virtuelle depuis vCenter Server vers une entité de stockage et ainsi garantir que la couche de stockage répond aux conditions requises.

VASA devient essentiel lorsque vous utilisez Virtual Volumes, vSAN, VAIO (vSphere APIs for I/O Filtering) et des stratégies de machine virtuelle de stockage. Reportez-vous à [Chapitre 13 Utilisation de fournisseurs de stockage](#).

VAAI (vSphere APIs for Array Integration)

Les API VAAI incluent les composants suivants :

- API d'accélération matérielle. Permet aux baies de s'intégrer à vSphere afin que vSphere puisse décharger certaines opérations de stockage sur la baie. Cette intégration réduit considérablement la surcharge du CPU sur l'hôte. Reportez-vous à [Chapitre 16 Accélération matérielle du stockage](#).
- API à provisionnement dynamique de la baie. Permet de surveiller l'utilisation de l'espace sur les baies de stockage à provisionnement dynamique pour empêcher des conditions de manque d'espace et pour effectuer une réclamation d'espace. Reportez-vous à [ESXi et provisionnement dynamique de la baie](#).

API vSphere pour gestion de chemins multiples

Connues sous l'appellation PSA (Pluggable Storage Architecture), ces API permettent aux partenaires de stockage de créer et de fournir des plug-ins de gestion de chemins multiples et d'équilibrage de charge optimisés pour chaque baie. Les plug-ins communiquent avec les baies de stockage et déterminent la meilleure stratégie de sélection de chemins pour augmenter les performances d'E/S et la fiabilité de l'hôte ESXi vers la baie de stockage. Pour plus d'informations, consultez [Architecture de stockage enfichable et gestion des chemins](#).

Démarrage avec un modèle de stockage traditionnel dans un environnement vSphere

La configuration de votre stockage ESXi dans les environnements traditionnels comprend la configuration des systèmes et périphériques de stockage, l'activation des adaptateurs de stockage et la création de banques de données.

Ce chapitre contient les rubriques suivantes :

- Types de stockage physique pris en charge par ESXi
- Affichage des périphériques de stockage disponibles pour un hôte ESXi
- Adaptateurs de stockage disponibles sur un hôte ESXi
- Caractéristiques des banques de données ESXi
- Utilisation de périphériques à mémoire persistante avec ESXi
- Utilisation d'ESXi avec un SAN

Types de stockage physique pris en charge par ESXi

Dans les environnements de stockage traditionnels, le processus de gestion de stockage d'ESXi débute avec l'espace de stockage préalloué par votre administrateur stockage sur différents systèmes de stockage. ESXi prend en charge le stockage local et en réseau.

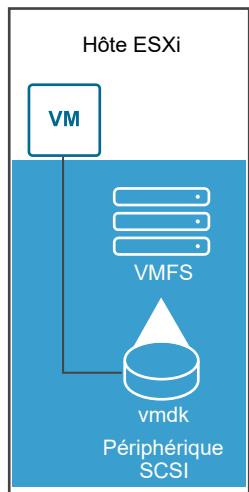
Stockage local

Le stockage local peut se composer de disques durs internes situés à l'intérieur de votre hôte ESXi. Il peut également inclure des systèmes de stockage externes situés à l'extérieur et connectés directement à l'hôte par le biais de protocoles tels que SAS ou SATA.

Le stockage local ne requiert pas de réseau de stockage pour communiquer avec votre hôte. Vous avez besoin d'un câble connecté à l'unité de stockage et, si nécessaire, d'un HBA compatible dans votre hôte.

L'illustration suivante décrit une machine virtuelle utilisant un stockage SCSI local.

Figure 2-1. Stockage local



Dans cet exemple de topologie de stockage local, l'hôte ESXi utilise une connexion unique à un périphérique de stockage. Sur ce périphérique, vous pouvez créer une banque de données VMFS que vous utilisez pour stocker les fichiers de disque de la machine virtuelle.

Bien que cette configuration de stockage soit possible, elle n'est pas recommandée. L'utilisation de connexions uniques entre des périphériques de stockage et des hôtes crée des points de défaillance uniques (SPOF) pouvant causer des interruptions lorsqu'une connexion devient instable ou échoue. Toutefois, puisque la plupart des périphériques de stockage local ne prennent pas en charge les connexions multiples, vous ne pouvez pas utiliser plusieurs chemins d'accès pour accéder au stockage local.

ESXi prend en charge divers périphériques de stockage local, notamment SCSI, IDE, SATA, USB, SAS, Flash et les périphériques NVMe.

Note Vous ne pouvez pas utiliser de lecteurs IDE/ATA ou USB pour stocker des machines virtuelles.

Le stockage local ne prend pas en charge le partage sur plusieurs hôtes. Seul un hôte peut accéder à une banque de données sur un périphérique de stockage local. Par conséquent, bien que vous puissiez utiliser un stockage local pour créer des machines virtuelles, vous ne pouvez pas utiliser les fonctionnalités de VMware qui exigent un stockage partagé, telles que HA et vMotion.

Cependant, si vous utilisez un cluster d'hôtes disposant uniquement de périphériques de stockage local, vous pouvez implémenter vSAN. vSAN transforme des ressources de stockage locales en stockage partagé défini par logiciel. Avec vSAN, vous pouvez utiliser des fonctionnalités qui exigent un stockage partagé. Pour plus d'informations, voir la documentation *Administration de VMware vSAN*.

Stockage en réseau

Le stockage en réseau est composé de systèmes de stockage externes que votre hôte ESXi utilise pour stocker des fichiers de machine virtuelle à distance. En règle générale, l'hôte accède à ces systèmes sur un réseau de stockage haut-débit.

Les périphériques de stockage en réseau sont partagés. Les banques de données sur des périphériques de stockage en réseau sont accessibles par plusieurs hôtes simultanément. ESXi prend en charge plusieurs technologies de stockage en réseau.

Outre le stockage en réseau traditionnel abordé dans cette rubrique, VMware prend en charge les technologies de stockage partagé virtualisé telles que vSAN. vSAN transforme les ressources de stockage internes de vos hôtes ESXi en stockage partagé qui fournit des fonctionnalités telles que High Availability et vMotion aux machines virtuelles. Pour plus d'informations, voir la documentation *Administration de VMware vSAN*.

Note Un même LUN ne peut pas être présenté à un hôte ESXi ou à plusieurs hôtes via différents protocoles de stockage. Pour accéder au LUN, les hôtes doivent toujours utiliser un seul protocole, par exemple uniquement Fibre Channel ou uniquement iSCSI.

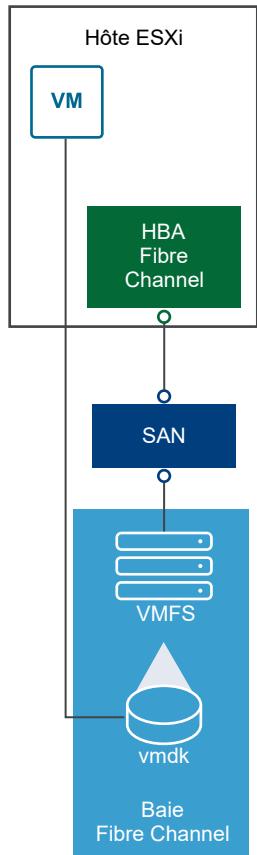
Fibre Channel (FC)

Stocke des fichiers de machine virtuelle à distance sur un réseau de zone de stockage FC (SAN). FC SAN est un réseau haut débit spécialisé qui connecte vos hôtes à des périphériques de stockage haute performance. Le réseau utilise le protocole Fibre Channel pour acheminer le trafic SCSI ou NVMe depuis des machines virtuelles vers des périphériques FC SAN.

Pour se connecter au FC SAN, votre hôte doit être équipé d'adaptateurs de bus hôte (HBA) Fibre Channel. À moins d'utiliser un stockage de connexion directe Fibre Channel, vous avez besoin de commutateurs Fibre Channel pour acheminer le trafic de stockage. Si votre hôte contient des adaptateurs FCoE (Fibre Channel over Ethernet), vous pouvez vous connecter à vos périphériques Fibre Channel partagés à l'aide d'un réseau Ethernet.

Stockage Fibre Channel décrit les machines virtuelles utilisant le stockage Fibre Channel.

Figure 2-2. Stockage Fibre Channel



Dans cette configuration, un hôte se connecte à une infrastructure SAN, qui est constituée de commutateurs Fibre Channel et de baies de stockage, en utilisant un adaptateur Fibre Channel. Les LUN d'une baie de stockage deviennent disponibles pour l'hôte. Vous pouvez accéder aux LUN et créer des banques de données pour vos besoins de stockage. Les banques de données utilisent le format VMFS.

Pour plus d'informations spécifiques sur la configuration du SAN Fibre Channel, consultez [Chapitre 3 Utilisation d'ESXi avec un SAN Fibre Channel](#).

Internet SCSI (iSCSI)

Stocke des fichiers de machine virtuelle sur des périphériques de stockage iSCSI à distance. iSCSI rassemble le trafic de stockage SCSI dans le protocole TCP/IP, de sorte qu'il puisse être acheminé via des réseaux TCP/IP standard et non le réseau FC spécialisé. Grâce à une connexion iSCSI, votre hôte sert d'initiateur qui communique avec une cible, située dans des systèmes de stockage iSCSI à distance.

ESXi offre les types de connexions iSCSI suivants :

iSCSI matériel

Votre hôte se connecte au stockage via un adaptateur tiers capable de décharger la gestion de réseau et iSCSI. Les adaptateurs matériels peuvent être dépendants et indépendants.

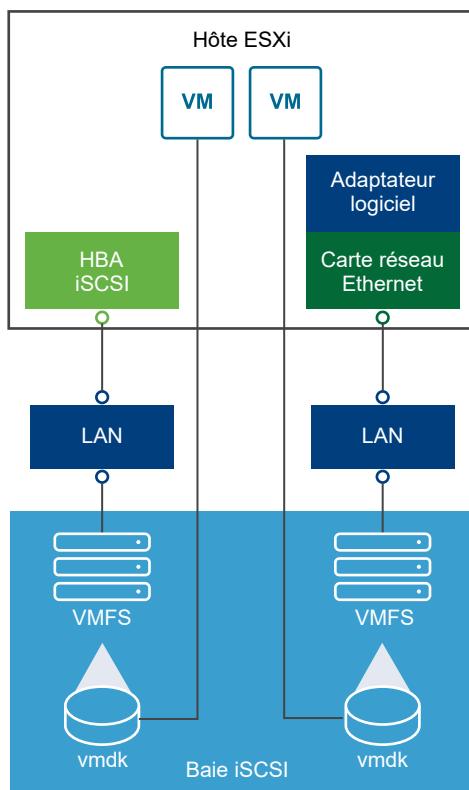
iSCSI logiciel

Votre hôte utilise un initiateur iSCSI logiciel dans le VMkernel pour se connecter au stockage. Avec ce type de connexion iSCSI, votre hôte ne requiert qu'un adaptateur réseau standard pour la connectivité réseau.

Vous devez configurer les initiateurs iSCSI de l'hôte pour qu'il accède et affiche les périphériques de stockage iSCSI.

Le stockage iSCSI décrit différents types d'initiateurs iSCSI.

Figure 2-3. Stockage iSCSI



Dans l'exemple de gauche, l'hôte utilise l'adaptateur iSCSI matériel pour se connecter au système de stockage iSCSI.

Dans l'exemple de droite, l'hôte utilise un adaptateur iSCSI logiciel et un adaptateur d'interface réseau Ethernet pour se connecter au stockage iSCSI.

Les périphériques de stockage iSCSI du système de stockage deviennent disponibles pour l'hôte. Vous pouvez accéder aux périphériques de stockage et créer des banques de données VMFS pour vos besoins de stockage.

Pour plus d'informations spécifiques sur la configuration du SAN iSCSI, consultez [Chapitre 4 Utilisation d'ESXi avec un SAN iSCSI](#).

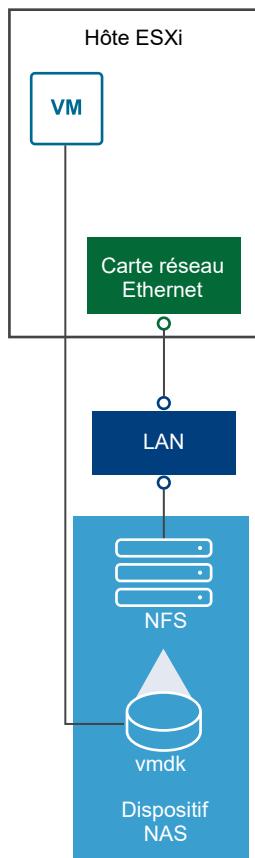
Stockage relié au réseau (NAS)

Stocke les fichiers de machine virtuelle sur des serveurs de fichiers à distance accessibles sur un réseau TCP/IP standard. Le client NFS intégré dans ESXi utilise le protocole NFS (Network File System) versions 3 et 4.1 pour communiquer avec les serveurs NAS/NFS. Pour une connectivité réseau, l'hôte requiert un adaptateur réseau standard.

Vous pouvez monter un volume NFS directement sur l'hôte ESXi. Vous utilisez ensuite des banques de données NFS pour stocker et gérer des machines virtuelles de la même manière que vous utilisez des banques de données VMFS.

Stockage NFS décrit une machine virtuelle utilisant la banque de données NFS pour stocker ses fichiers. Dans cette configuration, l'hôte se connecte au serveur NAS stockant les fichiers du disque virtuel via un adaptateur réseau normale.

Figure 2-4. Stockage NFS



Pour des informations spécifiques sur la configuration du stockage NFS, consultez [Concepts et opérations de banque de données NFS](#).

SAS (Serial Attached SCSI) partagé

Stocke des machines virtuelles sur des systèmes de stockage directement reliés au SAS qui offrent un accès partagé à plusieurs hôtes. Ce type d'accès permet à plusieurs hôtes d'accéder à la même banque de données VFMS sur un LUN.

Stockage NVMe over Fabrics

VMware NVMe over Fabrics (NVMe-oF) fournit une connectivité à distance entre un hôte et un périphérique de stockage cible sur une baie de stockage partagée. VMware prend en charge différentes technologies, notamment NVMe over RDMA (avec la technologie RoCE v2), NVMe over Fibre Channel et NVMe over TCP/IP. Pour plus d'informations, consultez [Chapitre 8 À propos du stockage VMware NVMe](#).

Comparaison des types de stockage

La prise en charge de certaines fonctionnalités de vSphere peut dépendre de la technologie de stockage que vous utilisez.

Le tableau suivant compare les technologies de stockage en réseau pris en charge par ESXi.

Tableau 2-1. Stockage en réseau pris en charge par ESXi

Technologie	Protocoles	Transferts	Interface
Fibre Channel	FC/SCSI, FC/NVMe	Bloquer l'accès de données/LUN	FC HBA
Fibre Channel sur Ethernet	FCoE/SCSI	Bloquer l'accès de données/LUN	Adaptateur réseau convergé (FCoE matériel)
iSCSI	IP/SCSI	Bloquer l'accès de données/LUN	<ul style="list-style-type: none"> ■ Carte NIC compatible iSCSI HBA ou iSCSI (iSCSI matériel) ■ Adaptateur réseau (iSCSI logiciel)
NAS	IP/NFS	Fichier (pas d'accès direct à LUN)	Adaptateur réseau

Le tableau suivant compare les fonctions de vSphere pris en charge par différents types de stockage.

Tableau 2-2. Fonctions vSphere pris en charge par le stockage

Type de stockage	Démarrage VM	vMotion	Banque de données	RDM	Cluster VM	VMware HA et DRS	API de stockage - Protection
Stockage local	Oui	Non	VMFS	Non	Oui	Non	Oui
Fibre Channel	Oui	Oui	VMFS	Oui	Oui	Oui	Oui

Tableau 2-2. Fonctions vSphere pris en charge par le stockage (suite)

Type de stockage	Démarrage VM	vMotion	Banque de données	RDM	Cluster VM	VMware HA et DRS	API de stockage - Protection
iSCSI	Oui	Oui	VMFS	Oui	Oui	Oui	Oui
NAS sur NFS	Oui	Oui	NFS 3 et NFS 4.1	Non	Non	Oui	Oui

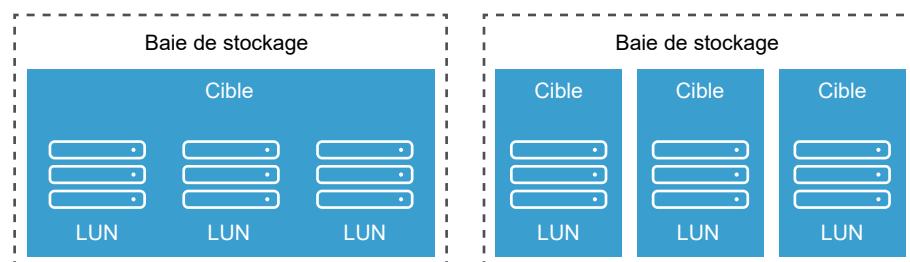
Note Le stockage local prend en charge un cluster de machines virtuelles sur un seul hôte (connu également sous le nom cluster dans une boîte). Un disque virtuel partagé est requis. Pour plus d'informations sur cette configuration, consultez la documentation *Gestion des ressources vSphere*.

Représentations de périphériques et de cibles

Dans un contexte ESXi, le terme cible identifie une unité de stockage unique accessible par l'hôte. Les termes périphérique de stockage et LUN décrivent un volume logique représentant l'espace de stockage sur une cible. Dans le contexte ESXi, les deux termes signifient également un volume de stockage présenté à l'hôte à partir d'une unité de stockage cible et disponible pour le formatage. Périphérique de stockage et LUN sont souvent interchangeables.

Différents fournisseurs de stockage présentent les systèmes de stockage pour les hôtes ESXi de différentes manières. Certains fournisseurs présentent une cible unique comportant plusieurs LUN ou périphériques de stockage, tandis que d'autres proposent plusieurs cibles disposant chacune d'un LUN.

Figure 2-5. Représentations LUN et de cibles



Dans cette illustration, trois LUN sont disponibles pour chaque configuration. Dans un cas, l'hôte se connecte à une cible, mais cette cible comporte trois LUN à utiliser. Chaque LUN représente un volume de stockage individuel. Dans l'autre exemple, l'hôte détecte trois cibles différentes, chacune disposant d'un LUN.

Les cibles accessibles via le réseau ont des noms uniques fournis par les systèmes de stockage. Les cibles iSCSI utilisent des noms iSCSI, alors que les cibles Fibre Channel utilisent des noms mondiaux dits Noms mondiaux (WWN).

Note ESXi ne prend pas en charge l'accès au même LUN via différents protocoles de transport, tels que iSCSI et Fibre Channel.

Un périphérique, ou LUN, est identifié par son nom UUID. Si un LUN est partagé par plusieurs hôtes, il doit être présenté à tous les hôtes ayant le même UUID.

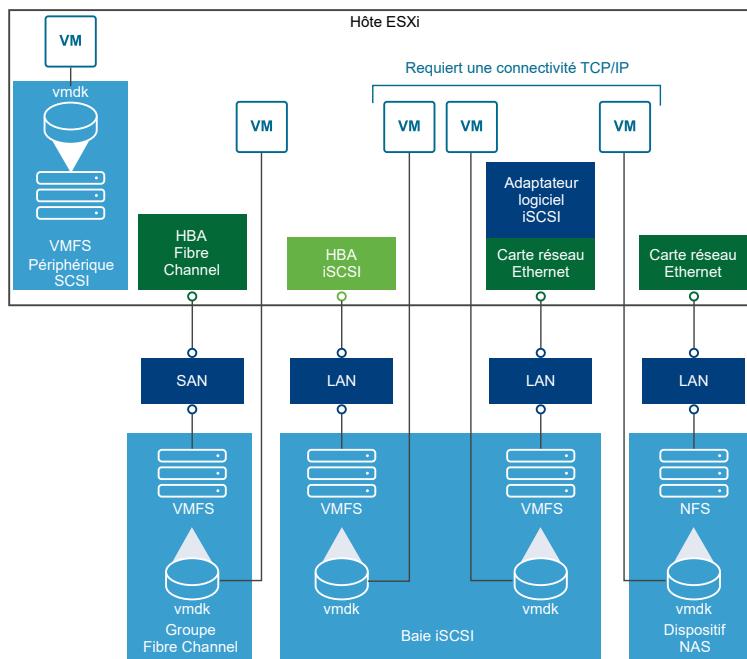
Accès des machines virtuelles au stockage

Lorsqu'une machine virtuelle communique avec son disque virtuel stocké sur une banque de données, elle lance des commandes SCSI ou NVMe. Étant donné que les banques de données peuvent résider sur plusieurs types de stockage physique, ces commandes sont encapsulées dans d'autres formes, selon le protocole utilisé par l'hôte ESXi pour se connecter à un périphérique de stockage.

Quel que soit le type de périphérique de stockage utilisé par votre hôte, le disque virtuel apparaît toujours en tant que périphérique SCSI ou NVMe monté pour la machine virtuelle. Le disque virtuel masque une couche de stockage physique au système d'exploitation de la machine virtuelle. Cette action permet d'exécuter des systèmes d'exploitation non certifiés pour un équipement de stockage spécifique, tel que SAN, dans une machine virtuelle.

L'illustration suivante décrit cinq machines virtuelles utilisant différents types de stockage afin d'illustrer leurs différences.

Figure 2-6. Machines virtuelles accédant à différents types de stockage



Note Ce diagramme est uniquement destiné à des fins conceptuelles. Ce n'est pas une configuration recommandée.

Affichage des périphériques de stockage disponibles pour un hôte ESXi

Lorsque votre hôte ESXi se connecte aux systèmes de stockage basés sur des blocs, les LUN ou les périphériques de stockage prenant en charge l'ESXi deviennent disponibles pour l'hôte.

Une fois les périphériques enregistrés avec votre hôte, vous pouvez afficher tous les périphériques réseau et locaux disponibles et vérifier leurs informations. Si vous utilisez des plug-ins de gestion multivoie tiers, les périphériques de stockage disponibles via les plug-ins apparaissent également dans la liste.

Note Si une baie prend en charge la fonction ALUA (Asymmetric Logical Unit Access) implicite et qu'elle possède seulement des chemins inactifs, l'enregistrement du périphérique échoue. Le périphérique peut s'enregistrer auprès de l'hôte une fois que la cible active un chemin inactif et que l'hôte détecte le chemin comme actif. Le paramètre `/Disk/FailDiskRegistration` système avancé contrôle ce comportement de l'hôte.

Pour chaque adaptateur de stockage, vous pouvez afficher une liste distincte de périphériques de stockage disponibles pour cet adaptateur.

En règle générale, lorsque vous consultez les périphériques de stockages, vous voyez les informations suivantes.

Informations du périphérique de stockage	Description
Nom	Appelé également Nom d'affichage. C'est un nom que l'hôte ESXi affecte à un périphérique selon le type de stockage et le fabricant. Vous pouvez généralement remplacer ce nom par le nom de votre choix. Reportez-vous à la section Renommer des périphériques de stockage .
Identificateur	Identificateur universel unique intrinsèque au périphérique. Reportez-vous à la section Noms et identifiants de périphérique de stockage ESXi .
État opérationnel	Indique si le périphérique est attaché ou détaché. Reportez-vous à la section Déconnexion des périphériques de stockage .
LUN	LUN (Logical Unit Number) à l'intérieur de la cible SCSI. Le numéro de LUN est fourni par le système de stockage. Si une cible possède un seul LUN, le numéro de LUN est toujours zéro (0). Reportez-vous à la section Représentations de périphériques et de cibles .
Type	Type de périphérique, par exemple, disque ou CD-ROM.
Type de lecteur	Informations précisant si le périphérique est en lecteur Flash ou un simple disque dur. Pour plus d'informations sur les lecteurs Flash et les périphériques NVMe, reportez-vous à Chapitre 7 Utilisation de périphériques Flash avec les hôtes ESXi .
Transport	Protocole de transport utilisé par votre hôte pour accéder au périphérique. Le protocole dépend du type de stockage utilisé. Reportez-vous à la section Types de stockage physique pris en charge par ESXi .
Capacité	Capacité totale du périphérique de stockage.
Propriétaire	Le plug-in, tel que le NMP ou un plug-in tiers, que l'hôte utilise pour gérer les chemins vers le périphérique de stockage. Reportez-vous à la section Architecture de stockage enfichable et gestion des chemins .
Accélération matérielle	Informations indiquant que le périphérique de stockage assiste l'hôte avec des opérations de gestion de machine virtuelle. L'état peut être Pris en charge, Non pris en charge ou Inconnu. Reportez-vous à la section Chapitre 16 Accélération matérielle du stockage .
Format de secteur	Indique si le périphérique utilise un format de secteur traditionnel, 512n ou avancé, tel que 512e ou 4Kn. Reportez-vous à la section Formats de secteur des périphériques .
Emplacement	Chemin d'accès au périphérique de stockage dans l'inventaire /vmfs/devices/.
Format de partition	Un système de partition utilisé par le périphérique de stockage. Ce peut être un format MBR (master boot record) ou un format GPT (GUID partition table). Les périphériques GPT peuvent prendre en charge des banques de données d'une taille supérieure à 2 To. Reportez-vous à la section Formats de secteur des périphériques .
Partitions	Partitions logiques et principales, y compris une banque de données VMFS, si configurée. Reportez-vous à la section Chapitre 9 Utilisation des banques de données .
Règles de gestion multivoie	Stratégie de sélection de chemin et règle de type de baie de stockage utilisées par l'hôte pour gérer les chemins de stockage. Reportez-vous à la section Chapitre 10 Présentation de la gestion multivoie et du basculement .
Chemins	Chemins utilisés pour accéder au stockage et leur état. Reportez-vous à la section Désactiver les chemins de stockage .

Affichage des périphériques de stockage d'un hôte ESXi

Afficher tous les périphériques de stockage disponibles pour un hôte ESXi. Si vous utilisez des plug-ins de gestion multivoie tiers, les périphériques de stockage disponibles via les plug-ins apparaissent également dans la liste.

La vue Périphériques de stockage vous permet de répertorier les périphériques de stockage des hôtes, d'analyser leurs informations et de modifier leurs propriétés.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Périphériques de stockage**.

Tous les périphériques de stockage accessibles par l'hôte sont répertoriés dans le tableau Périphériques de stockage.

- 4 Pour afficher les détails d'un périphérique spécifique, sélectionnez-le dans la liste.
- 5 Utilisez les icônes pour effectuer des tâches de gestion du stockage de base.
La disponibilité d'icônes spécifiques varie selon le type et la configuration du périphérique.
- 6 Utilisez les onglets suivants pour accéder à des informations supplémentaires et modifiez les propriétés du périphérique sélectionné.

Onglet	Description
Propriétés	Afficher les propriétés et caractéristiques du périphérique. Afficher et modifier les stratégies de gestion multivoie du périphérique. Reportez-vous à la section Affichage et gestion des chemins .
Chemins	Afficher les chemins disponibles pour le périphérique. Désactivez ou activez un chemin sélectionné. Reportez-vous à la section Désactiver les chemins de stockage .
Détails de la partition	Affiche des informations sur les partitions et leurs formats.

Affichage des périphériques de stockage d'un adaptateur

Afficher une liste des périphériques de stockage accessibles grâce à un adaptateur de stockage spécifique sur un hôte ESXi.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**.

Tous les adaptateurs de stockage installés sur l'hôte sont répertoriés dans le tableau Adaptateurs de stockage.

- 4** Sélectionnez l'adaptateur dans la liste et cliquez sur l'onglet **Périphériques**.

Les périphériques de stockage auxquels l'hôte peut accéder grâce à l'adaptateur sont affichés.

- 5** Utilisez les icônes pour effectuer des tâches de gestion du stockage de base.

La disponibilité d'icônes spécifiques varie selon le type et la configuration du périphérique.

Icône	Description
Régénérer	Actualiser les informations sur les adaptateurs de stockage, la topologie et les systèmes de fichiers.
Déconnexion des périphériques de stockage	Détacher le périphérique sélectionné de l'hôte.
Joindre des périphériques de stockage	Attacher le périphérique sélectionné à l'hôte.
Renommer des périphériques de stockage	Modifier le nom complet du périphérique sélectionné.
Utiliser le voyant de localisation sur les périphériques de stockage ESXi	Allumer le voyant du localisateur pour les périphériques sélectionnés.
Utiliser le voyant de localisation sur les périphériques de stockage ESXi	Éteindre le voyant du localisateur pour les périphériques sélectionnés.
Marquage de périphériques de stockage sur des hôtes ESXi	Marquer les périphériques sélectionnés en tant que disques Flash.
Marquage de périphériques de stockage sur des hôtes ESXi	Marquer les périphériques sélectionnés en tant que disques HDD.
Marquage de périphériques de stockage sur des hôtes ESXi	Marquer les périphériques sélectionnés en tant que locaux pour l'hôte.
Marquage de périphériques de stockage sur des hôtes ESXi	Marquer les périphériques sélectionnés en tant que distants pour l'hôte.
Effacer des périphériques de stockage	Effacer les partitions sur les périphériques sélectionnés.
Modifier les paramètres de réservation perpétuelle	Marquer le périphérique sélectionné comme étant perpétuellement réservé.
Modifier les paramètres de réservation perpétuelle	Effacez la réservation perpétuelle du périphérique sélectionné.

Adaptateurs de stockage disponibles sur un hôte ESXi

Les adaptateurs de stockage assurent la connectivité de votre hôte ESXi à un réseau ou une unité de stockage spécifique. ESXi prend en charge différentes catégories d'adaptateurs, y compris SCSI, NVMe, iSCSI, RAID, Fibre Channel, Fibre Channel over Ethernet (FCoE) et Ethernet. ESXi accède directement aux adaptateurs via des pilotes de périphériques dans le VMkernel.

Selon le type de stockage utilisé, vous devrez peut-être activer ou configurer un adaptateur de stockage sur votre hôte.

Vous pouvez afficher les informations des adaptateurs de stockage disponibles et les vérifier.

Conditions préalables

Vous devez activer certains adaptateurs, par exemple l'adaptateur iSCSI logiciel, pour pouvoir afficher leurs informations. Pour configurer les adaptateurs, reportez-vous à la section [Chapitre 5 Configuration des adaptateurs iSCSI et iSER et du stockage](#).

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**.
- 4 Utilisez les icônes pour effectuer des tâches liées aux adaptateurs de stockage.

La disponibilité d'icônes spécifiques dépend de la configuration du stockage.

Icône	Description
Ajouter un adaptateur logiciel	Ajoutez un adaptateur de stockage. Applicable à l'adaptateur iSCSI logiciel.
Régénérer	Actualisez les informations sur les adaptateurs de stockage, la topologie et les systèmes de fichiers de l'hôte.
Réanalyser le stockage	Réanalyser tous les adaptateurs de stockage de l'hôte pour découvrir les périphériques de stockage ou les banques de données VMFS récemment ajoutés.
Réanalyser un adaptateur	Réanalysez l'adaptateur sélectionné pour détecter les périphériques de stockage nouvellement ajoutés.

- 5 Pour afficher les détails d'un adaptateur spécifique, sélectionnez-le dans la liste.
- 6 Utilisez les onglets dans Détails adaptateur pour accéder à des informations supplémentaires et modifier les propriétés de l'adaptateur sélectionné.

Onglet	Description
Propriétés	Vérifiez les propriétés générales de l'adaptateur qui incluent généralement le nom et le modèle de l'adaptateur, ainsi que les identifiants uniques formés selon les normes de stockage spécifiques. Pour certains types d'adaptateurs, vous pouvez utiliser cet onglet pour configurer des propriétés supplémentaires, par exemple l'authentification.
Périphériques	Affichez les périphériques de stockage auxquels l'adaptateur peut accéder. Utilisez l'onglet pour effectuer des tâches de gestion de périphériques de base. Reportez-vous à la section Affichage des périphériques de stockage d'un adaptateur .
Chemins	Repérez et gérez tous les chemins que l'adaptateur utilise pour accéder aux périphériques de stockage.
Cibles (Fibre Channel et iSCSI)	Vérifiez et gérez les cibles accessibles via l'adaptateur.
Liaison de port réseau (iSCSI uniquement)	Configurez la liaison de port des logiciels et adaptateurs iSCSI matériels dépendants.
Options avancées (iSCSI uniquement)	Configurez les paramètres avancés d'iSCSI.

Caractéristiques des banques de données ESXi

Les banques de données sont des conteneurs logiques, analogues à des systèmes de fichiers, qui masquent les informations de chaque périphérique de stockage et fournissent un modèle uniforme pour stocker des fichiers de machine virtuelle. Vous pouvez afficher toutes les banques de données disponibles pour vos hôtes ESXi et analyser leurs propriétés.

Les banques de données sont ajoutées à vCenter Server de la façon suivante :

- Vous pouvez créer une banque de données VMFS, une banque de données NFS version 3 ou 4.1, ou une banque de données Virtual Volumes à l'aide de l'assistant Nouvelle banque de données. Une banque de données vSAN est automatiquement créée lorsque vous activez vSAN.
- Lorsque vous ajoutez un hôte ESXi à vCenter Server, toutes les banques de données sur l'hôte sont ajoutées à vCenter Server.

Le tableau suivant fournit des informations détaillées sur les banques de données que vous pouvez afficher lorsque vous effectuez une analyse des banques de données avec vSphere Client. Certaines caractéristiques peuvent ne pas être disponibles ou ne pas s'appliquer à tous les types de banques de données.

Tableau 2-3. Informations sur les banque de données

Informations sur les banque de données	Type de banque de données applicable	Description
Nom	VMFS NFS vSAN vVol	Nom modifiable affecté à la banque de données. Pour plus d'informations sur la manière de renommer une banque de données, consultez Modifier le nom d'une banque de données .
Type	VMFS NFS vSAN vVol	Système de fichiers utilisé par la banque de données. Pour plus d'informations sur les banques de données VMFS et NFS et sur la manière de les gérer, reportez-vous à Chapitre 9 Utilisation des banques de données . Pour obtenir des informations sur les banques de données vSAN, reportez-vous à la documentation de Administration de VMware vSAN . Pour plus d'informations sur Virtual Volumes, reportez-vous à Chapitre 14 Utilisation de VMware vSphere Virtual Volumes .
Sauvegarde de périphériques	VMFS NFS vSAN	Informations relatives au stockage sous-jacent, comme le périphérique de stockage sur lequel la banque de données est déployée (VMFS), le serveur et le dossier (NFS) ou les groupes de disques (vSAN).
Points de terminaison de protocole	vVol	Informations sur les points de terminaison du protocole correspondant. Reportez-vous à la section Points de terminaison de protocole .
Extensions	VMFS	Extensions individuelles de la banque de données et capacité correspondante.

Tableau 2-3. Informations sur les banques de données (suite)

Informations sur les banques de données	Type de banque de données applicable	Description
Type de lecteur	VMFS	Type de périphérique de stockage sous-jacent (par exemple, un lecteur Flash ou disque dur ordinaire). Pour des détails, veuillez vous reporter au Chapitre 7 Utilisation de périphériques Flash avec les hôtes ESXi .
Capacité	VMFS NFS vSAN vVol	Inclut la capacité totale, l'espace alloué et l'espace libre.
Point de montage	VMFS NFS vSAN vVol	Chemin d'accès à la banque de données dans le répertoire <code>/vmfs/volumes/</code> de l'hôte.
Ensembles de capacités	VMFS Note Une banque de données VMFS multi-extensions assume les capacités d'une seule de ses extensions. NFS vSAN vVol	Informations sur les services de données de stockage fournies par l'entité de stockage sous-jacente. Vous ne pouvez pas les modifier.
Storage I/O Control	VMFS NFS	Informations sur l'activation de la priorisation E/S du stockage dans l'ensemble des clusters. Consultez la documentation de <i>Gestion des ressources vSphere</i> .
Accélération matérielle	VMFS NFS vSAN vVol	Informations précisant si l'entité de stockage sous-jacente prend en charge l'accélération matérielle. L'état peut être Pris en charge, Non pris en charge ou Inconnu. Pour des détails, veuillez vous reporter au Chapitre 16 Accélération matérielle du stockage . Note NFS 4.1 ne prend pas en charge l'accélération matérielle.
Balises	VMFS NFS vSAN vVol	Capacités de la banque de données que vous définissez et associez à des banques de données sous forme de balises. Pour plus d'informations, consultez Affecter des balises à des banques de données .
Connectivité avec les hôtes	VMFS NFS vVol	Hôtes sur lesquels la banque de données est montée.
Gestion multivoie	VMFS vVol	Règles de sélection de chemin d'accès utilisées par l'hôte pour accéder aux espaces de stockage. Pour plus d'informations, consultez Chapitre 10 Présentation de la gestion multivoie et du basculement .

Afficher les informations relatives aux banques de données

Accédez à la vue Banques de données avec le navigateur de vSphere Client.

Utilisez la vue Banques de données pour répertorier toutes les banques de données disponibles dans l'inventaire d'infrastructure vSphere, analyser les informations et modifier les propriétés.

Procédure

- 1 Accédez à n'importe quel objet de l'inventaire qui est un objet parent valide d'une banque de données, comme un hôte, un cluster ou un centre de données, puis cliquez sur l'onglet **Banques de données**.

Les banques de données disponibles dans l'inventaire figurent dans le panneau central.

- 2 Utilisez les options du menu contextuel d'une banque de données pour effectuer des tâches basiques sur la banque de données sélectionnée.

Les options disponibles varient en fonction du type de la banque de données et de sa configuration.

Option	Description
Enregistrer la VM	Enregistrer une machine virtuelle existante dans l'inventaire. Consultez la documentation de <i>Administration d'une machine virtuelle vSphere</i> .
Augmenter la capacité de la banque de données	Augmenter la capacité de la banque de données VMFS ou ajouter une extension. Reportez-vous à la section Augmenter la capacité d'une banque de données VMFS .
Parcourir les fichiers	Accédez à l'explorateur de fichiers de la banque de données. Reportez-vous à la section Accéder au navigateur de banque de données .
Renommer	Modifier le nom de la banque de données. Reportez-vous à la section Modifier le nom d'une banque de données .
Monter une banque de données	Monter la banque de données sur certains hôtes. Reportez-vous à la section Monter des banques de données .
Démonter une banque de données	Démonter la banque de données de certains hôtes. Reportez-vous à la section Démontage des banques de données .
Mode de maintenance	Utiliser le mode de maintenance de banque de données. Consultez la documentation de <i>Gestion des ressources vSphere</i> .
Configurer Storage I/O Control (VMFS)	Activer Storage I/O Control pour la banque de données VMFS. Consultez la documentation de <i>Gestion des ressources vSphere</i> .
Modifier la récupération d'espace (VMFS)	Modifier les paramètres de récupération d'espace pour la banque de données VMFS. Reportez-vous à la section Configurer la récupération fixe pour la banque de données VMFS6 existante .
Supprimer la banque de données (VMFS)	Supprimer la banque de données VMFS. Reportez-vous à la section Supprimer des banques de données VMFS .
Balises et attributs personnalisés	Utiliser des balises pour coder les informations sur la banque de données. Reportez-vous à la section Affecter des balises à des banques de données .

- 3 Pour afficher les détails d'une banque de données spécifique, cliquez sur une banque de données sélectionnée.

- 4 Utilisez les onglets pour accéder à des informations supplémentaires et modifier les propriétés des banques de données.

Onglet	Description
Résumé	Afficher les statistiques et la configuration de la base de données sélectionnée.
Surveiller	Afficher les alarmes, les données de performance, l'allocation des ressources, les événements et autres informations sur l'état relatives à la banque de données.
Configurer	Afficher et modifier les propriétés de la banque de données. Les éléments de menu qui s'affichent dépendent du type de banque de données.
Autorisations	Attribuer ou modifier les autorisations pour la banque de données sélectionnée.
Fichiers	Accédez à l'explorateur de fichiers de la banque de données.
Hôtes	Affichez les hôtes sur lesquels la banque de données est montée.
VM	Affichez les machines virtuelles résidant sur la banque de données.

Utilisation de périphériques à mémoire persistante avec ESXi

ESXi prend en charge les périphériques à mémoire persistante de nouvelle génération, également appelés périphériques à mémoire non volatile (NVM). Ces périphériques combinent les performances et la vitesse de la mémoire avec la persistance du stockage traditionnel. Ils peuvent conserver les données stockées en cas de redémarrages ou de défaillances de la source d'alimentation.

Les machines virtuelles qui nécessitent une bande passante élevée, une latence faible et la persistance peuvent bénéficier de cette technologie. Il s'agit, par exemple, des machines virtuelles qui fournissent l'accélération des bases de données et l'analyse de la charge de travail.

Pour utiliser la mémoire persistante avec votre hôte ESXi, vous devez être familiarisé avec les concepts suivants.

Banque de données PMem

Une fois la mémoire persistante ajoutée à votre hôte ESXi, l'hôte détecte le matériel, puis le formate et le monte comme une banque de données PMem locale. ESXi utilise VMFS-L comme format de système de fichiers. Une seule banque de données PMem locale par hôte est prise en charge.

Note Lorsque vous gérez la mémoire persistante physique, assurez-vous de supprimer toutes les machines virtuelles de l'hôte et de placer ce dernier en mode de maintenance.

Pour réduire la surcharge administrative, la banque de données PMem offre un modèle de gestion simplifié. Les tâches de banque de données traditionnelles ne s'appliquent généralement pas à la banque de données, car l'hôte effectue automatiquement toutes les opérations requises en arrière-plan. En tant qu'administrateur, vous ne pouvez pas afficher la banque de données dans la vue Banques de données de vSphere Client, ni effectuer d'autres

actions classiques sur la banque de données. La seule opération possible est la surveillance des statistiques pour la banque de données PMem.

La banque de données PMem permet de stocker les périphériques NVDIMM virtuels et les disques virtuels traditionnels d'une machine virtuelle. Le répertoire de base de machine virtuelle contenant les fichiers `vmx` et `vmware.log` ne peut pas être placé sur la banque de données PMem.

Modes d'accès PMem

ESXi expose la mémoire persistante à une machine virtuelle dans deux modes différents. Les machines virtuelles prenant en charge PMem peuvent avoir un accès direct à la mémoire persistante. Les machines virtuelles traditionnelles peuvent utiliser les disques virtuels rapides stockés sur la banque de données PMem.

Mode à accès direct

Dans ce mode, également nommé mode PMem virtuel (vPMem), une région PMem peut être présentée à une machine virtuelle en tant que module NVDIMM (Non-Volatile Dual In-line Memory Module). La machine virtuelle utilise le module NVDIMM comme une mémoire adressable en octets standard pouvant persister pendant les cycles d'alimentation.

Vous pouvez ajouter un ou plusieurs modules NVDIMM lors du provisionnement de la machine virtuelle.

Les machines virtuelles doivent être dans la version matérielle ESXi 6.7 ou version ultérieure, et disposer d'un système d'exploitation invité prenant en charge PMem. Le périphérique NVDIMM est compatible avec les systèmes d'exploitation invités les plus récents qui prennent en charge la mémoire persistante, par exemple, Windows 2016.

Chaque périphérique NVDIMM est automatiquement stocké sur la banque de données PMem.

Mode de disque virtuel

Ce mode, également nommé mode de disques PMem virtuels (vPMemDisk), est disponible sur toute machine virtuelle traditionnelle et il prend en charge n'importe quelle version matérielle, y compris toutes les versions héritées. Il n'est pas nécessaire que les machines virtuelles prennent en charge PMem. Lorsque vous utilisez ce mode, vous créez un disque virtuel SCSI standard et associez une stratégie de stockage de machine virtuelle PMem au disque. La stratégie place automatiquement le disque sur la banque de données PMem.

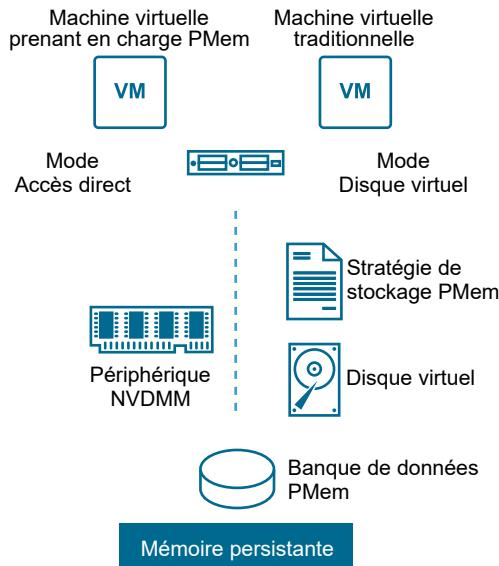
Stratégie de stockage PMem

Pour placer le disque virtuel sur la banque de données PMem, vous devez appliquer la stratégie de stockage PMem locale de l'hôte par défaut sur le disque. La stratégie n'est pas modifiable.

Elle ne peut être appliquée qu'aux disques virtuels. Étant donné que le répertoire de base de machine virtuelle ne se trouve pas sur la banque de données PMem, veillez à le placer sur une banque de données standard quelconque.

Après avoir attribué la stratégie de stockage PMem pour le disque virtuel, vous ne pouvez pas la modifier via la boîte de dialogue **Modifier les paramètres VM**. Pour modifier la stratégie, migrez la machine virtuelle ou clonez-la.

Le graphique suivant illustre la façon dont les composants de mémoire persistante interagissent.



Pour plus d'informations sur la configuration et la gestion de machines virtuelles dotées de modules NVDIMM ou de disques virtuels à mémoire persistante, consultez la documentation *Gestion des ressources vSphere* et *Administration d'une machine virtuelle vSphere*.

Surveiller les statistiques de la banque de données PMem

Vous pouvez utiliser vSphere Client et la commande esxcli pour vérifier la capacité de la banque de données PMem et certains de ses autres attributs.

Cependant, contrairement aux banques de données standard, comme les VMFS ou vVol, la banque de données PMem ne figure pas dans la vue Banques de données de vSphere Client. Les tâches administratives de la banque de données normale ne s'appliquent pas à la banque de données PMem.

Procédure

- ◆ Passez en revue les informations de la banque de données PMem.

Option	Description
vSphere Client	<ol style="list-style-type: none"> Accédez à l'hôte ESXi et cliquez sur Résumé. Dans le panneau Matériel, vérifiez que la Mémoire persistante s'affiche et vérifiez sa capacité.
Commande esxcli	Utilisez la commande <code>esxcli storage filesystem list</code> pour afficher la banque de données PMem.

Exemple : Affichage de la banque de données PMem

L'exemple de sortie suivant s'affiche lorsque vous utilisez la commande `esxcli storage filesystem list` pour répertorier la banque de données.

# esxcli storage filesystem list	Mount Point	Volume Name	UUID	Mounted	Type	Size
	Free					
/vmfs/volumes/5xxx... 12718178304	ds01-102		5xxx...	true	VMFS-6	14227079168
/vmfs/volumes/59ex... 19697500160	ds02-102		59ex...	true	VMFS-6	21206401024
/vmfs/volumes/59bx... 4274847744			59bx...	true	vfat	4293591040
/vmfs/volumes/pmem:5ax... 11504975872	PMemDS-56ax...	pmem:5a0x...	pmem:5a0x...	true	PMEM	12880707584

Utilisation d'ESXi avec un SAN

L'utilisation d'ESXi avec un SAN signifie plus de souplesse, plus d'efficacité et plus de fiabilité. L'utilisation d'ESXi avec un SAN prend également en charge la gestion centralisée et les technologies de basculement et d'équilibrage de charge.

L'utilisation d'ESXi avec un SAN vous offre les avantages suivants :

- Vous pouvez stocker vos données de manière sécurisée et configurer plusieurs chemins vers votre lieu de stockage afin d'éliminer tout risque de défaillance d'un point de stockage unique.
- Un hôte ESXi peut accéder aux périphériques de stockage présentés depuis plusieurs baies de stockage, y compris des baies provenant de différents fournisseurs.
- L'utilisation d'un SAN avec les systèmes ESXi prolonge la résistance aux pannes sur le serveur. Lorsque vous utilisez un stockage SAN, toutes les applications peuvent être immédiatement redémarrées sur un autre hôte suite à la panne de l'hôte d'origine.
- Vous pouvez effectuer la migration en direct des machines virtuelles à l'aide de VMware vMotion.
- Utilisez VMware High Availability (HA) avec un SAN pour redémarrer des machines virtuelles dans leur dernier état connu sur un serveur différent en cas de défaillance de leur hôte.
- Utilisez VMware Fault Tolerance (FT) pour répliquer des machines virtuelles protégées sur deux hôtes différents. Les machines virtuelles continuent à fonctionner sans interruption sur l'hôte secondaire en cas de défaillance de l'hôte principal.

- Utilisez VMware Distributed Resource Scheduler (DRS) pour migrer les machines virtuelles depuis un hôte vers un autre afin d'obtenir un équilibrage de charge. Le stockage se trouvant sur une baie SAN partagée, les applications continuent de s'exécuter de manière transparente.
- Si vous utilisez des clusters VMware DRS, mettez l'hôte ESXi en mode maintenance afin que le système migre toutes les machines virtuelles en service vers d'autres hôtes ESXi. Ensuite, vous pouvez effectuer les mises à niveau ou d'autres opérations de maintenance sur l'hôte d'origine.

La portabilité et l'encapsulation de machines virtuelles VMware complètent la nature partagée de ce stockage. Lorsque les machines virtuelles se trouvent sur un stockage SAN, vous pouvez rapidement arrêter une machine virtuelle sur un serveur et la démarrer sur un autre serveur, ou la suspendre sur un serveur et reprendre l'activité sur un autre serveur sur le même réseau. Ainsi, vous pouvez migrer des ressources informatiques tout en maintenant un accès partagé cohérent.

Cas d'utilisation d'ESXi et du SAN

Lorsque l'ESXi est utilisé avec un SAN, il peut bénéficier de multiples fonctionnalités vSphere, y compris Storage vMotion, Distributed Resource Scheduler (DRS), High Availability, etc.

L'utilisation de l'ESXi avec un SAN est efficace pour les tâches suivantes :

Consolidation du stockage et simplification de l'architecture de stockage

Si vous travaillez avec plusieurs hôtes et que chacun d'entre eux utilise plusieurs machines virtuelles, le stockage sur les hôtes n'est plus suffisant. Vous allez devoir utiliser un stockage externe. Le SAN peut fournir une architecture système simple et offrir d'autres avantages.

Maintenance sans interruption de service

Lors de la maintenance d'une infrastructure ou d'un hôte ESXi, utilisez vMotion pour migrer les machines virtuelles vers un autre hôte. Si le stockage partagé se trouve sur le SAN, vous pouvez effectuer les opérations de maintenance sans aucune interruption pour les utilisateurs des machines virtuelles. Les processus de travail de VM continuent au cours d'une migration.

Équilibrage de charge

Vous pouvez ajouter un hôte à un cluster DRS et les ressources de l'hôte font partie des ressources du cluster. La répartition et l'utilisation du CPU et des ressources mémoire de tous les hôtes et des machines virtuelles du cluster sont constamment surveillées. DRS compare ces mesures à une utilisation idéale des ressources. L'utilisation idéale prend en compte les attributs des pools de ressources du cluster et des machines virtuelles, la demande actuelle et la cible de déséquilibre. Si besoin est, DRS effectue ou recommande des migrations de machine virtuelle.

Récupération d'urgence

Vous pouvez utiliser VMware High Availability pour configurer plusieurs hôtes ESXi comme un cluster. Le cluster offre une récupération rapide à la suite de pannes et une haute disponibilité à moindre coût pour les applications s'exécutant dans les machines virtuelles.

Migrations de baies et mises à niveau du stockage simplifiées

Lorsque vous achetez de nouveaux systèmes de stockage, utilisez Storage vMotion pour effectuer des migrations en direct des machines virtuelles d'un stockage existant vers leurs nouvelles destinations. Vous pouvez effectuer les migrations sans aucune interruption des machines virtuelles.

Informations détaillées sur l'utilisation du stockage SAN avec l'ESXi

L'utilisation d'un SAN avec un hôte ESXi diffère de l'utilisation classique d'un SAN de différentes manières.

- Vous ne pouvez pas utiliser les outils d'administration du SAN pour accéder aux systèmes d'exploitation des machines virtuelles qui résident sur le stockage. Avec les outils traditionnels, vous pouvez uniquement surveiller le système d'exploitation VMwareESXi. Pour surveiller les machines virtuelles, vous devez utiliser vSphere Client.
- Le HBA visible aux outils d'administration du SAN fait partie du système ESXi et non de la machine virtuelle.
- En règle générale, votre système ESXi effectue la gestion multivoie pour vous.

Prendre des décisions LUN

Vous devez planifier la configuration du stockage de vos systèmes ESXi avant de formater les LUN avec les banques de données VMFS.

Lorsque vous prenez une décision LUN, les considérations suivantes s'appliquent :

- Chaque LUN doit avoir le bon niveau RAID et des caractéristiques de stockage correctes pour les applications s'exécutant dans les machines virtuelles utilisant le LUN.
- Chaque LUN ne doit contenir qu'une banque de données VMFS.
- Si plusieurs machines virtuelles ont accès au même VMFS, utilisez les partages de disque pour classer les machines virtuelles par ordre de priorité.

Vous pourriez souhaiter utiliser moins de LUN mais de plus grande taille pour les raisons suivantes :

- Plus de souplesse de création des machines virtuelles sans avoir à demander plus d'espace de stockage à l'administrateur.
- Plus de souplesse de redimensionnement des disques virtuels, de prise de snapshots et de bien d'autres choses encore.
- Moins de banques de données VMFS à gérer.

Vous pourriez souhaiter utiliser moins de LUN et de plus petite taille pour les raisons suivantes :

- Gain d'espace.
- Différentes applications pourraient nécessiter des caractéristiques RAID différentes.
- Plus de souplesse grâce à la définition de la règle de gestion multivoie et des partages de disque par LUN.
- L'utilisation du service de cluster de Microsoft (Microsoft Cluster Service) exige que chaque ressource de disque en cluster soit dans sa LUN respective.
- Meilleures performances car un volume unique subit moins de contention.

Lorsque les caractéristiques de stockage d'une machine virtuelle ne sont pas disponibles, il peut s'avérer difficile de déterminer le nombre et la taille des LUN à provisionner. Vous pouvez essayer d'utiliser un schéma prédictif ou adaptatif.

Utilisation du schéma prédictif pour prendre les décisions de LUN

Essayez en utilisant le schéma prédictif.

Procédure

- 1 Mettez en place plusieurs LUN avec différentes caractéristiques de stockage.
- 2 Créez une banque de données VMFS sur chaque LUN, en étiquetant chaque banque de données selon ses caractéristiques.
- 3 Créez des disques virtuels qui contiendront les données des applications de la machine virtuelle dans les banques de données VMFS créées sur les LUN avec le niveau RAID approprié aux conditions requises des applications.
- 4 Utilisez les partages de disque pour distinguer les machines virtuelles disposant des priorités les plus hautes de celles ayant les priorités les plus basses.

Note Les parts de disque sont uniquement utiles au sein d'un hôte défini. Les parts assignées aux machines virtuelles sur un hôte n'exercent aucun effet sur des machines virtuelles sur d'autres hôtes.

- 5 Exécutez les applications pour déterminer si les performances de la machine virtuelle sont acceptables.

Utilisation du schéma adaptatif pour prendre les décisions de LUN

Vous pouvez essayer le schéma adaptatif.

Procédure

- 1 Mettez en place une LUN (RAID 1+0 ou RAID 5) de grande taille et activez la mise en cache des écritures.
- 2 Créez un VMFS sur cette LUN.
- 3 Créez quatre ou cinq disques virtuels sur le VMFS.

- 4 Exécutez les applications pour déterminer si les performances du disque sont acceptables.

Résultats

Si les performances sont acceptables, vous pouvez placer des disques virtuels supplémentaires sur le VMFS. Si les performances ne sont pas acceptables, créez un nouveau LUN de grande taille avec un niveau RAID différent et répétez la procédure. Utilisez la migration afin de ne pas perdre les données des machines virtuelles lorsque vous recréez la LUN.

Sélection de l'emplacement des machines virtuelles

Si vous souhaitez optimiser les performances de vos machines virtuelles, l'emplacement du stockage est un facteur important. Selon vos besoins de stockage, vous pouvez sélectionner un stockage avec des performances élevées et une haute disponibilité ou un stockage avec des performances inférieures.

Le stockage peut être divisé en plusieurs niveaux, selon un certain nombre de facteurs :

- Niveau élevé Offre de hautes performances et une grande disponibilité. Peut offrir des snapshots intégrés pour faciliter les sauvegardes et les restaurations instantanées. Prend en charge la réPLICATION, la redondance complète des processeurs de stockage et les lecteurs SAS. Utilise des axes de prix élevé.
- Niveau intermédiaire Offre des performances de milieu de gamme, une disponibilité plus faible, quelques redondances de processeurs de stockage et des lecteurs SCSI ou SAS. Peut fournir des snapshots. Utilise des axes de prix moyen.
- Niveau inférieur Offre des performances faibles, peu de redondance de stockage interne. Utilise des lecteurs SCSI bas de gamme ou SATA.

Les machines virtuelles ne doivent pas toutes se trouver sur le stockage possédant les meilleures performances et la plus grande disponibilité tout au long de leur cycle de vie.

Lors du choix de l'emplacement d'une machine virtuelle, les considérations suivantes s'appliquent :

- Criticité de la machine virtuelle
- Exigences en matière de performances et de disponibilité
- Exigences en matière de restauration instantanée
- Exigences en matière de sauvegarde et de réPLICATION

Une machine virtuelle peut changer de niveau tout au long de son cycle de vie en raison de modifications de la criticité ou de la technologie. Son importance est relative et peut changer pour diverses raisons, parmi lesquelles les modifications apportées à l'organisation, les processus opérationnels, les obligations réglementaires, la planification suite à un incident, etc.

Applications de gestion tierces

Vous pouvez utiliser les applications de gestion tierces avec votre hôte ESXi.

La majorité des matériels SAN sont délivrés avec le logiciel de gestion du stockage. Dans la majorité des cas, ce logiciel est une application Web qui peut être utilisée avec tout navigateur Web connecté à votre réseau. Dans certains autres cas, ce logiciel s'exécute habituellement sur le système de stockage ou sur un serveur unique, indépendamment des serveurs utilisant le SAN pour le stockage.

Utilisez le logiciel de gestion tiers pour effectuer les tâches suivantes :

- La gestion des baies de stockage, y compris la création de LUN, la gestion de la mémoire cache des baies, le mappage de LUN et la sécurité des LUN.
- La configuration de la réPLICATION, des points de vérification, des snapshots ou de la mise en miroir.

Si vous exécutez le logiciel de gestion du SAN sur une machine virtuelle, vous bénéficiez de tous les avantages d'une machine virtuelle, y compris le basculement à l'aide de vMotion et de VMware HA. Toutefois, en raison du niveau supplémentaire d'indirection, il se peut que le logiciel de gestion ne soit pas en mesure de voir le SAN. Dans ce cas, utilisez un RDM.

Note Le succès d'exécution d'un logiciel de gestion par une machine virtuelle dépend du système de stockage.

Considérations sur la sauvegarde de stockage SAN

Une stratégie de sauvegarde appropriée est l'un des aspects les plus importants de la gestion d'un SAN. Dans un environnement SAN, les sauvegardes ont deux objectifs. Le premier objectif est d'archiver des données en ligne sur des supports hors ligne. Ce processus est répété régulièrement pour toutes les données en ligne, selon un calendrier. Le second objectif est de fournir un accès aux données hors ligne pour une restauration en cas de problème. Par exemple, la récupération de bases de donnée nécessite souvent la récupération des fichiers de journalisation archivés qui ne sont pas en ligne à ce moment.

La programmation d'une sauvegarde dépend de plusieurs facteurs :

- L'identification des applications critiques nécessitant des cycles de sauvegarde plus rapprochés dans une période donnée.
- Les points de restauration et les objectifs de période restaurée. Définissez la précision nécessaire de vos points de récupération et la durée d'attente souhaitée.
- Le taux de changement (RoC) associé aux données. Par exemple, si vous utilisez une réPLICATION synchrone/asynchrone, le RoC affecte la quantité de bande passante requise entre les périphériques de stockage primaires et secondaires.
- L'impact global sur un environnement SAN, les performances de stockage et les autres applications.
- L'identification des horaires de pointe sur le SAN. Les sauvegardes prévues pendant ces heures de pointe peuvent ralentir les applications et le processus de sauvegarde.
- Le temps passé à programmer toutes les sauvegardes dans le centre de données.

- Le temps passé à sauvegarder une application spécifique.
- La disponibilité des ressources pour l'archivage des données, telles que l'accès des supports hors ligne.

Incluez un objectif de temps de restauration pour chaque application lorsque vous concevez votre stratégie de sauvegarde. C'est-à-dire que vous devez envisager le temps et les ressources nécessaires pour effectuer une sauvegarde. Par exemple, si une sauvegarde programmée stocke tant de données que leur restauration cause un délai considérable, réexaminez la programmation des sauvegardes. Vous pouvez effectuer des sauvegardes plus fréquemment, de façon à sauvegarder moins de données à la fois, et diminuer ainsi le délai de restauration.

Si une application nécessite une récupération dans un délai précis, le processus de sauvegarde doit fournir un horaire et un traitement des données pour ce délai. La récupération rapide peut exiger l'utilisation des volumes de récupération qui résident sur le stockage en ligne. Ce processus permet de réduire ou d'éliminer le besoin d'accéder aux supports hors ligne lents pour récupérer des composants de données manquants.

Utilisation des modules de sauvegarde tiers

Vous pouvez utiliser des solutions de sauvegarde tierces pour protéger le système, l'application et les données utilisateur dans vos machines virtuelles.

Les API de stockage - Protection des données proposées par VMware peuvent fonctionner avec des produits tiers. Lors de l'utilisation des API, le logiciel tiers peut effectuer les sauvegardes sans charger les hôtesESXi du traitement des tâches de sauvegarde.

Les produits tiers utilisant les API de stockage - Protection des données peuvent effectuer les tâches de sauvegarde suivantes :

- Effectuer une sauvegarde d'images complète, différentielle et incrémentielle, et la restauration des machines virtuelles.
- Effectuer, au niveau du fichier, une sauvegarde des machines virtuelles qui utilisent les systèmes d'exploitation Windows et Linux pris en charge.
- Vérifiez la cohérence des données en utilisant VSS (Microsoft Volume Shadow Copy Services) pour les machines virtuelles qui exécutent les systèmes d'exploitation Microsoft Windows pris en charge.

Étant donné que les API de stockage - Protection des données utilisent les capacités de snapshot de VMFS, les sauvegardes ne nécessitent pas d'arrêter les machines virtuelles. Ces sauvegardes ne sont pas perturbatrices ; elles peuvent être effectuées à tout moment et ne nécessitent pas des fenêtres de sauvegarde étendues.

Pour plus d'informations sur les API de stockage - Protection des données et l'intégration aux produits de sauvegarde, consultez l'[article 1021175 de la base de connaissances VMware](#).

Utilisation d'ESXi avec un SAN Fibre Channel

3

ESXi prend en charge Fibre Channel (FC), un protocole de stockage que le SAN utilise pour transférer le trafic de données des serveurs d'hôtes au stockage partagé. Cette section fournit une première approche de l'utilisation d'ESXi avec Fibre Channel SAN. Pour plus d'informations, consultez la documentation de votre fournisseur.

Concepts du SAN Fibre Channel

Si vous êtes administrateur vSphere et que vous envisagez de configurer les hôtes pour fonctionner avec des SAN, vous devez avoir une connaissance pratique des concepts SAN. Vous trouverez des informations sur les SANs en livre et sur Internet. Du fait que ce secteur technologique évolue constamment, cherchez les ressources les plus récentes.

Réseau de zone de stockage (SAN)

Un réseau de zone de stockage (SAN) est un réseau à haute vitesse spécialisé qui connecte des serveurs hôtes à des sous-systèmes de stockage à hautes performances. Les composants SAN comprennent les adaptateurs de bus hôte (HBA), les commutateurs qui aident à diriger le trafic de stockage, les câbles, les processeurs de stockage (SPs), et les baies de disques de stockage.

Fabric SAN

Une topologie SAN avec au moins un commutateur présent sur le réseau forme une structure SAN.

Protocole Fibre Channel (FC)

Pour transférer le trafic des serveurs hôtes vers le stockage partagé, le SAN utilise le protocole Fibre Channel (FC) qui regroupe les commandes SCSI ou NVMe dans des trames Fibre Channel.

Zonage

Pour restreindre l'accès d'un serveur aux baies de stockage non allouées à ce serveur, le SAN utilise le zonage. Classiquement, des zones sont créées pour chaque groupes de serveurs accédant à un groupe partagé de périphériques de stockage et de LUN. Ces zones définissent quels HBA peuvent se connecter à quels SPs. Les périphériques en dehors d'une zone ne sont pas visibles aux périphériques inclus dans cette zone.

Le zonage a les effets suivants :

- Réduit le nombre de cibles et de LUN présentées à l'hôte.
- Contrôle et isole les chemins dans une infrastructure d'interconnexion.
- Interdit aux systèmes non ESXi l'accès à un système de stockage particulier et empêche toute destruction potentielle des données VMFS.
- Peut être utilisé pour séparer des environnements différents, par exemple, un environnement de tests d'un environnement de production.

Avec les hôtes ESXi, utilisez un zonage à initiateur unique ou un zonage à initiateur unique et à cible unique. La dernière étant la méthode de zonage la plus pratiquée. L'utilisation d'un zonage plus restrictif évite les problèmes et les risques de mauvaises configurations et le SAN.

Pour des instructions plus détaillées et les bonnes méthodes de zonage, contactez l'éditeur de la baie de stockage ou du commutateur.

Masquage de LUN

Le zonage est similaire au masquage des LUN, fréquemment utilisé pour l'administration des permissions. Le masquage des LUN est un processus qui rend un LUN disponible pour certains hôtes, mais indisponibles pour d'autres hôtes.

Gestion multivoie

Lors du transfert de données entre le serveur hôte et le stockage, le SAN utilise une technique connue sous le nom de gestion multivoie. La fonction de chemin multiple permet de disposer de plusieurs chemins physiques depuis un hôte ESXi vers une LUN dans un système de stockage.

Basculement de chemin

De manière générale, un chemin unique partant d'un hôte vers un LUN se compose d'un HBA, de ports de commutateur, de câbles de connexion et du port de contrôleur de stockage. Si un des composants du chemin subit une défaillance, l'hôte sélectionne un autre chemin disponible pour l'E/S. Le processus de détection d'un chemin défaillant et de changement vers un autre chemin est connu sous le nom de basculement de chemin.

Ports dans le SAN Fibre Channel

Dans le contexte de ce document, un port est une connexion à partir d'un périphérique dans le SAN. Chaque nœud du SAN, tel qu'un hôte, un périphérique de stockage ou un composant d'infrastructure, dispose d'un ou de plusieurs ports qui le connectent au SAN. Les ports sont identifiés de plusieurs manières.

WWPN (World Wide Port Name)

Un identificateur global unique pour un port qui permet à certaines applications d'accéder au port. Le commutateur FC détecte le WWPN d'un périphérique ou d'un hôte et affecte une adresse de port au périphérique.

Port_ID (ou adresse du port)

Dans un SAN, chaque port dispose d'un ID de port unique qui sert d'adresse FC pour le port. Cet ID unique permet le routage des données via le SAN vers ce port. Les commutateurs FC affectent l'ID du port lorsque le périphérique se connecte à l'infrastructure d'interconnexion. L'ID du port est valide uniquement lorsque le périphérique est connecté.

Lorsque N-Port ID Virtualization (NPIV) est utilisé, un seul port FC HBA (N-port) peut s'enregistrer sur l'infrastructure d'interconnexion en utilisant plusieurs WWPN. Cette méthode permet à un N-port de réclamer plusieurs adresses d'interconnexion, chacune d'entre-elles apparaissant en tant qu'entité unique. Lorsque l'hôte ESXi utilise un SAN, ces nombreux identificateurs exclusifs permettent l'affectation des WWN à des machines virtuelles individuelles dans le cadre de leur configuration.

Types de baie de stockage Fibre Channel

ESXi prend en charge différents systèmes de stockage et de baies. Elles entrent dans les catégories suivantes.

Système de stockage actif-actif

Prend en charge l'accès simultané aux LUN par tous les ports de stockage qui sont disponibles sans dégradation importante des performances. Tous les chemins sont actifs, sauf si un chemin est défaillant.

Système de stockage actif-passif

Un système dans lequel un processeur de stockage fournit l'accès à un LUN donné. Les autres processeurs sont utilisés en tant que sauvegarde pour le LUN et peuvent fournir l'accès à d'autres E/S de LUN. L'E/S peut uniquement être envoyée avec succès vers un port actif pour un LUN spécifique. Si l'accès via le port de stockage actif échoue, un des processeurs de stockage passifs peut être activé par les serveurs qui y accèdent.

Système de stockage asymétrique

Prend en charge Asymmetric Logical Unit Access (ALUA). Les systèmes de stockage conforme à ALUA offrent des niveaux différents d'accès par port. Avec ALUA, l'hôte peut déterminer les états des ports cibles et classer les chemins par priorité. L'hôte utilise certains des chemins actifs comme étant principaux et d'autres comme secondaires.

Accès des machines virtuelles aux données sur un SAN Fibre Channel

ESXi stocke les fichiers disque d'une machine virtuelle dans une banque de données VMFS se trouvant sur un périphérique de stockage du SAN. Lorsque les systèmes d'opérations invités de machine virtuelle envoient des commandes SCSI ou NVMe à leurs disques virtuels, la couche de virtualisation SCSI ou NVMe convertit ces commandes de fichiers en VMFS.

Lorsqu'une machine virtuelle interagit avec son disque virtuel stocké sur un SAN, le processus suivant a lieu :

- 1 Lorsque le système d'exploitation invité sur une machine virtuelle lit ou écrit sur le disque SCSI ou NVMe, il envoie des commandes SCSI ou NVMe au disque virtuel.
- 2 Les pilotes de périphériques dans le système d'exploitation de la machine virtuelle communiquent avec les contrôleurs SCSI ou NVMe virtuels.
- 3 Le contrôleur SCSI virtuel ou NVMe transmet la commande au VMkernel.
- 4 Le VMkernel effectue les tâches suivantes :
 - a Localisation du fichier de disque virtuel approprié dans le volume VMFS.
 - b Mappage des requêtes de blocs sur le disque virtuel sur les blocs sur le périphérique physique approprié.
 - c Envoi de la demande d'E/S modifiée à partir du pilote du périphérique du VMkernel vers le HBA physique.
- 5 Le HBA physique effectue les tâches suivantes :
 - a Préparation de la demande d'E/S selon les règles du protocole FC.
 - b Transmission de la requête au SAN.
- 6 En fonction d'un port que le HBA utilise pour se connecter à l'infrastructure, l'un des commutateurs SAN reçoit la demande. Le commutateur achemine la demande vers le périphérique de stockage approprié.

Ce chapitre contient les rubriques suivantes :

- Configuration de l'environnement ESXi Fibre Channel
- Démarrage ESXi à partir du SAN Fibre Channel
- Meilleures pratiques pour le stockage Fibre Channel
- Utilisation de Fibre Channel NPIV avec des machines virtuelles vSphere

Configuration de l'environnement ESXi Fibre Channel

Cette rubrique décrit les étapes de configuration que vous devez suivre lors de la configuration de votre environnement SAN Fibre Channel pour que celui-ci fonctionne avec ESXi. En

préparation de la configuration de votre SAN Fibre Channel et du système ESXi, passez en revue la conditions requises et les recommandations.

Conditions requises de SAN Fibre Channel ESXi

- Assurez-vous que les systèmes ESXi prennent en charge les combinaisons micrologicielles et matérielles de stockage SAN que vous utilisez. Pour obtenir une liste à jour, consultez le [Guide de compatibilité de VMware](#).
- Configurez votre système pour avoir un seul volume VMFS par LUN.
- Sauf si vous utilisez des serveurs sans disque, ne configurez pas la partition de diagnostic sur un LUN SAN.

Si vous utilisez un serveur sans disque démarrant à partir d'un SAN, il est approprié d'utiliser une partition de diagnostic partagée.
- Utilisez les RDM pour accéder aux disques bruts. Pour plus d'informations, consultez [Chapitre 11 Mappage de périphérique brut](#).
- Pour que les chemins multiples fonctionnent correctement, chaque LUN doit présenter le même ID de LUN pour tous les hôtes ESXi.
- Assurez-vous que le pilote du périphérique de stockage définit une file d'attente suffisamment grande. Vous pouvez définir la profondeur de file d'attente pour le HBA physique lors de la configuration du système.
- Sur les machines virtuelles qui exécutent Microsoft Windows, augmentez la valeur du paramètre `TimeoutValue SCSI` à 60. Avec cette augmentation, Windows peut tolérer des E/S différentes provenant d'un basculement de chemin. Pour plus d'informations, consultez [Définir le délai d'expiration du SE invité Windows](#).

Restrictions de SAN Fibre Channel ESXi

Lorsque vous utilisez ESXi avec un SAN, certaines restrictions s'appliquent.

- ESXi ne prend pas en charge les périphériques de bande connectés au FC.
- Vous ne pouvez pas utiliser un logiciel de chemins multiples à l'intérieur d'une machine virtuelle pour effectuer un équilibrage de charge E/S sur un LUN physique unique. Cependant, lorsque votre machine virtuelle Microsoft Windows utilisez des disques dynamiques, cette restriction ne s'applique pas. Pour plus d'informations sur la configuration des disques dynamiques, consultez [Configuration de la mise en miroir des disques dynamiques](#).

Définition des allocations de LUN

Cette rubrique fournit des informations générales sur l'allocation des LUN lorsque votre ESXi fonctionne avec le SAN.

Lorsque vous définissez les allocations de LUN, tenez compte des points suivants :

Provisionnement de stockage

Pour garantir que le système ESXi reconnaissse les LUN au démarrage, provisionnez tous les LUN aux HBA appropriés avant de connecter le SAN au système ESXi.

Provisionnez tous les LUN à tous les HBA ESXi en même temps. Le basculement de HBA fonctionne uniquement si tous les HBA voient les mêmes LUN.

Pour les LUN qui sont partagés entre plusieurs hôtes, veillez à ce que les ID de LUN soient cohérents sur les différents hôtes.

DRS vMotion et VMware

Vous utilisez vCenter Server et vMotion ou DRS, veillez à ce que les LUN des machines virtuelles soient provisionnés pour tous les hôtes ESXi. Cette action permet de déplacer le plus facilement les machines virtuelles.

Baies actives/actives par rapport à baies actives/passives.

Lorsque vous utilisez vMotion ou DRS avec un matériel de stockage SAN actif-passif, vérifiez bien que dans tous les systèmes ESXi les chemins vers tous les processeurs de stockage sont cohérents. Sans cette vérification, une migration vMotion peut provoquer un écrasement de chemin.

Pour les baies de stockage actives/passives non énumérées dans la section Compatibilité de stockage/SAN, VMware ne prend pas en charge le basculement des ports de stockage. Dans ces cas, vous devez connecter le serveur au port actif sur la baie de stockage. Cette configuration garantit que les LUN sont présentés à l'hôte ESXi.

Configuration des HBA Fibre Channel

En général, les FC HBA que vous utilisez sur votre hôte ESXi fonctionnent correctement avec les paramètres de configuration par défaut.

Vous devez suivre les instructions de configuration fournies par votre fournisseur de baie de stockage. Lors de la configuration du FC HBA, prenez en considération les aspects suivants.

- Ne mélangez pas les FC HBA de différents fournisseurs sur un même serveur. Il est possible d'avoir différents modèles du même HBA, mais on ne peut pas accéder à un même LUN via deux types différents de HBA; ceci est possible uniquement via un même type.
- Assurez-vous que le niveau du microprogramme sur chaque HBA est le même.
- Définissez la valeur du délai d'expiration pour la détection d'un basculement. Pour assurer une performance optimale, ne modifiez pas la valeur par défaut.
- ESXi prend en charge la connectivité Fibre Channel de bout en bout de 32 Gbits/s.

Configuration de Fibre Channel over Ethernet

Un hôte ESXi peut utiliser le protocole Fibre Channel over Ethernet (FCoE) pour accéder au stockage Fibre Channel. Le protocole FCoE encapsule les trames Fibre Channel dans des trames Ethernet. Par conséquent, votre hôte n'a pas besoin de liaisons Fibre Channel spéciales pour se connecter au stockage Fibre Channel. L'hôte peut utiliser Ethernet sans perte 10 Gbits pour fournir le trafic Fibre Channel.

Adaptateurs Fibre Channel over Ethernet

VMware prend en charge les adaptateurs FCoE matériels, des cartes CNA (Converged Network Adapters) spéciales complètement déchargées qui contiennent des fonctions de réseau et Fibre Channel sur la même carte.

Lorsque ce type d'adaptateur est installé, l'hôte détecte et peut utiliser les deux composants CNA. Dans vSphere Client, le composant de mise en réseau est un adaptateur réseau standard (vmnic) et le composant Fibre Channel un adaptateur FCoE (vmhba).

Pour plus d'informations sur les adaptateurs pouvant être utilisés avec VMware FCoE, reportez-vous au *Guide de compatibilité VMware*

Workflow de configuration

Cette rubrique décrit les étapes d'installation et de configuration que vous devez suivre lors de la configuration de votre environnement SAN Fibre Channel pour que celui-ci fonctionne avec ESXi.

Suivez ces étapes pour configurer votre environnement SAN ESXi.

- 1 Configurez votre SAN si ce n'est déjà fait. La plupart des SAN existants ne nécessitent que quelques modifications mineures pour fonctionner avec ESXi.
- 2 Assurez-vous que tous les composants SAN remplissent les conditions requises.
- 3 Apportez toute modification nécessaire à la baie de stockage.
La plupart des fournisseurs possèdent leur propre documentation pour la configuration d'un SAN pour que celui-ci fonctionne avec VMware ESXi.
- 4 Configurez les HBA pour les hôtes connectés au SAN.
- 5 Installez ESXi sur les hôtes.
- 6 Créez des machines virtuelles et installez les systèmes d'exploitation client.
- 7 (Facultatif) Configurez votre système pour le basculement de VMware HA ou pour utiliser Microsoft Cluster Services.
- 8 Mettez à niveau ou modifiez votre environnement selon vos besoins.

Démarrage ESXi à partir du SAN Fibre Channel

Lorsque vous paramétrez votre hôte pour qu'il démarre depuis un SAN, l'image de démarrage de votre hôte est archivée sur une ou plusieurs numéros d'unité logique (LUN) du système de

stockage du SAN. Lorsque l'hôte démarre, il se lance à partir de la LUN se trouvant sur le SAN et non pas à partir du disque local.

ESXi prend en charge des démarrages par le biais d'un adaptateur de bus hôte (HBA) Fibre Channel ou d'un adaptateur de réseau convergé (CNA) Fibre Channel sur Ethernet (FCoE).

Avantages du démarrage à partir d'un SAN

Le démarrage à partir du SAN présente de nombreux avantages pour votre environnement ESXi. Cependant, dans certains cas, le démarrage à partir du SAN n'est pas compatible avec vos hôtes. Avant de configurer votre système pour un démarrage à partir du SAN, vous devez décider si cela est nécessaire pour votre environnement.

Attention Lorsque vous utilisez le démarrage à partir du SAN avec plusieurs hôtes ESXi, chaque hôte doit posséder sa propre LUN de démarrage. Si vous configurez de nombreux hôtes pour partager le LUN de démarrage, une corruption de l'image d'ESXi peut se produire.

Si vous utilisez le démarrage à partir du SAN, les avantages pour votre environnement sont les suivants :

- Coût moins élevé des serveurs. Les serveurs sont plus denses et leur température de fonctionnement beaucoup moins élevée sans stockage interne.
- Remplacement plus facile des serveurs. Vous pouvez remplacer les serveurs par un nouveau serveur que vous pointez vers l'ancien emplacement de démarrage.
- Gain d'espace. Les serveurs sans disques locaux sont souvent moins volumineux.
- Processus de sauvegarde plus faciles. Vous pouvez sauvegarder les images de démarrage du système dans le SAN dans le cadre des procédures de sauvegarde générales du SAN. Vous pouvez également utiliser les fonctionnalités avancées de la baie, telles que les snapshots de l'image de démarrage.
- Gestion améliorée. La création et la gestion de l'image du système d'exploitation sont encore plus faciles et plus efficaces.
- Meilleure fiabilité. Vous pouvez accéder au disque de démarrage via différents chemins. Le disque est ainsi protégé en ne représentant pas un point unique de panne.

Exigences et considérations lors du démarrage à partir du SAN Fibre Channel

Votre configuration de démarrage ESXi doit répondre à certaines exigences particulières.

Tableau 3-1. Conditions requises du démarrage à partir du SAN

Serveur	Description
Spécifications système ESXi	Respectez les recommandations du fournisseur pour le démarrage du serveur à partir d'un SAN.
Conditions requises d'une carte	Configurez la carte afin qu'elle puisse accéder au LUN de démarrage. Consultez la documentation du fabricant.

Tableau 3-1. Conditions requises du démarrage à partir du SAN (suite)

Serveur	Description
Contrôle d'accès	<ul style="list-style-type: none"> ■ Chaque hôte doit ne pouvoir accéder qu'à son propre LUN de démarrage et non aux LUN de démarrage des autres hôtes. Utilisez le logiciel du système de stockage pour vérifier que l'hôte accède uniquement aux LUN qui lui sont assignés. ■ Plusieurs serveurs peuvent partager une partition de diagnostic. Vous pouvez utiliser un masquage des LUN spécifiques à la baie pour obtenir cette configuration.
Prise en charge de la gestion de chemins multiples	La gestion de chemins multiples vers un LUN de démarrage sur des baies actives/passives n'est pas pris en charge car le BIOS ne prend pas en charge la gestion de chemins multiples et ne peut pas activer un chemin de veille.
Considérations SAN	Si la baie n'est pas certifiée pour une topologie à connexion directe, les connexions SAN doivent se faire via une topologie à commutateur. Si la baie est certifiée pour la topologie à connexion directe, les connexions SAN peuvent être établies directement sur la baie. Le démarrage à partir du SAN est pris en charge à la fois pour la topologie à commutateur et à connexion directe.
Considérations spécifiques au matériel	Si vous exécutez un IBM eServer BladeCenter et que vous utilisez le démarrage à partir du SAN, vous devez désactiver les lecteurs IDE sur les lames.

Préparation pour le démarrage ESXi à partir du SAN

Lorsque vous préparez votre hôte ESXi pour qu'il démarre à partir d'un SAN, vous effectuez plusieurs tâches.

Ce workflow décrit le processus d'activation d'un démarrage générique à partir du SAN sur des serveurs montés sur rack. Pour plus d'informations sur l'activation de l'option de démarrage à partir du SAN sur des serveurs lame ou d'autres types d'hôtes, reportez-vous à la documentation du partenaire.

Pour plus d'informations, consultez <https://www.vmware.com/resources/compatibility/search.php>.

Procédure

1 Configurer des composants SAN et un système de stockage

Lorsque vous paramétrez votre hôte ESXi pour qu'il démarre depuis un LUN SAN, configurez les composants du SAN et un système de stockage.

2 Configurer l'adaptateur de stockage pour un démarrage à partir du SAN

Lorsque vous configuez votre hôte pour effectuer un démarrage à partir du SAN, vous devez activer l'adaptateur de démarrage dans le BIOS de l'hôte. Vous devez ensuite configurer l'adaptateur de démarrage afin de lancer une connexion primitive vers le LUN de démarrage cible.

3 Configurer votre système pour effectuer un démarrage à partir du support d'installation

Lorsque vous configurez votre hôte pour effectuer un démarrage à partir du SAN, vous devez d'abord démarrer l'hôte à partir du support d'installation de VMware. Pour démarrer à partir du support d'installation, modifiez la séquence de démarrage du système dans la configuration du BIOS.

Configurer des composants SAN et un système de stockage

Lorsque vous paramétrez votre hôte ESXi pour qu'il démarre depuis un LUN SAN, configurez les composants du SAN et un système de stockage.

La configuration des composants SAN étant propre au fournisseur, reportez-vous à la documentation produit de chaque élément.

Procédure

- 1 Connectez les câbles réseau en vous référant au guide de câblage correspondant à votre configuration.

Vérifiez le câblage du commutateur, le cas échéant.

- 2 Configurez la baie de stockage.

- a À partir de la baie de stockage SAN, rendez l'hôte ESXi visible sur le SAN. Ce processus est souvent considéré comme la création d'un objet.
- b À partir de la baie de stockage SAN, configurez l'hôte pour avoir les WWPN des adaptateurs de l'hôte comme noms de port ou noms de noeud.
- c Créez et attribuez des LUN.
- d Enregistrez les adresses IP des commutateurs et des baies de stockage.
- e Enregistrez le WWPN de chaque SP.

Attention Si vous utilisez un processus d'installation par script pour installer l'ESXi en mode de démarrage à partir du SAN, prenez des mesures spécifiques afin d'éviter toute perte accidentelle de données.

Configurer l'adaptateur de stockage pour un démarrage à partir du SAN

Lorsque vous configurez votre hôte pour effectuer un démarrage à partir du SAN, vous devez activer l'adaptateur de démarrage dans le BIOS de l'hôte. Vous devez ensuite configurer l'adaptateur de démarrage afin de lancer une connexion primitive vers le LUN de démarrage cible.

Conditions préalables

Déterminez le WWPN de l'adaptateur de stockage.

Procédure

- ◆ Configurez l'adaptateur de stockage pour effectuer un démarrage à partir du SAN.
Étant donné que la configuration des adaptateurs de démarrage est propre au fournisseur, consultez la documentation de votre fournisseur.

Configurer votre système pour effectuer un démarrage à partir du support d'installation

Lorsque vous configurez votre hôte pour effectuer un démarrage à partir du SAN, vous devez d'abord démarrer l'hôte à partir du support d'installation de VMware. Pour démarrer à partir du support d'installation, modifiez la séquence de démarrage du système dans la configuration du BIOS.

La modification de la séquence de démarrage dans le BIOS étant propre au fournisseur, reportez-vous à la documentation du fournisseur pour plus d'instructions. La procédure suivante explique comment modifier la séquence de démarrage sur un hôte IBM.

Procédure

- 1 Mettez sous tension votre système et entrez l'utilitaire d'installation/de configuration du BIOS système.
- 2 Sélectionnez **Options de démarrage** et appuyez sur Entrée.
- 3 Sélectionnez **Options des séquences de démarrage** et appuyez sur Entrée.
- 4 Modifiez le **Premier dispositif de démarrage** en [CD-ROM].

Résultats

Vous pouvez maintenant installer l'ESXi.

Meilleures pratiques pour le stockage Fibre Channel

Lorsque vous utilisez ESXi avec un SAN Fibre Channel, suivez les recommandations pour éviter des problèmes de performances.

vSphere Client offre de nombreuses fonctionnalités pour collecter des informations sur les performances. Ces informations sont affichées sous forme graphique et sont régulièrement mises à jour.

Vous pouvez utiliser les utilitaires de commande `resxtop` ou `esxtop`. Les utilitaires fournissent une vue détaillée du mode d'utilisation des ressources de ESXi. Pour plus d'informations, consultez la documentation *Gestion des ressources vSphere*.

Consultez votre représentant de stockage pour savoir si votre système de stockage prend en charge les fonctionnalités d'accélération matérielle API de stockage - Intégration de baie. Le cas échéant, consultez la documentation du fournisseur pour activer la prise en charge de l'accélération matérielle du côté du système de stockage. Pour plus d'informations, consultez [Chapitre 16 Accélération matérielle du stockage](#).

Prévention des problèmes de SAN Fibre Channel

Lorsque vous utilisez ESXi avec un SAN Fibre Channel, suivez les directives spécifiques afin d'éviter des problèmes de SAN.

Pour éviter des problèmes avec votre configuration SAN, suivez ces conseils :

- Placez une seule banque de données VMFS sur chaque LUN.
- Ne changez pas la politique de chemin que le système définit, sauf si vous comprenez les implications de tels changements.
- Documentez tout ce que vous faites. Incluez des informations sur le zonage, le contrôle d'accès, le stockage, le commutateur, le serveur et la configuration HBA FC, les versions de logiciel et de microprogramme, et le plan des câbles de stockage.
- Plan en cas de panne :
 - Faîtes plusieurs copies de vos mappages topologiques. Pour chaque élément, envisagez les conséquences sur votre SAN si cet élément tombe en panne.
 - Vérifiez chaque lien, commutateurs, HBA et autres éléments pour vous assurer que vous n'avez omis aucun point de panne critique dans votre architecture.
- Assurez-vous que les HBA Fibre Channel sont installés dans les slots corrects de l'hôte, selon la vitesse de l'emplacement et du bus. Équilibrez la charge de bus PCI entre les divers bus du serveur.
- Familiarisez-vous avec les différents points de contrôle de votre réseau de stockage, sur tous les points de visibilité, y compris les graphiques de performance de l'hôte, les statistiques des commutateurs FC et des performances de stockage.
- Soyez prudent lorsque vous modifiez les ID des LUN qui prennent en charge des banques de données en cours d'utilisation par votre hôte ESXi. Si vous modifiez les ID, la banque de données devient inactive et ses machines virtuelles tombent en panne. Resignez la banque de données pour la réactiver. Reportez-vous à [Administration des banques de données VMFS dupliquées](#).

Après avoir modifié l'ID du LUN, réanalysez le stockage pour réinitialiser l'ID sur votre hôte. Pour plus d'informations sur l'utilisation de la réanalyse, consultez [Réanalyser les opérations de stockage ESXi](#).

Désactiver l'enregistrement automatique de l'hôte ESXi

Certaines baies de stockage imposent l'enregistrement des hôtes ESXi dans les baies. ESXi effectue un enregistrement d'hôte automatique en envoyant le nom de l'hôte et l'adresse IP à la baie. Si vous préférez utiliser le logiciel de gestion de stockage pour effectuer un enregistrement manuel, désactivez la fonctionnalité d'enregistrement automatique d'ESXi.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.

- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Système**, cliquez sur **Paramètres système avancés**.
- 4 Dans Paramètres système avancés, sélectionnez le paramètre **Disk.EnableNaviReg** et cliquez sur l'icône **Edit**.
- 5 Modifiez la valeur sur 0.

Résultats

Cette opération désactive l'enregistrement automatique de l'hôte qui est activé par défaut.

Optimisation des performances du stockage SAN Fibre Channel

Plusieurs facteurs contribuent à l'optimisation d'un environnement SAN classique.

si l'environnement est correctement configuré, les composants de la structure SAN (en particulier les commutateurs SAN) ne sont que des contributeurs mineurs, à cause de leurs latences basses par rapport aux serveurs et aux baies de stockage. Assurez-vous que les chemins dans le commutateur de la structure ne sont pas saturés, c'est-à-dire que le commutateur fonctionne avec le débit maximal.

Performances des baies de stockage

Les performances des baies de stockage sont l'un des principaux facteurs contribuant aux performances de la totalité de l'environnement SAN.

Si vous rencontrez des problèmes avec les performances des baies de stockage, consultez la documentation du fournisseur de votre baie de stockage pour obtenir tous les renseignements utiles.

Pour améliorer les performances des baies dans l'environnement vSphere, suivez ces directives générales :

- Lorsque vous attribuez des LUN, souvenez-vous que plusieurs hôtes peuvent accéder au LUN et que plusieurs machines virtuelles peuvent s'exécuter sur chaque hôte. Un LUN utilisé par un hôte peut servir à des E/S provenant d'applications très variées et exécutées sur différents systèmes d'exploitation. En raison de ces charges de travail très variées, le groupe RAID contenant les LUN ESXi n'inclut généralement pas les LUN utilisés par d'autres serveurs qui n'exécutent pas d'ESXi.
- Assurez-vous que le cache de lecture/écriture est disponible.
- Les baies de stockage SAN nécessitent des modifications et des ajustements permanents pour s'assurer que les charges d'E/S sont équilibrés sur tous les chemins d'accès des baies de stockage. Pour répondre à cette exigence, répartissez les chemins d'accès vers les LUN entre tous les SP pour assurer un équilibrage de charge optimal. Une surveillance attentive permet de savoir lorsqu'il est nécessaire de rééquilibrer la répartition des LUN.

Le réglage de baies de stockage statiquement équilibrées consiste à surveiller des statistiques de performances spécifiques telles que les opérations d'E/S par seconde, les blocs par seconde et le temps de réponse. La distribution de la charge de travail des LUN visant à répartir la charge de travail entre tous les SP est également importante.

Note L'équilibrage de charge dynamique n'est pas pris en charge actuellement avec ESXi.

Performances des serveurs avec Fibre Channel

Vous devez tenir compte de différents facteurs pour garantir des performances optimales des serveurs.

Chaque application de serveur doit avoir accès à son stockage désigné aux conditions suivantes :

- Vitesse d'E/S élevée (nombre d'opérations d'entrée-sortie par seconde)
- Rendement élevé (mégaoctets par seconde)
- Latence minimale (temps de réponse)

Comme chaque application a différentes exigences, ces objectifs peuvent être remplis en sélectionnant un groupe RAID approprié sur la baie de stockage.

Pour atteindre les objectifs de performance, procédez comme suit :

- Placez chaque LUN sur un groupe RAID qui offre les niveaux de performance nécessaires. Surveillez les activités et l'utilisation des ressources des autres LUN dans le groupe RAID attribué. Un groupe RAID haute performance ayant un nombre excessif d'applications effectuant des E/S risque de ne pas satisfaire aux exigences de performance requises par une application exécutée sur l'hôte ESXi.
- Assurez-vous que chaque hôte dispose d'un nombre suffisant de HBA pour augmenter le débit des applications sur l'hôte en période de pointe. Les entrées/sorties réparties sur plusieurs HBA présentent un débit plus rapide et moins de latence pour chaque application.
- Pour assurer la redondance en cas de panne éventuelle du HBA, assurez-vous que l'hôte est connecté à une infrastructure à double redondance.
- Lors de l'allocation de groupes LUN ou RAID aux systèmes ESXi, n'oubliez pas que plusieurs systèmes d'exploitation utilisent et partagent cette ressource. Les performances des LUN requises par l'hôte ESXi peuvent être beaucoup plus élevées que lorsque vous utilisez des machines physiques standard. Par exemple, si vous pensez exploiter quatre applications à fortes E/S, allouez quatre fois les capacités de performance aux LUN de l'ESXi.
- Lorsque vous utilisez plusieurs systèmes ESXi avec vCenter Server, les exigences de performance requises pour le sous-système de stockage augmentent en conséquence.
- Le nombre d'E/S en attente requises par les applications exécutées sur le système ESXi doit correspondre au nombre d'E/S pouvant être traitées par le HBA et la baie de stockage.

Utilisation de Fibre Channel NPIV avec des machines virtuelles vSphere

La virtualisation d'ID N-Port virtuel (NPIV) est une norme ANSI T11 qui décrit comment un port HBA unique Fibre Channel peut s'enregistrer dans la structure avec plusieurs noms worldwide mondiaux (WWPN). Cela permet au N-Port attaché à la structure de posséder des adresses de structure multiples. Chaque adresse s'affiche comme une entité unique sur l'infrastructure Fibre Channel. Vous pouvez configurer vos machines virtuelles pour utiliser Fibre Channel NPIV.

Comment fonctionne l'accès à un LUN par NPIV

NPIV permet à un unique port HBA FC d'enregistrer plusieurs identifiants WWN (World Wide Name) uniques dans la structure, chacun pouvant être attribué à une machine virtuelle. Lors de l'utilisation de NPIV, un administrateur SAN peut surveiller et router l'accès au stockage pour une machine virtuelle.

Seules les machines virtuelles dotées de RDM peuvent avoir des affectations WWN, et elles utilisent ces affectations pour tout le trafic RDM.

Lorsqu'une machine virtuelle possède un WWN qui lui est assigné, le fichier de configuration de la machine virtuelle (.vmx) est mis à jour pour inclure une paire WWN. Cette paire est composée d'un nom de port mondial (WWPN) et d'un nom de noeud mondial (WWNN). Au démarrage de cette machine virtuelle, VMkernel active un port virtuel (VPORT) sur le port physique HBA utilisé pour accéder au LUN. Le VPORT est un HBA virtuel qui s'affiche dans la structure FC comme un HBA physique. En tant que son identifiant unique, le VPORT utilise la paire WWN qui a été attribuée à la machine virtuelle.

Chaque VPORT est spécifique de la machine virtuelle. Le VPORT est détruit sur l'hôte et ne figure plus dans la structure FC lorsque la machine virtuelle est mise hors tension. Lorsqu'une machine virtuelle est migrée d'un hôte vers un autre, le VPORT se ferme sur le premier hôte et s'ouvre sur l'hôte de destination.

Si les machines virtuelles ne possèdent pas d'affectations WWN, elles peuvent accéder aux LUN de stockage au moyen des WWN des HBA physiques de leur hôte.

Conditions nécessaires pour l'utilisation de NPIV

Si vous prévoyez d'activer NPIV sur vos machines virtuelles, vous devez connaître certaines conditions préalables.

- NPIV ne peut être utilisé que pour des machines virtuelles avec disques RDM. Les machines virtuelles dotées de disques virtuels standard utilisent les noms WWN des HBA physiques de l'hôte.
- Les HBA doivent prendre en charge NPIV.

Pour plus d'informations, consultez le *Guide de compatibilité VMware* ainsi que la documentation du fournisseur.

- Utilisez des HBA du même type. VMware ne prend pas en charge les HBA hétérogènes sur le même hôte ayant accès aux mêmes LUN.
- Si un hôte utilise de multiples HBA physiques en tant que chemins vers le stockage, sélectionnez tous les chemins physiques vers la machine virtuelle. Cela est nécessaire afin de prendre en charge le chemins multiples, même si un seul chemin sera actif à la fois.
- Vérifiez que les HBA physiques sur l'hôte peuvent détecter tous les LUN devant être accessibles par les machines virtuelles compatibles NPIV exécutées sur cet hôte.
- Les commutateurs de structure doivent prendre en charge NPIV.
- Lorsque vous configurez un LUN pour un accès NPIV au niveau du stockage, assurez-vous que le numéro de LUN NPIV et l'ID NPIV de la cible correspondent au LUN physique et à l'ID cible.
- Choisissez la zone des WWPN NPIV de telle sorte qu'ils se connectent à tous les systèmes de stockage accessibles par les hôtes du cluster, même si la machine virtuelle n'utilise pas le stockage. Si vous ajoutez de nouveaux systèmes de stockage à un cluster incluant une ou plusieurs machines virtuelles compatibles NPIV, ajoutez les nouvelles zones, de telle sorte que les WWPN NPIV puissent détecter les nouveaux ports cibles du système de stockage.

Capacités et limitations NPIV

Découvrez les capacités et limitations spécifiques de l'utilisation de NPIV avec ESXi.

ESXi avec NPIV prend en charge les éléments suivants :

- NPIV prend en charge vMotion. Lorsque vous utilisez vMotion pour migrer une machine virtuelle, elle conserve le WWN assigné.
Si vous migrez une machine virtuelle activée par NPIV vers un hôte qui ne prend pas en charge NPIV, VMkernel repasse à l'utilisation d'un HBA physique pour acheminer l'E/S.
- Si votre environnement FC SAN prend en charge les E/S simultanées sur les disques depuis une baie active-active, les E/S simultanées vers deux ports NPIV différents sont également prises en charge.

Lorsque vous utilisez ESXi avec NPIV, les limitations suivantes s'appliquent :

- Étant donné que la technologie NPIV est une extension du protocole FC, elle exige un commutateur FC et ne fonctionne pas sur les disques FC directement reliés.
- Lorsque vous clonez une machine virtuelle ou un modèle avec un WWN assigné, les clones ne conservent pas le WWN.
- NPIV ne prend pas en charge Storage vMotion.
- La désactivation et la réactivation du NPIV sur un commutateur FC alors que des machines virtuelles sont exécutées peut provoquer la panne du lien FC et l'arrêt des E/S.

Configurer ou modifier des attributions WWN

Attribuez des paramètres WWN à une machine virtuelle. Vous pourrez modifier des attributions WWN ultérieurement.

Vous pouvez créer de 1 à 16 paires de WWN, pouvant être mappées vers les premières HBA FC physiques 1 à 16 de l'hôte.

De manière générale, vous ne devez pas changer les attributions WWN existantes sur votre machine virtuelle. Dans certaines circonstances, par exemple, lorsque des WWN attribués manuellement provoquent des conflits sur le SAN, il peut être nécessaire de changer ou de supprimer les WWN.

Conditions préalables

- Avant de configurer un WWN, vérifiez que l'hôte ESXi peut accéder à la liste de contrôle d'accès LUN de stockage configurée du côté baie.
- Si vous souhaitez modifier les WWN existants, mettez la machine virtuelle hors tension.

Procédure

- 1 Cliquez avec le bouton droit de la souris sur la machine virtuelle dans l'inventaire et sélectionnez **Modifier les paramètres**.
- 2 Cliquez sur **Options VM** et développez **Fibre Channel NPIV**.
- 3 Créez ou modifiez les attributions WWN en sélectionnant l'une des options suivantes :

Option	Description
Désactivez temporairement NPIV pour cette machine virtuelle.	Désactivez mais ne supprimez pas les attributions WWN existantes pour la machine virtuelle.
Laisser tel quel	Conserver les attributions WWN existantes. La section Attributions de WWN en lecture seule affiche les valeurs de noeud et de port des attributions WWN existantes.
Générer nouveaux WWN	Générer de nouveaux WWN, en écrasant les WWN existants. Les WWN des HBA ne sont pas affectés. Spécifiez le nombre de WWNN et de WWPN. Un minimum de deux WWPN est requis pour prendre en charge le basculement avec NPIV. Généralement, un seul WWNN est créé pour chaque machine virtuelle.
Supprimer l'attribution WWN	Supprimer les WWN attribués à la machine virtuelle. La machine virtuelle utilise les WWN du HBA pour accéder au LUN de stockage.

- 4 Cliquez sur **OK** pour enregistrer vos modifications.

Étape suivante

Enregistrez les nouveaux WWN dans la structure.

Utilisation d'ESXi avec un SAN iSCSI

4

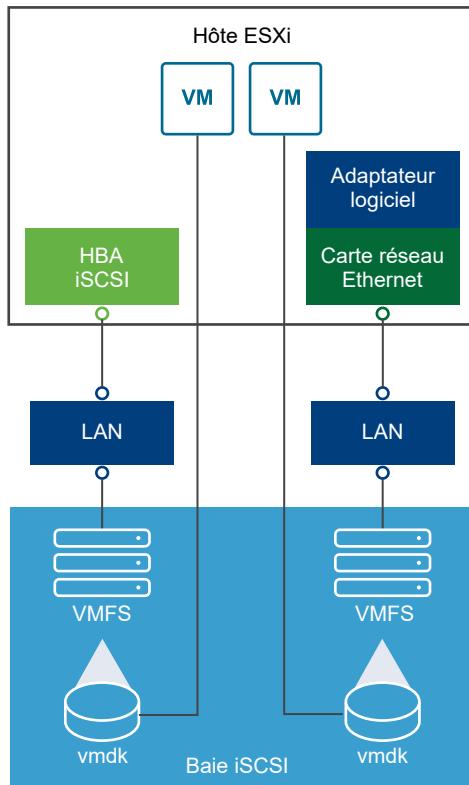
ESXi peut se connecter à un stockage SAN externe à l'aide du protocole iSCSI (Internet SCSI). Outre le protocole iSCSI traditionnel, ESXi prend également en charge iSER (iSCSI Extensions for RDMA).

Le protocole iSER permet à l'hôte d'utiliser la même infrastructure iSCSI, mais remplace le transport TCP/IP par le transport RDMA (Remote Direct Memory Access).

À propos du SAN iSCSI

Le SAN iSCSI utilise des connexions Ethernet entre les hôtes et les sous-systèmes de stockage haute performance.

Du côté hôte, les composants SAN iSCSI comprennent les adaptateurs de bus hôte (HBA) iSCSI ou les cartes d'interface réseau (NIC). Le réseau iSCSI comprend également les commutateurs et les routeurs qui acheminent le trafic de stockage, les câbles, les processeurs de stockage (SPs) et les systèmes de disque de stockage.



Le SAN iSCSI utilise une architecture client-serveur.

Le client, appelé initiateur iSCSI, agit sur votre hôte ESXi. Il lance des sessions iSCSI en émettant des commandes SCSI et en les transmettant, encapsulées dans le protocole iSCSI, à un serveur iSCSI. Le serveur est connu sous le nom de cible iSCSI. En général, la cible iSCSI représente un système de stockage physique sur le réseau.

Elle peut également être un SAN iSCSI virtuel, par exemple un émulateur cible iSCSI s'exécutant sur une machine virtuelle. La cible iSCSI répond aux commandes de l'initiateur en transmettant les données iSCSI requises.

Chemins multiples iSCSI

Lors du transfert de données entre le serveur hôte et le stockage, le SAN utilise une technique connue sous le nom de gestion multivoie. Avec la gestion multivoie, votre hôte ESXi peut disposer de plusieurs chemins physiques vers un LUN sur un système de stockage.

De manière générale, un chemin unique partant d'un hôte vers un LUN se compose d'un adaptateur iSCSI ou NIC, de ports de commutateur, de câbles de connexion et du port de contrôleur de stockage. Si un des composants du chemin subit une défaillance, l'hôte sélectionne un autre chemin disponible pour l'E/S. Le processus de détection d'un chemin défaillant et de changement vers un autre chemin est connu sous le nom de basculement de chemin.

Pour plus d'informations sur la gestion chemins multiples, consultez [Chapitre 10 Présentation de la gestion multivoie et du basculement](#).

Nœuds et ports du SAN iSCSI

Une entité simple détectable sur le SAN iSCSI, telle qu'un initiateur ou une cible, représente un nœud iSCSI.

Chaque nœud possède un nom de nœud. ESXi utilise plusieurs méthodes pour identifier un nœud.

Adresse IP

Chaque nœud iSCSI peut être associé à une adresse IP de sorte que le matériel d'acheminement et de commutation du réseau puisse établir la connexion entre l'hôte et le stockage. Cette adresse est semblable à l'adresse IP que vous attribuez à votre ordinateur pour bénéficier de l'accès au réseau de votre entreprise ou à Internet.

nom iSCSI

Nom unique international permettant d'identifier le nœud. iSCSI utilise les formats IQN (iSCSI Qualified Name) et EUI (Extended Unique Identifier).

Par défaut, ESXi génère des noms iSCSI uniques pour vos initiateurs iSCSI, par exemple, `iqn.1998-01.com.vmware:iscsitestox-68158ef2`. Il n'est généralement pas nécessaire de modifier la valeur par défaut, mais si vous la modifiez, veillez à ce que le nouveau nom iSCSI que vous saisissez soit unique mondialement.

Alias iSCSI

Un nom plus explicite pour le port ou le périphérique iSCSI utilisé à la place du nom iSCSI. Les alias iSCSI ne sont pas uniques et sont destinés à être un nom convivial à associer à un port.

Chaque nœud possède un ou plusieurs ports qui le connectent au SAN. Les ports iSCSI sont les points limites d'une session iSCSI.

Conventions de dénomination iSCSI

iSCSI utilise un nom unique spécial pour identifier un nœud iSCSI, cible ou initiateur.

Les noms iSCSI sont formatées de deux manières différentes. Le format le plus courant est le format IQN.

Pour plus d'informations sur les exigences de dénomination iSCSI et les profils de chaîne, reportez-vous aux sections RFC 3721 et RFC 3722 sur le site Web IETF.

Format IQN (iSCSI Qualified Name)

Le format IQN présente le nom sous la forme `iqn.yyyy-mm.naming-authority:unique`, où :

- `yyyy-mm` représente l'année et le mois où l'autorité de dénomination a été établie.

- *naming-authority* représente la syntaxe inverse du nom de domaine Internet de l'autorité de dénomination. Par exemple, l'autorité de dénomination `iscsi.vmware.com` peut avoir le nom `iqn.1998-01.com.vmware.iscsi` au format IQN. Le nom indique que le nom de domaine `vmware.com` a été enregistré en janvier 1998 et que `iscsi` est un sous-domaine géré par `vmware.com`.
- *unique name* représente n'importe quel nom à votre guise, par exemple le nom de votre hôte. L'autorité de dénomination doit s'assurer que tous les éventuels noms attribués après les deux-points sont uniques, comme :
 - `iqn.1998-01.com.vmware.iscsi:name1`
 - `iqn.1998-01.com.vmware.iscsi:name2`
 - `iqn.1998-01.com.vmware.iscsi:name999`

Format EUI (Enterprise Unique Identifier)

Le format EUI se présente sous la forme `eui.16_hex_digits`.

Par exemple, `eui.0123456789ABCDEF`.

Les 16 chiffres hexadécimaux sont des représentations de texte d'un nombre 64 bits au format EUI (extended unique identifier) de l'IEEE. Les 24 premiers bits représentent l'identifiant d'une société que l'IEEE enregistre avec une société spécifique. Les 40 bits restants sont attribués par l'entité possédant l'identifiant de cette société et doivent être uniques.

Initiateurs iSCSI

Pour accéder aux cibles iSCSI, votre hôte ESXi utilise des initiateurs iSCSI.

L'initiateur est un logiciel ou un matériel installé sur votre hôte ESXi. L'initiateur iSCSI est issu de la communication entre votre hôte et un système de stockage iSCSI externe et envoie des données au système de stockage.

Dans l'environnement ESXi, les adaptateurs iSCSI configurés sur votre hôte jouent le rôle d'initiateurs. ESXi prend en charge plusieurs types d'adaptateurs iSCSI.

Pour plus d'informations sur la configuration et l'utilisation des adaptateurs iSCSI, reportez-vous à la section [Chapitre 5 Configuration des adaptateurs iSCSI et iSER et du stockage](#).

Adaptateur de logiciel iSCSI

Un adaptateur de logiciel iSCSI est un code VMware intégré au VMkernel. À l'aide de l'adaptateur iSCSI logiciel, votre hôte peut se connecter au périphérique de stockage iSCSI via des adaptateurs réseau standard. L'adaptateur de logiciel iSCSI gère le traitement iSCSI tout en communiquant avec l'adaptateur réseau. Avec l'adaptateur de logiciel iSCSI, vous pouvez employer la technologie iSCSI sans acheter de matériel spécialisé.

Adaptateur de matériel iSCSI

Un adaptateur de matériel iSCSI est un adaptateur tiers qui décharge le traitement iSCSI et le réseau de votre hôte. Les adaptateurs matériels iSCSI se divisent en plusieurs catégories.

- **Dependent Hardware iSCSI Adapter.** Dépend du réseau VMware et des interfaces de configuration et de gestion iSCSI fournies par VMware.

Ce type d'adaptateur peut être un adaptateur réseau standard disposant de la fonction de déchargement iSCSI pour le même port. La fonction de déchargement iSCSI dépend de la configuration du réseau pour obtenir les paramètres IP, MAC et d'autres paramètres utilisés pour les sessions iSCSI. La carte réseau Broadcom 5709 sous licence iSCSI est un exemple d'adaptateur dépendant.

- **Independent Hardware iSCSI Adapter.** Implémente ses propres protocoles réseau et ses propres interfaces de configuration et de gestion iSCSI.

En général, une carte disposant uniquement de la fonction de déchargement iSCSI ou de la fonction de déchargement iSCSI et NIC standard est un adaptateur iSCSI matériel indépendant. La fonction de déchargement iSCSI dispose d'une fonction de gestion indépendante de la configuration, qui assigne les paramètres IP, MAC et d'autres paramètres pour les sessions iSCSI. L'adaptateur QLogic QLA4052 est un exemple d'adaptateur indépendant.

Les adaptateurs de matériel iSCSI doivent avoir une licence. Sinon, ils pourraient ne pas apparaître dans le client ou vSphere CLI. Contactez votre vendeur pour avoir des renseignements sur la licence.

Utilisation du protocole iSER avec ESXi

Outre le protocole iSCSI traditionnel, ESXi prend en charge le protocole d'extensions iSCSI pour RDMA (iSER). Lorsque le protocole iSER est activé, l'infrastructure iSCSI située sur l'hôte ESXi peut utiliser le transport d'accès direct à la mémoire à distance (RDMA) au lieu du protocole TCP/IP.

Le protocole iSCSI traditionnel transporte des commandes SCSI sur un réseau TCP/IP entre un initiateur iSCSI situé sur un hôte et une cible iSCSI située sur un périphérique de stockage. Le protocole iSCSI encapsule les commandes et assemble les données en paquets pour la couche TCP/IP. Lorsque les données arrivent, le protocole iSCSI désassemble les paquets TCP/IP, afin que les commandes SCSI puissent être différencierées et remises au périphérique de stockage.

Le protocole iSER diffère du protocole iSCSI traditionnel, car il remplace le modèle de transfert de données TCP/IP par le transport d'accès direct à la mémoire à distance (RDMA). Grâce à la technologie de placement direct des données du RDMA, le protocole iSER peut transférer directement des données entre la mémoire tampon de l'hôte ESXi et les périphériques de stockage. Cette méthode permet d'éliminer le traitement et la copie des données engendrés par le protocole TCP/IP et peut également réduire la latence et la charge du CPU sur le périphérique de stockage.

Dans l'environnement iSER, le protocole iSCSI fonctionne exactement comme avant, mais il utilise une infrastructure RDMA sous-jacente au lieu de l'interface basée sur TCP/IP.

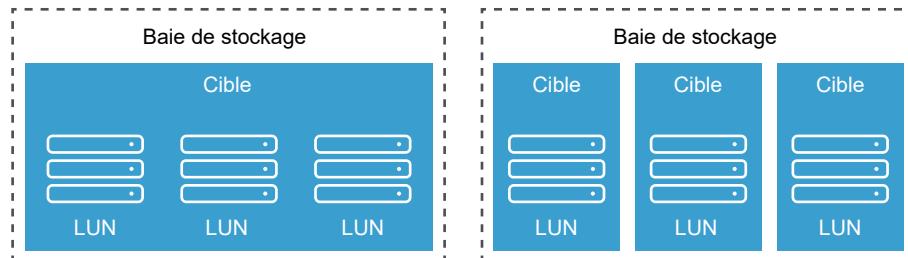
Comme le protocole iSER préserve la compatibilité avec l'infrastructure iSCSI, le processus d'activation du protocole iSER sur l'hôte ESXi est semblable au processus pour le protocole iSCSI. Reportez-vous à la section [Configurer iSER avec ESXi](#).

Établissement des connexions iSCSI

Dans un contexte ESXi, le terme cible identifie une unité de stockage unique accessible par l'hôte. Les termes périphérique de stockage et LUN décrivent un volume logique représentant l'espace de stockage sur une cible. En général, les termes périphérique et LUN, dans un contexte ESXi signifient qu'un volume SCSI est présenté à l'hôte depuis une unité de stockage cible et disponible pour un formatage.

Les différents fournisseurs de stockage iSCSI présentent le stockage sur des hôtes de différentes manières. Certains fournisseurs présentent plusieurs LUN sur une seule cible, alors que d'autres présentent plusieurs cibles disposant chacune d'un LUN.

Figure 4-1. Représentations LUN / Cible



Dans ces exemples, trois LUN sont disponibles dans chacune de ces configurations. Dans le premier cas, l'hôte détecte une cible, mais cette cible possède trois LUN utilisables. Chaque LUN représente un volume de stockage individuel. Dans le second cas, l'hôte détecte trois cibles différentes, chacune possédant un LUN.

Les initiateurs iSCSI basés sur l'hôte établissent des connexions sur chaque cible. Les systèmes de stockage avec une cible unique contenant plusieurs LUN présentent un trafic vers tous les LUN sur une seule connexion. Sur un système possédant trois cibles avec un LUN chacune, l'hôte utilise des connexions distinctes vers les trois LUN.

Ces informations sont utiles lorsque vous essayez d'agrégier le trafic de stockage sur plusieurs connexions à partir de l'hôte doté de plusieurs adaptateurs iSCSI. Vous pouvez définir le trafic d'une cible vers un adaptateur particulier et utiliser un adaptateur différent pour le trafic vers une autre cible.

Types de systèmes de stockage iSCSI

Votre hôte prend en charge les types de stockage ESXi suivants : actif-actif, actif-passif et conforme à ALUA.

Système de stockage actif-actif

Prend en charge l'accès simultané aux LUN par tous les ports de stockage qui sont disponibles sans dégradation importante des performances. Tous les chemins sont toujours actifs, sauf si un chemin est défaillant.

Système de stockage actif-passif

Un système dans lequel un processeur de stockage fournit l'accès à un LUN donné. Les autres processeurs sont utilisés en tant que sauvegarde pour le LUN et peuvent fournir l'accès à d'autres E/S de LUN. L'E/S peut uniquement être envoyée avec succès vers un port actif pour un LUN spécifique. Si l'accès via le port de stockage actif échoue, un des processeurs de stockage passifs peut être activé par les serveurs qui y accèdent.

Système de stockage asymétrique

Prend en charge Asymmetric Logical Unit Access (ALUA). Les systèmes de stockage conformes à ALUA offrent des niveaux différents d'accès par port. Avec ALUA, les hôtes peuvent déterminer les états des ports cibles et classer les chemins par priorité. L'hôte utilise certains des chemins actifs comme étant principaux et d'autres comme secondaires.

Système de stockage de ports virtuels

Prend en charge l'accès à tous les LUN disponibles via un port virtuel unique. Les systèmes de stockage de ports virtuels sont des périphériques de stockage actifs-actifs qui cachent leurs nombreuses connexions via un seul port. La gestion multivoie ESXi ne permet pas d'établir de multiples connexions depuis un port spécifique vers le stockage par défaut. Certains fournisseurs de stockage fournissent des gestionnaires de sessions pour établir et gérer de multiples connexions vers leur stockage. Ces systèmes de stockage traitent les basculements de ports et l'équilibrage des connexions de manière transparente. Cette fonctionnalité est souvent appelée basculement transparent.

Découverte, authentification et contrôle d'accès

Vous pouvez utiliser plusieurs méthodes pour découvrir votre stockage et y limiter l'accès.

Vous devez configurer votre hôte et le système de stockage iSCSI pour qu'il prenne en charge votre politique de contrôle d'accès au stockage.

Découverte

Une session de découverte fait partie du protocole iSCSI. Elle renvoie l'ensemble des cibles auxquelles vous pouvez accéder sur un système de stockage iSCSI. Les deux types de découverte disponibles sur ESXi sont les découvertes dynamique et statique. La découverte dynamique obtient une liste des cibles accessibles à partir du système de stockage iSCSI. La découverte statique peut accéder uniquement à une cible particulière par nom cible et adresse.

Pour plus d'informations, consultez [Configurer la découverte dynamique ou statique pour iSCSI et iSER sur l'hôte ESXi](#).

Authentification

Les systèmes de stockage iSCSI authentifient un initiateur par un nom et une paire de clés. L'ESXi prend en charge le protocole d'authentification CHAP. Pour utiliser l'authentification CHAP, l'hôte ESXi et le système de stockage iSCSI doivent avoir la fonction CHAP activée et disposer d'informations d'identification communes.

Pour plus d'informations sur l'activation de CHAP, consultez [Configuration des paramètres CHAP pour les adaptateurs de stockage iSCSI ou iSER](#)

Contrôle d'accès

Le contrôle d'accès est une règle configurée sur le système de stockage iSCSI. La plupart des mises en œuvre prennent en charge un ou plusieurs des trois types de contrôle d'accès :

- Par nom d'initiateur
- Par adresse IP
- Par protocole CHAP

Seuls les initiateurs qui respectent toutes les règles peuvent accéder au volume iSCSI.

L'utilisation exclusive du CHAP pour le contrôle d'accès peut ralentir les réanalyses parce que l'hôte ESXi peut découvrir toutes les cibles, mais échoue ensuite à l'étape d'authentification. Les réanalyses iSCSI sont plus rapides si l'hôte détecte uniquement les cibles qu'il peut authentifier.

Accès des machines virtuelles aux données sur un SAN iSCSI

ESXi stocke les fichiers disque d'une machine virtuelle dans une banque de données VMFS se trouvant sur un périphérique de stockage du SAN. Lorsque les systèmes d'exploitation invités de la machine virtuelle envoient des commandes SCSI à leurs disques virtuels, la couche de virtualisation SCSI traduit ces commandes en opérations de fichier VMFS.

Lorsqu'une machine virtuelle interagit avec son disque virtuel stocké sur un SAN, le processus suivant a lieu :

- 1 Lorsque le système d'exploitation invité sur une machine virtuelle lit ou écrit sur le disque SCSI, il envoie des commandes SCSI au disque virtuel.
- 2 Les pilotes de périphériques dans le système d'exploitation de la machine virtuelle communiquent avec les contrôleurs SCSI virtuels.
- 3 Le contrôleur SCSI virtuel transmet les commandes au VMkernel.
- 4 Le VMkernel effectue les tâches suivantes :
 - a Localisation du fichier de disque virtuel approprié dans le volume VMFS.

- b Mappage des requêtes de blocs sur le disque virtuel sur les blocs sur le périphérique physique approprié.
 - c Envoi de la demande d'E/S modifiée à partir du pilote du périphérique du VMkernel vers l'initiateur iSCSI, matériel ou logiciel.
- 5 Si l'initiateur iSCSI est un adaptateur iSCSI matériel, indépendant ou dépendant, l'adaptateur effectue les tâches suivantes :
- a Encapsulation des demandes d'E/S dans les unités de données de protocole (PDU) iSCSI.
 - b Encapsulation des PDU iSCSI dans les paquets TCP/IP.
 - c Envoi des paquets IP via Ethernet au système de stockage iSCSI.
- 6 Si l'initiateur iSCSI est un adaptateur iSCSI logiciel, les actions suivantes ont lieu :
- a L'initiateur iSCSI encapsule les demandes d'E/S dans les PDU iSCSI.
 - b L'initiateur envoie les PDU iSCSI via des connexions TCP/IP.
 - c La pile TCP/IP VMkernel relaie les paquets TCP/IP vers un adaptateur réseau (NIC) physique.
 - d La carte réseau (NIC) physique envoie les paquets IP via Ethernet au système de stockage iSCSI.
- 7 Les commutateurs et les routeurs Ethernet sur le réseau acheminent la demande vers le périphérique de stockage approprié.

Correction des erreurs

Pour protéger l'intégrité des en-têtes et des données iSCSI, le protocole iSCSI propose des méthodes de correction des erreurs, plus connues sous le nom de résumés d'en-tête et de résumés de données.

Ces deux méthodes sont prises en charge par l'hôte ESXi et peuvent être activées. Ces méthodes sont utilisées pour vérifier l'en-tête et les données SCSI transférées entre les initiateurs et les cibles iSCSI dans les deux sens.

Les résumés d'en-tête et de données vérifient l'intégrité des données non cryptographiques en plus des contrôles de santé effectués par d'autres couches du réseau, telles que TCP et Ethernet. Les résumés vérifient le chemin de communication complet, y compris tous les éléments susceptibles de modifier le trafic au niveau du réseau, tels que les routeurs, les commutateurs et les proxys.

L'existence et le type des résumés sont négociés lorsqu'une connexion iSCSI est établie. Lorsque l'initiateur et la cible s'accordent sur une configuration de résumé, celui-ci doit être utilisé pour l'ensemble du trafic entre eux.

L'activation des résumés d'en-tête et de données nécessite un traitement supplémentaire à la fois pour l'initiateur et la cible, et peut affecter le débit et les performances d'utilisation du CPU.

Note Les systèmes qui utilisent les processeurs Intel Nehalem délestent les calculs de résumé iSCSI, en réduisant ainsi l'incidence sur les performances.

Pour plus d'informations sur l'activation des résumés d'en-tête et de données, reportez-vous à la section [Configuration des paramètres avancés iSCSI](#).

Ce chapitre contient les rubriques suivantes :

- [Démarrage à partir du SAN iSCSI](#)
- [Meilleures pratiques pour le stockage iSCSI](#)

Démarrage à partir du SAN iSCSI

Lorsque vous paramétrez votre hôte pour qu'il démarre depuis un SAN, l'image de démarrage de votre hôte est archivée sur une ou plusieurs numéros d'unité logique (LUN) du système de stockage du SAN. Lorsque l'hôte démarre, il se lance à partir de la LUN se trouvant sur le SAN et non pas à partir du disque local.

Vous pouvez utiliser le démarrage à partir du SAN si vous ne souhaitez pas effectuer de maintenance de l'archivage local ou si vous avez des configurations matérielles sans disques comme des systèmes lame.

ESXi prend en charge différentes méthodes de démarrage à partir du SAN iSCSI.

Tableau 4-1. Prise en charge du démarrage à partir du SAN iSCSI

Matériel iSCSI indépendant	iSCSI logiciel
Configurez le iSCSI HBA pour un démarrage à partir du SAN. Pour plus d'informations sur la configuration du HBA, consultez la section Configurer l'adaptateur iSCSI matériel indépendant pour le démarrage à partir du SAN .	Utilisez l'adaptateur iSCSI logiciel et un adaptateur réseau qui prend en charge le format de la table du microprogramme de démarrage iSCSI (iBFT). Pour plus d'informations, consultez Installation et configuration de VMware ESXi .

Recommandations générales pour le démarrage à partir du SAN iSCSI

Si vous prévoyez de paramétrer et d'utiliser un numéro d'unité logique (LUN) iSCSI en tant que périphérique de démarrage pour votre hôte, vous devez suivre certaines instructions générales.

Les directives suivantes s'appliquent au démarrage à partir du matériel iBFT et iSCSI indépendant.

- Consultez les recommandations de l'éditeur du matériel que vous utilisez dans votre configuration de démarrage.
- Pour connaître les spécifications préalables et requises d'installation, consultez [Installation et Configuration vSphere](#).

- Utilisez des adresses IP statiques afin de réduire les risques de conflits DHCP.
- Utilisez des LUN différentes pour les banques de données VMFS et les partitions de démarrage.
- Configurez correctement les ACL sur votre système de stockage.
 - Le LUN de démarrage doit uniquement être visible pour l'hôte qui utilise le LUN. Aucun autre hôte sur le SAN n'est autorisé à voir ce LUN de démarrage.
 - Si un LUN est utilisé pour une banque de données VMFS, plusieurs hôtes peuvent partager ce LUN.
- Configurez une partition de diagnostic.
 - Vous pouvez placer la partition de diagnostic sur le LUN de démarrage uniquement avec du matériel iSCSI indépendant. Si vous configurez la partition de diagnostic dans la LUN de démarrage, cette LUN ne peut pas être partagée sur plusieurs hôtes. Si un LUN séparé est utilisé pour la partition de diagnostic, plusieurs hôtes peuvent partager ce LUN.
 - Si vous démarrez à partir de SAN en utilisant iBFT, vous ne pouvez pas configurer une partition de diagnostic sur un LUN SAN. Pour collecter les informations de diagnostic de votre hôte, utilisez vSphereESXi Dump Collector sur un serveur distant. Pour plus d'informations sur ESXi Dump Collector, consultez *Installation et configuration de vCenter Server et Mise en réseau vSphere*.

Préparation du SAN iSCSI

Avant de configurer votre hôte pour qu'il démarre à partir d'un LUN du logiciel iSCSI, préparez et configurez votre réseau de zone de stockage.

Attention Si vous utilisez une installation basée sur des scripts pour installer ESXi lors du démarrage à partir d'un SAN, prenez des mesures particulières afin d'éviter toutes pertes de données non intentionnelles.

Procédure

- 1 Connectez les câbles réseau en vous référant au guide de câblage s'appliquant à votre configuration.
- 2 Vérifiez la connectivité IP entre votre système de stockage et votre serveur.

Vérifiez la configuration de tous les routeurs ou commutateurs de votre réseau de stockage. Les systèmes de stockage doivent être en mesure de vérifier la connexion aux adaptateurs iSCSI de vos hôtes.

3 Configurez le système de stockage.

- a Créez un volume (ou une LUN) sur le système de stockage depuis lequel votre hôte va démarrer.
- b Configurez le système de stockage afin que votre hôte puisse accéder à la LUN qui lui est assignée.

Cette étape pourrait impliquer la mise à jour des ACL avec les adresses IP, les noms iSCSI et le paramètre d'authentification CHAP utilisé sur l'hôte. Certains systèmes de stockage, en plus de devoir fournir les informations d'accès à l'hôte ESXi, exigent également d'associer de manière explicite le LUN assigné à l'hôte.

- c Assurez-vous que la LUN est présentée correctement à l'hôte.
- d Assurez-vous qu'aucun autre système n'a accès à la LUN configurée.
- e Notez le nom du logiciel iSCSI et les adresses IP des cibles assignée à l'hôte.

Vous devez avoir ces informations pour configurer vos adaptateurs iSCSI.

Configurer l'adaptateur iSCSI matériel indépendant pour le démarrage à partir du SAN

Si votre hôte ESXi utilise un adaptateur iSCSI matériel indépendant, tel que QLogic HBA, vous pouvez configurer l'adaptateur pour démarrer depuis le SAN.

Cette procédure vous explique comment activer le QLogic iSCSI HBA pour qu'il démarre à partir du SAN. Pour plus d'informations et plus de détails sur les paramètres de configuration de l'adaptateur QLogic, rendez-vous sur le site Web de QLogic.

Procédure

- 1 Démarrez le support d'installation et redémarrez l'hôte.
- 2 Utilisez le BIOS pour paramétriser l'hôte afin qu'il démarre d'abord à partir du support d'installation.
- 3 Au cours du POST du serveur, appuyez sur les touches Ctrl+q pour entrer dans le menu de configuration de QLogic iSCSI HBA.
- 4 Sélectionnez le port d'E/S à configurer.

Par défaut, le mode Adaptateur démarrage est paramétré sur Désactiver.

- 5 Configurez le HBA.
 - a Depuis le menu **Options Fast!UTIL**, sélectionnez **Paramètres de configuration > Paramètres de l'adaptateur hôte**.
 - b (Facultatif) Configurez les paramètres suivants pour l'adaptateur de votre hôte : adresse IP initiatrice, masque de sous-réseau, passerelle, nom iSCSI initiateur et CHAP.
- 6 Configurez les paramètres iSCSI.

Reportez-vous à [Configuration des paramètres de démarrage de iSCSI](#).

- 7 Enregistrez vos changements et redémarrez le système.

Configuration des paramètres de démarrage de iSCSI

Configurez les paramètres de démarrage d'iSCSI afin que votre hôte ESXi puisse démarrer à partir d'un LUN iSCSI.

Procédure

- 1 Dans le menu **Options Fast!UTIL**, sélectionnez **Paramètres de configuration > Paramètres de démarrage iSCSI**.
- 2 Avant de définir SendTargets, définissez le mode Adaptateur démarrage sur **Manuel**.
- 3 Sélectionnez **Paramètres du périphérique de démarrage principal**.
 - a Saisissez la découverte **IP cible** et **Port cible**.
 - b Configurez les paramètres des zones de texte **LUN de démarrage** et **Nom iSCSI**.
 - Si une seule cible iSCSI et un seul LUN sont disponibles à l'adresse cible, ne renseignez pas **LUN de démarrage** et **Nom iSCSI**.
Une fois que votre hôte atteint le système de stockage cible, ces zones de texte sont renseignées avec les informations appropriées.
 - Si plusieurs cibles iSCSI et LUN sont disponibles, entrez des valeurs pour **LUN de démarrage** et **Nom iSCSI**.
 - c Enregistrez vos changements.
- 4 Depuis le menu **Paramètres de démarrage iSCSI**, sélectionnez le périphérique de démarrage principal.
Une réanalyse automatique du HBA détecte les nouveaux LUN cibles.
- 5 Sélectionnez la cible iSCSI.
S'il y a plusieurs LUN dans la cible, vous pouvez sélectionnez un ID LUN spécifique en appuyant sur **Entrée** après avoir localisé le périphérique iSCSI.
- 6 Retournez dans le menu **Paramètres du périphérique de démarrage principal**. Après la réanalyse, **LUN de démarrage** et **Nom iSCSI** sont renseignés. Changez la valeur du **LUN de démarrage** sur l'ID LUN approprié.

Meilleures pratiques pour le stockage iSCSI

Lorsque vous utilisez ESXi avec le SAN iSCSI, suivez les recommandations de VMware pour éviter des problèmes.

Consultez votre représentant de stockage pour savoir si votre système de stockage prend en charge les fonctionnalités d'accélération matérielle API de stockage - Intégration de baie. Le cas échéant, consultez la documentation du fournisseur pour activer la prise en charge de l'accélération matérielle du côté du système de stockage. Pour plus d'informations, consultez [Chapitre 16 Accélération matérielle du stockage](#).

Prévention des problèmes de iSCSI SAN

Lorsque vous utilisez ESXi avec un SAN, vous devez suivre des directives spécifiques afin d'éviter des problèmes de SAN.

Suivez les conseils suivants :

- Placez une seule banque de données VMFS sur chaque LUN.
 - Ne changez pas la politique de chemin que le système définit, sauf si vous comprenez les implications de tels changements.
 - Documentez tout ce que vous faites. Incluez des informations sur la configuration, le contrôle d'accès, le stockage, le commutateur, le serveur et la configuration HBA iSCSI, les versions de logiciel et microprogramme, et le plan des câbles de stockage.
 - Plan en cas de panne :
 - Faîtes plusieurs copies de vos mappages topologiques. Pour chaque élément, envisagez les conséquences sur votre SAN si cet élément tombe en panne.
 - Rayez chaque lien, commutateurs, HBA et autres éléments pour vérifier que vous n'avez omis aucun point de panne critique dans votre architecture.
 - Assurez-vous que les HBA iSCSI sont installés dans les slots corrects de l'hôte ESXi selon la vitesse de l'emplacement et du bus. Équilibrez la charge de bus PCI entre les divers bus du serveur.
 - Familiarisez-vous avec les différents points de contrôle de votre réseau de stockage, sur tous les points de visibilité, y compris l'ESXi, les graphiques de performance, les statistiques des commutateurs Ethernet et des performances de stockage.
 - Modifiez les ID LUN uniquement lorsque les banques de données VMFS déployées sur les LUN n'ont pas de machines virtuelles en cours d'exécution. Si vous modifiez les ID, ces machines virtuelles en fonction sur les banque de données VMFS peuvent tomber en panne.
- Après avoir modifié l'ID du LUN, vous devez réanalyser le stockage pour réinitialiser l'ID sur votre hôte. Pour plus d'informations sur l'utilisation de la réanalyse, consultez [Réanalyser les opérations de stockage ESXi](#).
- Si vous changez le nom iSCSI par défaut de votre adaptateur iSCSI, assurez-vous que le nom que vous entrez est unique mondialement et correctement formaté. Pour éviter des problèmes d'accès de stockage, n'attribuez jamais le même nom iSCSI à différents adaptateurs, même sur différents hôtes.

Optimisation des performances du stockage SAN iSCSI

Plusieurs facteurs contribuent à l'optimisation d'un environnement SAN classique.

Si l'environnement de réseau est correctement configuré, les composants iSCSI fournissent un débit adéquat et une latence suffisamment basse pour les initiateurs et les cibles iSCSI. Si le réseau est congestionné et les liens, commutateurs et routeurs sont saturés, la performance iSCSI en souffre et risque de ne plus convenir à un environnement ESXi.

Performances des systèmes de stockage

Les performances des systèmes de stockage sont l'un des principaux facteurs contribuant aux performances de la totalité de l'environnement iSCSI.

En cas de problème de performances des systèmes de stockage, consultez la documentation de votre éditeur de systèmes de stockage.

Lors de l'attribution des LUN, souvenez-vous que chaque LUN partagé est accessible par plusieurs hôtes et que plusieurs machines virtuelles peuvent exécuter sur chaque hôte. Un LUN utilisé par l'hôte ESXi peut servir à des E/S provenant d'applications très variées et exécutées sur différents systèmes d'exploitation. En raison de ces charges de travail très variées, le groupe RAID contenant les LUN ESXi ne doit pas inclure de LUN utilisés par d'autres hôtes qui n'exécutent pas ESXi pour les applications intensives.

Activez le cache de lecture et le cache d'écriture.

L'équilibrage de charge est le processus distribution des requêtes d'E/S serveur sur tous les SP disponibles et les chemins d'accès au serveur d'hôte associé. Le but est d'optimiser les performances en termes de débit (E/S par seconde, mégaoctets par seconde ou temps de réponse).

Les systèmes de stockage SAN nécessitent des modifications et des ajustements permanents pour s'assurer que les charges d'E/S sont réparties sur tous les chemins d'accès des systèmes de stockage. Pour répondre à cette exigence, répartissez les chemins d'accès vers les LUN entre tous les SP pour assurer un équilibrage de charge optimal. Une surveillance attentive permet de savoir quand il est nécessaire de rééquilibrer manuellement la répartition des LUN.

L'ajustement des systèmes de stockage équilibrées de manière statique implique la surveillance de statistiques de performance spécifiques (nombre d'opérations d'entrée-sortie par seconde, blocs par seconde et temps de réponse) et la répartition de la charge de travail des LUN pour répartir la charge de travail sur tous les SP.

Performances de serveur avec iSCSI

Pour garantir des performances optimales de l'hôte ESXi, tenez compte de plusieurs facteurs.

Chaque application de serveur doit avoir accès à son stockage désigné aux conditions suivantes :

- Vitesse d'E/S élevée (nombre d'opérations d'entrée-sortie par seconde)
- Rendement élevé (mégaoctets par seconde)
- Latence minimale (temps de réponse)

Comme chaque application a différentes exigences, ces objectifs peuvent être remplis en sélectionnant un groupe RAID approprié sur le système de stockage.

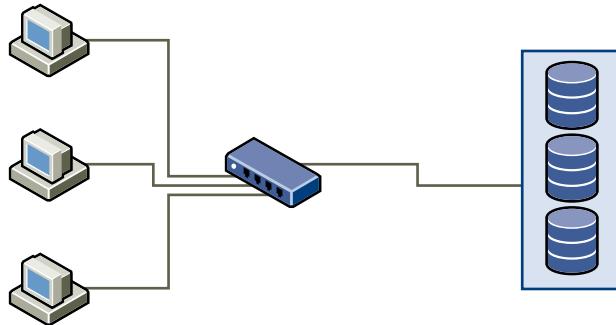
Pour atteindre les objectifs de performance, procédez comme suit :

- Placez chaque LUN sur un groupe RAID qui offre les niveaux de performance nécessaires. Surveillez les activités et l'utilisation des ressources des autres LUN dans le groupe RAID attribué. Un groupe RAID haute performance ayant un nombre excessif d'applications effectuant des E/S risque de ne pas satisfaire aux exigences de performance requises par une application exécutée sur l'hôte ESXi.
- Pour atteindre un débit maximal pour toutes les applications sur l'hôte pendant la période de pointe, installez un nombre suffisant de cartes réseau ou d'adaptateurs iSCSI matériels. Les entrées/sorties réparties sur plusieurs ports présentent un débit plus rapide et moins de latence pour chaque application.
- Pour assurer la redondance d'iSCSI logiciel, vérifiez que l'initiateur est connecté à tous les adaptateurs réseau utilisés pour la connectivité iSCSI.
- Lors de l'allocation de groupes LUN ou RAID aux systèmes ESXi, n'oubliez pas que plusieurs systèmes d'exploitation utilisent et partagent cette ressource. Les performances des LUN requises par l'hôte ESXi peuvent être beaucoup plus élevées que lorsque vous utilisez des machines physiques standard. Par exemple, si vous pensez exploiter quatre applications à fortes E/S, allouez quatre fois les capacités de performance aux LUN de l'ESXi.
- Lorsque vous utilisez plusieurs systèmes ESXi avec vCenter Server, les exigences de performance de stockage augmentent.
- Le nombre d'E/S en attente requises par applications exécutées sur un système ESXi doit correspondre au nombre d'E/S pouvant être traitées par le SAN.

Performances du réseau

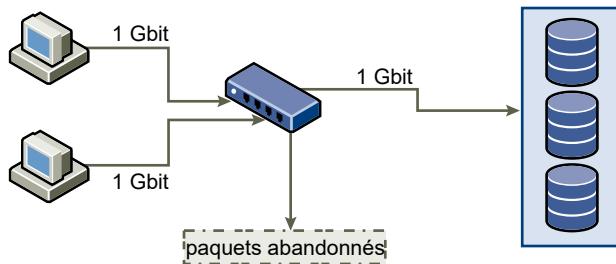
Généralement, un SAN consiste en un ensemble d'ordinateurs connectés à un ensemble de systèmes de stockage par un réseau de commutateurs. Il arrive souvent que plusieurs ordinateurs accèdent au même stockage.

Le graphique suivant montre plusieurs systèmes informatiques connectés à un système de stockage via un commutateur Ethernet. Dans cette configuration, chaque système est connecté au commutateur via un lien Ethernet unique. Le commutateur est connecté au système de stockage via un lien Ethernet unique.

Figure 4-2. Connexion au stockage par lien ethernet unique

Lorsque les systèmes lisent les données du stockage, le stockage répond en envoyant suffisamment de données pour remplir le lien entre les systèmes de stockage et le commutateur Ethernet. Il est peu probable qu'un système ou qu'une machine virtuelle exploite totalement la vitesse du réseau. Cette situation peut toutefois survenir lorsque de nombreux systèmes partagent un périphérique de stockage unique.

Lorsqu'ils écrivent des données sur le stockage, des systèmes ou machines virtuelles multiples peuvent tenter d'exploiter totalement la vitesse de leurs liens. Par conséquent, il peut arriver que le commutateur entre les systèmes et le système de stockage abandonne des paquets réseau. L'abandon de données peut se produire parce que le commutateur a plus de trafic à envoyer au système de stockage qu'un seul lien ne peut en transporter. La quantité de données que le commutateur peut transmettre est limitée par la vitesse du lien entre lui et le système de stockage.

Figure 4-3. Paquets abandonnés

La restauration de paquets réseau abandonnés provoque une forte détérioration des performances. En plus du temps passé à déterminer quelles données ont été abandonnées, leur retransmission utilise la bande passante qui peut autrement servir aux transactions actuelles.

Le trafic iSCSI est assuré sur le réseau par le protocole de contrôle de transmission TCP. TCP est un protocole de transmission fiable, qui veille à ce que les paquets abandonnés soient représentés, et enfin atteignent leur destination. TCP est conçu pour restaurer les paquets abandonnés, et les retransmettre rapidement et sans coupure. Toutefois, lorsque le commutateur abandonne des paquets régulièrement, les performances réseau peuvent en souffrir. Le réseau est encombré par les demandes de renvoi de données et les paquets renvoyés. Moins de données sont transférées que sur un réseau sans congestion.

La plupart des commutateurs Ethernet peuvent conserver en mémoire tampon, ou stocker, des données. Cette technique donne à chaque périphérique tentant d'envoyer des données une chance égale de rejoindre sa destination. La possibilité de conserver en mémoire tampon certaines transmissions, combinée avec de nombreux systèmes limitant le nombre de commandes en attente, réduit les transmissions en petites rafales. Les rafales de plusieurs systèmes peuvent être envoyées à un système de stockage à tour de rôle.

Si les transactions sont volumineuses et que plusieurs serveurs envoient des données via un port de commutateur unique, la capacité de mise en mémoire tampon peut être dépassée. Dans un tel cas, le commutateur abandonne les données qu'il ne peut pas envoyer, et le système de stockage doit demander une retransmission du paquet abandonné. Par exemple, si un commutateur Ethernet peut conserver en mémoire tampon 32 Ko, mais que le serveur envoie 256 Ko au périphérique de stockage, certaines de ces données sont abandonnées.

La plupart des commutateurs administrables fournissent des informations sur les paquets abandonnés, qui ressemblent à ceci :

```
*: interface is up
IHQ: pkts in input hold queue      IQD: pkts dropped from input queue
OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
TRTL: throttle count
```

Tableau 4-2. Exemple d'information du commutateur

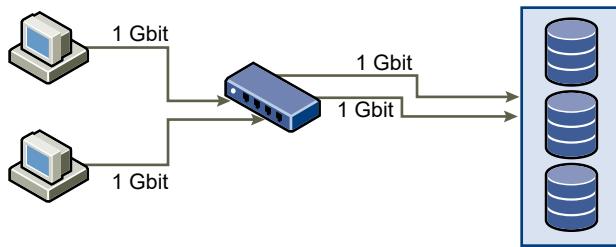
Interface	IHQ	IQD	OHQ	OQD	RXBS	RXPS	TXBS	TXPS	TRTL
*	3	9922	0	0	4763030 00	62273	4778400 00	63677	0

Dans cet exemple provenant d'un commutateur Cisco, la bande passante utilisée est de 476303000 bits/seconde, moins de la moitié de la bande passante physique. Le port met en mémoire tampon les paquets entrants mais en a abandonné quelques-uns. La ligne finale de ce résumé d'interface indique dans la colonne IQD que le port a déjà abandonné presque 10 000 paquets arrivants.

Pour éviter ce problème il est nécessaire de modifier la configuration en s'assurant que plusieurs liens ethernet arrivants ne se retrouvent en goulot d'étranglement sur un seul lien sortant, provoquant une surcharge du lien trop abonné. Lorsque plusieurs liens transmettant à quasi saturation sont redirigés vers un plus petit nombre de liens, le surabonnement devient possible.

En règle générale, les applications ou systèmes écrivant une grande quantité de données sur le stockage doivent éviter le partage des liens Ethernet vers un périphérique de stockage. Ces types d'applications sont les plus efficaces avec des connexions multiples aux périphériques de stockage.

L'illustration Multiple connexions du commutateur au stockage montre des connexions multiples du commutateur au stockage.

Figure 4-4. Connexions multiples du commutateur au stockage

L'utilisation de VLANs ou de VPNs n'apporte pas de solution adéquate au problème du surabonnement des liens en configurations partagées. Les VLANs et autres partitionnements virtuels d'un réseau fournissent un moyen de concevoir logiquement un réseau. Toutefois, ils ne modifient pas les capacités physiques des liens et des transmissions entre les commutateurs. Lorsque le trafic de stockage et les autres trafics sur le réseau partagent des connexions physiques, le surabonnement et la perte de paquets peuvent devenir possibles. Cela est aussi vrai pour les VLANs qui partagent des transmissions intercommutateur. La conception des performances pour un SAN doit prendre en compte les limitations physiques du réseau, pas les allocations logiques.

Consultation des statistiques des commutateurs Ethernet

Souvent les commutateurs ethernet fournissent des moyens de surveiller leur bon fonctionnement.

Les commutateurs dont certains ports opèrent à débit maximal souvent n'assurent pas une performance optimale. Si vous avez des ports dans votre SAN iSCSI opérant presque au maximum, réduisez leur charge. Si le port est connecté à un système ESXi ou à un stockage iSCSI, vous pouvez réduire sa charge par équilibrage de charge manuel.

Si le port est connecté entre de nombreux commutateurs ou routeurs, pensez à installer des liens supplémentaires entre ces composants afin de pouvoir gérer une plus grande charge. Les commutateurs ethernet fournissent aussi fréquemment des informations sur les erreurs de transmission, les paquets en file d'attente, et les paquets ethernet abandonnés. Si le commutateur rapporte régulièrement de telles conditions pour les ports utilisés par le trafic iSCSI, la performance du SAN iSCSI sera réduite.

Configuration des adaptateurs iSCSI et iSER et du stockage

5

Pour que ESXi puisse fonctionner avec SAN iSCSI, vous devez configurer votre environnement iSCSI. Pour fonctionner correctement, votre environnement doit respecter certaines recommandations spécifiques. En outre, plusieurs restrictions existent lorsque vous utilisez ESXi avec un SAN iSCSI.

Recommandations du stockage iSCSI

- Vérifiez que votre hôte ESXi prend en charge le matériel et le microprogramme du stockage SAN iSCSI. Pour obtenir une liste à jour, consultez le *Guide de compatibilité VMware*.
- Afin de garantir que l'hôte reconnaisse bien les LUN au démarrage, configurez toutes les cibles de stockage iSCSI de façon à ce que votre hôte puisse y accéder et les exploiter. Configurez votre hôte de façon à ce qu'il puisse découvrir toutes les cibles iSCSI.
- Configurez une partition de diagnostic sur un stockage local, sauf si vous utilisez des serveurs sans disques. En cas d'utilisation de serveurs sans disque qui démarrent à partir d'un SAN iSCSI, consultez [Recommandations générales pour le démarrage à partir du SAN iSCSI](#) pour plus d'informations sur les partitions de diagnostic avec iSCSI.
- Définissez le pilote de contrôleur SCSI dans le système d'exploitation client sur une file suffisamment grande.
- Sur les machines virtuelles qui exécutent Microsoft Windows, augmentez la valeur du paramètre `TimeoutValue` SCSI. Lorsque ce paramètre est configuré, les machines virtuelles Windows peuvent mieux tolérer les E/S différées provenant d'un basculement de chemin. Pour plus d'informations, consultez [Définir le délai d'expiration du SE invité Windows](#).
- Configurez votre environnement de façon à n'avoir qu'une seule banque de données VMFS pour chaque LUN.

Restrictions du stockage iSCSI

- ESXi ne prend en charge pas les périphériques à bande connectés par iSCSI.
- Vous ne pouvez pas utiliser le logiciel multi-chemins de machine virtuelle pour réaliser un équilibrage E/S vers une LUN matérielle unique.

- ESXi ne prend pas en charge la gestion de multivoie lorsque vous combinez des adaptateurs matériels indépendants à des adaptateurs logiciels ou matériels dépendants.

Paramétrage de l'environnement ESXi iSCSI

Le processus de préparation de votre environnement iSCSI implique les étapes suivantes.

Étape	Détails
1. Configurer le stockage iSCSI	Pour plus d'informations, reportez-vous à la documentation du fournisseur de stockage. En outre, suivez les recommandations disponibles dans Meilleures pratiques pour le stockage iSCSI .
2. Configurer les adaptateurs iSCSI/iSER	Utilisez un workflow approprié pour configurer votre adaptateur : <ul style="list-style-type: none"> ■ Configurer des adaptateurs iSCSI matériel indépendants ■ Configurer des adaptateurs iSCSI matériel dépendants ■ Configurer l'adaptateur iSCSI logiciel ■ Configurer iSER avec ESXi
3. Créer une banque de données sur un stockage iSCSI.	Création de banques de données

mise en réseau iSCSI

Pour certains types d'adaptateurs iSCSI, vous devez configurer la mise en réseau VMkernel.

Vous pouvez vérifier la configuration réseau grâce à l'utilitaire `vmkping`.

L'adaptateur iSCSI matériel indépendant ne nécessite pas de mise en réseau VMkernel. Sur ce type d'adaptateur, vous pouvez configurer des paramètres réseau tels qu'une adresse IP, un masque de sous-réseau et une passerelle par défaut.

Tous les types d'adaptateurs iSCSI prennent en charge les protocoles IPv4 et IPv6.

Adaptateur iSCSI (vmhba)	Description	Mise en réseau VMkernel	Paramètres réseau de l'adaptateur
Adaptateur iSCSI matériel indépendant	Adaptateur tiers qui décharge la gestion de réseau et iSCSI de votre hôte.	Non requis.	Pour plus d'informations, consultez Modifier des paramètres réseau pour du matériel iSCSI .
Adaptateur iSCSI logiciel	Utilise des cartes NICs standards pour connecter votre hôte à une cible iSCSI distante sur le réseau IP.	Requis. Pour plus d'informations, consultez Configuration du réseau pour iSCSI et iSER .	S.O.

Adaptateur iSCSI (vmhba)	Description	Mise en réseau VMkernel	Paramètres réseau de l'adaptateur
Adaptateur iSCSI matériel dépendant	Adaptateur tiers qui dépend de la mise en réseau VMware, de la configuration iSCSI et des interfaces de gestion.	Requis Pour plus d'informations, consultez Configuration du réseau pour iSCSI et iSER .	S.O.
Adaptateur VMware iSER	Utilise un adaptateur réseau compatible RDMA pour connecter votre hôte à une cible iSCSI distante.	Requis Pour plus d'informations, consultez Configuration du réseau pour iSCSI et iSER .	S.O.

Méthodes de détection

Pour tous les types d'adaptateurs iSCSI, vous devez définir l'adresse de détection dynamique ou l'adresse de détection statique. Vous devez également fournir le nom cible du système de stockage. Pour les adaptateurs de logiciels iSCSI et les adaptateurs de matériels iSCSI dépendants, l'adresse doit être accessible par un ping à l'aide de `vmkping`.

Reportez-vous à la section [Configurer la découverte dynamique ou statique pour iSCSI et iSER sur l'hôte ESXi](#).

Authentification CHAP

Activez le paramètre CHAP sur l'initiateur et du côté du système de stockage. Une fois que l'authentification est activée, elle s'applique à toutes les cibles non encore détectées. Elle ne s'applique pas aux cibles déjà détectées.

Reportez-vous à la section [Configuration des paramètres CHAP pour les adaptateurs de stockage iSCSI ou iSER](#).

Ce chapitre contient les rubriques suivantes :

- [Configurer des adaptateurs iSCSI matériel indépendants](#)
- [Configurer des adaptateurs iSCSI matériel dépendants](#)
- [Configurer l'adaptateur iSCSI logiciel](#)
- [Configurer iSER avec ESXi](#)
- [Modifier les propriétés générales des adaptateurs iSCSI ou iSER](#)
- [Configuration du réseau pour iSCSI et iSER](#)
- [Configurer la liaison de port pour les protocoles iSCSI ou iSER](#)
- [Utilisation de trames Jumbo avec iSCSI et iSER](#)
- [Configurer la découverte dynamique ou statique pour iSCSI et iSER sur l'hôte ESXi](#)

- Configuration des paramètres CHAP pour les adaptateurs de stockage iSCSI ou iSER
- Configuration des paramètres avancés iSCSI
- Gestion des sessions iSCSI

Configurer des adaptateurs iSCSI matériel indépendants

Un adaptateur iSCSI matériel indépendant est un adaptateur tiers spécialisé capable d'accéder au stockage iSCSI via TCP/IP. Cet adaptateur iSCSI traite tout le traitement et toute la gestion iSCSI et réseau du système ESXi.

Conditions préalables

- Vérifiez si l'adaptateur doit disposer d'une licence.
- Installez l'adaptateur sur votre hôte ESXi.

Pour en savoir plus sur la gestion des licences, l'installation et les mises à jour de microprogrammes, reportez-vous à la documentation du fournisseur.

Le processus de configuration de l'adaptateur iSCSI matériel indépendant comprend les étapes suivantes.

Étape	Description
Afficher des adaptateurs de matériel iSCSI dépendants	Affichez un adaptateur iSCSI matériel indépendant et vérifiez qu'il est correctement installé et prêt pour la configuration.
Modifier les propriétés générales des adaptateurs iSCSI ou iSER	Au besoin, modifiez le nom et l'alias iSCSI par défaut attribués à vos adaptateurs iSCSI. Pour les adaptateurs iSCSI matériels indépendants, vous pouvez également modifier les paramètres IP par défaut.
Modifier des paramètres réseau pour du matériel iSCSI	Modifiez les paramètres réseau par défaut afin que l'adaptateur est configuré correctement pour le SAN iSCSI.
Configurer la découverte dynamique ou statique pour iSCSI et iSER sur l'hôte ESXi	Configurez la découverte dynamique. Avec la découverte dynamique, chaque fois que l'initiateur contacte un système de stockage iSCSI donné, il envoie la demande SendTargets au système. Le système iSCSI répond en fournissant une liste de cibles disponibles à l'initiateur. Outre la méthode de découverte dynamique, vous pouvez utiliser la découverte statique et entrer manuellement des informations pour les cibles.
Configurer CHAP pour un adaptateur de stockage iSCSI ou iSER	Si votre environnement iSCSI utilise le protocole CHAP (Challenge Handshake Authentication Protocol), configurez-le pour votre adaptateur.
Activer les trames Jumbo pour l'iSCSI matériel indépendant	Si votre environnement iSCSI prend en charge les trames Jumbo, activez-les pour l'adaptateur.

Afficher des adaptateurs de matériel iSCSI dépendants

Sur un hôte ESXi, affichez un adaptateur iSCSI matériel indépendant et vérifiez qu'il est correctement installé et prêt pour la configuration.

Après avoir installé un adaptateur iSCSI matériel indépendant sur l'hôte, celui-ci figure dans la liste des adaptateurs de stockage disponibles pour la configuration. Vous pouvez consulter ses propriétés.

Conditions préalables

Privilège nécessaire :**Hôte.Configuration.Configuration de la partition de stockage**

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**.
S'il est installé, l'adaptateur iSCSI matériel apparaît dans la liste des adaptateurs de stockage.
- 4 Sélectionnez l'adaptateur à afficher.

Les détails par défaut de l'adaptateur s'affichent.

Informations sur les adaptateurs	Description
Modèle	Modèle de l'adaptateur.
nom iSCSI	Nom unique formé selon les normes iSCSI qui identifie l'adaptateur iSCSI. Vous pouvez modifier le nom iSCSI.
Alias iSCSI	Surnom utilisé au lieu du nom iSCSI. Vous pouvez modifier l'alias iSCSI.
Adresse IP	Adresse assignée au HBA iSCSI.
Cibles	Nombre de cibles auxquelles il a été accédé via l'adaptateur.
Périphériques	Tous les périphériques de stockage ou LUN auxquels l'adaptateur peut accéder.
Chemins	Tous les chemins que l'adaptateur l'utilise pour accéder aux périphériques de stockage.

Modifier des paramètres réseau pour du matériel iSCSI

Après avoir installé un adaptateur iSCSI matériel indépendant sur un hôte ESXi, vous pouvez avoir besoin de modifier ses paramètres réseau par défaut pour que l'adaptateur soit configuré correctement pour le SAN iSCSI.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**, puis sélectionnez l'adaptateur (vmhba#) à configurer.
- 4 Cliquez dans l'onglet **Paramètres réseau**, puis sur **Modifier**.

- 5 Dans la section Paramètres IPv4, désactivez IPv4 ou sélectionnez la méthode pour obtenir les adresses IP.

Note L'option DHCP automatique et l'option statique s'excluent mutuellement.

Option	Description
Aucun paramètre IPv4	Désactivez IPv4.
Obtenir automatiquement les paramètres IPv4	Utilisez DHCP pour obtenir les paramètres IP.
Utiliser des paramètres IPv4 statiques	Entrez l'adresse IP IPv4, le masque de sous-réseau et la passerelle par défaut de l'adaptateur iSCSI.

- 6 Dans la section Paramètres IPv6, désactivez IPv6 ou sélectionnez une option appropriée pour obtenir des adresses IPv6.

Note L'option automatique et l'option statique s'excluent mutuellement.

Option	Description
Aucun paramètre IPv6	Désactivez IPv6.
Activer IPv6	Sélectionnez une option permettant d'obtenir les adresses IPv6.
Obtenir adresse IPv6 automatiquement via DHCP	Utilisez DHCP pour obtenir les adresses IPv6.
Obtenez les adresses IPv6 automatiquement par Annonce de Routage	Utilisez l'annonce de routage pour obtenir les adresses IPv6.
Remplacer l'adresse de lien local pour IPv6	Remplacez l'adresse IP de lien local en configurant une adresse IP statique.
Adresses IPv6 statiques	<ol style="list-style-type: none"> Cliquez sur Ajouter pour ajouter une nouvelle adresse IPv6. Entrez l'adresse IPv6 et la longueur du préfixe de sous-réseau, puis cliquez sur OK.

- 7 Dans la section Paramètres DNS, fournissez l'adresse IP d'un serveur DNS préféré et celle d'un serveur DNS secondaire.

Vous devez indiquer ces deux valeurs.

Configurer des adaptateurs iSCSI matériel dépendants

Un adaptateur iSCSI matériel dépendant est un adaptateur tiers qui dépend du réseau VMware et des interfaces de configuration et de gestion iSCSI fournies par VMware.

La carte réseau Broadcom 5709 est un exemple d'adaptateur iSCSI dépendant. Lors de l'installation sur un hôte, elle présente ses deux composants, un adaptateur réseau standard et un moteur iSCSI, au même port. Le moteur iSCSI apparaît sur la liste d'adaptateurs de stockage en tant qu'adaptateur iSCSI (vmhba).

L'adaptateur iSCSI est activé par défaut. Pour le rendre fonctionnel, vous devez le connecter, via un adaptateur virtuel VMkernel (vmk), à un adaptateur réseau physique (vmnic) qui lui est associé. Vous pouvez alors configurer l'adaptateur iSCSI.

Après avoir configuré l'adaptateur iSCSI matériel dépendant, les données de découverte et d'authentification sont transmises à l'aide de la connexion réseau. Le trafic iSCSI est envoyé via le moteur iSCSI, en contournant le réseau.

La procédure complète d'installation et de configuration des adaptateurs iSCSI matériels dépendants comprend plusieurs étapes.

Étape	Description
Affichage des adaptateurs iSCSI matériel dépendants	Affichez un adaptateur iSCSI matériel dépendant pour vérifier qu'il est correctement chargé.
Modifier les propriétés générales des adaptateurs iSCSI ou iSER	Si nécessaire, modifiez le nom iSCSI par défaut et l'alias attribués à votre adaptateur.
Déterminer l'association entre les adaptateurs iSCSI et les adaptateurs réseau	Vous devez créer des connexions réseau pour lier des adaptateurs iSCSI dépendants et des adaptateurs réseau physiques. Pour pouvoir créer des connexions correctement, déterminez le nom de la carte réseau physique à laquelle l'adaptateur iSCSI matériel dépendant est associé.
Configurer la liaison de port pour les protocoles iSCSI ou iSER	Configurez les connexions pour le trafic entre le composant iSCSI et les adaptateurs réseau physiques. Le processus de configuration de ces connexions est appelé liaison de port.
Configurer la découverte dynamique ou statique pour iSCSI et iSER sur l'hôte ESXi	Configurez la découverte dynamique. Avec la découverte dynamique, chaque fois que l'initiateur contacte un système de stockage iSCSI donné, il envoie la demande SendTargets au système. Le système iSCSI répond en fournissant une liste de cibles disponibles à l'initiateur. Outre la méthode de découverte dynamique, vous pouvez utiliser la découverte statique et entrer manuellement des informations pour les cibles.
Configurer CHAP pour un adaptateur de stockage iSCSI ou iSER	Si votre environnement iSCSI utilise le protocole CHAP (Challenge Handshake Authentication Protocol), configurez-le pour votre adaptateur.
Configurer CHAP pour une cible	Vous pouvez également configurer des informations d'identification CHAP différentes pour chaque adresse de découverte ou cible statique.
Activer les trames Jumbo pour la mise en réseau	Si votre environnement iSCSI prend en charge les trames Jumbo, activez-les pour l'adaptateur.

Considérations sur l'iSCSI matériel dépendant

Lorsque vous utilisez des adaptateurs iSCSI matériel dépendants avec ESXi, certaines considérations s'appliquent.

- Lorsque vous utilisez un adaptateur iSCSI matériel dépendant, le rapport de performances pour une carte réseau associée à l'adaptateur ne montre que peu ou pas d'activité, même lorsque le trafic iSCSI est intense. Cela est dû au contournement de la pile réseau habituelle par le trafic iSCSI.

- Si vous utilisez un commutateur virtuel tiers désactivez l'épinglage automatique. Utilisez l'accrochage manuel à la place, en veillant à connecter un adaptateur VMkernel (vmk) à une carte NIC physique adéquate (vmnic). Pour plus d'informations, consultez la documentation du fournisseur de commutateurs virtuels.
- L'adaptateur iSCSI Broadcom réassemble les données dans le matériel, dont l'espace tampon est limité. Lorsque vous utilisez l'adaptateur iSCSI Broadcom dans un réseau congestionné ou sous une lourde charge, activez le contrôle de flux pour éviter la dégradation des performances.

Le contrôle de flux gère la vitesse de transmission des données entre deux nœuds pour éviter qu'un expéditeur rapide ne dépasse un récepteur lent. Pour de meilleurs résultats, activez le contrôle de flux aux points de terminaison du chemin d'E/S, sur les hôtes et les systèmes de stockage iSCSI.

Pour activer le contrôle de flux pour l'hôte, utilisez la commande `esxcli system module parameters`. Pour plus d'informations, consultez l'article de la base de connaissances VMware à l'adresse <http://kb.vmware.com/kb/1013413>

- Les adaptateurs de matériel dépendants prennent en charge IPv4 et IPv6.

Affichage des adaptateurs iSCSI matériel dépendants

Sur un hôte ESXi, affichez un adaptateur iSCSI matériel dépendant pour vérifier qu'il est correctement chargé.

S'il est installé, l'adaptateur iSCSI matériel dépendant (vmhba#) figure dans la liste des adaptateurs de stockage sous, par exemple, la catégorie Adaptateur iSCSI Broadcom. Si l'adaptateur matériel dépendant ne figure pas dans la liste des adaptateurs de stockage, vérifiez s'il a besoin d'une licence. Consultez la documentation du fabricant.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**.
- 4 Sélectionnez l'adaptateur (vmhba#) à afficher.

Les détails par défaut de l'adaptateur apparaissent, y compris le nom iSCSI, l'alias iSCSI et l'état.

Étape suivante

Bien que l'adaptateur iSCSI dépendant soit activé par défaut, pour le rendre fonctionnel, vous devez configurer les communications réseau pour le trafic iSCSI et lier l'adaptateur à un port VMkernel approprié. Définissez ensuite les adresses de découverte et les paramètres CHAP.

Déterminer l'association entre les adaptateurs iSCSI et les adaptateurs réseau

Sur un hôte ESXi, les connexions réseau lient les adaptateurs iSCSI et les adaptateurs réseau physiques dépendants. Pour pouvoir créer des connexions correctement, vous devez déterminer le nom de la carte réseau physique avec laquelle l'adaptateur iSCSI matériel dépendant est associé.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**.
- 4 Sélectionnez l'adaptateur iSCSI (vmhba#) et cliquez sur l'onglet **Liaison de port réseau** sous Détails adaptateur.
- 5 Cliquez sur **Ajouter**.

L'adaptateur réseau (vmnic#) qui correspond à l'adaptateur iSCSI dépendant est répertorié dans la colonne Adaptateurs réseau physiques.

Étape suivante

Si la colonne Adaptateur VMkernel est vide, créez un adaptateur VMkernel (vmk#) pour l'adaptateur réseau physique (vmnic#) puis reliez-les au matériel iSCSI dépendant associé. Reportez-vous à la section [Configuration du réseau pour iSCSI et iSER](#).

Configurer l'adaptateur iSCSI logiciel

L'implémentation du protocole iSCSI logiciel vous permet d'utiliser des cartes réseau standard pour connecter votre hôte à une cible iSCSI distante sur le réseau IP. L'adaptateur iSCSI logiciel qui est intégré dans l'ESXi facilite cette connexion en communiquant avec les cartes NIC physiques par la pile réseau.

Considérez les points suivants lorsque vous utilisez les adaptateurs iSCSI logiciels :

- Désignez un adaptateur réseau séparé pour iSCSI. N'utilisez pas d'iSCSI sur des adaptateurs 100Mbps ou plus lents.
- Évitez de coder en dur le nom de l'adaptateur logiciel, vmhbaXX, dans les scripts. Il est possible que le nom change d'une version d'ESXi à l'autre, ce qui peut provoquer l'échec de vos scripts existants s'ils utilisent l'ancien nom codé en dur. Le changement de nom n'affecte pas le comportement de l'adaptateur iSCSI logiciel.

Le processus de configuration de l'adaptateur iSCSI logiciel comprend plusieurs étapes.

Étape	Description
Ajouter ou supprimer l'adaptateur iSCSI logiciel	Activez votre adaptateur iSCSI logiciel pour que l'hôte puisse l'utiliser pour accéder au stockage iSCSI.
Modifier les propriétés générales des adaptateurs iSCSI ou iSER	Si nécessaire, modifiez le nom iSCSI par défaut et l'alias attribués à votre adaptateur.
Configurer la liaison de port pour les protocoles iSCSI ou iSER	Configurez les connexions pour le trafic entre le composant iSCSI et les adaptateurs réseau physiques. Le processus de configuration de ces connexions est appelé liaison de port.
Configurer la découverte dynamique ou statique pour iSCSI et iSER sur l'hôte ESXi	Configurez la découverte dynamique. Avec la découverte dynamique, chaque fois que l'initiateur contacte un système de stockage iSCSI donné, il envoie la demande SendTargets au système. Le système iSCSI répond en fournissant une liste de cibles disponibles à l'initiateur. Outre la méthode de découverte dynamique, vous pouvez utiliser la découverte statique et entrer manuellement des informations pour les cibles.
Configurer CHAP pour un adaptateur de stockage iSCSI ou iSER	Si votre environnement iSCSI utilise le protocole CHAP (Challenge Handshake Authentication Protocol), configurez-le pour votre adaptateur.
Configurer CHAP pour une cible	Vous pouvez également configurer des informations d'identification CHAP différentes pour chaque adresse de découverte ou cible statique.
Activer les trames Jumbo pour la mise en réseau	Si votre environnement iSCSI prend en charge les trames Jumbo, activez-les pour l'adaptateur.

Ajouter ou supprimer l'adaptateur iSCSI logiciel

Vous devez activer votre adaptateur iSCSI logiciel pour que l'hôte ESXi puisse l'utiliser pour accéder au stockage iSCSI. Vous pouvez supprimer l'adaptateur iSCSI logiciel si vous n'en avez pas besoin après son activation.

Vous ne pouvez activer qu'un seul adaptateur iSCSI logiciel.

Conditions préalables

Privilège nécessaire : **Hôte.Configuration.Configuration de la partition de stockage**

Note Si vous démarrez depuis iSCSI en utilisant l'adaptateur iSCSI logiciel, l'adaptateur est ajouté et la configuration réseau est créée lors du premier démarrage. Si vous supprimez l'adaptateur, il est ajouté à nouveau chaque fois que vous démarrez l'hôte.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.

3 Ajoutez ou supprimez l'adaptateur.

Option	Description
Ajouter l'adaptateur iSCSI logiciel	<p>a Sous Stockage, cliquez sur Adaptateurs de stockage, puis sur Ajouter un adaptateur logiciel.</p> <p>b Dans le menu déroulant, sélectionnez Adaptateur iSCSI logiciel et confirmez que vous voulez ajouter l'adaptateur.</p> <p>L'adaptateur iSCSI logiciel (vmhba#) est ajouté et figure dans la liste des adaptateurs de stockage. Après avoir ajouté l'adaptateur, l'hôte lui attribue le nom iSCSI par défaut. Vous pouvez maintenant terminer la configuration de l'adaptateur.</p>
Supprimer l'adaptateur iSCSI logiciel	<p>a Sous Stockage, cliquez sur Adaptateurs de stockage, puis sélectionnez l'adaptateur (vmhba#) à supprimer.</p> <p>b Cliquez sur l'onglet Propriétés.</p> <p>c Dans le menu Actions d'état de l'adaptateur, sélectionnez Désactiver et confirmez que vous souhaitez désactiver l'adaptateur.</p> <p>L'adaptateur sera marqué pour suppression. L'adaptateur sera supprimé de l'hôte lors du prochain redémarrage de l'hôte suivant.</p> <p>d Redémarrez l'hôte.</p> <p>Après le redémarrage, l'adaptateur ne figure plus dans la liste des adaptateurs de stockage. Toutes les machines virtuelles et autres données des périphériques de stockage associés à cet adaptateur deviennent inaccessibles. Vous pourrez activer l'adaptateur plus tard.</p>

Configurer iSER avec ESXi

Outre le protocole iSCSI traditionnel, ESXi prend en charge le protocole d'extensions iSCSI pour RDMA (iSER). Lorsque le protocole iSER est activé, l'infrastructure iSCSI située sur l'hôte ESXi peut utiliser le transport d'accès direct à la mémoire à distance (RDMA) au lieu du protocole TCP/IP. Vous pouvez configurer iSER sur votre hôte ESXi.

Pour plus d'informations sur le protocole iSER, consultez [Utilisation du protocole iSER avec ESXi](#).

La procédure complète d'installation et de configuration de VMware iSER comprend plusieurs étapes.

Étape	Description
Installer et afficher un adaptateur réseau prenant en charge RDMA	Pour configurer iSER avec ESXi, vous devez d'abord installer un adaptateur réseau prenant en charge RDMA, par exemple, Mellanox Technologies MT27700 Family ConnectX-4. Après installation de ce type d'adaptateur, vSphere Client affiche ses deux composants, un adaptateur RDMA et un adaptateur réseau physique vmnic#.
Activer l'adaptateur iSER VMware	Pour pouvoir utiliser l'adaptateur compatible RDMA pour iSCSI, utilisez esxcli pour activer le composant de stockage VMware iSER. Le composant figure dans vSphere Client en tant qu'adaptateur de stockage vmhba# sous la catégorie d'adaptateur VMware iSCSI over RDMA (iSER).

Étape	Description
Modifier les propriétés générales des adaptateurs iSCSI ou iSER	Si nécessaire, modifiez le nom et l'alias attribués par défaut à votre adaptateur de stockage iSER <code>vmhba#</code> .
Configurer la liaison de port pour les protocoles iSCSI ou iSER	<p>Vous devez créer des connexions réseau pour lier l'adaptateur de stockage iSER <code>vmhba#</code> et l'adaptateur réseau compatible RDMA <code>vmnic#</code>. Le processus de configuration de ces connexions est appelé liaison de port.</p> <p>Note iSER ne prend pas en charge l'association de cartes réseau. Lors de la configuration de la liaison de port, utilisez un seul adaptateur RDMA par vSwitch.</p>
Configurer la découverte dynamique ou statique pour iSCSI et iSER sur l'hôte ESXi	Configurez la découverte dynamique ou statique de votre adaptateur de stockage iSER <code>vmhba#</code> . Avec la découverte dynamique, chaque fois que l'initiateur contacte un système de stockage iSER donné, il envoie la demande SendTargets au système. Le système iSER répond en fournissant une liste de cibles disponibles à l'initiateur. Avec la découverte statique, vous entrez manuellement les informations des cibles.
Configurer CHAP pour un adaptateur de stockage iSCSI ou iSER	Si votre environnement utilise le protocole CHAP (Challenge Handshake Authentication Protocol), configurez-le pour votre adaptateur de stockage iSER <code>vmhba#</code> .
Configurer CHAP pour une cible	Vous pouvez également configurer des informations d'identification CHAP différentes pour chaque adresse de découverte ou cible statique.
Activer les trames Jumbo pour la mise en réseau	Si votre environnement prend en charge les trames Jumbo, activez-les pour l'adaptateur de stockage iSER <code>vmhba#</code> .

Installer et afficher un adaptateur réseau prenant en charge RDMA

ESXi prend en charge les adaptateurs réseau compatibles avec RDMA, par exemple, Mellanox Technologies MT27700 Family ConnectX-4. Une fois que vous avez installé cet adaptateur sur votre hôte, vSphere Client affiche ses deux composants, un adaptateur RDMA et un adaptateur réseau physique.

Vous pouvez utiliser vSphere Client pour afficher l'adaptateur RDMA et son adaptateur réseau correspondant.

Procédure

- Dans vSphere Client, accédez à l'hôte ESXi.
- Sous **Mise en réseau**, cliquez sur **Adaptateurs RDMA**.

Dans cet exemple, l'adaptateur RDMA figure dans la liste en tant que `vmrdma0`. La colonne **Liaison montante couplée** affiche le composant réseau comme adaptateur réseau physique `vmnic1`.

The screenshot shows the vSphere Client interface with the 'Configure' tab selected. In the left sidebar, under 'Storage', 'RDMA adapters' is selected. A table lists one adapter: 'vmrdma0' with 'nmlx5_rdma' as the driver, 'Active' state, and 'vmnic1' as the paired uplink. Below the table, it says 'RDMA Device: vmrdma0'. Under 'Properties', it shows 'Vmkernel adapters binding' with 'Description: MT27700 Family [ConnectX-4]', 'MTU: 1024', and 'Speed: 56 Gbit/s'.

- 3 Pour vérifier la description de l'adaptateur, sélectionnez l'adaptateur RDMA dans la liste, puis cliquez sur l'onglet **Propriétés**.

Résultats

Vous pouvez utiliser le composant réseau `vmnic#` de l'adaptateur pour des configurations de stockage comme iSER ou NVMe over RDMA. Pour les étapes de configuration d'iSER, consultez [Configurer iSER avec ESXi](#). Pour plus d'informations sur NVMe over RDMA, reportez-vous à [Configuration d'adaptateurs pour le stockage NVMe over RDMA \(RoCE v2\)](#).

Activer l'adaptateur iSER VMware

Pour pouvoir utiliser l'adaptateur compatible RDMA pour iSCSI, utilisez `esxcli` pour activer le composant de stockage VMware iSER. Une fois le composant activé, il figure dans vSphere Client en tant qu'adaptateur de stockage `vmhba#` sous la catégorie Adaptateur VMware iSCSI sur RDMA (iSER).

Conditions préalables

- Assurez-vous que votre stockage iSCSI prend en charge le protocole iSER.
- Installez l'adaptateur compatible RDMA sur votre hôte ESXi. Pour plus d'informations, consultez [Installer et afficher un adaptateur réseau prenant en charge RDMA](#).
- Pour les adaptateurs compatibles RDMA qui prennent en charge RDMA sur une carte Ethernet convergée (RoCE), déterminez la version RoCE que l'adaptateur utilise.
- Utilisez le commutateur compatible RDMA.
- Activez le contrôle de flux sur l'hôte ESXi. Pour activer le contrôle de flux pour l'hôte, utilisez la commande `esxcli system module parameters`. Pour de plus amples détails, consultez l'article de la base de connaissances VMware à <http://kb.vmware.com/kb/1013413>.
- Assurez-vous de configurer des ports de commutateur RDMA pour créer des connexions sans perte de données entre l'initiateur iSER et la cible.

Procédure

- Utilisez ESXi Shell ou l'interface de ligne de commande vSphere pour activer l'adaptateur de stockage iSER VMware et définir sa version RoCE.

- Activez l'adaptateur de stockage iSER.

```
esxcli rdma iser add
```

- Vérifiez que l'adaptateur iSER a été ajouté.

```
esxcli iscsi adapter list
```

Le résultat est semblable à l'exemple suivant.

Adapter	Driver	State	UID	Description
vmhba64	iser	unbound	iscsi.vmhba64	VMware iSCSI over RDMA (iSER) Adapter

- Spécifiez la version de RoCE que iSER utilise pour se connecter à la cible.

Utilisez la version de RoCE de l'adaptateur compatible RDMA. La commande que vous entrez est semblable à l'exemple suivant :

```
esxcli rdma iser params set -a vmhba64 -r 1
```

Lorsque la commande est terminée, un message semblable au message suivant figure dans le journal VMkernel.

```
vmkernel[0]:2020-02-18T18:26:15.949Z cpu6:2100717 opID=45abe37e)iser: iser_set_roce:  
Setting roce type: 1 for vmhba: vmhba64  
vmkernel[0]:2020-02-18T18:26:15.949Z cpu6:2100717 opID=45abe37e)iser: iser_set_roce:  
Setting rdma port: 3260 for vmhba: vmhba64
```

Si vous ne spécifiez pas la version de RoCE, l'hôte prend la valeur par défaut à savoir la version RoCE la plus élevée prise en charge par l'adaptateur compatible RDMA.

- 2 Utilisez vSphere Client pour afficher l'adaptateur iSER.
 - a Dans vSphere Client, accédez à l'hôte ESXi.
 - b Cliquez sur l'onglet **Configurer**.
 - c Sous **Stockage**, cliquez sur **Adaptateurs de stockage** et examinez la liste des adaptateurs.

Si vous avez activé l'adaptateur, il figure en tant qu'adaptateur de stockage `vmhba#` dans la liste sous la catégorie Adaptateur iSCSI over RDMA (iSER) VMware.

The screenshot shows the 'Storage Adapters' section of the vSphere Client. The main table lists several adapters:

Adapter	Type	Status	Identifier	Targets	Devices	Paths
vmhba33	Block SCSI	Unknown	--	1	2	2
vmhba64	iSCSI	Unbound	lser-vmnic9(ign-1998-01.com.vmware.prim)	0	0	0
vmhba65	iSCSI	Unbound	lser-vmnic10(ign-1998-01.com.vmware.prim)	0	0	0
vmhba66	iSCSI	Unbound	lser-vmnic4(ign-1998-01.com.vmware.prim)	0	0	0
vmhba67	iSCSI	Unbound	lser-vmnic5(ign-1998-01.com.vmware.prim)	0	0	0
vmhba1	Block SCSI	Unknown	--	0	0	0
vmhba2	Block SCSI	Unknown	--	1	1	1

The 'Properties' tab is selected in the bottom navigation bar. The 'General' section shows:

- Name: vmhba64
- Model: VMware iSCSI over RDMA (iSER) Adapter
- iSCSI Name: ign-1998-01.com.vmware.prim-fcoe-005.eng.vmw
- iSCSI Alias: lser-vmnic9
- Target Discovery: Send Targets, Static Targets

The 'Authentication' section shows:

- Method: None

- 3 Sélectionnez le stockage iSER `vmhba#` pour passer en revue ses propriétés ou effectuer les tâches suivantes.

Option	Description
Configurer la liaison de ports pour l'adaptateur de stockage iSER	Vous devez créer des connexions réseau pour lier l'adaptateur de stockage iSER <code>vmhba#</code> et l'adaptateur réseau compatible RDMA <code>vmnic#</code> . Le processus de configuration de ces connexions est appelé liaison de port. Pour obtenir des informations générales sur la liaison de port, consultez Configuration du réseau pour iSCSI et iSER. Pour configurer la liaison de port pour iSER, consultez Configurer la liaison de port pour les protocoles iSCSI ou iSER.
Configurer la découverte dynamique ou statique pour l'adaptateur de stockage iSER	Pour plus d'informations, consultez Configurer la découverte dynamique ou statique pour iSCSI et iSER sur l'hôte ESXi.
Configurer le protocole CHAP (Challenge Handshake Authentication Protocol) pour l'adaptateur de stockage iSER	Pour plus d'informations, consultez Configurer CHAP pour un adaptateur de stockage iSCSI ou iSER.

Étape suivante

Pour plus d'informations, reportez-vous à l'article de la base de connaissances VMware à l'adresse <https://kb.vmware.com/s/article/79148>.

Modifier les propriétés générales des adaptateurs iSCSI ou iSER

Vous pouvez modifier le nom et l'alias par défaut attribués à vos adaptateurs de stockage iSCSI ou iSER par l'hôte ESXi. Pour les adaptateurs iSCSI matériels indépendants, vous pouvez également modifier les paramètres IP par défaut.

Important Lorsque vous modifiez des propriétés par défaut de vos adaptateurs, assurez-vous d'utiliser les formats appropriés pour leurs noms et leurs adresses IP.

Conditions préalables

Privilège requis : **Hôte.Configuration.Configuration de la partition de stockage**

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**, puis sélectionnez l'adaptateur (vmhba#) à configurer.
- 4 Cliquez sur l'onglet **Propriétés**, puis sur **Modifier** dans le panneau Général.
- 5 (Facultatif) Modifiez les propriétés générales suivantes.

Option	Description
nom iSCSI	Nom unique formé selon les normes iSCSI qui identifie l'adaptateur iSCSI. Si vous modifiez le nom, assurez-vous que le nom entré est unique dans le monde entier et correctement formaté. Sinon, certains périphériques de stockage risquent de ne pas reconnaître l'adaptateur iSCSI.
Alias iSCSI	Nom convivial que vous utilisez à la place du nom iSCSI.

Résultats

Si vous modifiez le nom iSCSI, il sera utilisé pour de nouvelles sessions iSCSI. Pour les sessions existantes, les nouveaux paramètres ne sont utilisés qu'une fois que vous vous êtes déconnecté, puis reconnecté.

Étape suivante

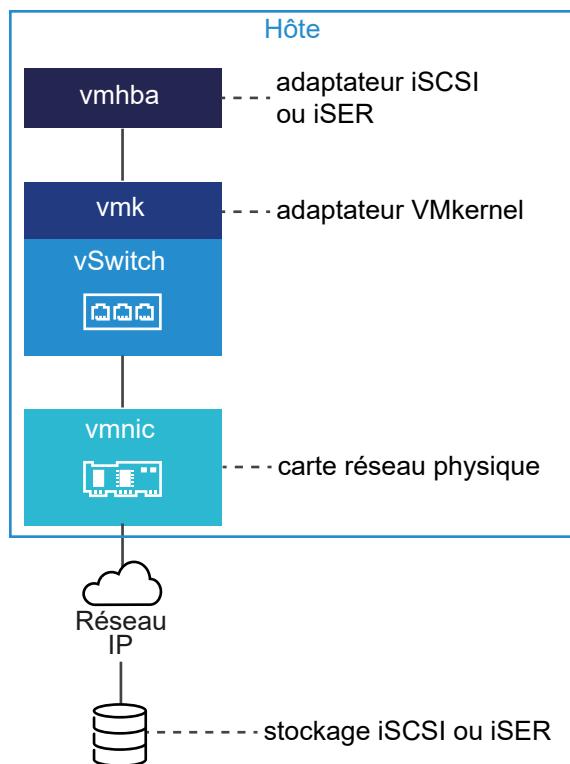
Pour connaître les autres étapes de configuration que vous pouvez effectuer pour les adaptateurs de stockage iSCSI ou iSER, reportez-vous aux rubriques suivantes :

- [Configurer des adaptateurs iSCSI matériel indépendants](#)
- [Configurer des adaptateurs iSCSI matériel dépendants](#)
- [Configurer l'adaptateur iSCSI logiciel](#)
- [Configurer iSER avec ESXi](#)

Configuration du réseau pour iSCSI et iSER

Certains types d'adaptateurs iSCSI dépendent de la mise en réseau VMkernel. Il s'agit notamment des adaptateurs iSCSI logiciels, des adaptateurs iSCSI matériels dépendants et des adaptateurs iSER (VMware iSCSI sur RDMA). Si votre environnement inclut l'un de ces adaptateurs, vous devez configurer les connexions pour le trafic entre le composant iSCSI ou iSER et les adaptateurs réseau physiques.

La configuration de la connexion réseau implique de créer un adaptateur virtuel VMkernel pour chaque adaptateur réseau physique, d'utiliser le mappage 1:1 entre chaque adaptateur réseau physique et virtuel, puis d'associer l'adaptateur VMkernel à un adaptateur iSCSI ou iSER approprié. Ce processus porte le nom de liaison de port.



Lorsque vous configurez la liaison de port, suivez ces règles :

- Vous pouvez connecter l'adaptateur iSCSI logiciel n'importe quelle carte réseau physique disponible sur votre hôte.
- Les adaptateurs iSCSI dépendants doivent uniquement être connectés à leurs propres cartes réseau physiques.
- Vous devez connecter l'adaptateur iSER uniquement à l'adaptateur réseau compatible RDMA.

Pour des considérations spécifiques sur la manière d'utiliser les connections du réseau avec un adaptateur iSCSI logiciel, reportez-vous à l'article de la base de connaissances VMware à l'adresse <http://kb.vmware.com/kb/2038869>.

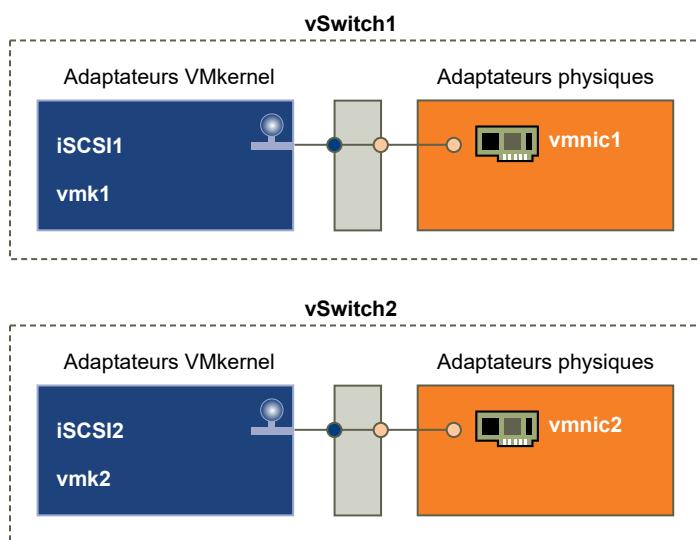
Multiples adaptateurs réseau dans une configuration iSCSI ou iSER

Si l'hôte dispose de plusieurs adaptateurs réseau physiques pour iSCSI ou iSER, vous pouvez utiliser les adaptateurs pour la gestion multivoie.

Vous pouvez utiliser plusieurs adaptateurs physiques dans une configuration à commutateur unique ou à commutateurs multiples.

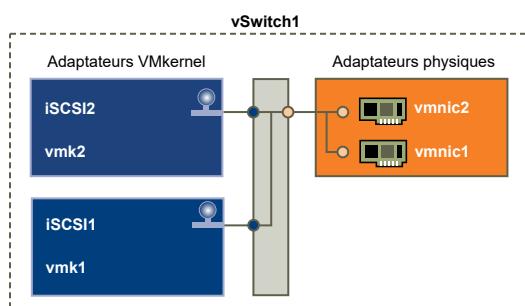
Dans une configuration à commutateurs multiples, vous désignez un commutateur vSphere distinct pour chaque paire d'adaptateurs virtuel-physique.

Figure 5-1. Mappage d'adaptateurs 1:1 sur des commutateurs standard vSphere distincts



Une autre méthode consiste à ajouter toutes les cartes réseau et tous les adaptateurs VMkernel à un seul commutateur vSphere. Le nombre d'adaptateurs VMkernel doit correspondre au nombre d'adaptateurs physiques sur le commutateur vSphere Standard. La configuration à commutateur unique n'est pas appropriée pour iSER, car iSER ne prend pas en charge l'association de cartes réseau.

Figure 5-2. Mappage d'adaptateurs 1:1 sur un seul commutateur standard vSphere



Pour ce type de configuration, vous devez annuler la configuration du réseau par défaut et vous assurer que chaque adaptateur VMkernel correspond uniquement à un seul adaptateur physique actif, comme l'indique le tableau.

Adaptateur VMkernel (vmk#)	Adaptateur VMkernel physique (vmnic#)
vmk1 (iSCSI1)	Adaptateurs actifs vmnic1 Adaptateurs inutilisés vmnic2
vmk2 (iSCSI2)	Adaptateurs actifs vmnic2 Adaptateurs inutilisés vmnic1

Vous pouvez également utiliser des commutateurs distribués. Pour plus d'informations sur les commutateurs distribués vSphere et sur la manière de modifier la stratégie réseau par défaut, reportez-vous à la documentation *Mise en réseau vSphere*.

Les considérations suivantes s'appliquent lorsque vous utilisez plusieurs adaptateurs physiques :

- Les adaptateurs réseau physiques doivent se trouver sur le même sous-réseau que le système de stockage auquel ils se connectent.
- (S'applique uniquement à iSCSI et non à iSER) Si vous utilisez des commutateurs vSphere distincts, vous devez vous connecter à différents sous-réseaux IP. Dans le cas contraire, les adaptateurs VMkernel risquent de connaître des problèmes de connectivité et l'hôte ne parvient pas à détecter les LUN.
- La configuration à commutateur unique n'est pas appropriée pour iSER, car iSER ne prend pas en charge l'association de cartes réseau.

N'utilisez pas la liaison de port si l'une des conditions suivantes est remplie :

- Les ports iSCSI cibles de la baie se trouvent sur un domaine de diffusion et un sous-réseau IP différents.
- Les adaptateurs VMkernel utilisés pour la connectivité iSCSI se trouvent sur différents domaines de diffusion ou sous-réseaux IP, ou utilisent différents commutateurs virtuels.

Note Dans les configurations iSER, les adaptateurs VMkernel utilisés pour la connectivité d'iSER ne peuvent pas être utilisés pour le trafic convergé. Les adaptateurs VMkernel que vous avez créés pour activer la connectivité entre l'hôte ESXi avec iSER et la cible iSER doivent être utilisés uniquement pour le trafic iSER.

Recommandations pour la configuration de la mise en réseau avec un iSCSI logiciel

Lorsque vous configurez la mise en réseau avec un iSCSI logiciel, vous devez tenir compte de plusieurs recommandations.

Liaison de port iSCSI logicielle

Vous pouvez lier l'initiateur iSCSI logiciel sur l'hôte ESXi à un ou plusieurs ports VMkernel afin que le trafic iSCSI emprunte toujours exclusivement les ports liés. Les ports non liés ne sont pas utilisés pour le trafic iSCSI.

Lorsque la liaison de port est configurée, l'initiateur iSCSI crée des sessions iSCSI allant de tous les ports liés vers tous les portails cibles configurés.

Consultez les exemples suivants.

Ports VMkernel	Portails cibles	Sessions iSCSI
2 ports VMkernel liés	2 portails cibles	4 sessions (2 x 2)
4 ports VMkernel liés	1 portail cible	4 sessions (4 x 1)
2 ports VMkernel liés	4 portails cibles	8 sessions (2 x 4)

Note Assurez-vous que tous les portails cibles peuvent être atteints à partir de tous les ports VMkernel lorsque la liaison de port est utilisée, sans quoi les sessions iSCSI risquent de ne pas être créées. Il en résulte que l'opération de réanalyse peut prendre plus de temps que prévu.

Absence de liaison de port

Si vous n'utilisez pas la liaison de port, la couche de mise en réseau ESXi sélectionne le meilleur port VMkernel en fonction de sa table de routage. L'hôte utilise le port pour créer une session iSCSI avec le portail cible. En l'absence de liaison de port, une seule session est créée pour chaque portail cible.

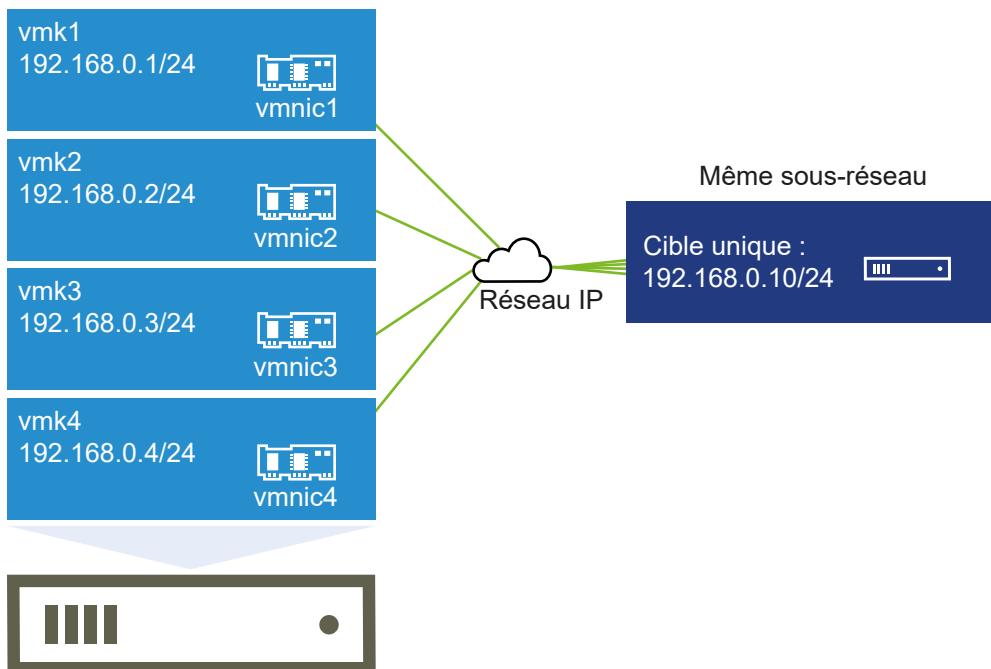
Consultez les exemples suivants.

Ports VMkernel	Portails cibles	Sessions iSCSI
2 ports VMkernel non liés	2 portails cibles	2 sessions
4 ports VMkernel non liés	1 portail cible	1 session
2 ports VMkernel non liés	4 portails cibles	4 sessions

Chemins multiples avec iSCSI logiciel

Exemple 1. Chemins multiples vers une cible iSCSI avec un portail réseau unique

Si votre cible n'a qu'un portail réseau, vous pouvez créer plusieurs chemins vers la cible en ajoutant plusieurs ports VMkernel à votre hôte ESXi et en les liant à l'initiateur iSCSI.

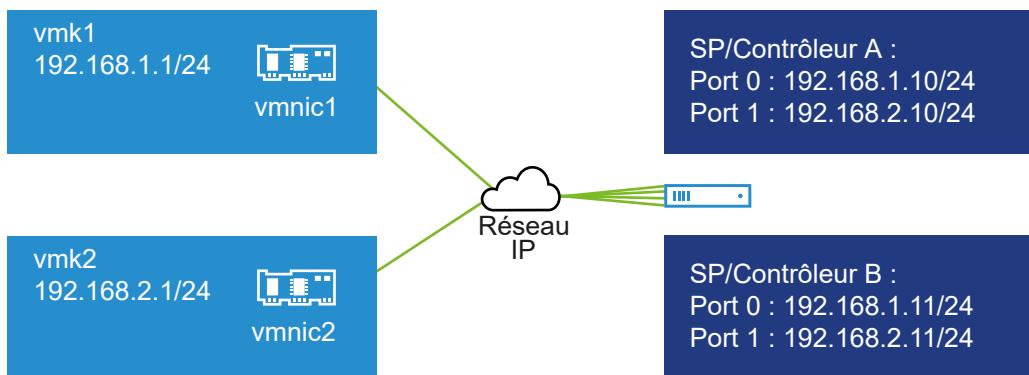


Dans cet exemple, tous les ports initiateurs et le portail cible sont configurés sur le même sous-réseau. La cible peut être atteinte par l'intermédiaire de tous les ports liés. Vous disposez de quatre ports VMkernel et d'un portail cible, de sorte que quatre chemins en tout sont créés.

Sans la liaison de port, un seul chemin est créé.

Exemple 2. Chemins multiples avec des ports VMkernel sur différents sous-réseaux

Vous pouvez créer plusieurs chemins en configurant plusieurs ports et portails cibles sur des sous-réseaux IP différents. En maintenant le port initiateur et le port cible sur des sous-réseaux différents, vous pouvez obliger ESXi à créer des chemins passant par des ports spécifiques. Dans cette configuration, vous n'utilisez pas la liaison de port, car celle-ci nécessite que tous les ports initiateurs et cibles se trouvent sur le même sous-réseau.



ESXi sélectionne vmk1 lors de la connexion au Port 0 du Contrôleur A et du Contrôleur B, car ces trois ports se trouvent tous sur le même sous-réseau. De même, vmk2 est sélectionné lors de la connexion au Port 1 du Contrôleur A et du Contrôleur B. Dans cette configuration, vous pouvez utiliser l'association de cartes réseau.

En tout, quatre chemins sont créés.

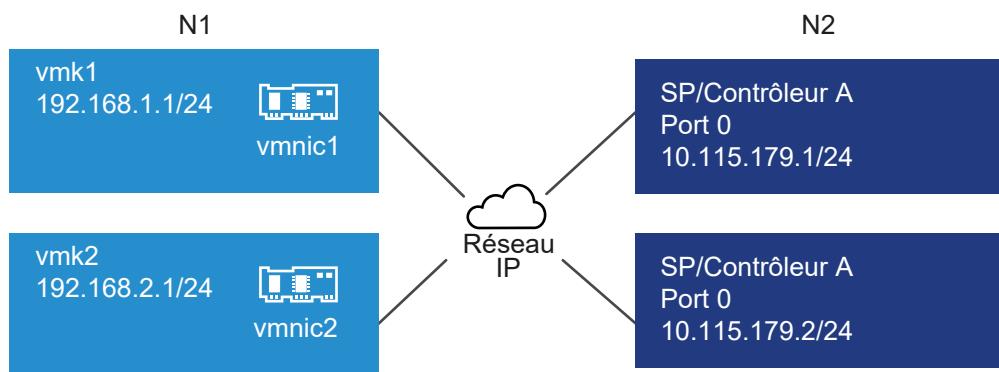
Chemins	Description
Chemin 1	vmk1 et Port0 du Contrôleur A
Chemin 2	vmk1 et Port0 du Contrôleur B
Chemin 3	vmk2 et Port1 du Contrôleur A
Chemin 4	vmk2 et Port1 du Contrôleur B

Routage avec iSCSI logiciel

Vous pouvez utiliser la commande `esxcli` pour ajouter des routes statiques pour votre trafic iSCSI. Une fois que vous avez configuré des routes statiques, les ports initiateur et cible sur différents sous-réseaux peuvent communiquer entre eux.

Exemple 1. Utilisation de routes statiques avec liaison de port

Dans cet exemple, vous maintenez tous les ports VMkernel liés dans un sous-réseau (N1) et vous configurez tous les portails cibles dans un autre sous-réseau (N2). Vous pouvez alors ajouter une route statique pour le sous-réseau cible (N2).

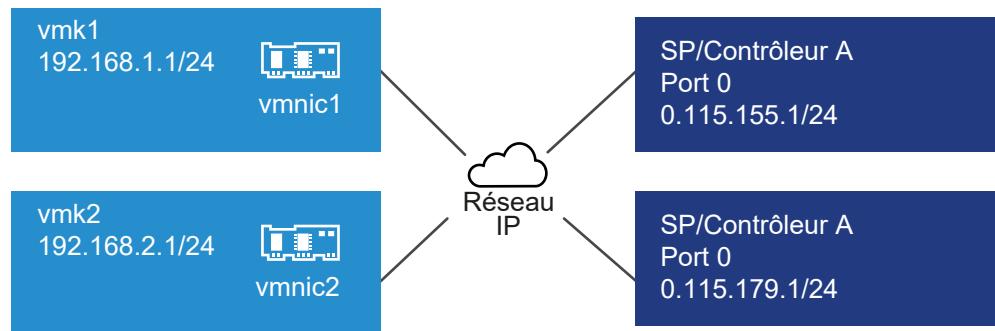


Utilisez la commande suivante :

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.179.0/24
```

Exemple 2. Utilisation de routes statiques pour créer plusieurs chemins

Dans cette configuration, vous utilisez le routage statique lorsque vous employez des sous-réseaux différents. La liaison de port ne peut pas être utilisée avec cette configuration.



Vous configurez vmk1 et vmk2 dans des sous-réseaux différents, à savoir 192.168.1.0 et 192.168.2.0. Vos portails cibles se trouvent également dans des sous-réseaux distincts, 10.115.155.0 et 10.115.179.0.

Vous pouvez ajouter la route statique vers 10.115.155.0 à partir de vmk1. Assurez-vous que la passerelle peut être atteinte à partir de vmk1.

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network 10.115.155.0/24
```

Vous ajoutez ensuite la route statique vers 10.115.179.0 à partir de vmk2. Assurez-vous que la passerelle peut être atteinte à partir de vmk2.

```
# esxcli network ip route ipv4 add -gateway 192.168.2.253 -network 10.115.179.0/24
```

Lors d'une connexion à l'aide du Port 0 du Contrôleur A, vmk1 est utilisé.

Lors d'une connexion à l'aide du Port 0 du Contrôleur B, vmk2 est utilisé.

Exemple 3. Routage avec une passerelle distincte par port VMkernel

À partir de vSphere 6.5, vous pouvez configurer une passerelle distincte par port VMkernel. Si vous utilisez le DHCP pour obtenir la configuration IP d'un port VMkernel, il est également possible d'obtenir des informations sur la passerelle à l'aide du DHCP.

Pour afficher les informations sur la passerelle par port VMkernel, utilisez la commande suivante :

```
# esxcli network ip interface ipv4 address list
```

Name	IPv4 Address	IPv4 Netmask	IPv4 Broadcast	Address Type	Gateway	DHCP	DNS
vmk0	10.115.155.122	255.255.252.0	10.115.155.255	DHCP	10.115.155.253	true	
vmk1	10.115.179.209	255.255.252.0	10.115.179.255	DHCP	10.115.179.253	true	
vmk2	10.115.179.146	255.255.252.0	10.115.179.255	DHCP	10.115.179.253	true	

Lorsque vous disposez de passerelles distinctes pour chaque port VMkernel, vous utilisez la liaison de port pour atteindre des cibles dans différents sous-réseaux.

Gestion du réseau iSCSI

Des considérations spéciales s'appliquent aux adaptateurs réseau, physiques et VMkernel qui sont associés à un adaptateur iSCSI.

Après la création de connexions réseau iSCSI, un indicateur iSCSI est activé dans vSphere Client. Cet indicateur indique qu'un adaptateur réseau virtuel ou physique particulier est dédié à l'iSCSI. Pour éviter des interruptions du trafic iSCSI, suivez ces recommandations et considérations lors de la gestion des adaptateurs réseau physiques et virtuels iSCSI :

- Assurez-vous que des adresses sont affectées aux adaptateurs réseau VMkernel ou sur le même sous-réseau que le portail de stockage iSCSI auquel ils se connectent.
- Les adaptateurs iSCSI utilisant des adaptateurs VMkernel ne peuvent pas se connecter aux ports iSCSI sur des sous-réseaux différents, même si les adaptateurs iSCSI découvrent ces ports.
- Lors de l'utilisation de commutateurs vSphere séparés pour connecter des adaptateurs réseau physiques et des adaptateurs VMkernel, assurez-vous que les commutateurs vSphere se connectent aux différents sous-réseaux IP.
- Si les adaptateurs VMkernel se trouvent sur le même sous-réseau, ils doivent se connecter à un même vSwitch.
- Si vous migrez des adaptateurs VMkernel vers un autre commutateur vSphere, déplacez les adaptateurs physiques associés.
- Ne modifiez pas la configuration des adaptateurs VMkernel dédiés à l'iSCSI ou les adaptateurs réseau physiques.
- N'apportez pas de changements qui pourraient rompre l'association des adaptateurs VMkernel et des adaptateurs réseau physiques. Vous pouvez rompre l'association si vous retirez l'un des adaptateurs ou le commutateur vSphere qui les connecte. Vous pouvez également modifier la stratégie réseau 1:1 pour leur connexion.

Dépannage du réseau iSCSI

Un avertissement indique une politique de groupe de ports non conforme pour un adaptateur VMkernel dédié à l'iSCSI.

Problème

La politique de groupe de ports d'un adaptateur VMkernel est considérée comme étant non conforme dans les cas suivants :

- L'adaptateur VMkernel n'est pas connecté à un adaptateur réseau physique actif.
- L'adaptateur VMkernel est connecté à plusieurs adaptateurs réseau physiques.
- L'adaptateur VMkernel est connecté à un ou plusieurs adaptateurs physiques en veille.
- L'adaptateur réseau physique actif est changé.

Solution

Définissez la stratégie réseau appropriée pour l'adaptateur VMkernel dédié à iSCSI. Reportez-vous à la section [Configurer la liaison de port pour les protocoles iSCSI ou iSER](#).

Configurer la liaison de port pour les protocoles iSCSI ou iSER

La liaison de port crée des connexions pour le trafic entre certains types d'adaptateurs iSCSI et iSER et les adaptateurs réseau physiques.

Les types d'adaptateurs suivants nécessitent la liaison de port :

- Adaptateur iSCSI logiciel
- Adaptateur iSCSI matériel dépendant
- Adaptateur iSCSI sur RDMA (iSER) VMware

Les tâches suivantes traitent de la configuration réseau avec un commutateur vSphere Standard et un adaptateur réseau physique unique. Si vous disposez de plusieurs adaptateurs réseau, reportez-vous à [Multiples adaptateurs réseau dans une configuration iSCSI ou iSER](#).

Note iSER ne prend pas en charge l'association de cartes réseau. Lors de la configuration de la liaison de port pour iSER, utilisez uniquement un adaptateur physique sur lequel RDMA est activé (vmnic #) et un adaptateur VMkernel (VMK #) par vSwitch.

Vous pouvez également utiliser VMware vSphere® Distributed Switch™ et VMware NSX® Virtual Switch™ dans la configuration de liaison de port. Pour obtenir des informations sur les commutateurs virtuels NSX, reportez-vous à la documentation sur *VMware NSX Data Center pour vSphere*.

Si vous utilisez vSphere Distributed Switch avec plusieurs ports de liaison montante, pour l'association de ports, créez un groupe de ports distribués distinct pour chaque carte NIC physique. Réglez ensuite la politique de groupes de façon à ce que chaque groupe de ports distribués n'ait qu'un seul port de liaison montante actif. Pour obtenir des informations détaillées sur les instances de Distributed Switch, reportez-vous à la documentation sur *Mise en réseau vSphere*.

Créer un adaptateur VMkernel unique pour iSCSI ou iSER

Connectez l'adaptateur VMkernel, qui exécute des services pour le stockage iSCSI, à un adaptateur réseau physique sur votre hôte ESXi. Vous utilisez ensuite l'adaptateur VMkernel créé dans la configuration de liaison de port avec les adaptateurs iSCSI ou iSER.

Conditions préalables

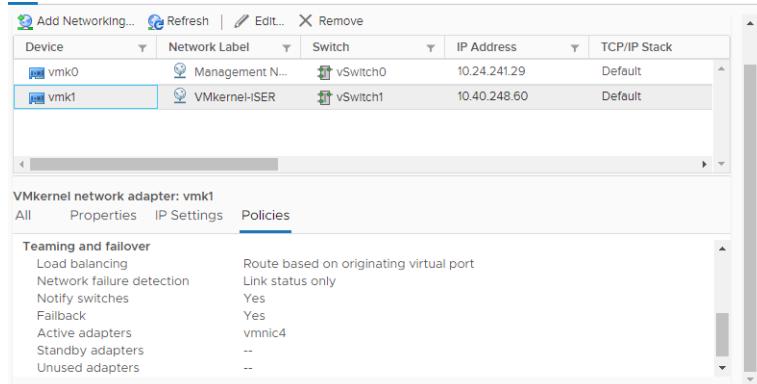
- Si vous créez un adaptateur VMkernel pour un iSCSI de matériel dépendant, vous devez utiliser l'adaptateur réseau physique (vmnic#) qui correspond au composant iSCSI. Reportez-vous à la section [Déterminer l'association entre les adaptateurs iSCSI et les adaptateurs réseau](#).
- Avec l'adaptateur iSER, assurez-vous que vous utilisez une vmnic# appropriée compatible avec RDMA. Reportez-vous à la section [Installer et afficher un adaptateur réseau prenant en charge RDMA](#).

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Sélectionnez **Ajouter une mise en réseau** dans le menu contextuel.
- 3 Sélectionnez **Adaptateur réseau VMkernel**, puis cliquez sur **Suivant**.
- 4 Sélectionnez **Nouveau commutateur standard** pour créer un commutateur vSphere Standard.
- 5 Cliquez sur l'icône **Ajouter des adaptateurs** et sélectionnez un adaptateur réseau (vmnic#) à utiliser pour iSCSI.
Veillez à affecter l'adaptateur à des adaptateurs actifs.
- 6 Entrez une étiquette de réseau.
Une étiquette de réseau est un nom convivial qui identifie l'adaptateur VMkernel que vous créez (par exemple iSCSI ou iSER).
- 7 Spécifiez les paramètres IP.
- 8 Passez vos informations en revue et cliquez sur **Terminer**.
Vous avez créé l'adaptateur virtuel VMkernel (vmk#) d'un adaptateur réseau physique (vmnic#) sur votre hôte.

9 Vérifiez votre configuration.

- Sous **Mise en réseau**, sélectionnez **Adaptateurs VMkernel** et sélectionnez l'adaptateur VMkernel (vmk#) dans la liste.
- Cliquez sur l'onglet **Stratégies** et vérifiez que l'adaptateur réseau physique correspondant (vmnic#) s'affiche en tant qu'adaptateur actif sous **Association et basculement**.



Étape suivante

Si votre hôte dispose d'un adaptateur réseau physique pour le trafic iSCSI, liez l'adaptateur VMkernel que vous avez créé à l'adaptateur iSCSI ou iSER.

Si vous disposez de plusieurs adaptateurs réseau, vous pouvez créer des adaptateurs VMkernel supplémentaires et effectuer la liaison iSCSI. Le nombre d'adaptateurs virtuels doit correspondre au nombre d'adaptateurs physiques sur l'hôte. Pour plus d'informations, consultez [Multiples adaptateurs réseau dans une configuration iSCSI ou iSER](#).

Lier des adaptateurs iSCSI ou iSER à des adaptateurs VMkernel

Dans l'hôte ESXi, liez un adaptateur iSCSI ou iSER à un adaptateur VMkernel.

Conditions préalables

Créez un adaptateur VMkernel virtuel pour chaque adaptateur réseau physique sur votre hôte. Si vous utilisez plusieurs adaptateurs VMkernel, configurez une stratégie réseau appropriée.

Privilège nécessaire :**Hôte.Configuration.Configuration de la partition de stockage**

Procédure

- Dans vSphere Client, accédez à l'hôte ESXi.
- Cliquez sur l'onglet **Configurer**.
- Sous **Stockage**, cliquez sur **Adaptateurs de stockage** et sélectionnez l'adaptateur iSCSI ou iSER approprié (vhba#) dans la liste.
- Cliquez sur l'onglet **Liaison de port réseau**, puis sur l'icône **Ajouter**.

- 5 Sélectionnez un adaptateur VMkernel à lier à l'adaptateur iSCSI ou iSER.

Note Assurez-vous que la stratégie réseau de l'adaptateur VMkernel est conforme aux conditions de liaison.

Vous pouvez lier l'adaptateur iSCSI logiciel à un ou plusieurs adaptateurs VMkernel. S'il s'agit d'un adaptateur iSCSI matériel dépendant ou de l'adaptateur iSER, seul un adaptateur VMkernel associé à la carte réseau physique appropriée est disponible.

- 6 Cliquez sur **OK**.

La connexion réseau figure dans la liste des liaisons de port réseau de l'adaptateur iSCSI ou iSER.

The screenshot shows the 'Storage Adapters' interface in the vSphere Client. At the top, there are buttons for 'Add Software Adapter', 'Refresh', 'Rescan Storage...', 'Rescan Adapter', and 'Remove'. Below this is a table titled 'Storage Adapters' with columns: Adapter, Type, Status, Identifier, Targets, Devices, and Paths. The table lists several adapters, including 'vmhba33' (Block SCSI, Unknown), 'vmhba64' (iSCSI, Unbound), 'vmhba65' (iSCSI, Unbound), 'vmhba66' (iSCSI, Online), 'vmhba67' (iSCSI, Unbound), and 'vmhba1' (Block SCSI, Unknown). Below the table, tabs for 'Properties', 'Devices', 'Paths', 'Dynamic Discovery', 'Static Discovery', 'Network Port Binding' (which is selected), and 'Advanced Options' are visible. A sub-table under 'Network Port Binding' shows a single entry: 'VMkernel-iSER (vSwitch1)' is bound to 'vmk1' with a 'Compliant' status and 'Not used' path. There are also 'Copy All' and '9 Items' buttons.

Vérifier les détails de liaison de port sur l'hôte ESXi

Vérifier les détails de mise en réseau de l'adaptateur VMkernel lié à l'adaptateur vmhba iSCSI ou iSER.

Procédure

- Dans vSphere Client, accédez à l'hôte ESXi.
- Cliquez sur l'onglet **Configurer**.
- Sous **Stockage**, cliquez sur **Adaptateurs de stockage** et sélectionnez l'adaptateur iSCSI ou iSER approprié dans la liste.
- Cliquez sur l'onglet **Liaison de port réseau** et sélectionnez l'adaptateur VMkernel dans la liste.
- Cliquez sur l'icône **Afficher les détails**.
- Consultez les informations relatives à l'adaptateur VMkernel et l'adaptateur physique en basculant entre les onglets disponibles.

Étape suivante

Pour connaître les autres étapes de configuration que vous pouvez effectuer pour les adaptateurs de stockage iSCSI ou iSER, reportez-vous aux rubriques suivantes :

- [Configurer des adaptateurs iSCSI matériel dépendants](#)
- [Configurer l'adaptateur iSCSI logiciel](#)
- [Configurer iSER avec ESXi](#)

Utilisation de trames Jumbo avec iSCSI et iSER

ESXi prend en charge l'utilisation des trames Jumbo avec iSCSI/iSER.

Les trames Jumbo sont des trames Ethernet dont la taille est supérieure à 1 500 octets. Le paramètre d'unité de transmission maximale (MTU) est utilisé généralement pour mesurer la taille des trames Jumbo.

Lorsque vous utilisez des trames Jumbo pour le trafic iSCSI, les considérations suivantes s'appliquent :

- Tous les composants réseau doivent prendre en charge les trames Jumbo.
- Vérifiez auprès de vos fournisseurs si vos cartes NIC physiques et vos adaptateurs iSCSI prennent en charge les trames Jumbo.
- Pour configurer et vérifier les commutateurs réseau physiques pour les trames Jumbo, consultez la documentation de votre fournisseur.

Le tableau suivant décrit le niveau de prise en charge d'ESXi concernant les trames Jumbo.

Tableau 5-1. Prise en charge des trames Jumbo

Type d'adaptateurs iSCSI	Prise en charge des trames Jumbo
iSCSI logiciel	Pris en charge
Matériel iSCSI dépendant	Pris en charge. Consultez le fournisseur.
Matériel iSCSI indépendant	Pris en charge. Consultez le fournisseur.
iSER VMware	Pris en charge. Consultez le fournisseur.

Activer les trames Jumbo pour la mise en réseau

Vous pouvez activer les trames Jumbo pour les adaptateurs de stockage ESXi qui utilisent la mise en réseau VMkernel pour leur trafic. Il s'agit notamment des adaptateurs iSCSI logiciels, iSCSI matériels dépendants et iSER VMware.

Pour activer les trames Jumbo, modifiez la valeur par défaut du paramètre MTU (Maximum Transmission Units). Vous pouvez modifier le paramètre MTU sur le commutateur vSphere que vous utilisez pour le trafic iSCSI. Pour plus d'informations, consultez la documentation *Mise en réseau vSphere*.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Mise en réseau**, cliquez sur **Commutateurs virtuels** et sélectionnez le commutateur vSphere que vous souhaitez modifier dans la liste.
- 4 Cliquez sur l'icône **Modifier les paramètres**.
- 5 Sur la page Propriétés, modifiez la valeur du paramètre MTU.

Cette étape définit le MTU pour toutes les cartes NIC physiques sur ce commutateur standard. Définissez la valeur MTU à la taille maximale de MTU parmi toutes les cartes NIC connectées au commutateur standard. ESXi prend en charge un paramètre MTU d'une taille allant jusqu'à 9 000 octets.

Activer les trames Jumbo pour l'iSCSI matériel indépendant

Pour activer les trames Jumbo pour les adaptateurs iSCSI matériels indépendants sur votre hôte ESXi, modifiez la valeur par défaut du paramètre d'unités de transmission maximale (MTU).

Utilisez les paramètres d'Options avancées pour modifier le paramètre MTU pour l'HBA iSCSI.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur l'option **Adaptateurs de stockage** et sélectionnez l'adaptateur iSCSI matériel indépendant dans la liste des adaptateurs.
- 4 Cliquez sur l'onglet **Options avancées** et cliquez sur **Modifier**.
- 5 Modifiez la valeur du paramètre MTU.

ESXi prend en charge un paramètre MTU d'une taille allant jusqu'à 9000 octets.

Configurer la découverte dynamique ou statique pour iSCSI et iSER sur l'hôte ESXi

Vous devez configurer les adresses de découverte cibles pour que l'adaptateur de stockage iSCSI ou iSER puisse identifier les ressources de stockage du réseau qui sont accessibles.

Le système ESXi prend en charge les méthodes de découvertes suivantes :

Découverte dynamique

Également appelée découverte SendTargets. Chaque fois que l'initiateur contacte un serveur iSCSI désigné, il envoie la demande de SendTargets au serveur. Le serveur répond en fournissant une liste de cibles disponibles à l'initiateur. Les noms et adresses IP de ces cibles figurent dans l'onglet **Découverte statique**. Si vous supprimez une cible statique ajoutée par la découverte dynamique, il se peut qu'elle soit réintégrée à la liste la prochaine fois qu'une analyse se produira, que l'adaptateur de stockage se réinitialisera ou que l'hôte redémarrera.

Note Avec un iSCSI logiciel ou matériel dépendant, ESXi filtre les adresses cibles selon la famille IP de l'adresse de serveur iSCSI spécifiée. S'il s'agit d'une adresse IPv4, les adresses IPv6 susceptible d'apparaître dans la réponse SendTargets provenant du serveur iSCSI sont filtrées. Lorsqu'un serveur iSCSI est spécifié par le biais de noms DNS ou que la réponse SendTargets du serveur iSCSI contient des noms DNS, ESXi utilise la famille IP de la première entrée résolue dans la recherche DNS.

Découverte statique

Outre la méthode de découverte dynamique, vous pouvez utiliser la découverte statique et entrer manuellement des informations pour les cibles. L'adaptateur iSCSI ou iSER utilise une liste de cibles que vous spécifiez pour contacter les serveurs iSCSI et communiquer avec eux.

Quand vous configurez la découverte statique ou dynamique, vous pouvez uniquement ajouter de nouvelles cibles iSCSI. Vous ne pouvez pas modifier les paramètres d'une cible existante. Pour apporter des modifications, supprimez la cible existante et ajoutez-en une nouvelle.

Conditions préalables

Privilège nécessaire : **Hôte.Configuration.Configuration de la partition de stockage**

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**, puis sélectionnez l'adaptateur (vmhba#) à configurer.

4 Configurez la méthode de découverte.

Méthode de découverte	Description
Découverte dynamique	<p>a Cliquez sur Découverte dynamique, puis cliquez sur Ajouter.</p> <p>b Tapez l'adresse IP ou le nom DNS du système de stockage et cliquez sur OK.</p> <p>c Scannez à nouveau l'adaptateur iSCSI</p> <p>Après avoir établi la session SendTargets avec le système iSCSI, votre hôte remplira la liste Découverte statique avec toutes les nouvelles cibles découvertes.</p> <p>Note Une cible découverte dynamiquement reste dans la liste même après sa suppression côté baie.</p>
Découverte statique	<p>a Cliquez sur Découverte statique, puis cliquez sur Ajouter.</p> <p>b Entrez les informations de la cible, puis cliquez sur OK</p> <p>c Scannez à nouveau l'adaptateur iSCSI</p>

Étape suivante

Pour connaître les autres étapes de configuration que vous pouvez effectuer pour les adaptateurs de stockage iSCSI ou iSER, reportez-vous aux rubriques suivantes :

- [Configurer des adaptateurs iSCSI matériel indépendants](#)
- [Configurer des adaptateurs iSCSI matériel dépendants](#)
- [Configurer l'adaptateur iSCSI logiciel](#)
- [Configurer iSER avec ESXi](#)

Supprimer des cibles iSCSI dynamiques ou statiques

Supprimez les serveurs iSCSI connectés à votre hôte ESXi.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**, puis sélectionnez l'adaptateur iSCSI à modifier dans la liste.
- 4 Basculez entre **Découverte dynamique** et **Découverte statique**.
- 5 Sélectionnez un serveur iSCSI à supprimer et cliquez sur **Supprimer**.
- 6 Scannez à nouveau l'adaptateur iSCSI

Si vous supprimez la cible statique qui a été découverte dynamiquement, vous devez la supprimer du système de stockage avant d'effectuer la nouvelle analyse. Dans le cas contraire, votre hôte découvrira et ajoutera automatiquement la cible à la liste des cibles statiques lorsque vous effectuerez une nouvelle analyse de l'adaptateur.

Configuration des paramètres CHAP pour les adaptateurs de stockage iSCSI ou iSER

Etant donné que les réseaux IP qu'utilise la technologie iSCSI pour se connecter aux cibles distantes ne protègent pas les données qu'ils transportent, vous devez sécuriser la connexion. L'un des protocoles que l'iSCSI applique est le protocole CHAP, qui vérifie la légitimité des initiateurs qui accèdent à des cibles sur le réseau.

Le protocole CHAP applique un algorithme de négociation à trois voies pour vérifier l'identité de votre hôte et, le cas échéant, de la cible iSCSI quand l'hôte et la cible établissent une connexion. La vérification repose sur une valeur privée prédefinie, dite secret CHAP, que l'initiateur et la cible partagent.

ESXi prend en charge l'authentification CHAP au niveau de l'adaptateur. Dans ce cas, toutes les cibles reçoivent les mêmes nom et secret CHAP de la part de l'initiateur iSCSI. Pour les adaptateurs iSCSI logiciels et dépendant du matériel, et pour les adaptateurs iSER, ESXi prend également en charge l'authentification CHAP en fonction de la cible, ce qui vous permet de configurer différentes informations d'identification pour chaque cible afin de renforcer la sécurité.

Sélection de la méthode d'authentification CHAP

ESXi prend en charge le protocole CHAP unidirectionnel pour tous les types d'initiateurs iSCSI et iSER, ainsi que le protocole CHAP bidirectionnel pour les logiciels et le matériel dépendant iSCSI, et pour iSER.

Avant de configurer CHAP, vérifiez si CHAP est activé sur le système de stockage iSCSI. Obtenez également des informations sur la méthode d'authentification CHAP que le système prend en charge. Si le protocole CHAP est activé, configurez-le pour vos initiateurs, en veillant à ce que les informations d'identification d'authentification CHAP correspondent à celles du stockage iSCSI.

ESXi prend en charge les méthodes d'authentification CHAP suivantes :

CHAP unidirectionnel

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

CHAP bidirectionnel

L'authentification CHAP bidirectionnelle ajoute un niveau supplémentaire de sécurité. Avec cette méthode, l'initiateur peut également authentifier la cible. VMware prend en charge cette méthode pour les adaptateurs iSCSI logiciels et dépendants du matériel, et pour les adaptateurs iSER.

Pour les adaptateurs iSCSI logiciels et dépendant du matériel, ainsi que pour les adaptateurs iSER, vous pouvez définir le CHAP unidirectionnel et le CHAP bidirectionnel pour chaque adaptateur ou au niveau cible. Le matériel indépendant iSCSI prend uniquement CHAP en charge au niveau de l'adaptateur.

Quand vous définissez les paramètres CHAP, indiquez un niveau de sécurité pour CHAP.

Note Lorsque vous définissez le niveau de sécurité CHAP, le type de réponse de la baie de stockage dépend de l'implémentation CHAP de la baie et est spécifique du fournisseur. Pour plus d'informations sur le comportement de l'authentification CHAP dans différentes configurations d'initiateur et de cible, consultez la documentation de la baie.

Tableau 5-2. Niveau de sécurité CHAP

Niveau de sécurité CHAP	Description	Adaptateurs de stockage pris en charge
Aucun	L'hôte n'applique pas l'authentification CHAP. Cette authentification est activée. Utilisez cette option pour la désactiver.	Matériel iSCSI indépendant iSCSI logiciel Matériel iSCSI dépendant iSER
Utiliser le protocole CHAP unidirectionnel si la cible l'impose	L'hôte préfère une connexion non CHAP, mais peut utiliser une connexion CHAP si la cible l'exige.	iSCSI logiciel Matériel iSCSI dépendant iSER
Utiliser le protocole CHAP unidirectionnel sauf si la cible l'interdit	L'hôte préfère CHAP, mais peut utiliser des connexions non CHAP si la cible ne gère pas CHAP.	Matériel iSCSI indépendant iSCSI logiciel Matériel iSCSI dépendant iSER
Utiliser le protocole CHAP unidirectionnel	L'hôte exige une authentification CHAP réussie. La connexion échoue si la négociation CHAP échoue.	Matériel iSCSI indépendant iSCSI logiciel Matériel iSCSI dépendant iSER
Utiliser le CHAP bidirectionnel	L'hôte et la cible prennent en charge le CHAP bidirectionnel.	iSCSI logiciel Matériel iSCSI dépendant iSER

Configurer CHAP pour un adaptateur de stockage iSCSI ou iSER

Lorsque vous configurez le nom et le secret du protocole CHAP au niveau de l'adaptateur iSCSI/iSER, toutes les cibles reçoivent les mêmes paramètres de l'adaptateur. Par défaut, toutes les adresses de découverte ou cibles statiques héritent des paramètres CHAP que vous configurez au niveau de l'adaptateur.

Le nom CHAP ne peut pas dépasser 511 caractères alphanumériques et le secret CHAP ne peut pas comporter 255 caractères alphanumériques maximum. Certains adaptateurs, par exemple l'adaptateur QLogic, peuvent avoir des limites plus basses, 255 pour le nom CHAP et 100 pour le secret CHAP.

Conditions préalables

- Avant de configurer des paramètres CHAP pour l'iSCSI logiciel ou matériel dépendant, déterminez s'il convient de configurer un CHAP unidirectionnel ou bidirectionnel. Les adaptateurs iSCSI matériels indépendants ne prennent pas en charge les CHAP bidirectionnels.
- Vérifier les paramètres CHAP configurés côté stockage. Les paramètres que vous configurez doivent correspondre à ceux présents côté stockage.
- Privilège nécessaire : **Hôte.Configuration.Configuration de la partition de stockage**

Procédure

- 1 Accédez à l'adaptateur de stockage iSCSI ou iSER.
 - a Dans vSphere Client, accédez à l'hôte ESXi.
 - b Cliquez sur l'onglet **Configurer**.
 - c Sous **Stockage**, cliquez sur **Adaptateurs de stockage**, puis sélectionnez l'adaptateur (vmhba#) à configurer.
- 2 Cliquez sur l'onglet **Propriétés**, puis sur **Modifier** dans le panneau **Authentification**.
- 3 Spécifiez la méthode d'authentification.
 - **Aucun**
 - **Utiliser le protocole CHAP unidirectionnel si la cible l'impose**
 - **Utiliser le protocole CHAP unidirectionnel sauf si la cible l'interdit**
 - **Utiliser le protocole CHAP unidirectionnel**
 - **Utiliser le CHAP bidirectionnel.** Pour configurer un CHAP bidirectionnel, vous devez sélectionner cette option.
- 4 Indiquez le nom du CHAP sortant.

Assurez-vous que le nom que vous indiquez concorde avec celui configuré côté stockage.

 - Pour définir le nom CHAP sur le nom de la carte iSCSI, sélectionnez **Utiliser nom initiateur**.
 - Pour définir le nom CHAP en n'utilisant pas le nom d'initiateur iSCSI, désélectionnez **Utiliser nom initiateur** et entrez un nom dans la zone de texte **Nom**.
- 5 Saisissez un secret pour le CHAP sortant destiné à être utilisé dans le processus d'authentification. Utilisez le même secret que celui que vous entrez côté stockage.
- 6 Si vous configurez un CHAP bidirectionnel, spécifiez les données d'identification du CHAP entrant.

Veillez à utiliser des secrets différents pour le CHAP sortant et le CHAP entrant.
- 7 Cliquez sur **OK**.
- 8 Scannez à nouveau l'adaptateur iSCSI

Résultats

Si vous modifiez les paramètres CHAP, ils sont utilisés pour de nouvelles sessions iSCSI. Pour les sessions existantes, les nouveaux paramètres ne sont pas utilisés tant que vous ne vous déconnectez pas et que vous ne vous reconnectez pas.

Étape suivante

Pour connaître les autres étapes de configuration que vous pouvez effectuer pour les adaptateurs de stockage iSCSI ou iSER, reportez-vous aux rubriques suivantes :

- [Configurer des adaptateurs iSCSI matériel indépendants](#)
- [Configurer des adaptateurs iSCSI matériel dépendants](#)
- [Configurer l'adaptateur iSCSI logiciel](#)
- [Configurer iSER avec ESXi](#)

Configurer CHAP pour une cible

Si vous utilisez des adaptateurs iSCSI logiciels et dépendant du matériel, ou un adaptateur de stockage iSER, vous pouvez configurer des données d'identification CHAP différentes pour chaque adresse de découverte ou cible statique.

Le nom CHAP ne peut pas excéder 511 et le secret CHAP 255 caractères alphanumériques.

Conditions préalables

- Avant de configurer les paramètres CHAP, déterminez s'il convient de configurer CHAP unidirectionnel ou bidirectionnel.
- Vérifier les paramètres CHAP configurés côté stockage. Les paramètres que vous configurez doivent correspondre à ceux présents côté stockage.
- Privilège nécessaire : **Hôte.Configuration.Configuration de la partition de stockage**

Procédure

- 1 Accédez à l'adaptateur de stockage iSCSI ou iSER.
 - a Dans vSphere Client, accédez à l'hôte ESXi.
 - b Cliquez sur l'onglet **Configurer**.
 - c Sous **Stockage**, cliquez sur **Adaptateurs de stockage**, puis sélectionnez l'adaptateur (vmhba#) à configurer.
- 2 Cliquez sur **Découverte dynamique** ou **Découverte statique**.
- 3 Dans la liste des cibles disponibles, sélectionnez une cible à configurer et cliquez sur **Authentification**.
- 4 Désélectionnez **Hériter des paramètres du parent** et spécifiez la méthode d'authentification.
 - **Aucun**

- Utiliser le protocole CHAP unidirectionnel si la cible l'impose
 - Utiliser le protocole CHAP unidirectionnel sauf si la cible l'interdit
 - Utiliser le protocole CHAP unidirectionnel
 - Utiliser le CHAP bidirectionnel. Pour configurer un CHAP bidirectionnel, vous devez sélectionner cette option.
- 5 Indiquez le nom du CHAP sortant.
- Assurez-vous que le nom que vous indiquez concorde avec celui configuré côté stockage.
- Pour définir le nom CHAP sur le nom de la carte iSCSI, sélectionnez **Utiliser nom initiateur**.
 - Pour définir le nom CHAP en n'utilisant pas le nom d'initiateur iSCSI, désélectionnez **Utiliser nom initiateur** et entrez un nom dans la zone de texte **Nom**.
- 6 Saisissez un secret pour le CHAP sortant destiné à être utilisé dans le processus d'authentification. Utilisez le même secret que celui que vous entrez côté stockage.
- 7 Si vous configurez un CHAP bidirectionnel, spécifiez les données d'identification du CHAP entrant.
- Veuillez à utiliser des secrets différents pour le CHAP sortant et le CHAP entrant.
- 8 Cliquez sur **OK**.
- 9 Scannez à nouveau l'adaptateur de stockage.

Résultats

Si vous modifiez les paramètres CHAP, ils sont utilisés pour de nouvelles sessions iSCSI. Pour les sessions existantes, les nouveaux paramètres ne sont appliqués qu'une fois que vous vous êtes déconnecté puis reconnecté.

Configuration des paramètres avancés iSCSI

Il peut être nécessaire de configurer des paramètres supplémentaires pour les initiateurs iSCSI sur votre hôte ESXi. Par exemple, certains systèmes de stockage iSCSI exigent la redirection ARP (Address Resolution Protocol) pour mouvoir le trafic iSCSI dynamiquement d'un port à l'autre. Dans ce cas, vous devez activer la redirection ARP sur votre hôte.

Le tableau suivant répertorie les paramètres iSCSI avancés que vous pouvez configurer à l'aide de vSphere Client. En outre, vous pouvez utiliser les commandes CLI vSphere pour configurer certains des paramètres avancés. Pour plus d'informations, reportez-vous à la documentation *Démarrage avec ESXCLI*.

Selon le type de vos adaptateurs, certains paramètres peuvent ne pas être disponibles.

Important Ne modifiez pas les paramètres iSCSI avancés, sauf si le support technique de VMware ou les fournisseurs de stockage vous demandent de les modifier.

Tableau 5-3. Paramètres supplémentaires des initiateurs iSCSI

Paramètre avancé	Description
Résumé d'en-tête	Augmente l'intégrité des données. Lorsque le paramètre de résumé d'en-tête est activé, le système effectue un total de contrôle sur chaque partie d'en-tête de l'unité de données de protocole (PDU) iSCSI. Le système vérifie les données à l'aide de l'algorithme CRC32C.
Résumé de données	Augmente l'intégrité des données. Lorsque le paramètre de résumé de données est activé, le système effectue un total de contrôle sur chaque partie de données PDU. Le système vérifie les données à l'aide de l'algorithme CRC32C.
	Note Les systèmes qui utilisent des processeurs Intel Nehalem déchargent les calculs de résumé iSCSI pour l'iSCSI logiciel. Ce déchargement permet de réduire l'impact sur les performances.
ErrorRecoveryLevel	Valeur de niveau de récupération des erreurs (Error Recovery Level, ERL) iSCSI que l'initiateur iSCSI sur l'hôte négocie lors d'une connexion.
LoginRetryMax	Nombre maximal de tentatives de connexion à une cible par l'initiateur iSCSI ESXi autorisé avant l'arrêt des tentatives.
MaxOutstandingR2T	Définit le nombre d'unités de données de protocole (PDU) prêtes à envoyer qui peut être en transition avant qu'une PDU d'accusé de réception ne soit reçue.
FirstBurstLength	Indique la quantité maximum de données non sollicitées qu'un initiateur iSCSI peut envoyer à la cible pendant l'exécution d'une commande SCSI, en octets.
MaxBurstLength	Charge utile de données SCSI maximum dans une séquence iSCSI d'entrée de données ou de sortie de données sollicitée, en octets.
MaxRecvDataSegLength	Longueur maximum de segment de données, en octets, qui peut être reçu dans une PDU iSCSI.
MaxCommands	Nombre maximal de commandes SCSI pouvant être mises en file d'attente sur l'adaptateur iSCSI.
DefaultTimeToWait	Nombre minimal de secondes à attendre avant de tenter une déconnexion ou une réattribution de tâche active après une fin ou une réinitialisation de connexion inattendue.
DefaultTimeToRetain	Nombre maximal de secondes pendant lequel la réattribution de la tâche active est toujours possible après une fin ou une réinitialisation de connexion.
LoginTimeout	Temps (en secondes) que l'initiateur passe à attendre la fin de la réponse de connexion.
LogoutTimeout	Temps (en secondes) que l'initiateur passe à attendre pour obtenir une réponse pour le PDU de demande de déconnexion.
RecoveryTimeout	Indique le laps de temps, en secondes, qui peut s'écouler pendant que s'exécute une récupération de session. Si le délai dépasse sa limite, l'initiateur iSCSI clôture la session.
No-Op Interval (Intervalle sans opération)	Indique l'intervalle, en secondes, entre les demandes en sortie sans opération envoyées par votre initiateur iSCSI à une cible iSCSI. Les demandes en sortie sans opération servent de mécanisme ping pour vérifier qu'une connexion entre l'initiateur iSCSI et la cible iSCSI est active.
No-Op Timeout (Délai de demande sans opération)	Indique le laps de temps, en secondes, qui peut s'écouler avant que votre hôte ne reçoive un message d'entrée sans opération (NOP-In). La cible iSCSI envoie le message en réponse à la demande en sortie sans opération. Dès que la limite de délai sans opération est dépassée, l'initiateur clôture la session actuelle et en démarre une nouvelle.

Tableau 5-3. Paramètres supplémentaires des initiateurs iSCSI (suite)

Paramètre avancé	Description
ARP Redirect (Redirection ARP)	Lorsque ce paramètre est activé, les systèmes de stockage peuvent déplacer le trafic iSCSI dynamiquement d'un port à un autre. Les systèmes de stockage qui effectuent des basculements sur la baie nécessitent le paramètre ARP.
Accusé de réception retardé	Lorsque ce paramètre est activé, les systèmes de stockage peuvent retarder un accusé de réception de paquets de données.

Configurer les paramètres avancés pour iSCSI sur un hôte ESXi

Les paramètres iSCSI avancés contrôlent des paramètres tels que le résumé de l'en-tête et des données, la redirection ARP, l'accusé de réception différé, etc.

Attention N'apportez aucune modification aux paramètres iSCSI avancés à moins de travailler avec l'équipe d'assistance VMware ou de disposer par d'autres biais d'informations précises sur les valeurs à attribuer aux paramètres.

Conditions préalables

Privilège nécessaire : **Hôte.Configuration.Configuration de la partition de stockage**

Procédure

- Dans vSphere Client, accédez à l'hôte ESXi.
- Cliquez sur l'onglet **Configurer**.
- Sous **Stockage**, cliquez sur **Adaptateurs de stockage**, puis sélectionnez l'adaptateur (vmhba#) à configurer.
- Configurer les paramètres avancés.

Option	Description
Au niveau de l'adaptateur	Cliquez sur l'onglet Options avancées et cliquez sur Modifier .
Au niveau de la cible	<ol style="list-style-type: none"> Cliquez sur Découverte dynamique ou Découverte statique. Dans la liste des cibles disponibles, sélectionnez une cible à configurer et cliquez sur Avancé.

- Saisissez toutes les valeurs obligatoires des paramètres avancés que vous voulez modifier.

Gestion des sessions iSCSI

Pour communiquer entre eux, les initiateurs iSCSI et les cibles établissent des sessions iSCSI. Vous pouvez consulter et gérer les sessions iSCSI grâce à vSphere CLI.

Par défaut, les initiateurs iSCSI logiciel et matériels dépendants lancent une session iSCSI entre chaque port d'initiateur et chaque port cible. Si votre initiateur ou cible iSCSI possède plus d'un seul port, votre hôte peut établir plusieurs sessions. Le nombre de sessions par défaut pour chaque cible est égal au nombre de ports sur les adaptateurs iSCSI multiplié par le nombre de ports cibles.

Grâce à vSphere CLI, vous pouvez afficher toutes les sessions en cours afin de les analyser et les déboguer. Pour créer davantage de chemins vers les systèmes de stockage, augmentez le nombre de sessions par défaut en dupliquant les sessions existantes entre l'adaptateur iSCSI et les ports cibles.

Vous pouvez aussi établir une session avec un port cible spécifique. Cette fonctionnalité est utile si votre hôte se connecte à un système de stockage à port unique, qui ne présente qu'un seul port cible à votre initiateur. Le système redirige ensuite les sessions supplémentaires vers un autre port cible. L'établissement d'une nouvelle session entre votre initiateur iSCSI et un autre port cible crée un chemin supplémentaire vers le système de stockage.

Les considérations s'appliquent à la gestion des sessions iSCSI :

- Certains systèmes de stockage ne prennent pas en charge les sessions multiples à partir du même nom d'initiateur ou point de terminaison. Dans un tel cas, les tentatives de créer les sessions multiples vers telles cibles peuvent provoquer une instabilité de votre environnement iSCSI.
- Les fournisseurs de stockages peuvent fournir des gestionnaires de sessions automatiques. L'utilisation des gestionnaires de sessions automatiques pour ajouter ou supprimer des sessions, ne garantit pas des résultats durables et peut perturber les performances du stockage.

Passer en revue les sessions iSCSI

Utilisez la commande vCLI pour afficher les sessions iSCSI entre un adaptateur iSCSI et un système de stockage.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes esxcli dans ESXi Shell.

Procédure

- ◆ Pour répertorier les sessions iSCSI, exécutez la commande suivante :

```
esxcli iscsi session list
```

La commande accepte les options suivantes :

Option	Description
-A --adapter= <i>str</i>	Le nom de l'adaptateur iSCSI, vmhba34, par exemple.
-s --sid= <i>str</i>	L'identificateur de session iSCSI.
-n --name= <i>str</i>	Le nom de la cible iSCSI, iqn.X, par exemple.

Ajout de sessions iSCSI

Utilisez vCLI afin d'ajouter une session iSCSI pour une cible que vous spécifierez ou pour dupliquer une session existante. En dupliquant les sessions, vous augmentez le nombre de sessions par défaut, et vous créez des chemins supplémentaires pour les systèmes de stockage.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes esxcli dans ESXi Shell.

Procédure

- ◆ Pour ajouter ou dupliquer une session iSCSI, exécutez la commande suivante :

```
esxcli iscsi session add
```

La commande accepte les options suivantes :

Option	Description
-A --adapter= <i>str</i>	Le nom de l'adaptateur iSCSI, vmhba34, par exemple. Cette option est requise.
-s --sid= <i>str</i>	L'ISID d'une session à dupliquer. Pour la trouver, répertoriez toutes les sessions.
-n --name= <i>str</i>	Le nom de la cible iSCSI, iqn.X, par exemple.

Étape suivante

Scannez à nouveau l'adaptateur iSCSI

Supprimer des sessions iSCSI

Utilisez la commande vCLI pour fermer une session iSCSI entre un adaptateur iSCSI et une cible.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes esxcli dans ESXi Shell.

Procédure

- ◆ Pour supprimer une session, exécutez la commande suivante :

```
esxcli iscsi session remove
```

La commande accepte les options suivantes :

Option	Description
-A --adapter= <i>str</i>	Le nom de l'adaptateur iSCSI, vmhba34, par exemple. Cette option est requise.
-s --isid= <i>str</i>	L'ISID d'une session à supprimer. Vous pouvez la trouver en listant toutes les sessions.
-n --name= <i>str</i>	Le nom de la cible iSCSI, iqn.X, par exemple.

Étape suivante

Scannez à nouveau l'adaptateur iSCSI

Gestion des périphériques de stockage

6

Gérez le périphérique de stockage en réseau ou local auquel votre hôte ESXi a accès.

Pour plus d'informations sur les périphériques de stockage qu'ESXi prend en charge, reportez-vous aux sections [Types de stockage physique pris en charge par ESXi](#) et [Représentations de périphériques et de cibles](#).

Ce chapitre contient les rubriques suivantes :

- Noms et identifiants de périphérique de stockage ESXi
- Réanalyser les opérations de stockage ESXi
- Identification des problèmes de connectivité de stockage ESXi
- Utiliser le voyant de localisation sur les périphériques de stockage ESXi
- Effacer des périphériques de stockage
- Modifier les paramètres de réservation perpétuelle

Noms et identifiants de périphérique de stockage ESXi

Dans l'environnement ESXi, chaque périphérique de stockage est identifié par plusieurs noms.

Identificateurs de périphérique

Selon le type de stockage, l'hôte ESXi utilise différents algorithmes et conventions pour générer un identificateur pour chaque périphérique de stockage.

Identifiants fournis par le stockage

L'hôte ESXi interroge un périphérique de stockage cible pour le nom du périphérique. À partir des métadonnées renvoyées, l'hôte extrait ou génère un identifiant unique pour le périphérique. L'identificateur est basé sur les normes de stockage spécifiques, est unique et permanent sur tous les hôtes, et dispose d'un des formats suivants :

- naa.xxx
- eui.xxx
- t10.xxx

Identificateur basé sur le chemin d'accès

Lorsque le périphérique ne fournit pas d'identifiant, l'hôte génère un `mpx.Nom path`, où `path` représente le premier chemin d'accès au périphérique, par exemple `mpx.vmhba1:C0:T1:L3`. Cet identifiant peut être utilisé de la même manière que les identités fournies par le stockage.

L'identificateur `mpx.path` est créé pour les périphériques locaux dans l'hypothèse que leurs noms de chemin sont uniques. Toutefois, cet identificateur n'est ni unique, ni permanent, et il peut changer après chaque redémarrage.

En général, le chemin vers le périphérique est au format suivant :

`vmhbaAdapter:CChannel:T Target:LLUN`

- `vmhbaAdapter` est le nom de l'adaptateur de stockage. Le nom fait référence à la carte physique sur l'hôte et non au contrôleur SCSI utilisé par les machines virtuelles.
- `CChannel` est le numéro de canal de stockage.

Les adaptateurs iSCSI logiciels et les adaptateurs iSCSI matériel dépendants utilisent le numéro de canal pour présenter plusieurs chemins menant à la même cible.

- `T Target` est le numéro cible. La numérotation de la cible est choisie par l'hôte et peut être modifiée en cas de changement de mappages des cibles visibles par l'hôte. Les cibles qui sont partagées par différents hôtes n'ont pas nécessairement le même numéro cible.
- `LLUN` est le numéro de LUN qui indique la position du LUN dans la cible. Le numéro de LUN est fourni par le système de stockage. Si une cible possède un seul LUN, le numéro de LUN est toujours zéro (0).

Par exemple, `vmhba1:C0:T3:L1` représente LUN1 sur la cible 3 accessible via l'adaptateur de stockage `vmhba1` et le canal 0.

Identifiant hérité

En plus des identifiants fournis par le périphérique ou `mpx.path`, ESXi génère un autre nom hérité pour chaque périphérique. L'identificateur est au format suivant :

`vml.number`

L'identificateur hérité inclut une série de chiffres qui sont uniques pour le périphérique. L'identifiant peut être obtenu en partie à partir des métadonnées obtenues via la commande SCSI INQUIRY. Pour les périphériques non locaux qui ne fournissent pas les identifiants SCSI INQUIRY, le `vml.number` est utilisé comme seul identifiant unique disponible.

Exemple : Affichage des noms de périphérique dans la vSphere CLI

Vous pouvez utiliser la commande `esxcli storage core device list` pour afficher tous les noms de périphérique dans vSphere CLI. Le résultat est similaire à l'exemple suivant :

```
# esxcli storage core device list
naa.XXX
    Display Name: DGC Fibre Channel Disk(naa.XXX)
    ...
    Other UIDs: vml.000XXX
```

```
mpx.vmhba1:C0:T0:L0
Display Name: Local VMware Disk (mpx.vmhba1:C0:T0:L0)
...
Other UIDs: vml.0000000000XYZ
```

Périphériques NVMe avec identifiants de périphérique NGUID

Pour les périphériques NVMe, ESXi génère des identifiants de périphérique basés sur les informations qu'il récupère des périphériques. En règle générale, les périphériques NVMe prennent en charge les identifiants aux formats EUI64 ou NGUID, ou utilisent les deux formats. NGUID est un identifiant d'espace de noms globalement unique qui utilise le format indicateur EUI64 16 octets.

Pour les terminaux qui prennent uniquement en charge le format NGUID, l'hôte crée deux identifiants : *eui.xxx (NGUID)* comme identifiant principal et *t10.xxx_controller_serial_number* comme identifiant secondaire.

Formats d'ID pris en charge par périphérique		Identifiant de périphérique généré par l'hôte
Format d'ID EUI64	Format d'ID NGUID	ESXi 8.0
oui	oui	<i>t10.xxx_EUI64</i>
oui	non	<i>t10.xxx_EUI64</i>
non	oui	<i>eui.xxx (NGUID)</i> comme ID principal <i>t10.xxx_controller_serial_number</i> comme ID secondaire

Vérifiez le mappage entre les identifiants de périphérique principal et secondaire

Utilisez la commande `esxcli storage core device uidmap list` pour vérifier les identifiants de périphérique. Le résultat est similaire à l'exemple suivant :

```
esxcli storage core device uidmap list
eui.0000xyz.....
Primary UID: eui.0000xyz.....
Alternative Primary UIDs: t10.0000abc....
Legacy UID: vml.0000000000766d68....
Alternative Legacy UIDs: vml.000000000080906....
```

Renommer des périphériques de stockage

L'hôte ESXi attribue un nom complet à un périphérique de stockage en fonction du type de stockage et du fabricant. Vous pouvez modifier le nom complet du périphérique.

Vous ne pouvez pas renommer certains types de périphériques locaux.

Procédure

- Dans vSphere Client, accédez à l'hôte ESXi.

- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Périphériques de stockage**.
- 4 Sélectionnez le périphérique à renommer, puis cliquez sur **Renommer**.
- 5 Modifiez le nom du périphérique et attribuez-lui un nom convivial.

Réanalyser les opérations de stockage ESXi

Lorsque vous effectuez des tâches de gestion des banques de données ou que vous modifiez la configuration SAN, il se peut que vous deviez réanalyser le stockage.

Lorsque vous effectuez des opérations de gestion de la banque de données VMFS, comme la création d'une banque de données VMFS ou d'un RDM, l'ajout d'une extension et l'augmentation ou la suppression d'une banque de données VMFS, votre hôte ou le vCenter Server réanalyse automatiquement le stockage et le met à niveau. Vous pouvez désactiver la fonctionnalité de réanalyse automatique en désactivant le filtre de réanalyse de l'hôte. Reportez-vous à la section [Désactivation des filtres de stockage](#).

Dans certains cas, vous devez effectuer une réanalyse manuelle. Vous pouvez réanalyser tout le stockage disponible de votre hôte ou de tous les hôtes dans un dossier, un cluster et un centre de données.

Si les modifications que vous apportez ne concernent que le stockage connecté à un adaptateur spécifique, effectuez une réanalyse pour cette carte.

Effectuez la réanalyse manuelle chaque fois que vous apportez les modifications suivantes.

- Zonage d'une nouvelle baie de disques sur un SAN.
- Créer de nouveaux LUN sur un SAN
- Modification du masquage de chemin sur un hôte.
- Reconnecter un câble
- Modification des paramètres CHAP (iSCSI uniquement).
- Ajout ou suppression de la détection ou des adresses statiques (iSCSI uniquement).
- Ajout d'un seul hôte dans le vCenter Server après la modification ou la suppression du vCenter Server d'une banque de données partagée par les hôtes du vCenter Server et un seul hôte.

Important Si vous réanalysez quand un chemin n'est pas disponible, l'hôte le supprime de la liste de chemins sur le périphérique. Ce chemin réapparaît dans la liste dès qu'il devient disponible et recommence à fonctionner.

Réanalyse du stockage

Lorsque vous apportez des modifications à la configuration de votre SAN, il est possible que vous deviez réanalyser le stockage. Vous pouvez réanalyser tout le stockage disponible de

votre hôte ESXi, de votre cluster ou de votre centre de données. Si les modifications que vous apportez ne concernent que le stockage accessible par un hôte spécifique, effectuez la réanalyse uniquement pour cet hôte.

Procédure

- 1 Dans le navigateur d'objets de vSphere Client, accédez à un hôte, un cluster, un centre de données ou un dossier contenant des hôtes.
- 2 Dans le menu contextuel, sélectionnez **Stockage > Réanalyser le stockage**.
- 3 Spécifiez l'étendue de la réanalyse.

Option	Description
Analyser les nouveaux périphériques de stockage	Réanalyse de tous les adaptateurs pour découvrir de nouveaux périphériques de stockage. Si de nouveaux périphériques sont découverts, ils apparaissent dans la liste des périphériques.
Analyser les nouveaux volumes VMFS	Réanalyse de tous les périphériques de stockage pour découvrir les nouvelles banques de données qui ont été ajoutées depuis la dernière analyse. Si de nouvelles banques de données sont découvertes, elles apparaissent dans la liste des banques de données.

Effectuer une réanalyse d'adaptateur

Lorsque vous modifiez votre configuration SAN et que ces modifications ne concernent que le stockage accessible par un adaptateur spécifique sur l'hôte ESXi, effectuez une réanalyse pour cet adaptateur uniquement.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**, puis sélectionnez l'adaptateur à réanalyser à partir de la liste.
- 4 Cliquez sur l'icône **Réanalyser un adaptateur**.

Modifier le nombre de périphériques de stockage analysés

La plage d'ID de LUN analysés pour un hôte ESXi peut être comprise entre 0 et 16 383. ESXi ignore les ID de LUN supérieurs à 16 383. Le paramètre `Disk.MaxLUN` configurable détermine la plage d'ID de LUN analysée. Ce paramètre a une valeur par défaut de 1 024.

Le paramètre `Disk.MaxLUN` détermine également le nombre de LUN que le code d'analyse SCSI tente de détecter en utilisant des commandes INQUIRY individuelles si la cible SCSI ne prend pas en charge la détection directe en utilisant REPORT_LUNS.

Vous pouvez modifier le paramètre `Disk.MaxLUN` en fonction de vos besoins. Par exemple, si votre environnement comporte un plus petit nombre de périphériques de stockage avec des ID de LUN compris entre 1 et 100, définissez la valeur sur 101. Cela permet d'améliorer la vitesse de découverte des périphériques sur les cibles ne prenant pas en charge `REPORT_LUNS`. Diminuer cette valeur peut raccourcir la durée de réanalyse et d'amorçage. Cependant, la durée de réanalyse des périphériques de stockage peut également dépendre d'autres facteurs, notamment du type de système de stockage et de la charge sur le système de stockage.

Dans d'autres cas, il peut être nécessaire d'augmenter la valeur si votre environnement utilise des ID de LUN supérieurs à 1023.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Système**, cliquez sur **Paramètres système avancés**.
- 4 Dans le tableau Paramètres système avancés, sélectionnez **Disk.MaxLUN** et cliquez sur l'icône **Modifier**.
- 5 Modifiez sa valeur selon vos besoins, puis cliquez sur **OK**.

La valeur que vous spécifiez est celle de l'ID du LUN suivant le dernier LUN à détecter.

Par exemple, pour détecter les ID des LUN 1 à 100, affectez à **Disk.MaxLUN** la valeur 101.

Identification des problèmes de connectivité de stockage ESXi

Quand votre hôte ESXi rencontre un problème lors de la connexion à un périphérique de stockage, l'hôte traite le problème comme permanent ou temporaire selon certains facteurs.

Les causes des problèmes de connectivité sont multiples. Bien qu'ESXi ne puisse toujours déterminer la cause de l'indisponibilité d'un périphérique de stockage ou de ses chemins, l'hôte fait la différence entre un état de perte permanente de périphérique (PDL) et un état « tous chemins hors service » (APD) passager du stockage.

Perte permanente de périphérique (PDL)

Il s'agit d'une condition survenant quand un périphérique de stockage est défaillant de façon permanente ou est administrativement supprimé ou exclu. Il n'est pas censé devenir disponible. Lorsque le périphérique devient non disponible de façon permanente, ESXi reçoit des codes de détection appropriés ou un rejet de connexion des baies de stockage et peut reconnaître que le périphérique est définitivement perdu.

« Tous chemins hors service » (APD)

Il s'agit d'une condition survenant lorsqu'un périphérique de stockage devient inaccessible pour l'hôte et qu'aucun chemin vers le périphérique n'est disponible. ESXi traite ceci comme une condition passagère car les problèmes relatifs au périphérique rencontrés sont généralement temporaires et le périphérique est censé redevenir disponible.

Problèmes de connectivité et vSphere High Availability

Lorsque le périphérique entre dans l'État PDL ou APD, vSphere High Availability (HA) peut détecter des problèmes de connectivité et fournir une récupération automatisée pour les machines virtuelles concernées sur l'hôte ESXi. À l'aide de VM Component Protection (VMCP), vSphere HA protège les machines virtuelles s'exécutant sur l'hôte du cluster vSphere HA contre les défaillances d'accès. Pour en savoir plus sur VMCP et sur la configuration des réponses pour les banques de données et les machines virtuelles lorsque l'état d'un périphérique devient APD ou PDL, reportez-vous à la documentation *Disponibilité vSphere*.

Détection des états PDL

Un périphérique de stockage est considéré comme en état de perte permanente de périphérique (PDL) lorsqu'il devient définitivement indisponible pour votre hôte ESXi.

Généralement, l'état PDL survient lorsqu'un périphérique est supprimé de façon non intentionnelle, que son identifiant unique est modifié ou quand le périphérique subit une erreur matérielle irrécupérable.

Lorsque la baie de stockage détermine que le périphérique est définitivement indisponible, il envoie des codes de détection d'erreur SCSI ou NVMe à l'hôte ESXi. Après avoir reçu ces erreurs, votre hôte reconnaît le périphérique comme défaillant et enregistre l'état du périphérique comme PDL. Pour que le périphérique soit considéré comme définitivement perdu, les codes de détection doivent être reçus sur tous ses chemins.

Après avoir enregistré l'état PDL du périphérique, l'hôte arrête ses tentatives de rétablissement de la connectivité ou l'envoi de commandes au périphérique.

vSphere Client affiche les informations suivantes relatives au périphérique :

- L'état opérationnel du périphérique passe à Lost Communication.
- Tous les chemins sont affichés comme Dead.
- Les banques de données du périphérique ne sont pas disponibles.

Si aucune connexion ouverte n'existe pour le périphérique ou lorsque la dernière connexion se ferme, l'hôte supprime le périphérique PDL et tous les chemins vers ce périphérique. Vous pouvez désactiver la suppression automatique des chemins en définissant le paramètre avancé de l'hôte `Disk.AutoremoveOnPDL` sur 0.

Si le périphérique revient à l'état PDL, l'hôte peut le découvrir, mais il le traite comme un nouveau périphérique. La cohérence des données pour les machines virtuelles sur le périphérique récupéré n'est pas garantie.

Note Lorsqu'un périphérique échoue sans envoyer les codes de détection SCSI appropriés ou les codes d'erreur NVMe, ou un rejet de connexion iSCSI, l'hôte ne peut pas détecter les conditions PDL. Dans ce cas, l'hôte continue à traiter les problèmes de connectivité comme APD, même lorsque le périphérique échoue en permanence.

Perte permanente de périphérique et codes de détection SCSI

L'exemple suivant de journal VMkernel d'un code de détection SCSI signale que le périphérique est dans un état PDL.

```
H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x25 0x0 or Logical Unit Not Supported
```

Perte permanente de périphérique et codes d'erreur NVMe

L'exemple suivant de journal VMkernel d'un code d'erreur NVMe signale que le périphérique est dans l'état PDL.

```
H:0x0 D:0xb P:0x0 or H:0x0 D:0x11a P:0x0
```

Perte permanente de périphérique et iSCSI

Pour les baies iSCSI avec un seul LUN par cible, le PDL est détecté par l'échec de connexion iSCSI. Une baie de stockage iSCSI rejette les tentatives de démarrage d'une session iSCSI de votre hôte avec une justification Target Unavailable. Comme pour les codes de détection, cette réponse doit être reçue sur tous les chemins menant au périphérique pour que celui-ci soit considéré comme définitivement perdu.

Perte permanente de périphérique et machines virtuelles

Après avoir enregistré l'état PDL du périphérique, l'hôte ferme toutes les E/S des machines virtuelles. vSphere HA peut détecter les PDL et redémarrer les machines virtuelles défaillantes.

Effectuer un retrait de périphérique de stockage prévu

Lorsqu'un périphérique de stockage présente des signes de dysfonctionnement, vous pouvez éviter les risques de PDL (perte de périphérique permanente) ou d'APD (tous chemins hors service). Effectuez un retrait planifié et une reconnexion pour ce périphérique de stockage.

Un retrait de périphérique prévu est la déconnexion intentionnelle d'un périphérique de stockage. Le retrait planifié d'un périphérique peut avoir divers motifs : mettre à niveau votre matériel ou reconfigurer vos périphériques de stockage, par exemple. Pour retirer et reconnecter un périphérique de stockage dans les règles de l'art, vous devez effectuer plusieurs tâches.

Tâche	Description
Migrez les machines virtuelles du périphérique que vous prévoyez de déconnecter.	Gestion de vCenter Server et des hôtes
Démontez la banque de données déployée sur le périphérique.	Reportez-vous à Démontage des banques de données .
Déconnectez le périphérique de stockage.	Reportez-vous à Déconnexion des périphériques de stockage .
Pour un périphérique iSCSI avec un seul LUN par cible, supprimez la cible statique de chaque HBA iSCSI comportant un chemin vers le périphérique de stockage.	Reportez-vous à Supprimer des cibles iSCSI dynamiques ou statiques .
Si nécessaire, reconfigurez le périphérique de stockage à l'aide de la console de baie.	Consultez la documentation du fabricant.
Reconnectez le périphérique de stockage.	Reportez-vous à Joindre des périphériques de stockage .
Montez la banque de données et redémarrez les machines virtuelles.	Reportez-vous à Monter des banques de données .

Déconnexion des périphériques de stockage

Déconnectez en toute sécurité un périphérique de stockage de votre hôte ESXi.

Il se peut que vous deviez déconnecter le périphérique pour le rendre inaccessible à votre hôte, lorsque, par exemple, vous effectuez une mise à niveau du matériel côté stockage.

Conditions préalables

- Le périphérique ne contient pas de banques de données.
- Aucune machine virtuelle n'utilise le périphérique en tant que disque RDM.
- Le périphérique ne contient pas de partition de diagnostic, ni de partition de travail.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Périphériques de stockage**.
- 4 Sélectionnez le périphérique à déconnecter, puis cliquez sur l'icône **Détacher**.

Résultats

Le périphérique devient inaccessible. L'état opérationnel du périphérique devient Démonté.

Étape suivante

Si plusieurs hôtes partagent le périphérique, déconnectez le périphérique de chaque hôte.

Joindre des périphériques de stockage

Reconnectez un périphérique de stockage que vous avez précédemment déconnecté de l'hôte ESXi.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Périphériques de stockage**.
- 4 Sélectionnez le périphérique de stockage déconnecté et cliquez sur l'icône **Joindre**.

Résultats

Le périphérique devient accessible.

Récupération à partir des états PDL

Une condition PDL (perte de périphérique permanente) non planifiée survient lorsqu'un périphérique de stockage devient indisponible de façon permanente sans avoir été détaché de façon adéquate de l'hôte ESXi.

Dans vSphere Client, les éléments suivants signalent que le périphérique est dans un état PDL :

- La banque de données déployée est indisponible.
- L'état opérationnel du périphérique passe à Lost Communication.
- Tous les chemins sont affichés comme Dead.
- Un avertissement concernant un périphérique inaccessible de façon permanente apparaît dans le fichier de journal VMkernel.

Pour récupérer de la condition PDL non planifiée et supprimer le périphérique indisponible de l'hôte, effectuez les tâches suivantes.

Tâche	Description
Mettez hors tension et annulez l'enregistrement de toutes les machines virtuelles qui s'exécutent sur la banque de données affectée par la condition PDL.	Reportez-vous à la section Administration d'une machine virtuelle vSphere .
Démontez la banque de données.	Reportez-vous à la section Démontage des banques de données .
Effectuez une nouvelle analyse de tous les hôtes ESXi ayant accès au périphérique. Note Si la nouvelle analyse est infructueuse et que l'hôte continue à répertorier le périphérique, il se peut que des E/S en attente ou des références actives existent encore. Recherchez tous les éléments qui peuvent encore avoir une référence active au périphérique ou à la banque de données. Ces éléments comprennent notamment des machines virtuelles, des modèles, des images ISO et des mappages de périphériques bruts.	Reportez-vous à la section Réanalyse du stockage .

Traitement des conditions APD passagères

Un périphérique de stockage est considéré comme en état APD lorsqu'il devient indisponible pour votre hôte ESXi pour une période de temps indéterminée.

Les causes d'un état APD peuvent être, par exemple, un commutateur défaillant ou un câble de stockage déconnecté.

Contrairement à l'état PDL, l'hôte traite l'état APD comme étant passager et s'attend à ce que le périphérique soit à nouveau disponible.

L'hôte continue à réessayer d'envoyer des commandes afin de rétablir la connectivité avec le périphérique. Si les commandes de l'hôte continuent à échouer pendant une période prolongée, l'hôte peut connaître des problèmes de performances. L'hôte et ses machines virtuelles peuvent éventuellement cesser de répondre.

Pour éviter ces problèmes, votre hôte utilise une fonction de traitement APD par défaut.

Lorsqu'un périphérique passe à l'état APD, l'hôte active un minuteur. Si ce minuteur est actif, l'hôte continue à réessayer des commandes de machine non virtuelle pendant une période de temps limitée.

Par défaut, le délai d'expiration APD est défini sur 140 secondes. Cette valeur est généralement plus longue que le délai nécessaire pour la plupart des périphériques dans le but de récupérer d'une perte de connexion. Si le périphérique devient disponible durant ce laps de temps, l'hôte et sa machine virtuelle continuent de fonctionner sans aucun problème.

Si le périphérique ne récupère pas et que le délai d'attente prend fin, l'hôte cesse ses tentatives et stoppe toute E/S de machine non virtuelle. Les tentatives d'E/S de la machine virtuelle continuent. vSphere Client affiche les informations suivantes concernant le périphérique dont le délai d'attente APD a expiré :

- L'état opérationnel du périphérique passe à `Dead or Error`.
- Tous les chemins sont affichés comme `Dead`.
- Les banques de données du périphérique sont grisées.

Même si le périphérique et les banques de données sont indisponibles, les machines virtuelles continuent de répondre. Vous pouvez mettre les machines virtuelles hors tension ou les déplacer vers une banque de données ou un hôte différent.

Si, par la suite, les chemins des périphériques deviennent opérationnels, l'hôte peut reprendre les E/S sur le périphérique et terminer le traitement APD spécial.

Désactiver le traitement APD de stockage

Le traitement du stockage Tous chemins hors service (All Paths Down, APD) est activé par défaut sur votre hôte ESXi. Lorsque cette fonctionnalité est activée et qu'un périphérique de stockage passe à l'état APD, l'hôte retente d'envoyer les commandes d'E/S de machine non virtuelle uniquement pendant une période limitée. Lorsque cette période expire, l'hôte arrête ses tentatives et met fin à toute E/S de machine non virtuelle. Vous pouvez alors désactiver la fonctionnalité de traitement APD de votre hôte.

Si vous désactivez le traitement APD, l'hôte retentera indéfiniment d'envoyer les commandes afin de se reconnecter au périphérique APD. Ce comportement peut amener les machines virtuelles de l'hôte à excéder leur délai d'attente E/S interne et ainsi à ne plus répondre ou à faire l'objet d'une défaillance. L'hôte peut se retrouver déconnecté de l'instance de vCenter Server.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Système**, cliquez sur **Paramètres système avancés**.
- 4 Dans le tableau Paramètres système avancés, sélectionnez le paramètre **Misc.APDHandlingEnable** et cliquez sur l'icône **Edit**.
- 5 Modifiez la valeur sur 0.

Résultats

Si vous avez désactivé le traitement APD, vous pouvez le réactiver et définir sa valeur sur 1 lorsqu'un périphérique passe à l'état APD. La fonction interne de traitement APD se met immédiatement en marche et le minuteur démarre avec la valeur actuelle de délai d'attente pour chaque périphérique APD.

Changer les limites de délai pour l'APD de stockage

Le paramètre de délai d'attente contrôle le nombre de secondes pendant lesquelles l'hôte ESXi doit réessayer les commandes d'E/S vers un périphérique de stockage dans un état « Tous chemins hors service » (All paths down, APD). Vous pouvez modifier la valeur de délai d'attente par défaut.

Le délai d'attente démarre immédiatement après que le périphérique entre dans l'état APD. Après expiration, l'hôte marque le périphérique APD comme étant inaccessible. L'hôte arrête ses nouvelles tentatives d'E/S ne provenant pas de machines virtuelles. L'hôte continue à réessayer l'E/S de la machine virtuelle.

Par défaut, le paramètre de délai d'attente sur votre hôte est défini sur 140 secondes. Vous pouvez augmenter la valeur du délai d'attente si, par exemple, des périphériques de stockage connectés à votre hôte ESXi prennent plus de 140 secondes à récupérer d'une perte de connexion.

Note Si vous modifiez le paramètre de délai d'attente au terme duquel le périphérique n'est plus disponible, la modification ne prend pas effet pour cet incident APD particulier.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Système**, cliquez sur **Paramètres système avancés**.

- 4 Dans le tableau Paramètres système avancés, sélectionnez le paramètre **Misc.APDTimeout**, puis cliquez sur l'icône **Edit**.
- 5 Modifiez la valeur par défaut.

Vous pouvez saisir une valeur comprise entre 20 et 99 999 secondes.

Vérifier l'état de la connexion d'un périphérique de stockage sur un hôte ESXi

Utilisez la commande `esxcli` pour vérifier l'état de la connexion d'un périphérique de stockage particulier.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- 1 Exécutez la commande `esxcli storage core device list -d=device_ID`.
- 2 Vérifiez l'état de la connexion dans la zone `Status`:
 - `on` - Le périphérique est connecté.
 - `dead` - Le périphérique est passé à l'état APD. Le minuteur APD démarre.
 - `dead timeout` - Le délai d'attente APD a expiré.
 - `not connected` - Le périphérique est dans l'état PDL.

Utiliser le voyant de localisation sur les périphériques de stockage ESXi

Utilisez le voyant de localisation pour identifier des périphériques de stockage spécifiques, afin de pouvoir les localiser parmi d'autres périphériques. Vous pouvez activer ou désactiver le voyant de localisation.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Périphériques de stockage**.
- 4 Dans la liste des périphériques de stockage, sélectionnez un ou plusieurs disques, et définissez le voyant de localisation.
 - Cliquez sur l'icône **Activer la LED**.
 - Cliquez sur l'icône **Désactiver la LED**.

Effacer des périphériques de stockage

Certaines fonctionnalités, telles que vSAN ou une ressource Virtual Flash, imposent que l'hôte ESXi utilise des périphériques de stockage propres. Vous pouvez effacer un disque dur ou un périphérique Flash, et supprimer toutes les données existantes.

Conditions préalables

- Assurez-vous que l'hôte est à l'état connecté.
- Vérifiez que les périphériques que vous prévoyez d'effacer ne sont pas en cours d'utilisation.
- Privilège requis : **Host.Config.Storage**

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Périphériques de stockage**.
- 4 Sélectionnez un ou plusieurs périphériques et cliquez sur l'icône **Effacer les partitions**.
- 5 Vérifiez que les informations de partition que vous effacez ne sont pas critiques.
- 6 Cliquez sur **OK** pour confirmer la modification.

Modifier les paramètres de réservation perpétuelle

Vous pouvez ajuster le paramètre de réservation perpétuelle sur les périphériques de stockage utilisés comme disques RDM (RAW Device Mapping) physiques dans les configurations WSFC (Windows Server Failover Clustering).

Les nœuds de cluster WSFC répartis sur plusieurs hôtes ESXi requièrent des disques RDM physiques. Les disques RDM sont partagés entre tous les hôtes sur lesquels les nœuds de cluster s'exécutent. L'hôte avec le nœud actif comprend des réservations SCSI-3 persistantes sur tous les périphériques RDM partagés. Lorsque le nœud actif est en cours d'exécution et que les périphériques sont verrouillés, aucun autre hôte ne peut écrire sur les périphériques. Si un autre hôte participant démarre alors que le nœud actif verrouille les périphériques, le démarrage peut être anormalement long, car l'hôte n'essaie pas de contacter les périphériques verrouillés. Le même problème peut également affecter les opérations de réanalyse.

Pour éviter ce problème, activez la réservation perpétuelle pour tous les périphériques sur les hôtes ESXi sur lesquels résident les nœuds WSFC secondaires avec RDM. Cette configuration informe l'hôte ESXi sur la réservation SCSI permanente sur les périphériques afin que l'hôte puisse ignorer les périphériques lors du processus de réanalyse de démarrage ou de stockage.

Si vous réactivez ultérieurement les périphériques marqués en tant que banques de données VMFS, supprimez la réservation pour éviter un comportement imprévisible de la banque de données.

Pour plus d'informations sur les clusters WSFC, consultez la documentation *Configuration du clustering de basculement Windows Server*.

Conditions préalables

Avant de marquer un périphérique comme étant perpétuellement réservé, assurez-vous qu'il ne contient pas de banque de données VMFS.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Périphériques de stockage**.
- 4 Dans la liste des périphériques de stockage, sélectionnez le périphérique et cliquez sur l'une des icônes suivantes.

Option	Description
Marquer comme perpétuellement réservé	Marquer le périphérique sélectionné comme étant perpétuellement réservé. Note Répétez la procédure pour chaque périphérique RDM participant au cluster WSFC.
Ne plus marquer comme perpétuellement réservé	Effacez la réservation perpétuelle pour le périphérique précédemment marqué.

Résultats

La configuration est stockée de façon permanente sur l'hôte ESXi et persiste lors des redémarrages.

Exemple

Vous pouvez également utiliser la commande `esxcli` pour marquer les périphériques participant au cluster WSFC.

- 1 Marquez le périphérique comme étant perpétuellement réservé.

```
esxcli storage core device setconfig -d naa.id --perennially-reserved=true
```

- 2 Vérifiez que le périphérique est perpétuellement réservé.

```
esxcli storage core device list -d naa.id
```

Dans la sortie de la commande `esxcli`, recherchez l'entrée `Is Perennially Reserved: true`.

- 3 Pour supprimer l'indicateur de réservation perpétuelle, exécutez la commande suivante.

```
esxcli storage core device setconfig -d naa.id --perennially-reserved=false
```

Utilisation de périphériques Flash avec les hôtes ESXi

7

Outre les disques durs (HDD) de stockage ordinaires, ESXi prend en charge les périphériques de stockage Flash.

À la différence des disques durs ordinaires qui sont des dispositifs électromécaniques contenant des pièces mobiles, les périphériques Flash utilisent des semiconducteurs comme support de stockage et ne comportent pas de pièce mobile. Les périphériques Flash sont généralement résilients et assurent un accès rapide aux données.

ESXi détecte les périphériques Flash à l'aide d'un mécanisme de requête basé sur les normes T10. Consultez votre fournisseur pour savoir si votre baie de stockage prend en charge le mécanisme ESXi de détection de périphériques Flash.

Une fois que l'hôte détecte les périphériques Flash, vous pouvez les utiliser pour plusieurs tâches et fonctionnalités.

Si vous utilisez le stockage NVMe, activez High-Performance Plug-in (HPP) afin d'améliorer les performances de votre stockage. Reportez-vous à la section [VMware High Performance Plug-In et Path Selection Schemes](#).

Pour obtenir des informations spécifiques sur l'utilisation du stockage NVMe avec ESXi, reportez-vous à [Chapitre 8 À propos du stockage VMware NVMe](#).

Tableau 7-1. Utilisation de périphériques Flash avec ESXi

Fonctionnalité	Description
vSAN	vSAN nécessite des périphériques flash. Pour plus d'informations, consultez la documentation <i>Administration de VMware vSAN</i> .
Banques de données VMFS	Créez des banques de données VMFS sur des périphériques Flash. Utilisez les banques de données pour les buts suivants : <ul style="list-style-type: none">■ Stocker des machines virtuelles. Certains systèmes d'exploitation invités peuvent identifier les disques virtuels stockés dans ces banques de données comme des disques Flash virtuels.■ Allouer de l'espace de banque de données au cache d'échange d'hôte ESXi. Reportez-vous à la section Configurer le cache d'échange d'hôte avec une banque de données VMFS.
Ressource Flash virtuelle (VFFS)	Si cela est requis par votre fournisseur, configurez une ressource Virtual Flash et utilisez-la pour les filtres de mise en cache d'E/S. Reportez-vous à la section Chapitre 15 Filtrage des E/S de machines virtuelles .

Périphériques Flash et machines virtuelles

Les systèmes d'exploitation invités peuvent identifier les disques virtuels résidant dans des banques de données basées sur Flash comme des disques Flash virtuels.

Les systèmes d'exploitation invités peuvent utiliser des commandes de requête standards telles que SCSI VPD Page (B1h) pour les périphériques SCSI et ATA IDENTIFY DEVICE (Word 217) pour les périphériques IDE.

Pour les clones reliés, les snapshots natifs et les disques delta, les commandes de requêtes signalent le statut Flash virtuel du disque de base.

Les systèmes d'exploitation peuvent détecter qu'un disque virtuel est un disque Flash dans les circonstances suivantes :

- La détection des disques Flash virtuels est prise en charge sur des machines virtuelles pour la version 8 et ultérieure du matériel virtuel.
- Les périphériques sauvegardant une banque de données VMFS partagée doivent être marqués comme Flash sur tous les hôtes.
- Si la banque de données VMFS inclut plusieurs extensions de périphérique, toutes les extensions physiques sous-jacentes doivent être basées sur Flash.

Ce chapitre contient les rubriques suivantes :

- [Meilleures pratiques pour les périphériques Flash sur les hôtes ESXi](#)
- [Marquage de périphériques de stockage sur des hôtes ESXi](#)
- [À propos des ressources Virtual Flash dans l'environnement vSphere](#)
- [Configurer le cache d'échange d'hôte avec une banque de données VMFS](#)

Meilleures pratiques pour les périphériques Flash sur les hôtes ESXi

Suivez ces meilleures pratiques lorsque vous utilisez des périphériques Flash dans l'environnement vSphere.

- Utilisez les périphériques Flash approuvés par le *Guide de compatibilité VMware*.
- Assurez-vous d'utiliser la dernière version du microprogramme avec des périphériques Flash. Vérifiez fréquemment les mises à jour avec vos fournisseurs de stockage.
- Surveillez attentivement le niveau d'utilisation du périphérique Flash et calculez sa durée de vie estimée. L'espérance de vie dépend du niveau d'utilisation continu du périphérique Flash. Reportez-vous à la section [Estimer la durée de vie des périphériques Flash](#).
- Si vous utilisez des périphériques NVMe pour le stockage, activez le High-Performance Plug-in (HPP) afin d'améliorer les performances de votre stockage. Pour obtenir des informations spécifiques sur l'utilisation des périphériques NVMe, consultez [VMware High Performance Plug-In et Path Selection Schemes](#)

Surveiller les périphériques Flash

Vous pouvez surveiller certains paramètres de périphériques Flash critiques, notamment Media Wearout Indicator, Temperature et Reallocated Sector Count, à partir d'un hôte ESXi.

Utilisez la commande `esxcli` pour surveiller les périphériques Flash.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Affichez les statistiques d'un périphérique Flash en exécutant la commande suivante :

```
esxcli storage core device smart get -d=flash_device_ID
```

Estimer la durée de vie des périphériques Flash

Lorsque vous travaillez avec des périphériques Flash, surveillez le degré d'activité avec lequel vous les utilisez et calculez leur durée de vie estimée.

En règle générale, les fournisseurs de stockage donnent des estimations fiables pour la durée de vie d'un périphérique Flash dans les conditions idéales. Par exemple, un fournisseur peut garantir une durée de vie de 5 ans au rythme de 20 Go d'écriture par jour. Cependant, l'espérance de vie plus réaliste du périphérique dépend du nombre d'écritures réellement générées par votre hôte ESXi. Suivez les étapes ci-dessous pour calculer la durée de vie du périphérique Flash.

Conditions préalables

Notez le nombre de jours s'étant écoulés depuis le dernier redémarrage de votre hôte ESXi. Par exemple, dix jours.

Procédure

- 1 Obtenez le nombre total de blocs écrits sur le périphérique Flash depuis le dernier redémarrage.

Exécutez la commande `esxcli storage core device stats get -d=device_ID`. Par exemple :

```
~ # esxcli storage core device stats get -d t10.xxxxxxxxxxxxxxx
Device: t10.xxxxxxxxxxxxxxx
Successful Commands: xxxxxxxx
Blocks Read: xxxxxxxx
Blocks Written: 629145600
Read Operations: xxxxxxxx
```

L'élément `Blocks Written` dans la sortie indique le nombre de blocs écrits sur le périphérique depuis le dernier redémarrage. Dans cet exemple, la valeur est 629,145,600. Après chaque redémarrage, elle se réinitialise à 0.

2 Calculez le nombre total d'écritures et convertissez en Go.

Un bloc équivaut à 512 octets. Pour calculer le nombre total d'écriture, multipliez la valeur Blocks Written par 512, et convertissez la valeur résultante en Go.

Dans cet exemple, le nombre total d'écritures depuis le dernier redémarrage est d'environ 322 Go.

3 Estimez le nombre moyen d'écritures par jour en Go.

Divisez le nombre total d'écritures par le nombre de jours depuis le dernier redémarrage.

Si le dernier redémarrage s'est produit il y a dix jours, vous obtenez 32 Go d'écritures par jour. Vous pouvez calculer la moyenne de ce nombre sur la période concernée.

4 Estimez la durée de vie de votre périphérique à l'aide de la formule suivante :

vendor provided number of writes per day fois *vendor provided life span* divisé par *actual average number of writes per day*

Par exemple, si votre fournisseur garantit une durée de vie de 5 ans au rythme de 20 Go d'écriture par jour et que la quantité réelle d'écriture par jour est de 30 Go, la durée de vie de votre périphérique Flash est d'environ 3,3 ans.

Garder les disques Flash sans formatage VMFS

Si vous utilisez l'option de partitionnement automatique du démarrage lors de l'installation ou du déploiement automatique de ESXi, elle crée une banque de données VMFS sur le stockage local de l'hôte. Dans certains cas, il vous faut garder vos disques Flash de stockage local sans formatage.

Problème

Par défaut, le partitionnement automatique déploie les systèmes de fichiers VMFS sur tous les disques de stockage locaux inutilisés sur l'hôte, y compris les disques Flash.

Cependant, si un disque Flash est au format VMFS, il devient indisponible pour des fonctionnalités telles que Virtual Flash et vSAN. Ces dernières requièrent un disque Flash non formaté et ne permettent pas le partage du disque avec un autre système de fichiers.

Solution

Pour vous assurer que le partitionnement automatique n'applique pas le format VMFS au disque Flash, utilisez les options de démarrage suivantes lors de la première installation d'ESXi ou du premier démarrage de l'hôte ESXi :

- **autoPartition=TRUE**
- **skipPartitioningSsds=TRUE**

Si vous utilisez Auto Deploy, définissez ces paramètres sur un hôte ESXi de référence.

1 Dans vSphere Client, accédez à l'hôte à utiliser en tant qu'hôte de référence et cliquez sur l'onglet **Configurer**.

- 2 Cliquez sur **Système** pour ouvrir les options système, puis cliquez sur **Paramètres système avancés**.
- 3 Définissez les éléments suivants.

Paramètre	Valeur
VMkernel.Boot.autoPartition	Vrai
VMkernel.Boot.skipPartitioningSsds	Vrai

- 4 Redémarrez l'hôte.

Si des disques Flash que vous prévoyez d'utiliser avec la ressource Virtual Flash et vSAN disposent déjà de banques de données VMFS, supprimez ces dernières.

Marquage de périphériques de stockage sur des hôtes ESXi

Lorsque vous configurez vSAN ou une ressource Virtual Flash, votre environnement de stockage doit inclure des périphériques Flash locaux. Cependant, ESXi risque de ne pas reconnaître certains périphériques de stockage comme périphériques Flash lorsque leurs fournisseurs ne prennent pas en charge la détection automatique de périphériques Flash. Dans d'autres cas, certains périphériques risquent de ne pas être détectés comme locaux, et ESXi les marque comme périphériques distants. Lorsque les périphériques ne sont pas reconnus comme périphériques Flash locaux, ils sont exclus de la liste de périphériques proposés pour vSAN ou une ressource Virtual Flash. Le marquage de ces périphériques comme périphériques Flash locaux les rend disponibles pour vSAN et une ressource Virtual Flash.

Marquer les périphériques de stockage en tant que Flash

Si ESXi ne reconnaît pas ses périphériques comme Flash, marquez-les comme périphériques Flash.

ESXi ne reconnaît pas certains périphériques comme Flash lorsque leurs fournisseurs ne prennent pas en charge la détection automatique des disques Flash. La colonne Type de lecteur des périphériques affiche le type HDD.

Attention Le marquage des disques durs en tant que périphériques Flash peut détériorer les performances des banques de données et des services qui les utilisent. Marquez les périphériques uniquement si vous êtes certains qu'ils sont bien des périphériques Flash.

Conditions préalables

Vérifiez que le périphérique n'est pas utilisé.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Périphériques de stockage**.

- 4 Dans la liste des périphériques de stockage, sélectionnez un ou plusieurs périphériques HDD, puis cliquez sur **Marquer en tant que disque Flash** ().
- 5 Cliquez sur **Oui** pour enregistrer vos modifications.

Résultats

Les périphériques deviennent des périphériques de type Flash.

Étape suivante

Si le périphérique Flash que vous marquez est partagé entre plusieurs hôtes, assurez-vous de marquer le périphérique dans tous les hôtes qui le partagent.

Marquer des périphériques de stockage comme locaux

ESXi vous permet de marquer des périphériques comme locaux. Cette action est utile dans les cas où ESXi ne parvient pas à déterminer si certains périphériques sont locaux.

Conditions préalables

- Assurez-vous que le périphérique n'est pas partagé.
- Mettez hors tension les machines virtuelles résidant sur le périphérique et démontez une banque de données associée.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Périphériques de stockage**.
- 4 Dans la liste des périphériques de stockage, sélectionnez un ou plusieurs périphériques distants et cliquez sur l'icône **Marquer en tant que local**.
- 5 Cliquez sur **Oui** pour enregistrer vos modifications.

À propos des ressources Virtual Flash dans l'environnement vSphere

Vous pouvez agréger des périphériques Flash locaux se trouvant sur un hôte ESXi au sein d'une couche de mise en cache virtualisée unique appelée ressource Flash virtuelle. Lorsque vous configurez la ressource Flash virtuelle, vous créez un nouveau système de fichiers, à savoir un système de fichiers Flash virtuel (VFFS, Virtual Flash File System). Le système VFFS est un dérivé de VMFS, qui est optimisé pour les périphériques Flash et utilisé pour regrouper les périphériques Flash physiques dans un pool de ressources de mise en cache unique. En sa qualité de ressource non permanente, il ne peut pas être utilisé pour stocker des machines virtuelles.

Une fois que vous avez configuré la ressource Virtual Flash, vous pouvez l'utiliser pour les filtres de mise en cache d'E/S. Reportez-vous à la section [Chapitre 15 Filtrage des E/S de machines virtuelles](#).

Considérations relatives aux ressources Virtual Flash

Plusieurs considérations s'appliquent lorsque vous configurez une ressource Virtual Flash.

- Vous ne pouvez disposer que d'une seule ressource Virtual Flash sur un seul hôte ESXi. La ressource Virtual Flash est gérée au niveau de l'hôte.
- Vous ne pouvez pas utiliser la ressource Virtual Flash pour stocker des machines virtuelles. La ressource Virtual Flash est exclusivement dédiée à la mise en cache.
- Vous ne pouvez pas utiliser des périphériques Flash locaux pour la ressource Virtual Flash.
- Vous pouvez créer la ressource Virtual Flash à partir de périphériques Flash mixtes. Tous les types de périphériques sont traités équitablement et aucune distinction n'est effectuée entre les connectivités SAS, SATA ou PCI express. Lors de la création de la ressource à partir de périphériques Flash mixtes, assurez-vous de regrouper les périphériques offrant des performances similaires pour optimiser les performances globales.
- Vous ne pouvez pas utiliser les mêmes périphériques Flash pour la ressource Virtual Flash et pour vSAN. Chacune nécessite son propre périphérique Flash exclusif et dédié.

Configurer une ressource Virtual Flash

Vous pouvez configurer une ressource Virtual Flash ou ajouter de la capacité à une ressource Virtual Flash existante.

Pour configurer une ressource Virtual Flash, vous utilisez des périphériques Flash locaux connectés à votre hôte ou votre cluster hôte. Pour accroître la capacité de votre ressource Virtual Flash, vous pouvez ajouter des périphériques supplémentaires, sans dépasser le nombre maximal indiqué dans la documentation *Configurations maximales*. Un périphérique Flash individuel doit être alloué de manière exclusive à la ressource Flash virtuelle. Aucune autre fonctionnalité vSphere, telle que vSAN ou VMFS, ne peut partager le périphérique avec la ressource Flash virtuelle.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Virtual Flash**, cliquez sur **Gestion des ressources Virtual Flash**.
- 4 Cliquez sur l'une des options suivantes.

Option	Description
Ajouter de la capacité	Si vous créez la ressource Virtual Flash sur un hôte individuel.
Ajouter de la capacité sur le cluster	Si vous créez la ressource Virtual Flash sur un cluster.

- 5 Dans la liste des entités disponibles, sélectionnez-en une ou plusieurs à utiliser pour la ressource Virtual Flash et cliquez sur **OK**.

Si vos périphériques Flash n'apparaissent pas dans la liste, reportez-vous à la section [Marquage de périphériques de stockage sur des hôtes ESXi](#).

Option	Description
Disque VMware local	<p>Sélectionnez n'importe quelle combinaison de périphériques Flash non réclamés.</p> <p>ESXi crée le volume VFFS sur l'un des périphériques, puis étend le volume sur le reste des périphériques. Le système configure la ressource Virtual Flash sur l'intégralité du volume VFFS.</p> <p>Si un volume VFFS existe sur votre hôte, vous ne pouvez pas sélectionner de périphérique non réclamé sans avoir préalablement sélectionné le volume VFFS existant.</p>
volume ID - Configurer en utilisant les étendues de volume VFFS existantes	<p>Si vous avez créé précédemment un volume VFFS sur l'un des périphériques Flash de l'hôte à l'aide de la commande <code>vmkfstools</code>, le volume s'affiche également dans la liste des entités éligibles. Vous pouvez sélectionner uniquement ce volume pour la ressource Virtual Flash ou le combiner avec les périphériques non réclamés. ESXi utilise le volume VFFS existant pour l'étendre sur d'autres périphériques.</p>

Résultats

La ressource Virtual Flash est créée. La zone Sauvegarde d'un périphérique répertorie tous les périphériques que vous utilisez pour la ressource Virtual Flash.

Étape suivante

Utilisez la ressource Virtual Flash pour les filtres de mise en cache d'E/S développés par le filtrage VAIO (vSphere APIs for I/O Filtering). Reportez-vous à la section [Utilisation de périphériques de stockage Flash avec des filtres d'E/S de cache](#).

Vous pouvez augmenter la capacité en ajoutant d'autres périphériques Flash à la ressource Virtual Flash.

Supprimer une ressource Virtual Flash

Il peut s'avérer nécessaire de supprimer une ressource Virtual Flash déployée sur des périphériques Flash locaux connectés à l'hôte ESXi. La suppression de la ressource Virtual Flash libère les périphériques pour les autres services.

Conditions préalables

- Vérifiez que la ressource Virtual Flash n'est pas utilisée pour les filtres d'E/S.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.

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

- 3 Sous **Virtual Flash**, cliquez sur **Gestion des ressources Virtual Flash**, puis sur **Supprimer tout**.

Résultats

Une fois que vous avez supprimé la ressource Virtual Flash et effacé le contenu du périphérique Flash, le périphérique est disponible pour d'autres opérations.

Définir une alarme pour l'utilisation de Virtual Flash

Définissez une alarme pour indiquer le dépassement du seuil d'utilisation spécifié d'une ressource Virtual Flash sur votre hôte ESXi.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Système**, cliquez sur **Paramètres système avancés**.
- 4 Sélectionnez le paramètre à modifier et cliquez sur le bouton **Modifier**.

Paramètre	Description
VFLASH.ResourceUsageThreshold	Le système déclenche l'alarme Utilisation des ressources vFlash de l'hôte lorsque le taux d'utilisation d'une ressource Virtual Flash dépasse le seuil défini. Le seuil est défini par défaut sur 80 %. Si nécessaire, vous pouvez modifier cette valeur. Dès que le taux d'utilisation de la ressource Virtual Flash descend au-dessous du seuil, l'alarme est effacée.

- 5 Cliquez sur **OK**.

Configurer le cache d'échange d'hôte avec une banque de données VMFS

Permettez à votre hôte ESXi de basculer dans le cache de l'hôte. Vous pouvez également modifier la quantité d'espace allouée au cache de l'hôte.

Vos hôtes ESXi peuvent utiliser une portion d'une entité de stockage Flash comme cache d'échange partagé entre toutes les machines virtuelles.

Le cache établi au niveau de l'hôte est constitué de fichiers sur un disque à faible latence utilisé par ESXi comme cache de réécriture pour les fichiers d'échange de machine virtuelle. Toutes les machines virtuelles exécutées sur l'hôte partagent le cache. L'échange de pages de machine virtuelle au niveau de l'hôte optimise l'espace du périphérique Flash qui peut être limité.

Conditions préalables

Créez une banque de données VMFS en utilisant des périphériques Flash comme sauvegarde. Reportez-vous à la section [Créer une banque de données VMFS](#).

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Configuration du cache de l'hôte**.
- 4 Sélectionnez la banque de données flash dans la liste, puis cliquez sur l'icône **Modifier**.
- 5 Attribuez suffisamment d'espace au cache de l'hôte.
- 6 Cliquez sur **OK**.

À propos du stockage VMware NVMe

8

Les périphériques de stockage à mémoire non volatile (NVM) utilisant la mémoire persistante sont de plus en plus populaires dans les centres de données. NVM Express (NVMe) est un protocole standardisé conçu spécifiquement pour la communication à plusieurs files d'attente haute performance avec des périphériques NVM. ESXi prend en charge le protocole NVMe pour se connecter à des périphériques de stockage locaux et en réseau.

Ce chapitre contient les rubriques suivantes :

- Concepts de VMware NVMe
- Conditions requises et limitations du stockage VMware NVMe
- Configuration d'adaptateurs pour le stockage NVMe over RDMA (RoCE v2)
- Configuration des adaptateurs pour le stockage NVMe over TCP
- Ajout d'adaptateurs logiciels NVMe
- Ajouter des contrôleurs pour NVMe over Fabrics
- Supprimer des adaptateurs NVMe logiciels

Concepts de VMware NVMe

Avant de commencer à utiliser le stockage NVMe dans l'environnement ESXi, vous pouvez vous familiariser avec les concepts de base de NVMe.

NVM Express (NVMe)

NVMe est une méthode de connexion et de transfert de données entre un hôte et un système de stockage cible. NVMe est conçu pour être utilisé avec un support de stockage plus rapide équipé d'une mémoire non volatile, tel que les périphériques Flash. Ce type de stockage peut atteindre une faible latence, une utilisation de CPU réduite et des performances élevées, il sert généralement d'alternative au stockage SCSI.

Transports NVMe

Le stockage NVMe peut être directement attaché à un hôte à l'aide d'une interface PCIe ou indirectement via différents transports d'infrastructure. VMware NVMe over Fabrics (NVMe-oF) fournit une connectivité à distance entre un hôte et un périphérique de stockage cible sur une baie de stockage partagée.

Les types de transport suivants existent actuellement pour NVMe.

Transport NVMe	Prise en charge d'ESXi
NVMe over PCIe	Stockage local.
NVMe over RDMA	Stockage NVMe-oF partagé. Avec la technologie RoCE v2.
NVMe over Fibre Channel	Stockage NVMe-oF partagé.
NVMe over TCP	Stockage NVMe-oF partagé.

Pour connaître les exigences de configuration spécifiques pour chaque transport, reportez-vous à la section [Conditions requises et limitations du stockage VMware NVMe](#).

Espaces de noms NVMe

Dans la baie de stockage NVMe, un espace de noms est un volume de stockage soutenu par une quantité de mémoire non volatile. Dans le contexte d'ESXi, l'espace de noms est analogue à un périphérique de stockage ou LUN. Lorsque votre hôte ESXi découvre l'espace de noms NVMe, un périphérique Flash représentant l'espace de noms apparaît dans la liste des périphériques de stockage dans vSphere Client. Vous pouvez utiliser le terminal pour créer une banque de données et stocker des machines virtuelles.

Contrôleurs NVMe

Un contrôleur est associé à un ou plusieurs espaces de noms NVMe et fournit un chemin d'accès entre l'hôte ESXi et les espaces de noms de la baie de stockage. Pour accéder au contrôleur, l'hôte peut utiliser deux mécanismes : la découverte de contrôleur et la connexion au contrôleur. Pour plus d'informations, consultez [Ajouter des contrôleurs pour NVMe over Fabrics](#).

Découverte de contrôleur

Avec ce mécanisme, l'hôte ESXi contacte d'abord un contrôleur de découverte. Le contrôleur de découverte renvoie une liste des contrôleurs disponibles. Après que vous sélectionnez un contrôleur auquel votre hôte peut accéder, tous les espaces de noms associés à ce contrôleur deviennent disponibles pour votre hôte.

Connexion au contrôleur

Votre hôte ESXi se connecte au contrôleur que vous spécifiez. Tous les espaces de noms associés à ce contrôleur deviennent disponibles pour votre hôte.

Sous-système NVMe

En général, un sous-système NVMe est une baie de stockage qui peut inclure plusieurs contrôleurs NVMe, plusieurs espaces de noms, un support de stockage de mémoire non volatile et une interface entre le contrôleur et le support de stockage de mémoire non volatile. Le sous-système est identifié par un nom qualifié NVMe (NQN) de sous-système.

VMware High-Performance Plug-in (HPP)

Par défaut, l'hôte ESXi utilise le HPP pour réclamer les cibles NVMe-oF. Lors de la sélection de chemins physiques pour les demandes d'E/S, le HPP applique un schéma PSS (Path Selection Schemes) approprié. Pour plus d'informations sur le HPP, reportez-vous à [VMware High Performance Plug-In et Path Selection Schemes](#). Pour modifier le mécanisme de sélection de chemin par défaut, reportez-vous à [Modification de la stratégie de sélection de chemin d'accès](#).

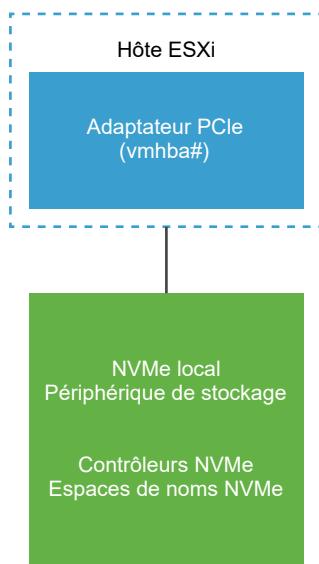
Architecture et composants de base de VMware NVMe

ESXi prend en charge le stockage local NVMe over PCIe et le stockage NVMe-oF partagé, tel que NVMe over Fibre Channel, NVMe over RDMA (RoCE v2) et NVMe over TCP.

Dans les environnements NVMe-oF, les cibles peuvent présenter des espaces de noms, équivalents aux LUN pour SCSI, à un hôte en mode d'accès actif/actif ou asymétrique. ESXi est en mesure de découvrir et d'utiliser les espaces de noms présentés dans l'une de ces manières. ESXi prend en charge *NVMe de bout en bout* et *sans émulation NVMe vers SCSI*.

VMware NVMe over PCIe

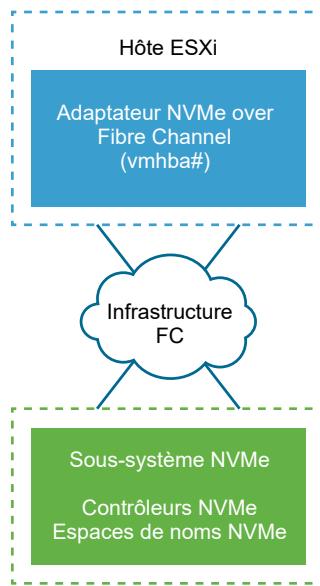
Dans cette configuration, votre hôte ESXi utilise un adaptateur de stockage PCIe pour accéder à un ou plusieurs périphériques de stockage NVMe locaux. Après l'installation de l'adaptateur sur l'hôte, ce dernier découvre les périphériques NVMe disponibles et ceux-ci figurent sur la liste des périphériques de stockage dans vSphere Client.



VMware NVMe over Fibre Channel

Cette technologie mappe NVMe sur le protocole Fibre Channel pour permettre le transfert de données et de commandes entre un hôte et un périphérique de stockage cible. Ce transport peut utiliser une infrastructure Fibre Channel existante mise à niveau pour prendre en charge NVMe.

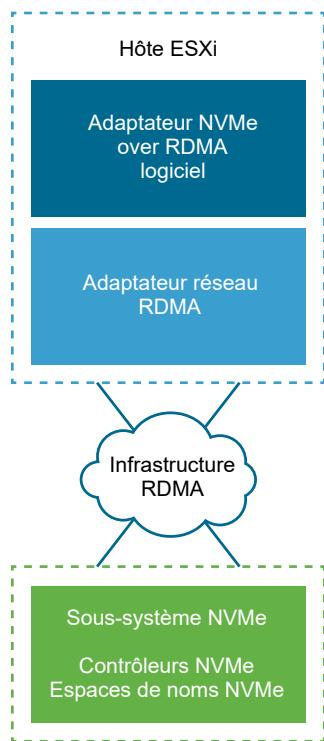
Pour accéder au stockage NVMe over Fibre Channel, installez un adaptateur de stockage Fibre Channel qui prend en charge NVMe sur votre hôte ESXi. Il n'est pas nécessaire de configurer l'adaptateur. Celui-ci se connecte automatiquement à un sous-système NVMe approprié et découvre tous les périphériques de stockage NVMe partagés qu'il peut atteindre. Vous pourrez ensuite reconfigurer l'adaptateur et déconnecter ses contrôleurs ou bien connecter d'autres contrôleurs qui n'étaient pas disponibles lors du démarrage de l'hôte. Pour plus d'informations, consultez [Ajouter des contrôleurs pour NVMe over Fabrics](#).



NVMe over RDMA (RoCE v2)

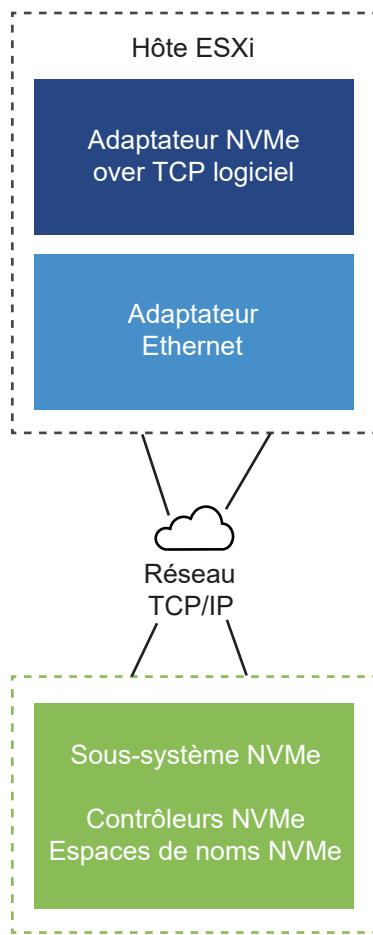
Cette technologie utilise un transport d'accès direct à la mémoire à distance (RDMA) entre deux systèmes sur le réseau. Le transport permet l'échange de données dans la mémoire principale en contournant le système d'exploitation ou le processeur d'un système. ESXi prend en charge la technologie RDMA over Converged Ethernet v2 (RoCE v2), ce qui permet un accès direct à la mémoire distante sur un réseau Ethernet.

Pour accéder au stockage, l'hôte ESXi utilise un adaptateur réseau RDMA installé sur votre hôte et un adaptateur de stockage NVMe over RDMA logiciel. Vous devez configurer les deux adaptateurs afin de les utiliser pour la découverte de stockage. Pour plus d'informations, consultez [Configuration d'adaptateurs pour le stockage NVMe over RDMA \(RoCE v2\)](#).



NVMe over TCP

Cette technologie utilise des connexions Ethernet entre deux systèmes. Pour accéder au stockage, l'hôte ESXi utilise un adaptateur réseau installé sur votre hôte et un adaptateur logiciel de stockage NVMe over TCP. Vous devez configurer les deux adaptateurs afin de les utiliser pour la découverte de stockage. Pour plus d'informations, consultez [Configuration des adaptateurs pour le stockage NVMe over TCP](#).



Conditions requises et limitations du stockage VMware NVMe

Lorsque vous utilisez la technologie NVMe avec VMware, vous devez suivre certaines directives et des exigences spécifiques.

Conditions requises pour NVMe over PCIe

Votre environnement de stockage ESXi doit inclure les composants suivants :

- Périphériques de stockage NVMe local.
- Hôte ESXi compatible.
- Adaptateur NVMe over PCIe matériel. Après l'installation de l'adaptateur, votre hôte ESXi le détecte et l'affiche dans vSphere Client en tant qu'adaptateur de stockage (vmhba) avec le protocole indiqué comme étant PCIe. Il n'est pas nécessaire de configurer l'adaptateur.

Conditions requises pour NVMe over RDMA (RoCE v2)

- Baie de stockage NVMe avec prise en charge du transport NVMe over RDMA (RoCE v2).

- Hôte ESXi compatible.
- Commutateurs Ethernet prenant en charge un réseau sans perte.
- Adaptateur réseau qui prend en charge RDMA over Converged Ethernet (RoCE v2). Pour configurer l'adaptateur, reportez-vous à [Configuration d'adaptateurs pour le stockage NVMe over RDMA \(RoCE v2\)](#).
- Adaptateur NVMe over RDMA logiciel. Ce composant logiciel doit être activé sur votre hôte ESXi et connecté à un adaptateur RDMA réseau approprié. Pour plus d'informations, consultez [Ajout d'adaptateurs logiciels NVMe](#).
- Contrôleur NVMe. Vous devez ajouter un contrôleur après avoir configuré l'adaptateur NVMe over RDMA logiciel. Reportez-vous à la section [Ajouter des contrôleurs pour NVMe over Fabrics](#).
- Ethernet sans perte. Reportez-vous à la section [Configuration de la technologie Ethernet sans perte pour NVMe sur RDMA](#).

Conditions requises pour NVMe over Fibre Channel

- Baie de stockage Fibre Channel prenant en charge NVMe. Pour plus d'informations, consultez [Chapitre 3 Utilisation d'ESXi avec un SAN Fibre Channel](#).
- Hôte ESXi compatible.
- Adaptateur NVMe matériel. En général, il s'agit d'un HBA Fibre Channel qui prend en charge NVMe. Lorsque vous installez l'adaptateur, votre hôte ESXi le détecte et l'affiche dans vSphere Client en tant qu'adaptateur Fibre Channel standard (vmhba) avec le protocole de stockage indiqué comme étant NVMe. Il n'est pas nécessaire de configurer l'adaptateur NVMe matériel pour l'utiliser.
- Contrôleur NVMe. Il n'est pas nécessaire de configurer le contrôleur. Après l'installation de l'adaptateur NVMe matériel requis, celui-ci se connecte automatiquement à toutes les cibles et à tous les contrôleurs qui sont accessibles à ce moment-là. Vous pourrez ensuite déconnecter les contrôleurs ou bien connecter d'autres contrôleurs qui n'étaient pas disponibles lors du démarrage de l'hôte. Reportez-vous à la section [Ajouter des contrôleurs pour NVMe over Fabrics](#).

Conditions requises pour NVMe over TCP

- Baie de stockage NVMe avec prise en charge du transport NVMe over TCP.
- Hôte ESXi compatible.
- Un adaptateur Ethernet. Pour configurer l'adaptateur, reportez-vous à [Configuration des adaptateurs pour le stockage NVMe over TCP](#).
- Adaptateur NVMe over TCP logiciel. Ce composant logiciel doit être activé sur votre hôte ESXi et connecté à un adaptateur réseau approprié. Pour plus d'informations, consultez [Ajout d'adaptateurs logiciels NVMe](#).

- Contrôleur NVMe. Vous devez ajouter un contrôleur après avoir configuré l'adaptateur NVMe over TCP logiciel. Reportez-vous à la section [Ajouter des contrôleurs pour NVMe over Fabrics](#).

Prise en charge du stockage partagé VMware NVMe over Fabrics

Dans l'environnement ESXi, les périphériques de stockage NVMe sont similaires aux périphériques de stockage SCSI et peuvent être utilisés comme stockage partagé. Suivez ces règles lors de l'utilisation du stockage NVMe-oF.

- Ne mélangez pas les types de transport pour accéder au même espace de noms.
- Assurez-vous que les chemins actifs sont présentés à l'hôte. Les espaces de noms ne peuvent pas être enregistrés tant que le chemin actif n'est pas découvert.

Fonctionnalité de stockage partagé	Stockage SCSI over Fabrics	Stockage NVMe over Fabrics
RDM	Pris en charge	Non pris en charge
Vidage de mémoire	Pris en charge	Pris en charge
Réservations SCSI-2	Pris en charge	Non pris en charge
VMDK en cluster	Pris en charge	Pris en charge
VMDK partagé avec signalement multi-écriture	Pris en charge	Pris en charge Dans vSphere 7.0 Update 1 et versions ultérieures. Pour plus d'informations, reportez-vous à l'article de la base de connaissances .
Virtual Volumes	Pris en charge	Pris en charge Dans vSphere 8.0 et versions ultérieures. Pour plus d'informations, consultez NVMe et Virtual Volumes .
Accélération matérielle avec plug-ins VAAI	Pris en charge	Non pris en charge
MPP par défaut	NMP	HPP (les cibles NVMe-oF ne peuvent pas être réclamées par le NMP)

Configuration de la technologie Ethernet sans perte pour NVMe sur RDMA

NVMe over RDMA dans ESXi nécessite un réseau Ethernet sans perte.

Pour établir des réseaux sans perte, vous pouvez sélectionner l'un des paramètres QoS disponibles.

Activer le contrôle de flux d'interruption globale

Dans cette configuration réseau, assurez-vous que le contrôle de flux d'interruption globale est activé sur les ports de commutateur réseau. Assurez-vous également que les cartes réseau compatibles RDMA dans l'hôte négocient automatiquement le contrôle de flux adapté.

Pour vérifier le contrôle de flux, exécutez la commande suivante :

```
#esxcli network nic get -n vmnicX
  Pause RX: true
  Pause TX: true
```

Si les options de commande ci-dessus ne sont pas définies sur true, exécutez la commande suivante.

```
#esxcli network nic pauseParams set -r true -t true -n vmnicX
```

Activer le contrôle de flux prioritaire

Pour que le trafic RoCE soit sans perte, vous devez configurer la valeur de priorité PFC sur 3 dans le commutateur physique et les hôtes. Vous pouvez configurer le PFC dans l'hôte ESXi de deux manières :

- Configuration automatique. Appliquez la configuration de PFC DCB automatiquement sur l'hôte RNIC, si le pilote RNIC prend en charge DCB et DCBx.

Vous pouvez vérifier les paramètres DCB actuels en exécutant la commande suivante :

```
#esxcli network nic dcb status get -n vmnicX
```

- Configuration manuelle. Dans certains cas, les pilotes RNIC fournissent une méthode pour configurer manuellement le PFC DCB à l'aide des paramètres spécifiques du pilote. Pour utiliser cette méthode, reportez-vous à la documentation du pilote propre au fournisseur. Par exemple, dans le pilote Mellanox ConnectX-4/5, vous pouvez définir la valeur de priorité PFC sur trois en exécutant la commande suivante, puis en redémarrant l'hôte.

```
#esxcli system module parameters set -m nmlx5_core -p "pfctx=0x08 pfcrx=0x08"
```

Activer PFC basé sur DSCP

Le mode PFC basé sur DSCP est une autre méthode de configuration de réseau sans perte. Dans les commutateurs et les hôtes physiques, vous devez définir la valeur DSCP sur 26. Pour utiliser cette option, reportez-vous à la documentation du pilote propre au fournisseur. Par exemple, dans le pilote Mellanox ConnectX-4/5, vous pouvez définir la valeur de balise DSCP sur 26 en exécutant les commandes suivantes.

- 1 Activez le mode d'approbation PFC et DSCP.

```
#esxcli system module parameters set -m nmlx5_core -p "pfctx=0x08 pfcrx=0x08 trust_state=2"
```

- 2 Définissez la valeur DSCP sur 26.

```
#esxcli system module parameters set -m nmlx5_rdma -p "dscp_force=26"
```

- 3 Vérifiez les paramètres pour vous assurer qu'ils sont corrects et définis.

```
esxcli system module parameters list -m nmlx5_core | grep 'trust_state\|pfcrx\|pfctx'
```

- 4 Redémarrez l'hôte.

Configuration d'adaptateurs pour le stockage NVMe over RDMA (RoCE v2)

Le processus de configuration de l'adaptateur sur l'hôte ESXi implique la configuration d'une liaison VMkernel pour un adaptateur réseau RDMA, puis l'activation d'un adaptateur NVMe over RDMA logiciel.

L'intégralité du processus de configuration inclut ces actions.

Action	Description
Voir les adaptateurs réseau RDMA	Après avoir installé un adaptateur réseau qui prend en charge RDMA (RoCE v2) sur votre hôte ESXi, utilisez vSphere Client pour vérifier l'adaptateur RDMA et un adaptateur réseau physique.
Configurer la liaison VMkernel pour l'adaptateur RDMA	La liaison de port pour NVMe sur RDMA implique la création d'un commutateur et la connexion de l'adaptateur réseau physique et de l'adaptateur VMkernel au commutateur. Grâce à cette connexion, l'adaptateur RDMA se trouve lié à l'adaptateur VMkernel. Dans la configuration, vous pouvez utiliser un commutateur vSphere Standard ou un commutateur vSphere Distributed Switch.
Ajout d'adaptateurs logiciels NVMe	Utilisez vSphere Client pour activer les adaptateurs de stockage logiciel pour NVMe over RDMA.
Ajouter des contrôleurs pour NVMe over Fabrics	Utilisez vSphere Client pour ajouter un contrôleur NVMe. Après l'ajout du contrôleur, les espaces de noms NVMe associés au contrôleur deviennent disponibles pour votre hôte ESXi. Les périphériques de stockage NVMe qui représentent les espaces de noms dans l'environnement ESXi s'affichent dans la liste des périphériques de stockage.

La vidéo suivante vous guide à travers les étapes de configuration des adaptateurs NVMe over RDMA.



(Configuration des adaptateurs NVMe over RDMA)

Voir les adaptateurs réseau RDMA

Après avoir installé un adaptateur réseau qui prend en charge RDMA (RoCE v2) sur votre hôte ESXi, utilisez vSphere Client pour vérifier l'adaptateur RDMA et un adaptateur réseau physique.

Procédure

- Sur votre hôte ESXi, installez un adaptateur qui prend en charge RDMA (RoCE v2) (par exemple, Mellanox Technologies MT27700 Family ConnectX-4).

L'hôte découvre l'adaptateur et vSphere Client affiche ses deux composants, un adaptateur RDMA et un adaptateur réseau physique.

- Dans vSphere Client, vérifiez que l'adaptateur RDMA est détecté par votre hôte.

a Accédez à l'hôte.

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

c Sous **Mise en réseau**, cliquez sur **Adaptateurs RDMA**.

Dans cet exemple, l'adaptateur RDMA figure dans la liste en tant que `vmrdma0`. La colonne **Liaison montante couplée** affiche le composant réseau comme adaptateur réseau physique `vmnic1`.

Name	Driver	State	Paired Uplink
vmrdma0	nmlx5_rdma	Active	vmnic1

- Pour vérifier la description de l'adaptateur, sélectionnez l'adaptateur RDMA dans la liste, puis cliquez sur l'onglet **Propriétés**.

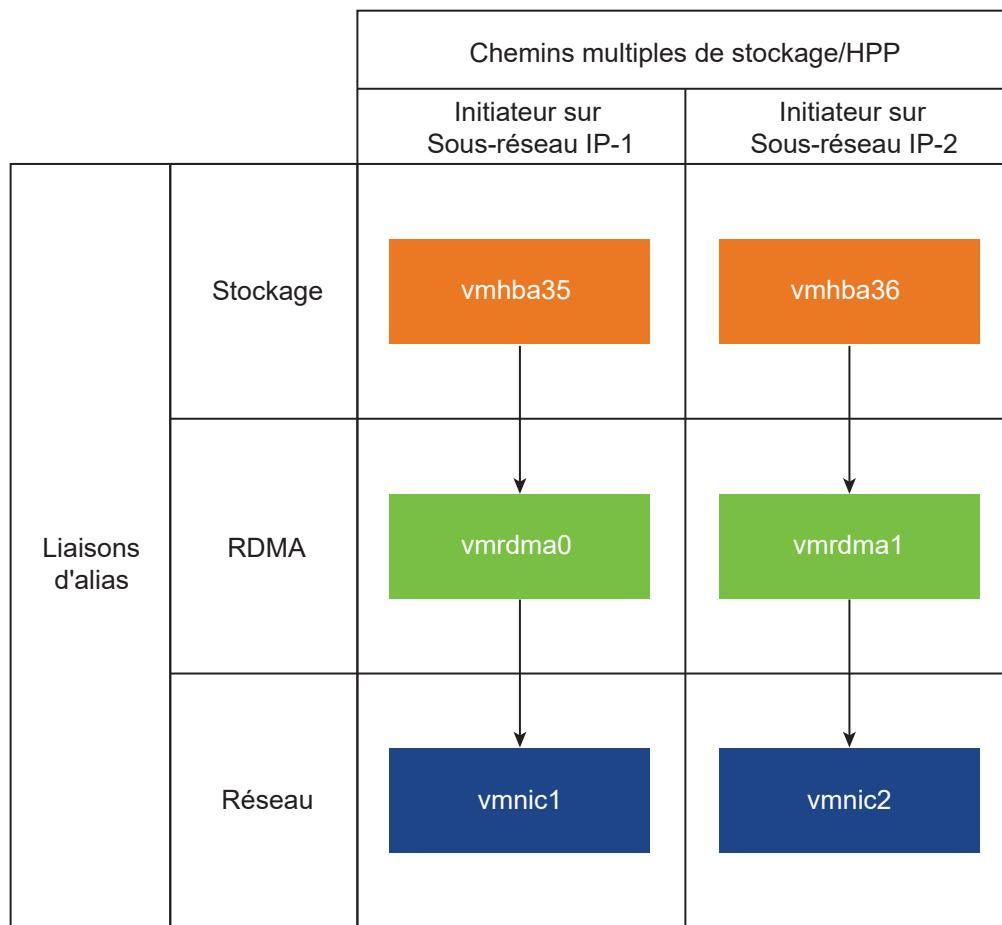
Étape suivante

Vous pouvez maintenant créer l'adaptateur NVMe over RDMA logiciel.

Configurer la liaison VMkernel pour l'adaptateur RDMA

La liaison de port pour NVMe sur RDMA implique la création d'un commutateur et la connexion de l'adaptateur réseau physique et de l'adaptateur VMkernel au commutateur. Grâce à cette connexion, l'adaptateur RDMA se trouve lié à l'adaptateur VMkernel. Dans la configuration, vous pouvez utiliser un commutateur vSphere Standard ou un commutateur vSphere Distributed Switch.

Le diagramme suivant affiche la liaison de port pour l'adaptateur NVMe sur RDMA.

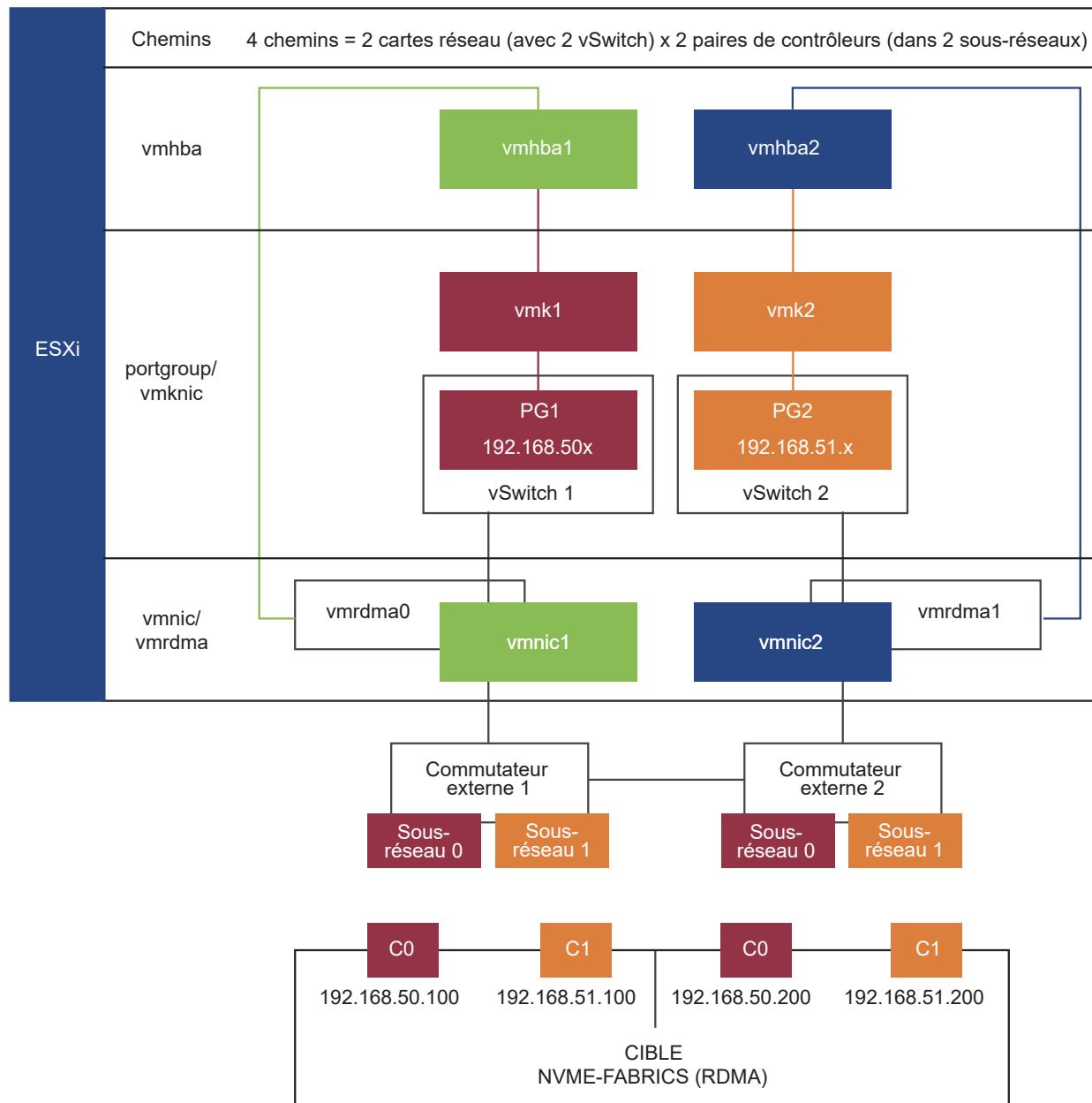


Pour plus d'informations sur la création de commutateurs, reportez-vous à la section *Créer un commutateur vSphere Standard* ou *Créer un vSphere Distributed Switch* dans la documentation de *Mise en réseau vSphere*.

Exemple de topologie réseau avec NVMe sur RDMA

Dans cet exemple, deux commutateurs standard vSphere et deux liaisons montantes (cartes réseau compatibles RDMA) fournissent une haute disponibilité. Ils se connectent à deux paires de contrôleurs dans deux sous-réseaux.

HA avec vSwitch et liaisons montantes multiples (RNIC)



Configurer la liaison VMkernel avec un commutateur standard vSphere

Vous pouvez configurer la liaison de port VMkernel pour l'adaptateur RDMA à l'aide d'un commutateur standard vSphere et d'une liaison montante par commutateur. La configuration de la connexion réseau implique de créer un adaptateur virtuel VMkernel pour chaque adaptateur réseau physique. Vous utilisez le mappage 1:1 entre chaque adaptateur réseau virtuel et physique.

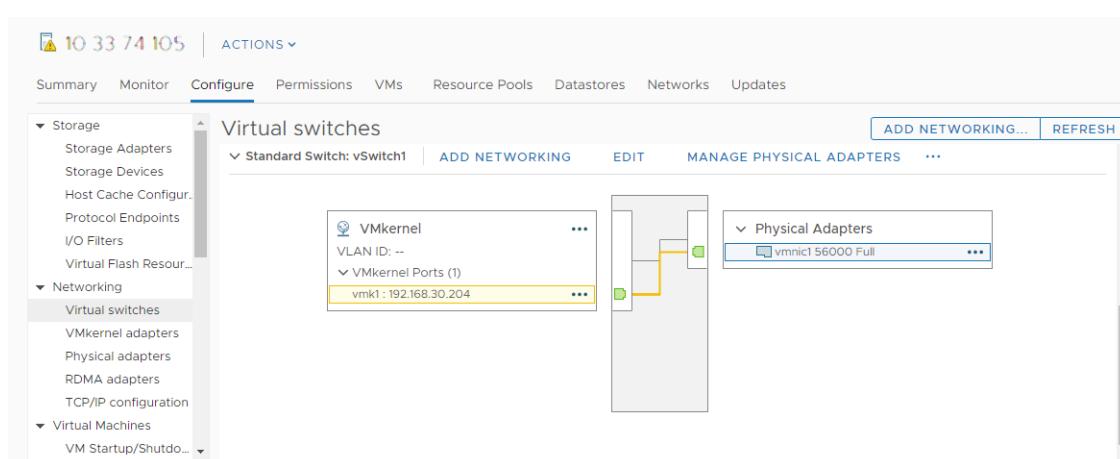
Procédure

- 1 Créez un commutateur standard vSphere avec un adaptateur VMkernel et le composant réseau.
 - a Dans vSphere Client, sélectionnez votre hôte, puis cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Actions > Ajouter une mise en réseau**.
 - c Sélectionnez **Adaptateur réseau VMkernel**, puis cliquez sur **SUIVANT**.
 - d Sélectionnez **Nouveau commutateur standard**, puis cliquez sur **SUIVANT**.
 - e Sous **Adaptateurs attribués**, cliquez sur **+**.
La liste des adaptateurs physiques disponibles s'affiche.
 - f Sélectionnez l'adaptateur physique requis `vmnic`, puis cliquez sur **OK**.

Note Assurez-vous de sélectionner l'adaptateur réseau physique qui correspond à l'adaptateur RDMA. Pour voir l'association entre l'adaptateur RDMA `vmrdma` et l'adaptateur réseau physique `vmnic`, reportez-vous à [Voir les adaptateurs réseau RDMA](#).

- g Sous **Paramètres de port VMkernel**, entrez les valeurs requises.
Si vous utilisez un VLAN pour le chemin de stockage, entrez l'ID de VLAN.
- h Dans la liste **Paramètres IP**, entrez les paramètres IPv4 VMkernel.
- i Sous Services disponibles, sélectionnez **NVMe over RDMA**.
- 2 Vérifiez que votre commutateur est correctement configuré.
 - a Dans l'onglet **Configurer**, sélectionnez **Commutateurs virtuels** sous **Mise en réseau**.
 - b Développez le commutateur et vérifiez sa configuration.

L'illustration montre que l'adaptateur réseau physique et l'adaptateur VMkernel sont connectés au commutateur vSphere Standard. Grâce à cette connexion, l'adaptateur RDMA est lié à l'adaptateur VMkernel.



- 3** Vérifiez la configuration de la liaison VMkernel pour l'adaptateur RDMA.
- Sous la liste **Mise en réseau**, cliquez sur **Adaptateurs RDMA**, puis sélectionnez l'adaptateur RDMA dans la liste.
 - Cliquez sur l'onglet **Liaison des adaptateurs VMkernel** et vérifiez que l'adaptateur VMkernel associé s'affiche sur la page.
- Dans cet exemple, l'adaptateur RDMA `vmrdma0` est couplé à l'adaptateur réseau `vmnic1` et est connecté à l'adaptateur VMkernel `vmk1`.

Configurer la liaison VMkernel avec un commutateur standard vSphere et l'association de cartes réseau

Vous pouvez configurer la liaison de port VMkernel pour l'adaptateur RDMA à l'aide d'un commutateur standard vSphere avec la configuration d'association de cartes réseau. Vous pouvez utiliser l'association de cartes réseau pour garantir la redondance du réseau. Vous pouvez configurer deux adaptateurs réseau (cartes réseau) ou plus en tant qu'équipe pour la haute disponibilité et l'équilibrage de charge.

Procédure

- Créez un commutateur standard vSphere avec un adaptateur VMkernel et le composant réseau au moyen de la configuration d'association de cartes réseau.
 - Dans vSphere Client, sélectionnez votre hôte et cliquez sur l'onglet **Réseaux**.
 - Cliquez sur **Actions > Ajouter une mise en réseau**.
 - Sélectionnez **Adaptateur réseau VMkernel**, puis cliquez sur **SUIVANT**.
 - Sélectionnez **Nouveau commutateur standard**, puis cliquez sur **SUIVANT**.
 - Sous **Adaptateurs attribués**, cliquez sur **+**.
Une liste des adaptateurs physiques disponibles s'affiche.
 - Sélectionnez l'adaptateur physique requis `vmnic` et ajoutez-le sous **Adaptateurs actifs**.

- g Sélectionnez un autre adaptateur physique `vmnic`, puis ajoutez-le sous **Adaptateurs inutilisés**.
 - h Sous **Paramètres de port VMkernel**, entrez les valeurs requises.
Si vous utilisez un VLAN pour le chemin de stockage, entrez l'ID de VLAN.
 - i Dans la liste **Paramètres IP**, spécifiez les paramètres IPv4 VMkernel.
 - j Sous Services disponibles, sélectionnez **NVMe over RDMA**.
- Répétez l'étape 1 pour configurer un commutateur standard existant.
- 2 Configurez votre commutateur pour la configuration de l'association de cartes réseau .
 - a Dans l'onglet **Configurer**, sélectionnez **Commutateurs virtuels** sous **Mise en réseau**.
 - b Sélectionnez l'adaptateur VMkernel approprié.
 - c Dans le menu contextuel, cliquez sur **Modifier les paramètres**.
 - d Sélectionnez **Association et basculement**.
 - e Sous **Adaptateurs actifs**, transférez l'adaptateur physique requis `vmnic`.
 - f Sous **Adaptateurs en veille > Ordre de basculement**, transférez les autres adaptateurs physiques.
 - g Définissez un équilibrage de charge et d'autres propriétés appropriés.
 - h Répétez les étapes pour configurer des adaptateurs VMkernel supplémentaires.
 - 3 Répétez les étapes 1 et 2 pour ajouter et configurer un ensemble supplémentaire de `rnic` associés. Pour vérifier que l'adaptateur est configuré, cliquez sur l'onglet **Configurer**, puis sélectionnez **Adaptateurs VMkernel**

Configurer la liaison VMkernel avec un vSphere Distributed Switch

Vous pouvez configurer la liaison de port VMkernel pour l'adaptateur RDMA à l'aide d'un vSphere Distributed Switch et d'une liaison montante par commutateur. La configuration de la connexion réseau implique de créer un adaptateur virtuel VMkernel pour chaque adaptateur réseau physique. Vous utilisez le mappage 1:1 entre chaque adaptateur réseau virtuel et physique.

Procédure

- 1 Créez un vSphere Distributed Switch avec un adaptateur VMkernel et le composant réseau.
 - a Dans vSphere Client, sélectionnez **Centre de données**, puis cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Actions**, puis sélectionnez **Distributed Switch > Nouveau Distributed Switch**.
 - c Sélectionnez un nom pour le commutateur.

Assurez-vous que l'emplacement du centre de données est présent dans votre hôte, puis cliquez sur **Suivant**.

- d Sélectionnez une version d'ESXi compatible, puis cliquez sur **Suivant**.
 - e Entrez le nombre de liaisons montantes requis, puis cliquez sur **Terminer**.
- 2** Ajoutez un ou plusieurs hôtes à votre commutateur virtuel distribué.
- a Dans vSphere Client, sélectionnez **Centre de données**, puis cliquez sur **Distributed Switches**.

Une liste des Distributed Switches disponibles s'affiche.
 - b Cliquez avec le bouton droit sur le Distributed Switch et sélectionnez **Ajouter et gérer des hôtes** dans le menu.
 - c Sélectionnez **Ajouter des hôtes**, puis cliquez sur **Suivant**.
 - d Sélectionnez votre hôte et cliquez sur **Suivant**.
 - e Sélectionnez **Attribuer une liaison montante**.
 - f Entrez la liaison montante correspondante pour attribuer la `vmnic`.
 - g Attribuez un adaptateur VMkernel, puis cliquez sur **Suivant**.
 - h Dans vSphere Client, sélectionnez le Distributed Switch, puis cliquez sur l'onglet **Ports**.

Vous pouvez afficher ici les liaisons montantes créées pour votre commutateur.
- 3** Créez des groupes de ports distribués pour le chemin de stockage NVMe sur RDMA.
- a Dans vSphere Client, sélectionnez le Distributed Switch requis.
 - b Cliquez sur **Actions** et sélectionnez **Groupe de ports distribués > Nouveau groupe de ports distribués**.
 - c Sous **Configurer les paramètres**, entrez les propriétés générales du groupe de ports.

Si vous avez configuré un VLAN spécifique, ajoutez-le dans l'ID de VLAN.

Note Des problèmes de connectivité réseau peuvent se produire si vous ne configurez pas correctement le VLAN.
- 4** Configurez les adaptateurs VMkernel.
- a Dans vSphere Client, développez la liste **DSwitch**, puis sélectionnez le groupe de ports distribués.
 - b Cliquez sur **Actions > Ajouter des adaptateurs VMkernel**.
 - c Dans la boîte de dialogue **Sélectionner des hôtes membres**, sélectionnez votre hôte et cliquez sur **OK**.
 - d Dans la boîte de dialogue **Configurer l'adaptateur VMkernel**, assurez-vous que le MTU correspond au MTU du commutateur.
 - e Sous **Services disponibles**, sélectionnez **NVMe over RDMA** pour le balisage approprié.

- f Cliquez sur **Terminer**.
- g Répétez l'étape b et l'étape c pour ajouter plusieurs cartes réseau compatibles RDMA.
- 5 Définissez les stratégies d'association de cartes réseau pour les groupes de ports distribués.
- Dans **Groupe de ports distribués**, cliquez sur **Actions > Modifier les paramètres**.
 - Cliquez sur **Association et basculement**, puis vérifiez les liaisons montantes actives.
 - Attribuez une liaison montante en tant que **Active** pour le groupe de ports et l'autre liaison montante comme **Inutilisée**.
Répétez l'étape c pour chacun des groupes de ports créés.

Étape suivante

Une fois la configuration terminée, cliquez sur **Configurer** et vérifiez si l'onglet Adaptateur physique sur votre hôte répertorie les DVSwitch pour les cartes réseau sélectionnées.

Configuration des adaptateurs pour le stockage NVMe over TCP

Le processus de configuration de l'adaptateur sur l'hôte ESXi implique la configuration de la liaison VMkernel pour un adaptateur réseau TCP, puis l'activation d'un adaptateur logiciel pour NVMe over TCP.

L'intégralité du processus de configuration inclut ces actions.

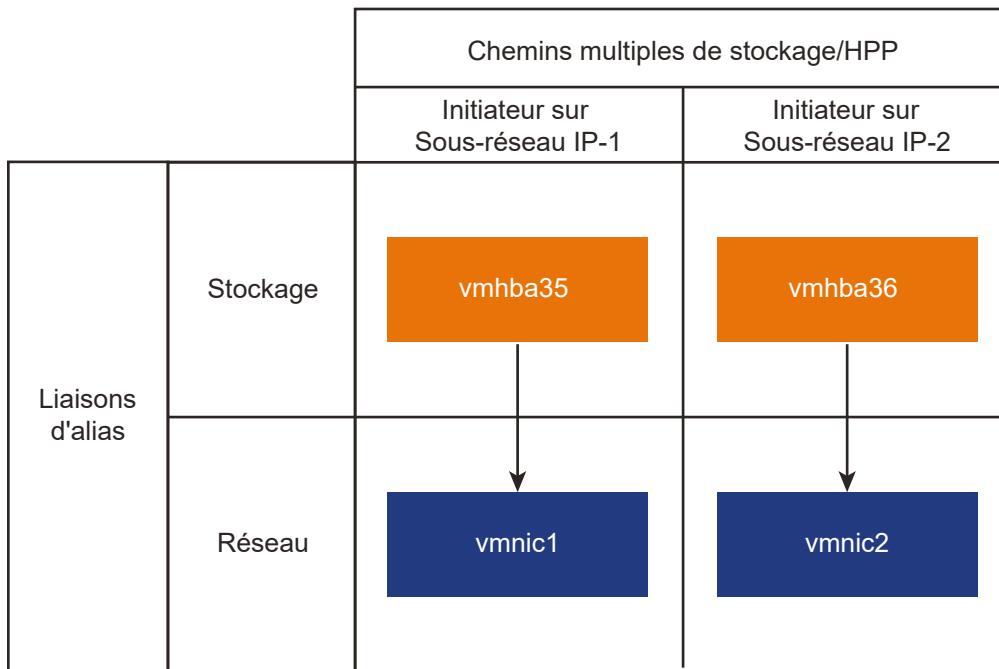
Action	Description
Configurer la liaison VMkernel pour l'adaptateur NVMe over TCP	La liaison VMkernel pour NVMe over TCP implique la création d'un commutateur virtuel et la connexion de l'adaptateur réseau physique et de l'adaptateur virtuel. Via cette connexion, l'adaptateur TCP est lié à l'adaptateur VMkernel. Dans la configuration, vous pouvez utiliser un commutateur vSphere Standard ou un commutateur vSphere Distributed Switch.
Ajout d'adaptateurs logiciels NVMe	Utilisez vSphere Client pour activer les adaptateurs de stockage logiciel pour NVMe over TCP.
Ajouter des contrôleurs pour NVMe over Fabrics	Utilisez vSphere Client pour ajouter un contrôleur NVMe. Après l'ajout du contrôleur, les espaces de noms NVMe associés au contrôleur deviennent disponibles pour votre hôte ESXi. Les périphériques de stockage NVMe qui représentent les espaces de noms dans l'environnement ESXi s'affichent dans la liste des périphériques de stockage.

Configurer la liaison VMkernel pour l'adaptateur NVMe over TCP

La liaison de port pour NVMe over TCP implique la création d'un commutateur virtuel et la connexion de l'adaptateur réseau physique et de l'adaptateur VMkernel au commutateur virtuel. Via cette connexion, l'adaptateur TCP est lié à l'adaptateur VMkernel. Dans la configuration,

vous pouvez utiliser un commutateur vSphere Standard ou un commutateur vSphere Distributed Switch.

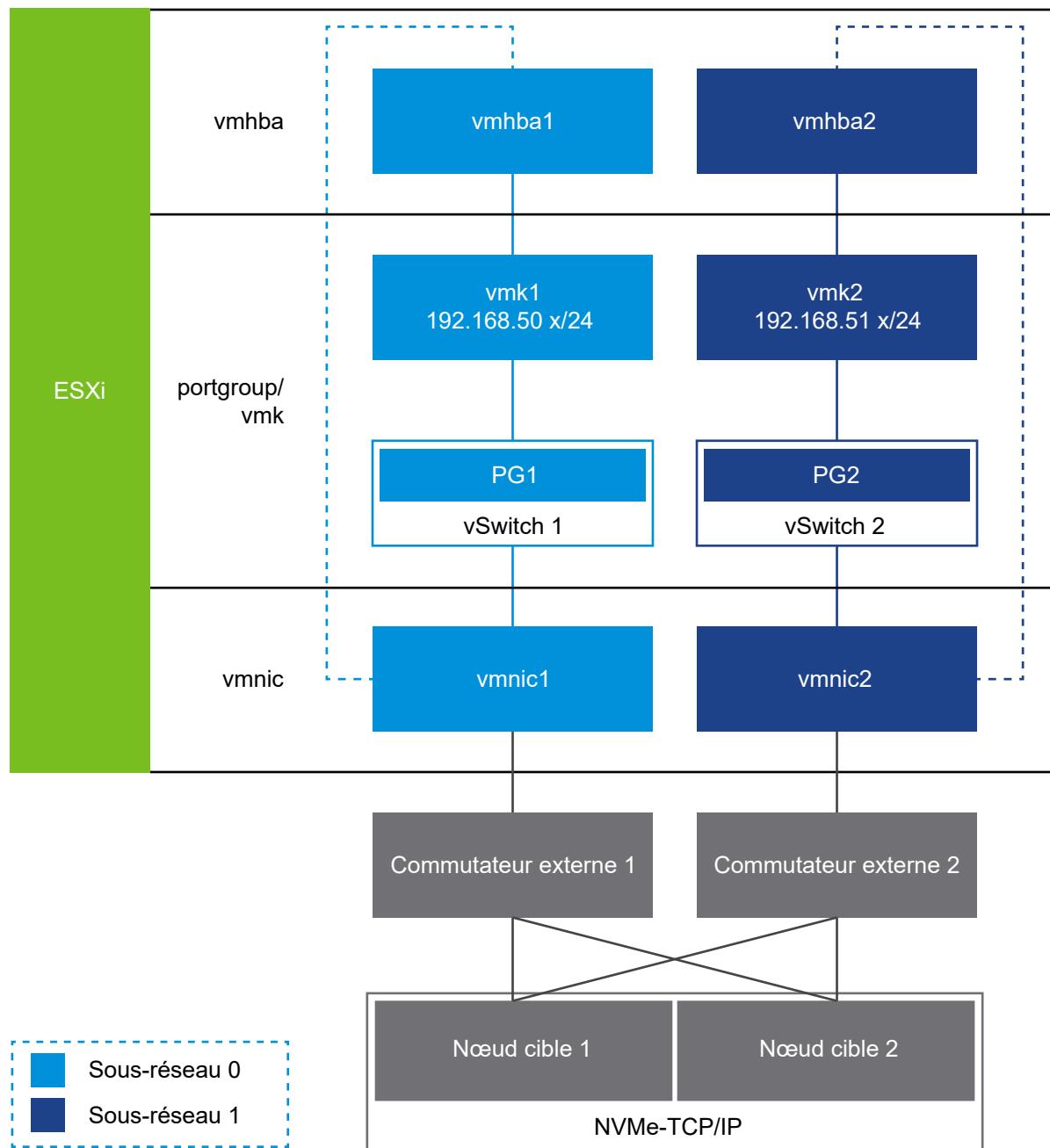
Le diagramme suivant affiche la liaison de port pour l'adaptateur NVMe over TCP.



Pour plus d'informations sur la création de commutateurs, reportez-vous à la section *Créer un commutateur vSphere Standard* ou *Créer un vSphere Distributed Switch* dans la documentation de *Mise en réseau vSphere*.

Exemple de topologie réseau avec NVMe over TCP

Dans cet exemple, deux commutateurs standard vSphere et deux adaptateurs réseau (vmnic) sur l'hôte fournissent une haute disponibilité. Ils se connectent à deux commutateurs externes.



Configurer la liaison VMkernel pour l'adaptateur TCP avec un commutateur standard vSphere

Vous pouvez configurer la liaison VMkernel pour l'adaptateur TCP à l'aide d'un commutateur vSphere standard et d'une liaison montante. La configuration de la connexion réseau implique de créer un adaptateur virtuel VMkernel pour chaque adaptateur réseau physique. Vous utilisez le mappage 1:1 entre chaque adaptateur réseau virtuel et physique.

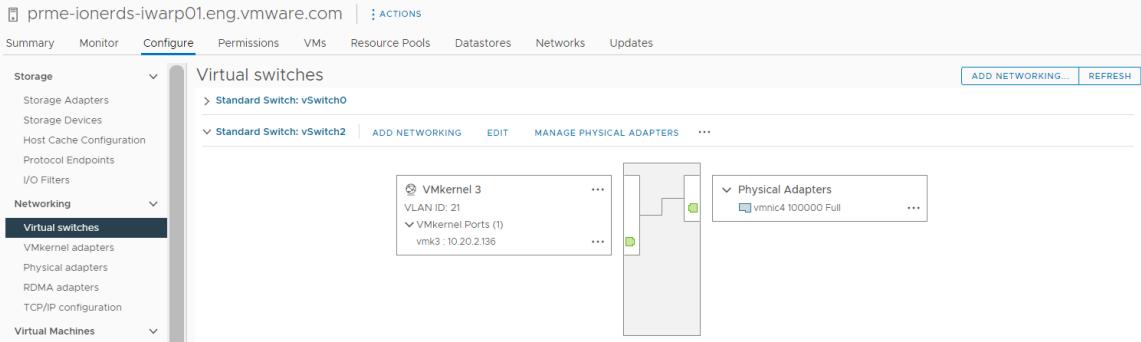
Procédure

- 1 Créez un commutateur standard vSphere avec un adaptateur VMkernel et le composant réseau.
 - a Dans vSphere Client, sélectionnez votre hôte, puis cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Actions > Ajouter une mise en réseau**.
 - c Sélectionnez **Adaptateur réseau VMkernel**, puis cliquez sur **SUIVANT**.
 - d Sélectionnez **Nouveau commutateur standard**, puis cliquez sur **SUIVANT**.
 - e Sous **Adaptateurs attribués**, cliquez sur **+**.
La liste des adaptateurs physiques disponibles s'affiche.
 - f Sélectionnez l'adaptateur physique requis `vminic`, puis cliquez sur **OK**.

Note Veillez à sélectionner l'adaptateur réseau physique qui correspond à l'adaptateur TCP/IP.

- g Sous **Paramètres de port VMkernel**, entrez les valeurs requises.
Si vous utilisez un VLAN pour le chemin de stockage, entrez l'ID de VLAN.
- h Dans la liste **Paramètres IP**, entrez les paramètres IPv4 VMkernel.
- i Sous **Services disponibles**, sélectionnez **NVMe over TCP** pour le balisage approprié.
- 2 Vérifiez que votre commutateur est correctement configuré.
 - a Dans l'onglet **Configurer**, sélectionnez **Commutateurs virtuels** sous **Mise en réseau**.
 - b Développez le commutateur et vérifiez sa configuration.

L'illustration montre que l'adaptateur réseau physique et l'adaptateur VMkernel sont connectés au commutateur vSphere Standard. Via cette connexion, l'adaptateur TCP est lié à l'adaptateur VMkernel.



- 3 Définissez les stratégies d'association de cartes réseau du commutateur vSphere Standard.

Note L'adaptateur NVMe over TCP ne prend pas en charge les fonctionnalités d'association de cartes réseau telles que le basculement et l'équilibrage de charge. Il utilise plutôt la gestion multivoie de stockage pour ces fonctionnalités. Cependant, si vous devez configurer l'association de cartes réseau pour d'autres charges de travail réseau sur la liaison montante servant l'adaptateur NVMe over TCP, procédez comme suit :

- a Dans l'onglet **Configurer**, sélectionnez **Commutateurs virtuels** sous **Mise en réseau**.
- b Sélectionnez l'adaptateur VMkernel approprié.
- c Dans le menu contextuel, cliquez sur **Modifier les paramètres**.
- d Sélectionnez **Association et basculement**.
- e Sous **Adaptateurs actifs**, transférez l'adaptateur physique requis `vmnic`.
- f Sous **Adaptateurs en veille > Ordre de basculement**, transférez les autres adaptateurs physiques.
- g Définissez un équilibrage de charge et d'autres propriétés appropriés.
- h Répétez les étapes pour configurer des adaptateurs VMkernel supplémentaires.

Pour vérifier si l'adaptateur est configuré, cliquez sur l'onglet **Configurer** et sélectionnez **Adaptateurs VMkernel**.

Configurer la liaison VMkernel pour l'adaptateur TCP avec un vSphere Distributed Switch

Vous pouvez configurer la liaison de port VMkernel pour l'adaptateur TCP à l'aide d'un vSphere Distributed Switch et d'une liaison montante par commutateur. La configuration de la connexion réseau implique de créer un adaptateur virtuel VMkernel pour chaque adaptateur réseau physique. Vous utilisez le mappage 1:1 entre chaque adaptateur réseau virtuel et physique.

Procédure

- 1 Créez un vSphere Distributed Switch avec un adaptateur VMkernel et le composant réseau.
 - a Dans vSphere Client, sélectionnez **Centre de données**, puis cliquez sur l'onglet **Réseaux**.
 - b Cliquez sur **Actions**, puis sélectionnez **Distributed Switch > Nouveau Distributed Switch**.
 - c Sélectionnez un nom pour le commutateur.
Assurez-vous que l'emplacement du centre de données est présent dans votre hôte, puis cliquez sur **Suivant**.
 - d Sélectionnez une version d'ESXi compatible, puis cliquez sur **Suivant**.
 - e Entrez le nombre de liaisons montantes requis, puis cliquez sur **Terminer**.

- 2 Ajoutez un ou plusieurs hôtes à votre commutateur virtuel distribué.
 - a Dans vSphere Client, sélectionnez **Centre de données**, puis cliquez sur **Distributed Switches**.

Une liste des Distributed Switches disponibles s'affiche.
 - b Cliquez avec le bouton droit sur le Distributed Switch et sélectionnez **Ajouter et gérer des hôtes** dans le menu.
 - c Sélectionnez **Ajouter des hôtes**, puis cliquez sur **Suivant**.
 - d Sélectionnez votre hôte et cliquez sur **Suivant**.
 - e Sélectionnez **Attribuer une liaison montante**.
 - f Entrez la liaison montante correspondante pour attribuer la `vmnic`.
 - g Attribuez un adaptateur VMkernel, puis cliquez sur **Suivant**.
 - h Dans vSphere Client, sélectionnez le Distributed Switch, puis cliquez sur l'onglet **Ports**.

Vous pouvez afficher ici les liaisons montantes créées pour votre commutateur.
- 3 Créez des groupes de ports distribués pour le chemin de stockage NVMe over TCP.
 - a Dans vSphere Client, sélectionnez le Distributed Switch requis.
 - b Cliquez sur **Actions** et sélectionnez **Groupe de ports distribués > Nouveau groupe de ports distribués**.
 - c Sous **Configurer les paramètres**, entrez les propriétés générales du groupe de ports.

Si vous avez configuré un VLAN spécifique, ajoutez-le dans l'ID de VLAN.

Note Des problèmes de connectivité réseau peuvent se produire si vous ne configurez pas correctement le VLAN.
- 4 Configurez les adaptateurs VMkernel.
 - a Dans vSphere Client, développez la liste **DSwitch**, puis sélectionnez le groupe de ports distribués.
 - b Cliquez sur **Actions > Ajouter des adaptateurs VMkernel**.
 - c Dans la boîte de dialogue **Sélectionner des hôtes membres**, sélectionnez votre hôte et cliquez sur **OK**.
 - d Dans la boîte de dialogue **Configurer l'adaptateur VMkernel**, assurez-vous que le MTU correspond au MTU du commutateur.
 - e Cliquez sur **Terminer**.
 - f Répétez les étapes b et c pour ajouter plusieurs cartes réseau compatibles TCP.

- 5 Définissez les stratégies d'association de cartes réseau pour les groupes de ports distribués.

Note L'adaptateur NVMe over TCP ne prend pas en charge les fonctionnalités d'association de cartes réseau telles que le basculement et l'équilibrage de charge. Il utilise plutôt la gestion multivoie de stockage pour ces fonctionnalités. Cependant, si vous devez configurer l'association de cartes réseau pour d'autres charges de travail réseau sur la liaison montante servant l'adaptateur NVMe over TCP, procédez comme suit :

- a Dans **Groupe de ports distribués**, cliquez sur **Actions > Modifier les paramètres**.
- b Cliquez sur **Association et basculement**, puis vérifiez les liaisons montantes actives.
- c Attribuez une liaison montante en tant que **Active** pour le groupe de ports et l'autre liaison montante comme **Inutilisée**.

Répétez l'étape c pour chacun des groupes de ports créés.

Étape suivante

Une fois la configuration terminée, cliquez sur **Configurer** et vérifiez si l'onglet Adaptateur physique sur votre hôte répertorie les DVSwitch pour les cartes réseau sélectionnées.

Ajout d'adaptateurs logiciels NVMe

ESXi prend en charge les adaptateurs logiciels NVMe over RDMA et NVMe over TCP. Utilisez vSphere Client pour ajouter les adaptateurs de stockage logiciel pour NVMe over RDMA ou NVMe over TCP.

Conditions préalables

- Sur votre hôte ESXi, installez un adaptateur qui prend en charge les types de stockage suivants.
 - Adaptateur NVMe over RDMA. Par exemple, Mellanox Technologies MT27700 Family ConnectX-4.
 - Adaptateur NVMe over TCP. Par exemple, i40en.
- Configurez la liaison VMkernel pour vos adaptateurs.
 - Pour NVMe over RDMA, reportez-vous à la section [Configurer la liaison VMkernel pour l'adaptateur RDMA](#).
 - Pour NVMe over TCP, reportez-vous à la section [Configurer la liaison VMkernel pour l'adaptateur NVMe over TCP](#).

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.

- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**, puis cliquez sur l'icône **Ajouter un adaptateur logiciel**.
- 4 Sélectionnez le type d'adaptateur requis.
 - **Adaptateur NVMe over RDMA**
 - **Adaptateur NVMe over TCP**

- 5 En fonction de votre sélection à l'étape 4, sélectionnez un adaptateur RDMA ou un adaptateur réseau TCP approprié (`vmnic`) dans le menu déroulant.

Note Si vous obtenez un message d'erreur qui vous empêche de créer l'adaptateur logiciel, assurez-vous que la liaison VMkernel pour l'adaptateur est correctement configurée. Pour plus d'informations, reportez-vous à [Configurer la liaison VMkernel pour l'adaptateur RDMA](#) et [Configurer la liaison VMkernel pour l'adaptateur NVMe over TCP](#).

Résultats

Les adaptateurs logiciels NVMe over RDMA et NVMe over TCP s'affichent dans la liste en tant qu'adaptateurs de stockage `vhba`. Vous pouvez supprimer les adaptateurs si vous devez libérer l'adaptateur réseau RDMA et TCP sous-jacent à d'autres fins.

Ajouter des contrôleurs pour NVMe over Fabrics

Utilisez vSphere Client pour ajouter un contrôleur NVMe. Après l'ajout du contrôleur, les espaces de noms NVMe associés au contrôleur deviennent disponibles pour votre hôte ESXi. Les périphériques de stockage NVMe qui représentent les espaces de noms dans l'environnement ESXi s'affichent dans la liste des périphériques de stockage.

Conditions préalables

- Assurez-vous que votre hôte ESXi dispose des adaptateurs appropriés pour votre type de stockage. Reportez-vous à la section [Conditions requises et limitations du stockage VMware NVMe](#).
- Si vous utilisez le stockage NVMe over RDMA (RoCE v2), effectuez les tâches suivantes :
 - [Configurer la liaison VMkernel pour l'adaptateur RDMA](#)
 - [Ajout d'adaptateurs logiciels NVMe](#)
- Si vous utilisez le stockage NVMe over TCP, effectuez les tâches suivantes :
 - [Configurer la liaison VMkernel pour l'adaptateur NVMe over TCP](#)
 - [Ajout d'adaptateurs logiciels NVMe](#)

Note Avec NVMe over Fibre Channel, après l'installation de l'adaptateur requis, celui-ci se connecte automatiquement à toutes les cibles accessibles à ce moment-là. Vous pourrez ensuite reconfigurer l'adaptateur et déconnecter ses contrôleurs ou bien connecter d'autres contrôleurs qui n'étaient pas disponibles lors du démarrage de l'hôte.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**, puis sélectionnez l'adaptateur (vmhba#) à configurer.
- 4 Cliquez sur l'onglet **Contrôleurs** et cliquez sur **Ajouter un contrôleur**.
- 5 Dans la boîte de dialogue **Ajouter un contrôleur**, sélectionnez l'une des méthodes de découverte suivantes.

Option	Description
Automatiquement	<p>Cette option indique que votre hôte peut détecter automatiquement les contrôleurs et accepter la connexion à n'importe quel contrôleur disponible.</p> <p>a Spécifiez les paramètres suivants pour que détecte les contrôleurs.</p> <ul style="list-style-type: none"> ■ Pour NVMe over RDMA (RoCE v2), l'adresse IP et le numéro de port de transport. ■ Pour NVMe over TCP, l'adresse IP, le numéro de port de transport et le paramètre de résumé. <p>b Cliquez sur Détecter des contrôleurs.</p> <p>c Dans la liste des contrôleurs, sélectionnez le contrôleur à utiliser.</p>
Manuellement	<p>Avec cette méthode, vous entrez manuellement les détails du contrôleur. L'hôte demande une connexion à un contrôleur spécifique à l'aide des paramètres que vous spécifiez :</p> <ul style="list-style-type: none"> ■ NQN du sous-système ■ Identification du port cible. <ul style="list-style-type: none"> ■ Pour NVMe over RDMA (RoCE v2), l'adresse IP et le numéro de port de transport (facultatif). ■ Pour NVMe over TCP, l'adresse IP, le numéro de port de transport (facultatif) et le paramètre de résumé (facultatif). ■ Pour NVMe over Fibre Channel, WorldWideNodeName et WorldWidePortName. ■ Taille de la file d'attente administrative. Paramètre facultatif qui spécifie la taille de la file d'attente administrative du contrôleur. La valeur par défaut est 16. ■ Délai d'expiration de la conservation. Paramètre facultatif permettant de spécifier, en secondes, le délai d'expiration de la conservation entre l'adaptateur et le contrôleur. La valeur du délai d'attente par défaut est de 60 secondes. <p>Note La taille de la file d'attente d'E/S et le numéro de file d'attente d'E/S sont des paramètres facultatifs qui peuvent être définis uniquement via esxcli.</p>

Résultats

Le contrôleur s'affiche dans la liste des contrôleurs. Votre hôte peut maintenant découvrir les espaces de noms NVMe qui sont associés au contrôleur. Les périphériques de stockage NVMe qui représentent les espaces de noms dans l'environnement ESXi apparaissent dans la liste des périphériques de stockage dans vSphere Client.

Supprimer des adaptateurs NVMe logiciels

Utilisez vSphere Client pour supprimer les adaptateurs NVMe over RDMA ou NVMe over TCP logiciels. Vous pouvez supprimer l'adaptateur si vous devez libérer l'adaptateur réseau RDMA ou Ethernet sous-jacent à d'autres fins.

Vous ne pouvez pas supprimer les adaptateurs NVMe over PCIe et NVMe over Fibre Channel.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Adaptateurs de stockage**, puis sélectionnez l'adaptateur (`vmhba#`) à supprimer.
- 4 Supprimez le contrôleur NVMe connecté à l'adaptateur.
 - a Cliquez sur l'onglet **Contrôleurs**.
 - b Sélectionnez le contrôleur et cliquez sur **Supprimer**.
Le contrôleur NVMe est déconnecté et disparaît de la liste.
- 5 Cliquez sur l'icône **Supprimer** (Supprimer l'adaptateur de stockage de l'hôte) pour supprimer l'adaptateur NVMe over RDMA ou l'adaptateur NVMe over TCP.

9

Utilisation des banques de données

Les banques de données sont des conteneurs logiques, analogues à des systèmes de fichiers, qui masquent les informations du stockage physique et fournissent un modèle uniforme pour stocker des fichiers de machine virtuelle. Les banques de données peuvent également être utilisées pour le stockage d'images ISO, de modèles de machine virtuelle et d'images de disquette.

vCenter Server et ESXi prennent en charge les types suivants de banques de données.

Tableau 9-1. Types de banque de données

Type de banque de données	Description
VMFS (version 5 et 6)	Les banques de données que vous déployez sur des périphériques de stockage des blocs utilisent le format VMFS (vSphere Virtual Machine File System) natif. VMFS est un format de système de fichiers haute performance qui est optimisé pour stocker les machines virtuelles. Reportez-vous à la section Concepts de banque de données VMFS .
NFS (version 3 et 4.1)	Un client NFS intégré dans ESXi utilise le protocole NFS (Network File System) sur TCP/IP pour accéder à un volume NFS désigné. Le volume se trouve sur un serveur NAS. L'hôte ESXi monte le volume comme une banque de données NFS et l'utilise pour ses besoins de stockage. ESXi prend en charge les versions 3 et 4.1 du protocole NFS. Reportez-vous à Concepts et opérations de banque de données NFS
vSAN	vSAN agrège tous les périphériques de capacité locaux disponibles sur les hôtes en une banque de données unique partagée par tous les hôtes dans le cluster vSAN. Consultez la documentation de Administration de VMware vSAN .
vVol	La banque de données Virtual Volumes représente un conteneur de stockage dans vCenter Server et vSphere Client. Reportez-vous à la section Chapitre 14 Utilisation de VMware vSphere Virtual Volumes .

Selon votre type de stockage, certaines des tâches suivantes sont disponibles pour les banques de données.

- Créer des banques de données. Vous pouvez utiliser vSphere Client pour créer certains types de banques de données.
- Effectuer des opérations administratives sur les banques de données. Plusieurs opérations, telles que le changement de nom d'une banque de données, sont disponibles pour tous les types de banques de données. D'autres s'appliquent à des types spécifiques de banques de données.
- Organiser les banques de données. Par exemple, vous pouvez les regrouper dans des dossiers en fonction des pratiques professionnelles. Après le groupement des banques de données, vous pouvez attribuer simultanément les mêmes autorisations et alarmes sur les banques de données du groupe.
- Ajouter les banques de données à des clusters de banques de données. Un cluster de banques de données est un ensemble de banques de données avec des ressources partagées et une interface de gestion partagée. Lorsque vous créez le cluster de banques de données, vous pouvez utiliser Storage DRS pour gérer les ressources de stockage. Pour plus d'informations sur les clusters de banques de données, consultez la documentation *Gestion des ressources vSphere*.

Ce chapitre contient les rubriques suivantes :

- Concepts de banque de données VMFS
- Crédit de banques de données
- Opérations administratives de base pour les banques de données
- Utilisation du navigateur de banque de données
- Gestion des banques de données VMFS
- Concepts et opérations de banque de données NFS

Concepts de banque de données VMFS

Pour stocker des disques virtuels, ESXi utilise des banques de données. Les banques de données sont des conteneurs logiques qui cachent les spécificités du stockage physique aux machines virtuelles et fournissent un modèle uniforme pour stocker les fichiers de machine virtuelle. Les banques de données que vous déployez sur des périphériques de stockage des blocs utilisent le format VMFS (vSphere Virtual Machine File System) natif. Il s'agit d'un format de système de fichiers haute performance qui est optimisé pour stocker les machines virtuelles.

Utilisez vSphere Client pour configurer une banque de données VMFS d'avance sur un périphérique de stockage basé sur des blocs détecté par votre hôte ESXi.

Pour créer une banque de données VMFS, reportez-vous à la section [Créer une banque de données VMFS](#). Après avoir créé une banque de données, vous pouvez effectuer des opérations d'administration de base, comme renommer, démonter ou supprimer la banque de données. Vous pouvez également effectuer des tâches plus avancées, comme développer la banque de données, gérer les banques de données dupliquées ou collecter des informations de diagnostic sur la banque de données. Pour plus d'informations, reportez-vous aux sections suivantes :

- [Opérations administratives de base pour les banques de données](#)
- [Gestion des banques de données VMFS](#)

Versions des banques de données VMFS

Plusieurs versions du système de fichiers VMFS ont été publiées depuis son introduction. Actuellement, ESXi prend en charge VMFS5 et VMFS6.

Pour toutes les versions de VMFS prises en charge, ESXi offre une prise en charge complète de la lecture et de l'écriture. Sur les banques de données VMFS prises en charge, vous pouvez créer et mettre sous tension des machines virtuelles.

Tableau 9-2. Accès de l'hôte aux versions VMFS

VMFS	ESXi
VMFS6	Lire et écrire
VMFS5	Lire et écrire

Le tableau suivant compare les principales caractéristiques de VMFS5 et de VMFS6. Pour obtenir des informations supplémentaires, reportez-vous à *Configurations maximales*.

Tableau 9-3. Comparaison de VMFS5 et de VMFS6

Caractéristiques et fonctionnalités	VMFS5	VMFS6
Accès aux hôtes ESXi version 6.5 et versions ultérieures	Oui	Oui
Accès aux hôtes ESXi version 6.0 et versions antérieures	Oui	Non
Banques de données par hôte	512	512
Périphériques de stockage 512n	Oui	Oui (par défaut)
Périphériques de stockage 512e	Oui. Non pris en charge sur les périphériques 512e locaux.	Oui (par défaut)
Périphériques de stockage 4Kn	Non	Oui
Récupération d'espace automatique	Non	Oui
Récupération d'espace manuelle avec la commande esxcli. Reportez-vous à la section Récupérer manuellement l'espace de stockage accumulé sur VMFS5 .	Oui	Oui

Tableau 9-3. Comparaison de VMFS5 et de VMFS6 (suite)

Caractéristiques et fonctionnalités	VMFS5	VMFS6
Récupération d'espace à partir du système d'exploitation invité	Limitée	Oui
Partitionnement des périphériques de stockage GPT	Oui	Oui
Partitionnement des périphériques de stockage MBR	Oui Pour une banque de données VMFS5 ayant été précédemment mise à niveau depuis VMFS3.	Non
Périphériques de stockage d'une capacité supérieure à 2 To pour chaque extension VMFS	Oui	Oui
Prise en charge des machines virtuelles à disques virtuels haute capacité ou de disques d'une capacité supérieure à 2 To.	Oui	Oui
Prise en charge des petits fichiers de 1 Ko	Oui	Oui
Utilisation par défaut des mécanismes de verrouillage ATS uniquement sur les périphériques de stockage prenant en charge ATS. Reportez-vous à la section Mécanismes de verrouillage VMFS .	Oui	Oui
Taille du bloc	Standard 1 Mo	Standard 1 Mo
Snapshots par défaut	VMFSsparse pour les disques virtuels d'une capacité inférieure à 2 To. SEsparse pour les disques virtuels d'une capacité supérieure à 2 To.	SEsparse
Type d'émulation de disque virtuel	512n	512n
vMotion	Oui	Oui
Storage vMotion sur différents types de banques de données	Oui	Oui
High Availability et Fault Tolerance	Oui	Oui
DRS et Storage DRS	Oui	Oui
RDM	Oui	Oui

Lorsque vous utilisez des banques de données VMFS, tenez compte des remarques suivantes :

- Extensions de banque de données. Une banque de données VMFS étendue doit uniquement utiliser des périphériques de stockage homogènes, soit 512n, 512e ou 4Kn. La banque de données étendue ne peut pas s'étendre sur des périphériques de formats différents.

- Taille de bloc. La taille de bloc sur une banque de données VMFS définit la taille de fichier maximale et la quantité d'espace qu'occupe un fichier. Les banques de données VMFS5 et VMFS6 prennent en charge la taille de bloc de 1 Mo.
- Storage vMotion. Storage vMotion prend en charge la migration entre les banques de données VMFS, vSAN et Virtual Volumes. vCenter Server effectue des vérifications de compatibilité pour valider Storage vMotion sur différents types de banques de données.
- DRS de stockage. Les banques de données VMFS5 et VMFS6 peuvent coexister dans le même cluster de banques de données. Cependant, toutes les banques de données du cluster doivent utiliser des périphériques de stockage homogènes. Ne mélangez pas des périphériques de différents formats dans le même cluster de banques de données.
- Formats de partition des périphériques. Toute nouvelle banque de données VMFS5 ou VMFS6 utilise la table de partition GUID (GPT, GUID partition table) pour formater le périphérique de stockage. Le format GPT vous permet de créer des banques de données d'une capacité supérieure à 2 To. Si votre banque de données VMFS5 a été précédemment mise à niveau depuis VMFS3, elle continue à utiliser le format de partition MBR (Master Boot Record) qui est caractéristique de VMFS3. La conversion vers GPT survient uniquement lorsque vous agrandissez la banque de données pour lui donner une taille supérieure à 2 To.

Banques de données VMFS comme référentiel

ESXi peut formater des périphériques de stockage SCSI tels que des banques de données VMFS. Les banques de données VMFS servent principalement de référentiel aux machines virtuelles.

Note Ayez toujours une seule banque de données VMFS par LUN.

Vous pouvez stocker plusieurs machines virtuelles sur la même banque de données VMFS. Chaque machine virtuelle, encapsulée dans un ensemble de fichier, occupe un répertoire unique et distinct. Pour le système d'exploitation au sein de la machine virtuelle, VMFS conserve la sémantique du système de fichiers interne, qui garantit un comportement d'application adéquat et une intégrité des données pour les applications s'exécutant dans les machines virtuelles.

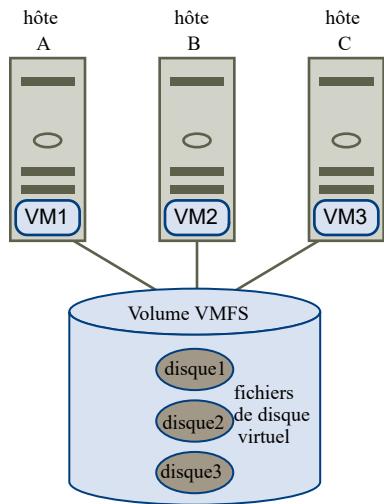
Lorsque vous exécutez plusieurs machines virtuelles, VMFS fournit des mécanismes de verrouillage spécifiques pour les fichiers de machine virtuelle. En conséquence, les machines virtuelles peuvent fonctionner en toute sécurité dans un environnement SAN dans lequel plusieurs hôtes ESXi partagent la même banque de données VMFS.

Outre les machines virtuelles, les banques de données VMFS peuvent stocker d'autres fichiers, tels que des modèles de machine virtuelles et des images ISO.

Partager une banque de données VMFS entre des hôtes

En tant que système de fichiers en cluster, VMFS permet à plusieurs hôtes ESXi d'accéder simultanément à la même banque de données VMFS.

Figure 9-1. Partager une banque de données VMFS entre des hôtes



Pour des informations sur le nombre maximal d'hôtes pouvant se connecter à une banque de données VMFS unique, voir le document *Configurations maximales*.

Pour s'assurer que plusieurs hôtes n'accèdent pas à la même machine virtuelle en même temps, VMFS met en œuvre un verrouillage sur disque.

Le partage du volume VMFS entre plusieurs hôtes offre plusieurs avantages, notamment :

- Vous pouvez utiliser VMware Distributed Resource Scheduling (DRS) et VMware High Availability (HA).

Vous pouvez distribuer des machines virtuelles à travers différents serveurs physiques. Cela signifie que vous exécutez un mélange de machines virtuelles sur chaque serveur de sorte qu'il ne reçoive pas de demandes trop importantes dans la même zone, simultanément. Si un serveur échoue, vous pouvez redémarrer les machines virtuelles sur un autre serveur physique. Si la panne se produit, le verrouillage sur disque pour chaque machine virtuelle est libéré. Pour plus d'informations sur VMware DRS, consultez la documentation *Gestion des ressources vSphere*. Pour plus d'informations sur VMware HA, consultez la documentation *Disponibilité vSphere*.
- Vous pouvez utiliser vMotion pour migrer des machines virtuelles en cours d'exécution depuis un serveur physique vers un autre. Pour obtenir des informations sur la migration de machines virtuelles, reportez-vous à la documentation *Gestion de vCenter Server et des hôtes*.

Pour créer une banque de données partagée, montez la banque de données sur les hôtes ESXi qui nécessitent l'accès à la banque de données. Reportez-vous à la section [Monter des banques de données](#).

Mises à jour des métadonnées VMFS

Une banque de données VMFS contient, entre autres, les fichiers, les répertoires, les liens symboliques, les fichiers descripteurs RDM des machines virtuelles. La banque de données maintient également une vue cohérente de toutes les informations de mappage pour ces objets. Ces informations de mappage sont appelées métadonnées.

Les métadonnées sont mises à jour chaque fois que vous réalisez des opérations de gestion de banque de données ou de machine virtuelle Exemples d'opérations nécessitant une mise à jour des métadonnées :

- Création, agrandissement ou verrouillage d'un fichier de la machine virtuelle
- Modification des attributs d'un fichier
- Démarrage ou arrêt d'une machine virtuelle
- Création ou suppression d'une banque de données VMFS
- Développement d'une banque de données VMFS
- Création d'un modèle
- Déploiement d'une machine virtuelle à partir d'un modèle
- Migration d'une machine virtuelle avec vMotion

Lorsque des modifications sont apportées aux métadonnées dans un environnement de stockage partagé, VMFS utilise des mécanismes de verrouillage spéciaux pour protéger ses données et empêcher plusieurs hôtes d'écrire simultanément sur les métadonnées.

Formats de snapshot sur VMFS

Lorsque vous créez un snapshot, l'état du disque virtuel est préservé, ce qui empêche le système d'exploitation invité d'écrire sur le disque. Un disque delta ou enfant est alors créé. Le disque delta représente la différence entre l'état actuel du disque de machine virtuelle et son état lors de la création du snapshot précédent. Sur la banque de données VMFS, le disque delta est un disque clairsemé.

Les disques clairsemés utilisent le mécanisme de copie sur écriture, dans lequel le disque virtuel ne contient aucune donnée jusqu'à ce que les données y soient copiées par une opération d'écriture. Cette optimisation économise de l'espace de stockage.

Selon le type de votre banque de données, les disques delta utilisent différents formats clairsemés.

Formats de snapshot	VMFS5	VMFS 6
VMFSsparse	Pour les disques virtuels d'une capacité inférieure à 2 To.	S.O.
SEsparse	Pour les disques virtuels d'une capacité supérieure à 2 To.	Pour tous les disques.

VMFSsparse

VMFS5 utilise le format VMFSsparse pour les disques virtuels d'une capacité inférieure à 2 To.

VMFSsparse est mis en œuvre au-dessus de VMFS. La couche VMFSsparse traite les E/S émises vers un snapshot de machine virtuelle. Techniquement, VMFSsparse est un fichier redo-log qui commence vide, immédiatement après la prise d'un snapshot de machine virtuelle. Le fichier redo-log se développe jusqu'à la taille de son vmdk de base, lorsque l'intégralité du vmdk est réécrit avec de nouvelles données après la prise d'un snapshot de machine virtuelle. Ce fichier redo-log est un fichier dans la banque de données VMFS. Lors de la création du snapshot, le vmdk de base attaché à la machine virtuelle est remplacé par le vmdk clairsemé récemment créé.

SEsparse

SEsparse est un format par défaut pour tous les disques delta sur les banques de données VMFS6. Sur VMFS5, SEsparse est utilisé pour les disques virtuels d'une taille égale ou supérieure à 2 To.

SEsparse est un format similaire à VMFSsparse avec certaines améliorations. Ce format utilise l'espace de façon rationnelle et prend en charge la technique de récupération d'espace. Avec la récupération d'espace, les blocs supprimés par le système d'exploitation invité sont marqués. Le système envoie des commandes à la couche SEsparse dans l'hyperviseur pour démapper ces blocs. Ce « démappage » aide à récupérer l'espace alloué par SEsparse une fois que le système d'exploitation invité a supprimé ces données. Pour plus d'informations sur la récupération d'espace, reportez-vous à [Récupération d'espace de stockage](#).

Migration de snapshots

Vous pouvez migrer les machines virtuelles avec des snapshots entre différentes banques de données. Les éléments suivants s'appliquent :

- Si vous migrez une machine virtuelle avec le snapshot VMFSsparse vers VMFS6, le format du snapshot devient SEsparse.
- Lorsqu'une machine virtuelle disposant d'un vmdk d'une taille inférieure à 2 To migre vers VMFS5, le format du snapshot devient VMFSsparse.
- Vous ne pouvez pas mélanger des fichiers redo-log VMFSsparse avec des fichiers redo-log SEsparse dans la même hiérarchie.

Mise à niveau des banques de données VMFS

Vous ne pouvez pas mettre à niveau une banque de données VMFS5 vers VMFS6. Si vous disposez d'une banque de données VMFS5 dans votre environnement, créez une banque de données VMFS6 et migrez les machines virtuelles de la banque de données VMFS5 vers VMFS6.

Création de banques de données

L'assistant Nouvelle banque de données vous permet de créer vos banques de données. Selon le type de votre stockage et vos besoins de stockage, vous pouvez créer une banque de données VMFS, NFS ou Virtual Volumes.

Une banque de données vSAN est automatiquement créée lorsque vous activez vSAN. Pour plus d'informations, reportez-vous à la documentation *Administration de VMware vSAN*.

Vous pouvez également utiliser l'assistant Nouvelle banque de données pour gérer les copies de banque de données VMFS.

- [Créer une banque de données VMFS](#)

Les banques de données VMFS servent de référentiel aux machines virtuelles. Vous pouvez configurer des banques de données VMFS sur tous les périphériques de stockage basés sur SCSI ou NVMe que l'hôte détecte, y compris Fibre Channel, iSCSI et les périphériques de stockage locaux.

- [Créer une banque de données NFS](#)

Vous pouvez utiliser l'assistant **Nouvelle banque de données** pour monter un volume NFS.

- [Créer une banque de données Virtual Volumes](#)

Vous utilisez l'assistant **Nouvelle banque de données** pour créer une banque de données Virtual Volumes.

Créer une banque de données VMFS

Les banques de données VMFS servent de référentiel aux machines virtuelles. Vous pouvez configurer des banques de données VMFS sur tous les périphériques de stockage basés sur SCSI ou NVMe que l'hôte détecte, y compris Fibre Channel, iSCSI et les périphériques de stockage locaux.

Conditions préalables

- 1 Installez et configurez tous les adaptateurs dont votre stockage a besoin.
- 2 Pour découvrir des périphériques de stockage récemment ajoutés, effectuez une réanalyse. Reportez-vous à la section [Réanalyser les opérations de stockage ESXi](#).
- 3 Vérifiez que les périphériques de stockage que vous prévoyez d'utiliser pour vos banques de données sont disponibles. Reportez-vous à la section [Affichage des périphériques de stockage disponibles pour un hôte ESXi](#).

Procédure

- 1 Dans le navigateur d'objets vSphere Client, accédez à un hôte, à un cluster ou à un centre de données.
- 2 Dans le menu contextuel, sélectionnez **Stockage > Nouvelle banque de données**.
- 3 Sélectionnez VMFS comme type de banque de données.
- 4 Entrez un nom de banque de données et, si nécessaire, sélectionnez l'emplacement pour la banque de données.

Le système impose une limite de 42 caractères pour le nom de la banque de données.

- 5 Sélectionnez le périphérique à utiliser pour votre banque de données.

Important Aucune valeur ne doit être affichée dans la colonne Volume du snapshot du périphérique que vous sélectionnez. Si une valeur est présente, le périphérique contient une copie d'une banque de données VMFS existante. Pour plus d'informations sur la gestion des copies de banques de données, consultez [Administration des banques de données VMFS dupliquées](#).

- 6 Spécifiez la version de la banque de données.

Option	Description
VMFS6	Format par défaut sur tous les hôtes qui prennent en charge VMFS6. Les hôtes ESXi de version 6.0 ou antérieures ne peuvent pas reconnaître la banque de données VMFS6.
VMFS5	La banque de données VMFS5 prend en charge l'accès par les hôtes ESXi de version 6.7 ou de version antérieure.

- 7 Définissez les détails de configuration de la banque de données.

Note La taille minimale requise pour une banque de données VMFS6 est de 2 Go.

- a Spécifiez la configuration de partition.

Option	Description
Utilisez toutes les partitions disponibles	Dédie la totalité du disque à une seule banque de données VMFS. Si vous sélectionnez cette option, tous les systèmes de fichiers et données stockés actuellement sur ce périphérique sont détruits.
Utilisez l'espace libre	Déploie une banque de données VMFS dans l'espace libre restant du disque.

- b Si vous jugez que l'espace alloué pour la banque de données est excessif, ajustez les valeurs de capacité dans le champ Taille de la banque de données.
Par défaut, tout l'espace libre sur le périphérique de stockage est alloué.
- c Pour VMFS6, spécifiez la taille de bloc et définissez les paramètres de récupération d'espace. Reportez-vous à la section [Récupération d'espace sur les banques de données VMFS](#).
- 8 Sur la page Prêt à terminer, passez en revue les informations de configuration de banque de données et cliquez sur **Terminer**.

Résultats

La banque de données sur le périphérique de stockage basé sur SCSI ou NVMe est créée. Elle est disponible pour tous les hôtes qui ont accès au périphérique.

Étape suivante

Après avoir créé la banque de données VMFS, vous pouvez effectuer les tâches suivantes :

- Modifier la capacité de la banque de données. Reportez-vous à la section [Augmenter la capacité d'une banque de données VMFS](#).
- Modifie les paramètres de récupération d'espace. Reportez-vous à la section [Configurer la récupération fixe pour la banque de données VMFS6 existante](#).
- Activer la prise en charge de vmdk partagé. Reportez-vous à la section [Configurer les paramètres des disques virtuels en cluster sur la banque de données VMFS6](#).

Créer une banque de données NFS

Vous pouvez utiliser l'assistant **Nouvelle banque de données** pour monter un volume NFS.

Conditions préalables

- Configurez l'environnement de stockage NFS.
- Si vous prévoyez d'utiliser l'authentification Kerberos avec la banque de données NFS 4.1, configurez les hôtes ESXi pour l'authentification Kerberos.
- Si vous prévoyez d'isoler le trafic NFS 3 sur un adaptateur VMkernel spécifique que vous connectez à la banque de données, créez et configurez l'adaptateur VMkernel sur la pile TCP/IP par défaut. Pour plus d'informations, consultez [Configurer la liaison VMkernel pour la banque de données NFS 3](#).

Procédure

- 1 Dans le navigateur d'objets vSphere Client, accédez à un hôte, à un cluster ou à un centre de données.
- 2 Dans le menu contextuel, sélectionnez **Stockage > Nouvelle banque de données**.
- 3 Sélectionnez NFS comme type de banque de données et spécifiez une version de NFS.
 - NFS 3
 - NFS 4.1

Important Si plusieurs hôtes accèdent à la même banque de données, vous devez utiliser le même protocole sur tous les hôtes.

- 4 Entrez les paramètres de banque de données.

Option	Description
Nom de la banque de données	Le système impose une limite de 42 caractères pour le nom de la banque de données.
Dossier	Nom du dossier du point de montage
Server	Nom du serveur ou adresse IP. Vous pouvez utiliser les formats IPv6 ou IPv4. Avec NFS 4.1, vous pouvez ajouter plusieurs adresses IP ou noms de serveur si le serveur NFS prend en charge la jonction. L'hôte ESXi utilise ces valeurs pour assurer la gestion de gestion multivoie sur le point de montage du serveur NFS.

- 5 Sélectionnez **Montage NFS lecture seule** si le volume est exporté en Lecture seule par le serveur NFS.
- 6 Pour connecter la banque de données NFS 3 à un adaptateur VMkernel spécifique, sélectionnez **Lier à vmknic**. Pour plus d'informations, consultez [Configurer la liaison VMkernel pour la banque de données NFS 3](#).

Note Seules les banques de données NFS 3 prennent en charge les connexions aux adaptateurs VMkernel.

- 7 Pour utiliser la sécurité Kerberos avec NFS 4.1, activez Kerberos et sélectionnez un modèle Kerberos approprié.

Option	Description
Utilisez Kerberos pour l'authentification uniquement (krb5)	Prend en charge la vérification d'identité
Utilisez Kerberos pour l'authentification et l'intégrité des données (krb5i)	Outre la vérification d'identité, il fournit des services d'intégrité des données. Ces services permettent de protéger le trafic NFS contre la falsification en vérifiant les modifications potentielles des paquets de données.

Si vous n'activez pas Kerberos, la banque de données utilise la sécurité AUTH_SYS par défaut.

- 8 Si vous créez une banque de données au niveau du centre de données ou du cluster, sélectionnez les hôtes qui assurent le montage de la banque de données.
- 9 Passez en revue les options de configuration puis cliquez sur **Terminer**.

Créer une banque de données Virtual Volumes

Vous utilisez l'assistant **Nouvelle banque de données** pour créer une banque de données Virtual Volumes.

Procédure

- 1 Dans le navigateur d'objets vSphere Client, accédez à un hôte, à un cluster ou à un centre de données.

- 2 Dans le menu contextuel, sélectionnez **Stockage > Nouvelle banque de données**.
- 3 Sélectionnez **vVol** comme type de banque de données.
- 4 Entrez le nom de la banque de données et sélectionnez un conteneur de stockage de sauvegarde dans la liste des conteneurs de stockage.

Assurez-vous d'utiliser un nom qui ne correspond pas à celui d'une autre banque de données de l'environnement de votre centre de données.

Si vous montez la même banque de données Virtual Volumes sur plusieurs hôtes, le nom de la banque de données doit être le même sur tous les hôtes.

- 5 Sélectionnez les hôtes qui exigent un accès à la banque de données.
- 6 Passez en revue les options de configuration puis cliquez sur **Terminer**.

Étape suivante

Après avoir créé la banque de données Virtual Volumes, vous pouvez effectuer les tâches suivantes :

- Renommer la banque de données, parcourir les fichiers de la banque de données, démonter la banque de données, etc. Reportez-vous à la section [Opérations administratives de base pour les banques de données](#).
-
- Note** Vous ne pouvez pas ajouter la banque de données Virtual Volumes à un cluster de banques de données.
-
- Provisionnez des machines virtuelles sur la banque de données Virtual Volumes. Reportez-vous à la documentation [Provisionner des machines virtuelles sur des banques de données Virtual Volumes](#) et [Administration d'une machine virtuelle vSphere](#).

Opérations administratives de base pour les banques de données

Après la création de banques de données, vous pouvez effectuer plusieurs opérations administratives sur les banques de données. Certaines opérations, telles que le changement de nom d'une banque de données, sont disponibles pour tous les types de banques de données. D'autres s'appliquent à des types spécifiques de banques de données.

Modifier le nom d'une banque de données

Utilisez vSphere Client pour modifier le nom d'une banque de données existante. Vous pouvez renommer la banque de données sur laquelle s'exécutent des machines virtuelles sans aucune incidence négative.

Note Si l'hôte est géré par vCenter Server, vous ne pouvez pas renommer la banque de données en accédant directement à l'hôte à partir de VMware Host Client. Vous devez renommer la banque de données depuis vCenter Server.

Procédure

- 1 Dans vSphere Client, accédez à la banque de données.
- 2 Cliquez avec le bouton droit sur la banque de données à renommer, puis sélectionnez **Renommer**.
- 3 Entrez un nouveau nom de banque de données.

Le système impose une limite de 42 caractères pour le nom de la banque de données.

Résultats

Le nouveau nom s'affiche sur tous les hôtes ayant accès à la banque de données.

Démontage des banques de données

Quand vous démontez une banque de données, il reste intact, mais ne peut être vu des hôtes que vous spécifiez. La banque de données continue d'apparaître sur les autres hôtes, où elle reste montée.

N'exécutez aucune opération de configuration qui puisse générer des E/S vers la banque de données lorsque le démontage est en cours.

Note Assurez-vous que la banque de données n'est pas utilisée par le signal de pulsation vSphere HA. Le signal de pulsation vSphere HA ne vous empêche pas de démonter la banque de données. Toutefois, si la banque de données est utilisée pour le signal de pulsation, son démontage peut provoquer la défaillance de l'hôte et le redémarrage de toutes les machines virtuelles actives.

Conditions préalables

Le cas échéant, avant de démonter les banques de données, assurez-vous que les conditions requises suivantes sont remplies :

- Aucune machine virtuelle ne doit se trouver dans la banque de données
- La fonctionnalité Storage DRS ne gère pas la banque de données.
- Storage I/O Control est désactivé pour cette banque de données.

Procédure

- 1 Dans vSphere Client, accédez à la banque de données.
- 2 Cliquez avec le bouton droit sur la banque de données et sélectionnez **Démonter la banque de données**.
- 3 Si la banque de données est partagée, sélectionnez les hôtes à partir desquels vous voulez démonter la banque de données.
- 4 Confirmez que vous voulez démonter la banque de données.

Résultats

Dès qu'une banque de données VMFS est démontée de tous les hôtes, elle est marquée comme étant inactive. Si vous démontez une banque de données NFS ou une banque de données Virtual Volumes de tous les hôtes, la banque de données ne figure plus dans l'inventaire. Vous pouvez monter la banque de données VMFS démontée. Pour monter la banque de données NFS ou Virtual Volumes qui a été supprimée de l'inventaire, utilisez l'assistant Nouvelle banque de données.

Étape suivante

Si vous avez démonté la banque de données VMFS dans le cadre d'une procédure de retrait, vous pouvez à présent déconnecter le périphérique de stockage assurant la sauvegarde de la banque de données. Reportez-vous à la section [Déconnexion des périphériques de stockage](#).

Monter des banques de données

Vous pouvez monter une banque de données que vous avez précédemment démontée. Vous pouvez également monter une banque de données sur des hôtes supplémentaires, afin qu'elle devienne une banque de données partagée.

Une banque de données VMFS qui a été démontée de tous les hôtes demeure dans l'inventaire, mais elle est marquée comme étant inaccessible. Reportez-vous à la section [Démontage des banques de données](#).

Vous pouvez utiliser cette tâche pour monter la banque de données VMFS sur un hôte spécifié ou sur plusieurs hôtes.

Si vous avez démonté une banque de données NFS ou une banque de données Virtual Volumes de tous les hôtes, la banque de données ne figure plus dans l'inventaire. Pour monter la banque de données NFS ou Virtual Volumes qui a été supprimée de l'inventaire, utilisez l'assistant Nouvelle banque de données.

Une banque de donnée de n'importe quel type qui est démontée de certains hôtes tout en étant montée sur d'autres est affichée comme étant active dans l'inventaire.

Procédure

- 1 Dans vSphere Client, accédez à la banque de données.
- 2 Cliquez avec le bouton droit sur la banque de données à monter et sélectionnez l'une des options suivantes :

- **Monter une banque de données**
- **Monter la banque de données sur des hôtes supplémentaires**

Vous pouvez également sélectionner l'option de liaison VMkernel pour la banque de données requise. Pour plus d'informations, consultez l'étape g sous [Configurer la liaison VMkernel pour la banque de données NFS 3](#).

Selon le type de banque de données que vous utilisez, une option ou une autre s'affiche.

- 3 Sélectionnez les hôtes qui doivent accéder à la banque de données et cliquez sur **OK**.
- 4 Pour répertorier tous les hôtes qui partagent la banque de données, accédez à la banque de données, puis cliquez sur l'onglet **Hôtes**.

Supprimer des banques de données VMFS

Vous pouvez supprimer n'importe quel type de banque de données VMFS, y compris les copies que vous avez montées sans nouvelle signature. Quand vous supprimez une banque de données, elle est détruite et disparaît de tous les hôtes qui y ont accès.

Note L'opération de suppression de la banque de données supprime définitivement tous les fichiers associés aux machines virtuelles de la banque de données. Bien que vous puissiez supprimer la banque de données sans la démonter, il est préférable de la démonter au préalable.

Conditions préalables

- Supprimez ou migrez toutes les machines virtuelles de la banque de données.
- Démontez la banque de données de tous les hôtes.
- Désactivez Storage DRS pour la banque de données.
- Désactivez Storage I/O Control pour la banque de données.
- Assurez-vous que la banque de données n'est pas utilisée pour le signal de pulsation vSphere HA.

Procédure

- 1 Dans vSphere Client, accédez à la banque de données.
- 2 Cliquez avec le bouton droit sur la banque de données à supprimer et sélectionnez **Supprimer la banque de données**.
- 3 Confirmez que vous souhaitez supprimer la banque de données.

Utilisation du navigateur de banque de données

Utilisez l'explorateur de fichiers de banque de données de votre environnement vSphere pour gérer le contenu de vos banques de données.

Accéder au navigateur de banque de données

Accédez à votre banque de données pour parcourir les dossiers et les fichiers qui y sont stockés et effectuer des tâches administratives sur vos dossiers et fichiers.

Procédure

- 1 Ouvrez le navigateur de banque de données.
 - a Affichez la banque de données dans l'inventaire.
 - b Cliquez avec le bouton droit sur la banque de données et sélectionnez **Parcourir les fichiers**.
- 2 Explorez le contenu de la banque de données en accédant aux dossiers et aux fichiers existants.
- 3 Effectuez des tâches administratives en utilisant les icônes et les options.

Icônes et options	Descriptions
Télécharger des fichiers	Télécharger un fichier vers la banque de données.
Télécharger un dossier (disponible uniquement dans vSphere Client)	Télécharger un dossier vers la banque de données.
Télécharger	Télécharger depuis la banque de données.
Nouveau dossier	Créer un dossier sur la banque de données.
Copier dans	Copier les dossiers ou les fichiers sélectionnés dans un nouvel emplacement, dans la même banque de données ou dans une autre.
Déplacer vers	Déplacer les dossiers ou les fichiers sélectionnées vers un nouvel emplacement, dans la même banque de données ou dans une autre.
Remplacer le nom par	Renommer les fichiers sélectionnés.
Supprimer	Supprimer les dossiers ou les fichiers sélectionnés.
Gonfler	Convertir un disque virtuel dynamique sélectionné en disque virtuel statique. Cette option s'applique uniquement aux disques à provisionnement dynamique.

Télécharger des fichiers ou des dossiers vers des banques de données

Utilisez l'explorateur de banques de données pour télécharger les fichiers vers les banques de données sur l'hôte ESXi. Si vous utilisez vSphere Client, vous pouvez également télécharger les dossiers.

En plus de leur utilisation classique de stockage de fichiers pour les machines virtuelles, les banques de données peuvent stocker des données ou des fichiers liés aux machines virtuelles. Par exemple, vous pouvez télécharger des images ISO de systèmes d'exploitation depuis un ordinateur local vers une banque de données sur l'hôte. Vous pouvez ensuite utiliser ces images pour installer des systèmes d'exploitation invités sur les nouvelles machines virtuelles.

Note Vous ne pouvez pas télécharger les fichiers directement dans les banques de données Virtual Volumes. Vous devez préalablement créer un dossier dans la banque de données Virtual Volumes, puis télécharger les fichiers dans ce dossier. Les dossiers créés dans les banques de données Virtual Volumes pour le stockage des blocs ont un espace de capacité de stockage limité à 4 Go. La banque de données Virtual Volumes prend en charge les téléchargements directs de dossiers.

Conditions préalables

Privilège nécessaire : **Banque de données.Parcourir la banque de donnée**

Procédure

- 1 Ouvrez le navigateur de banque de données.
 - a Affichez la banque de données dans l'inventaire.
 - b Cliquez avec le bouton droit sur la banque de données et sélectionnez **Parcourir les fichiers**.
- 2 (Facultatif) Créez un dossier où enregistrer le fichier ou le dossier.
- 3 Téléchargez le fichier ou le dossier.

Option	Description
Télécharger un fichier	<ol style="list-style-type: none"> a Sélectionnez le dossier cible et cliquez sur Télécharger des fichiers. b Localisez l'élément à télécharger sur l'ordinateur local, puis cliquez sur Ouvrir.
Télécharger un dossier (disponible uniquement dans vSphere Client)	<ol style="list-style-type: none"> a Sélectionnez la banque de données ou le dossier cible et cliquez sur Télécharger des dossiers. b Localisez l'élément à télécharger sur l'ordinateur local, puis cliquez sur Ok.

- 4 Actualisez l'explorateur de fichiers de la banque de données pour afficher les fichiers ou les dossiers téléchargés dans la liste.

Étape suivante

Vous pouvez rencontrer des problèmes lors du déploiement d'un modèle OVF précédemment exporté, puis téléchargé dans une banque de données. Pour plus d'informations et chercher une solution, consultez l'article [2117310](#) de la base de connaissances VMware.

Télécharger des fichiers à partir de banques de données

Utilisez l'explorateur de fichiers de la banque de données pour télécharger sur votre ordinateur local des fichiers de la banque de données accessibles sur votre hôte ESXi.

Conditions préalables

- Privilège nécessaire : **Banque de données.Parcourir la banque de donnée**
- Privilèges lorsqu'une machine virtuelle est chiffrée : **Opérations de chiffrement.Déchiffrer et Opérations de chiffrement.Accès direct**

Procédure

- 1 Ouvrez le navigateur de banque de données.
 - a Affichez la banque de données dans l'inventaire.
 - b Cliquez avec le bouton droit sur la banque de données et sélectionnez **Parcourir les fichiers**.
- 2 Accédez au fichier à télécharger et cliquez sur **Télécharger**.
- 3 Suivez les invites pour enregistrer le fichier sur votre ordinateur local.

Renommer les fichiers de banque de données

Utilisez le navigateur de la banque de données pour renommer des fichiers.

Conditions préalables

Privilège nécessaire : **Banque de données.Parcourir la banque de donnée**

Procédure

- 1 Ouvrez le navigateur de banque de données.
 - a Affichez la banque de données dans l'inventaire.
 - b Cliquez avec le bouton droit sur la banque de données et sélectionnez **Parcourir les fichiers**.
- 2 Accédez à un fichier à renommer.
- 3 Sélectionnez le fichier et cliquez sur **Renommer à**.
- 4 Spécifiez le nouveau nom et cliquez sur **OK**.

Déplacer ou copier des dossiers de banque de données ou des fichiers

Utilisez le navigateur de banque de données pour déplacer ou copier des dossiers et des fichiers vers un nouvel emplacement, sur la même banque de données ou sur une autre.

Note Les fichiers de disque virtuel sont déplacés ou copiés sans conversion de format. Si vous déplacez un disque virtuel vers une banque de données qui appartient à un hôte différent de l'hôte source, vous devrez éventuellement convertir le disque virtuel. Sinon, vous ne pourrez peut-être pas utiliser le disque.

Impossible de copier les fichiers de VM d'un serveur vCenter Server à un autre.

Conditions préalables

Privilège nécessaire : **Banque de données.Parcourir la banque de donnée**

Procédure

- 1 Ouvrez le navigateur de banque de données.
 - a Affichez la banque de données dans l'inventaire.
 - b Cliquez avec le bouton droit sur la banque de données et sélectionnez **Parcourir les fichiers**.
- 2 Recherchez un objet à déplacer ou à copier, un dossier ou un fichier.
- 3 Sélectionnez l'objet et cliquez sur **Déplacer vers** ou **Copier vers**.
- 4 Spécifiez l'emplacement de destination.
- 5 (Facultatif) Sélectionnez **Remplacez les fichiers et les dossiers dotés de noms identiques dans la destination**.
- 6 Cliquez sur **OK**.

Gonfler les disques virtuels dynamiques

Vous pouvez transformer un disque virtuel que vous avez créé au format dynamique en disque virtuel statique.

Pour gonfler le disque virtuel dynamique, vous devez utiliser le navigateur de banque de données.

Conditions préalables

- Assurez-vous que la banque de données sur laquelle réside la machine virtuelle offre suffisamment d'espace.
- Assurez-vous que le disque virtuel est dynamique.
- Supprimez les snapshots.
- Mettez la machine virtuelle hors tension.

Procédure

- 1 Dans vSphere Client, accédez au dossier du disque virtuel que vous souhaitez gonfler.
 - a Accédez à la machine virtuelle.
 - b Cliquez sur l'onglet **Banques de données**.
La banque de données sélectionnée stockant les fichiers de machine virtuelle est répertoriée.
 - c Cliquez avec le bouton droit sur la banque de données et sélectionnez **Parcourir les fichiers**.
Le navigateur de banque de données affiche le contenu de la banque de données.
- 2 Développez le dossier de la machine virtuelle et accédez au fichier de disque virtuel que vous voulez convertir.
Le fichier possède l'extension `.vmdk` et est marqué de l'icône de disque virtuel ().
- 3 Sélectionnez le fichier de disque virtuel et cliquez sur **Gonfler**.

Note L'option n'est peut-être pas disponible si le disque virtuel est dynamique ou lorsque la machine virtuelle est en cours d'exécution.

Résultats

Le disque virtuel gonflé occupe la totalité de l'espace de banque de données qui lui a été affecté à l'origine.

Gestion des banques de données VMFS

Après avoir créé une banque de données VMFS dans votre environnement vSphere, vous pouvez effectuer des tâches telles que l'extension de la banque de données, la gestion des banques de données en double ou la collecte d'informations de diagnostic de banque de données.

Pour obtenir des informations générales sur les banques Concepts de banque de données VMFS de données VMFS, consultez .

Pour créer une banque de données VMFS et effectuer des opérations de base, reportez-vous aux rubriques suivantes :

- [Créer une banque de données VMFS](#)
- [Opérations administratives de base pour les banques de données](#)

Mécanismes de verrouillage VMFS

Dans un environnement de stockage partagé, lorsque plusieurs hôtes accèdent à la même banque de données VMFS, des mécanismes de verrouillage spécifiques sont utilisés.

Ces mécanismes de verrouillage empêchent plusieurs hôtes d'écrire simultanément sur les métadonnées et évitent la corruption des données.

Selon sa configuration et le type de stockage sous-jacent, une banque de données VMFS peut utiliser différents types de mécanismes de verrouillage. Elle peut exclusivement utiliser le mécanisme de verrouillage ATS (atomic test and set) (ATS-only), ou utiliser une combinaison de réservations ATS et SCSI (ATS+SCSI).

Mécanisme ATS uniquement

Pour les périphériques de stockage prenant en charge les spécifications de VAAI basées sur les normes T10, VMFS fournit un verrouillage ATS également appelé verrouillage par assistance matérielle. L'algorithme ATS prend en charge le verrouillage discret par secteur de disque. Toutes les banques de données VMFS5 et VMFS6 récemment formatées utilisent le mécanisme ATS uniquement si le stockage sous-jacent le prend en charge ; elles n'utilisent jamais les réservations SCSI.

Lorsque vous créez une banque de données à plusieurs extensions utilisant ATS, vCenter Server exclut les périphériques non ATS. Ce filtrage vous permet d'utiliser uniquement les périphériques prenant en charge la primitive ATS.

Dans certains cas, vous devrez peut-être modifier le mécanisme de verrouillage par défaut d'une banque de données VMFS5 ou VMFS6. Pour plus d'informations, consultez [Modification du mécanisme de verrouillage à ATS+SCSI](#).

Note Si vous exécutez un environnement VMware vSAN ou que vous disposez de volumes VMFS uniquement ATS, ne désactivez pas ATS. La désactivation d'ATS peut entraîner une panne, car aucun mécanisme de verrouillage n'est disponible. Pour plus d'informations, reportez-vous à [l'article de la base de connaissances VMware](#).

Mécanisme ATS+SCSI

Une banque de données VMFS prenant en charge le mécanisme ATS+SCSI est configurée pour utiliser l'ATS et tente de s'en servir lorsque cela est possible. Si l'ATS échoue, la banque de données VMFS rétablit les réservations SCSI. Contrairement au verrouillage ATS, les réservations SCSI verrouillent l'intégralité d'un périphérique de stockage lorsqu'une opération nécessitant une protection des métadonnées est effectuée. Une fois l'opération terminée, VMFS libère la réservation et les autres opérations peuvent se poursuivre.

Les banques de données utilisant le mécanisme ATS+SCSI incluent les magasins de données VMFS5 ayant fait l'objet d'une mise à niveau à partir de VMFS3. En outre, les nouvelles banques de données VMFS5 ou VMFS6 sur périphériques de stockage ne prenant pas en charge ATS utilisent le mécanisme ATS+SCSI.

Si la banque de données VMFS revient à des réservations SCSI, vous remarquerez peut-être une dégradation des performances causée par des réservations SCSI excessives.

Afficher les informations sur le verrouillage VMFS

Utilisez la commande `esxcli` pour obtenir des informations sur le mécanisme de verrouillage utilisé par une banque de données VMFS.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Pour afficher des informations relatives aux mécanismes de verrouillage VMFS, exécutez la commande suivante :

```
esxcli storage vmfs lockmode list
```

Résultats

Le tableau répertorie les éléments que vous pouvez obtenir en sortie de la commande.

Tableau 9-4. Informations sur le verrouillage VMFS

Champs	Valeurs	Descriptions
Modes de verrouillage		Indique la configuration de verrouillage de la banque de données.
	ATS	La banque de données est configurée pour utiliser le mode de verrouillage ATS uniquement.
	ATS+SCSI	La banque de données est configurée pour utiliser le mode ATS. Si ATS échoue ou n'est pas pris en charge, la banque de données peut revenir à SCSI.
	ATS upgrade pending	La banque de données est en cours de mise à niveau en ligne vers le mode ATS uniquement.
	ATS downgrade pending	La banque de données est en cours de mise à niveau en ligne vers le mode antérieur à ATS, c'est-à-dire le mode ATS+SCSI.
Compatible avec ATS		Indique si la banque de données peut être configurée ou non pour le mode ATS uniquement.
Modes de mise à niveau d'ATS		Indique le type de mise à niveau pris en charge par la banque de données.
	None	La banque de données n'est pas compatible avec le mode ATS uniquement.

Tableau 9-4. Informations sur le verrouillage VMFS (suite)

Champs	Valeurs	Descriptions
	Online	La banque de données peut être utilisée pendant sa mise à niveau vers le mode ATS uniquement.
	Offline	La banque de données ne peut pas être utilisée pendant sa mise à niveau vers le mode ATS uniquement.
Raison d'incompatibilité avec ATS		Si la banque de données n'est pas compatible avec le mode ATS uniquement, l'élément indique la raison de l'incompatibilité.

Mécanisme de verrouillage ATS uniquement pour VMFS

Si vos banques de données VMFS utilisent le mécanisme de verrouillage ATS+SCSI, vous pouvez opter pour le verrouillage ATS uniquement.

Généralement, les banques de données VMFS5 qui ont précédemment été mises à niveau à partir de VMFS3 continuent à utiliser le mécanisme de verrouillage ATS+SCSI. Si les banques de données sont déployées sur un matériel compatible ATS, elles remplissent les conditions requises pour une mise à niveau vers le verrouillage ATS uniquement. Selon votre environnement vSphere, vous pouvez utiliser l'un des modes de mise à niveau suivants :

- La mise à niveau en ligne vers le mécanisme ATS uniquement est disponible pour la plupart des banques de données VMFS5 à extension unique. Pendant que vous effectuez la mise à niveau en ligne sur l'un des hôtes, les autres hôtes peuvent continuer à utiliser la banque de données.
- La mise à niveau hors-ligne vers ATS uniquement doit être utilisée pour les banques de données VMFS5 qui couvrent plusieurs extensions physiques. Les banques de données composées de plusieurs extensions ne remplissent pas les conditions requises pour la mise à niveau en ligne. Ces banques de données exigent qu'aucun hôte n'utilise activement les banques de données au moment de la demande de mise à niveau.

Se préparer à une mise à niveau vers le verrouillage ATS uniquement

Vous devez effectuer plusieurs opérations pour préparer votre environnement pour une mise à niveau en ligne ou hors ligne vers le verrouillage ATS uniquement.

Procédure

- 1 Mettez à niveau vers la toute dernière version de vSphere tous les hôtes qui accèdent à la banque de données VMFS5.

- 2** Déterminez si la banque de données est éligible à une mise à niveau de son mécanisme de verrouillage actuel en exécutant la commande `esxcli storage vmfs lockmode list`.

L'exemple de sortie suivant indique que la banque de données est éligible à une mise à niveau. Il indique également le mécanisme de verrouillage actuel et le mode de mise à niveau disponible pour la banque de données.

Locking Mode	ATS Compatible	ATS Upgrade Modes
ATS+SCSI	true	Online or Offline

- 3** Selon le mode de mise à niveau disponible pour la banque de données, effectuez l'une des actions suivantes :

Mode de mise à niveau	Action
En ligne	Vérifiez que tous les hôtes disposent d'une connectivité de stockage cohérente à la banque de données VMFS.
Hors ligne	Vérifiez qu'aucun hôte n'utilise activement la banque de données.

Mettre à niveau le mécanisme de verrouillage vers le mode ATS uniquement

Si une banque de données VMFS est compatible avec le mode ATS uniquement, vous pouvez mettre à niveau son mécanisme de verrouillage du mode ATS+SCSI vers le mode ATS uniquement.

La plupart des banques de données qui ne s'étendent pas sur plusieurs extensions sont éligibles pour une mise à niveau en ligne. Lorsque vous réalisez la mise à niveau en ligne sur l'un des hôtes ESXi, d'autres hôtes peuvent continuer d'utiliser la banque de données. La mise à niveau en ligne s'achève uniquement une fois que tous les hôtes ont fermé la banque de données.

Conditions préalables

Si vous prévoyez de terminer la mise à niveau du mécanisme de verrouillage en mettant la banque de données en mode maintenance, désactivez Storage DRS. Ce prérequis s'applique uniquement pour les mises à niveau en ligne.

Procédure

- 1** Mettez à niveau le mécanisme de verrouillage en exécutant la commande suivante :

```
esxcli storage vmfs lockmode set -a|--ats -l|--volume-label= VMFS label -u|--volume-uuid= VMFS UUID.
```

- 2 Pour une mise à niveau en ligne, vous devez effectuer des étapes supplémentaires.
 - a Fermez la banque de données sur tous les hôtes qui ont accès à la banque de données afin qu'ils soient en mesure de détecter le changement.
Vous pouvez utiliser l'une des méthodes suivantes :
 - Démontez, puis montez la banque de données.
 - Mettez la banque de données en mode de maintenance mode, puis quittez le mode de maintenance.
 - b Vérifiez que le mode de verrouillage de la banque de données est désormais défini sur ATS uniquement. Pour ce faire, exécutez la commande suivante :

```
esxcli storage vmfs lockmode list
```
 - c Si le mode de verrouillage est défini sur un autre état (Mise à niveau vers ATS en attente, par exemple), déterminez quel hôte n'a pas encore effectué la mise à niveau en exécutant la commande suivante :

```
esxcli storage vmfs host list
```

Modification du mécanisme de verrouillage à ATS+SCSI

Lorsque vous créez une banque de données VMFS5 sur un périphérique qui prend en charge le verrouillage ATS (atomic test and set), la banque de données utilise le mécanisme de verrouillage ATS uniquement. Dans certaines circonstances, il peut s'avérer nécessaire de rétrograder le verrouillage ATS uniquement vers ATS+SCSI.

Il se peut que vous deviez basculer vers le mécanisme de verrouillage ATS+SCSI lorsque, par exemple, votre périphérique de stockage est rétrogradé. Ou bien, lorsque des mises à jour du programme échouent et que le périphérique ne prend plus en charge ATS.

Le processus mis en œuvre pour rétrograder vers ATS+SCSI est similaire au processus de mise à niveau du verrouillage ATS uniquement. De même que pour la mise à niveau, selon votre configuration de stockage, vous pouvez rétrograder en mode en ligne ou hors ligne.

Note Si vous exécutez un environnement VMware vSAN ou que vous disposez de volumes VMFS uniquement ATS, ne désactivez pas ATS. La désactivation d'ATS peut entraîner une panne, car aucun mécanisme de verrouillage n'est disponible. Pour plus d'informations, reportez-vous à l'article de la base de connaissances VMware.

Procédure

- 1 Pour basculer vers le mécanisme de verrouillage ATS+SCSI, exécutez la commande suivante :

```
esxcli storage vmfs lockmode set -s|--scsi -l|--volume-label= VMFS label
-u|--volume-uuid= VMFS UUID.
```
- 2 Pour le mode en ligne, fermez la banque de données sur tous les hôtes qui ont accès à la banque de données afin qu'ils soient en mesure de détecter le changement.

Administration des banques de données VMFS dupliquées

Lorsqu'un périphérique de stockage contient une copie de banque de données VMFS, vous pouvez monter la banque de données avec sa signature existante ou lui assigner une nouvelle signature.

Chaque banque de données VMFS créée sur un périphérique de stockage a une signature unique, appelée UUID, qui est stockée dans le super-bloc de système de fichiers. Lorsque le périphérique de stockage est répliqué ou que son snapshot est pris côté baie, la copie résultante du périphérique est identique, octet par octet, au périphérique d'origine. Par exemple, si le périphérique de stockage d'origine contient une banque de données VMFS avec UUUIDX, la copie semble contenir une copie de la banque de données ayant le même UUUIDX.

En plus des snapshots des LUN et des réplications, certaines opérations de périphérique, telles que les modifications de l'ID de LUN, peuvent produire une copie de la banque de données d'origine.

ESXi peut détecter la copie de banque de données VMFS. Vous pouvez monter la copie de la banque de données avec son UUID d'origine ou changer l'UUID. Le processus de modification de l'UUID est appelé la resignature de la banque de données.

Que vous ayez choisi de resigner ou de monter sans resigner dépend de la manière dont les LUN sont masqués dans l'environnement de stockage. Si vos hôtes peuvent voir les deux copies du LUN, alors la resignature est la méthode optimale.

Conservation de la signature de banque de données existante

Si vous n'avez pas à resigner la copie d'une banque de données VMFS, vous pouvez la monter sans changer sa signature.

Vous pouvez conserver la signature si, par exemple, vous maintenez des copies synchronisées de machines virtuelles sur un site secondaire, dans le contexte d'un plan de récupération après sinistre. En cas de sinistre sur le site primaire, vous pouvez monter la copie de banque de données et démarrer les machines virtuelles sur le site secondaire.

Resignature de la copie de banque de données VMFS

Utilisez la resignature de banque de données si vous voulez conserver les données stockées dans la copie de banque de données VMFS.

Lors d'une resignature de copie VMFS, ESXi assigne une nouvelle signature (UUID) à la copie, et la monte en tant que banque de données distincte de l'original. Toutes les références à la signature originale des fichiers de configuration de la machine virtuelle sont mises à jour.

Lorsque vous effectuez une resignature de banque de données, prenez en compte les points suivants :

- La resignature d'une banque de données est irréversible.
- Après resignature, la réplique du périphérique de stockage qui contenait la copie VMFS ne sera plus traitée comme une réplique.

- Une banque de données éparpillée ne peut être resignée que si toutes ses parties sont en ligne.
- Le processus de resignature est tolérant aux pannes. Si le processus est interrompu, vous pourrez le reprendre plus tard.
- Vous pouvez monter la nouvelle banque de données VMFS sans risque de conflit entre son UUID et les UUID de toute autre banque de données depuis la hiérarchie des snapshots du périphérique.

Monter une copie de banque de données VMFS

Utilisez la resignature de banque de données si vous voulez conserver les données stockées dans la copie de banque de données VMFS. Si vous n'avez pas à resigner la copie d'une banque de données VMFS, vous pouvez la monter sans modifier sa signature.

Conditions préalables

- Effectuez une nouvelle analyse de stockage de votre hôte pour qu'il mette à jour l'affichage des périphériques de stockage présentés à l'hôte.
- Démontez la banque de données VMFS d'origine possédant le même UUID que la copie que vous envisagez de monter. Vous ne pouvez monter une copie de banque de données VMFS que si elle n'entre pas en conflit avec la banque de données VMFS d'origine.

Procédure

- 1 Dans le navigateur d'objets vSphere Client, accédez à un hôte, à un cluster ou à un centre de données.
- 2 Dans le menu contextuel, sélectionnez **Stockage > Nouvelle banque de données**.
- 3 Sélectionnez VMFS comme type de banque de données.
- 4 Entrez un nom de banque de données et, si nécessaire, sélectionnez l'emplacement pour la banque de données.
- 5 À partir de la liste des périphériques de stockage, sélectionnez le périphérique qui a une valeur spécifique affichée dans la colonne Volume du snapshot.
Le nom présent dans la colonne Volume du snapshot indique que le périphérique est une copie contenant une copie d'une banque de données VMFS existante.
- 6 Montez la banque de données.

Option	Description
Monter avec resignature	Dans Options de montage , sélectionnez Attribuer nouvelle signature et cliquez sur Suivant .
Monter sans resignature	Dans Options de montage, sélectionnez Garder signature existante .

- 7 Passez en revue les informations de configuration de la banque de données et cliquez sur **Terminer**.

Augmenter la capacité d'une banque de données VMFS

Vous pouvez augmenter la capacité d'une banque de données VMFS. Des capacités supplémentaires peuvent être nécessaires lorsque vous ajoutez des machines virtuelles à une banque de données ou lorsque les machines virtuelles qui s'exécutent sur une banque de données nécessitent plus d'espace.

Si une banque de données partagée possède des machines virtuelles sous tension et qu'elle est pleine à 100 %, vous pouvez augmenter la capacité de la banque de données. Vous pouvez effectuer cette action uniquement à partir de l'hôte sur lequel les machines virtuelles sous tension sont enregistrées.

Selon votre configuration de stockage, vous pouvez utiliser l'une des méthodes suivantes pour augmenter la capacité de la banque de données. Vous n'avez pas besoin de mettre hors tension les machines virtuelles lorsque vous utilisez l'une ou l'autre de ces méthodes d'augmentation de la capacité de la banque de données.

Étendre une banque de données existante

Augmentez la taille d'une banque de données extensible. La banque de données est considérée extensible lorsque le périphérique de stockage de support dispose d'espace libre immédiatement après l'extension de la banque de données.

Ajouter une extension

Augmentez la capacité d'une banque de données VMFS existante en ajoutant de nouveaux périphériques de stockage à la banque de données. La banque de données peut s'étendre sur plusieurs périphériques de stockage et s'afficher en tant que volume unique.

La banque de données VMFS étendue peut utiliser n'importe laquelle de ses extensions ou toutes ses extensions à tout moment. Elle ne doit pas nécessairement remplir une extension spécifique avant d'utiliser la suivante.

Note Les banques de données ne prenant en charge que le verrouillage par assistance matérielle, également appelé mécanisme ATS (atomic test and set), ne peuvent s'étendre sur des périphériques non ATS. Pour plus d'informations, consultez [Mécanismes de verrouillage VMFS](#).

Conditions préalables

Vous pouvez augmenter la capacité de la banque de données si le stockage de l'hôte répond à l'une des conditions suivantes :

- Le périphérique de support de la banque de données existante dispose de suffisamment d'espace libre.
- Vous avez ajouté de nouveaux périphériques de stockage à l'hôte.

Procédure

- 1 Dans vSphere Client, accédez à la banque de données.

- 2 Sélectionnez **Augmenter la capacité de banque de données** dans le menu contextuel de la banque de données.
- 3 Sélectionnez un périphérique dans la liste des périphériques de stockage.

Votre choix dépend de savoir si un périphérique de stockage extensible est disponible.

Option	Description
Pour étendre une extension de banque de données existante	Sélectionnez le périphérique dont la colonne Extensible contient la valeur Oui.
Pour ajouter une extension	Sélectionnez le périphérique dont la colonne Extensible contient la valeur Non.

- 4 Vérifiez **Structure de la partition** pour voir les configurations disponibles.
 - 5 Sélectionnez une option de configuration dans le panneau du bas.
- Selon la disposition actuelle du disque et vos sélections précédentes, les éléments de menu que vous voyez pourraient varier.

Élément de menu	Description
Utiliser l'espace libre pour étendre la banque de données	Une extension existante est agrandie par rapport à la capacité requise.
Utilisez l'espace libre	Déploie une extension dans l'espace libre restant du disque. Cet élément de menu est disponible uniquement lorsque vous ajoutez une extension.
Utilisez toutes les partitions disponibles	Dédie la totalité du disque à une seule extension. Cet élément de menu est disponible uniquement lorsque vous ajoutez une extension et que le disque que vous formatez n'est pas vierge. Le disque est reformatted et les banques de données et toutes les données qu'elles contiennent sont effacées.

- 6 Définissez la capacité de l'extension.

La taille d'extension minimale est 1,3 Go. Par défaut, l'espace libre entier sur le périphérique de stockage est disponible.

- 7 Cliquez sur **Suivant**.
- 8 Passez en revue la disposition proposée et la nouvelle configuration de votre banque de données et cliquez sur **Terminer**.

Note Si vous ne réanalysez le niveau du cluster à partir de vCenter Server, il se peut qu'il ne détecte aucune modification. Cela entraîne une disparité de l'utilisation ou l'espace actuel de la banque de données. Il est recommandé de réanalyser le niveau du cluster dans vCenter Server après avoir effectué toute forme d'extension au niveau de l'hôte.

Configurer les paramètres des disques virtuels en cluster sur la banque de données VMFS6

Si vous prévoyez d'utiliser un disque virtuel dans des configurations WSFC (Windows Server Failover Clustering), votre banque de données VMFS6 doit prendre en charge les disques virtuels en cluster. Utilisez vSphere Client pour configurer la prise en charge des disques mis en cluster.

Pour plus d'informations sur l'utilisation de disques virtuels en cluster dans les clusters de VM, reportez-vous à la documentation de *Configuration du clustering de basculement Windows Server*.

Conditions préalables

Procédez comme suit lorsque vous utilisez une banque de données pour les disques virtuels en cluster :

- La baie de stockage prend en charge le type de réservation SCSI-3 ATS, Write Exclusive – All Registrant (WEAR). Pour ce type de configuration, ESXi prend uniquement en charge les baies Fibre Channel.
- Les périphériques de stockage qui sauvegardent la banque de données sont réclamés par le NMP. ESXi ne prend pas en charge les plug-ins tiers (MPP) dans les configurations de disque virtuel en cluster.
- La banque de données est de type VMFS6. Vous ne pouvez pas développer ou étendre la banque de données.
- La banque de données VMFS6 est déployée sur le périphérique de stockage avec l'attribut Clustered VMDK Supported défini sur Yes.
- Les disques virtuels que vous utilisez pour le clustering sont au format Provisionnement statique immédiatement mis à zéro.

Procédure

- 1 Dans vSphere Client, accédez à la banque de données.
- 2 Cliquez sur l'onglet **Configurer**, puis sur **Général**.
- 3 Sous **Fonctionnalités de la banque de données**, cliquez sur l'une des options suivantes en regard de l'élément **VMDK en cluster**.

Option	Description
Activer	Pour activer la prise en charge des disques virtuels en cluster sur la banque de données. Après avoir activé la prise en charge, vous pouvez placer les disques virtuels mis en cluster sur cette banque de données VMFS.
Désactiver	Pour désactiver la prise en charge. Avant de désactiver, veillez à mettre hors tension toutes les machines virtuelles avec les disques virtuels en cluster.

- 4 Confirmez votre configuration.

Désactivation des filtres de stockage

Lorsque vous effectuez des opérations de gestion de banque de données VMFS, vCenter Server utilise des filtres de protection par défaut. Les filtres vous aident à éviter une corruption du stockage en extrayant uniquement les périphériques de stockage pouvant être utilisés pour une opération particulière. Les périphériques non conformes ne sont pas affichés pour la sélection. Vous pouvez désactiver les filtres pour afficher tous les périphériques.

Ces filtres sont disponibles par défaut.

Nom du filtre	Description
config.vpxd.filter.vmfsFilter (Filtre VMFS)	Élimine les périphériques de stockage, ou LUN, qui sont déjà utilisés par une banque de données VMFS ou un hôte géré par vCenter Server. Les LUN ne s'affichent pas comme des candidats au formatage avec une autre banque de données VMFS ou pour une utilisation en tant que RDM.
config.vpxd.filter.rdmFilter (Filtre RDM)	Élimine les LUN déjà référencés par un RDM sur un hôte géré par vCenter Server. Les LUN ne s'affichent pas comme des candidats au formatage avec VMFS ou pour une utilisation par un RDM différent. Pour permettre à vos machines virtuelles d'accéder au même LUN, celles-ci doivent partager le même fichier de mappage RDM. Pour plus d'informations sur ce type de configuration, reportez-vous à la documentation <i>Gestion des ressources vSphere</i> .
config.vpxd.filter.sameHostsAndTranportsFilter (Même filtre d'hôtes et de transports)	Élimine les LUN inéligibles pour une utilisation comme extensions de banque de données VMFS en raison d'incompatibilité d'hôte ou de stockage. Vous empêche d'ajouter les LUN suivants comme extensions : <ul style="list-style-type: none"> ■ LUN non exposés à tous les hôtes qui partagent la banque de données VMFS d'origine. ■ LUN utilisant un type de stockage différent de celui utilisé par la banque de données VMFS d'origine. Par exemple, vous ne pouvez pas ajouter une extension Fibre Channel à une banque de données VMFS sur un périphérique de stockage local.
config.vpxd.filter.hostRescanFilter (Filtre de réanalyse d'hôte)	Réanalyse automatiquement et met à niveau les banques de données VMFS après que vous avez effectué des opérations de gestion de banque de données. Ce filtre aide à fournir une vue cohérente de toutes les banques de données VMFS sur tous les hôtes gérés par vCenter Server. <p>Note Si vous présentez un nouveau LUN à un hôte ou un cluster, les hôtes exécutent automatiquement une réanalyse que le filtre de réanalyse d'hôte soit activé ou non.</p>

Conditions préalables

Avant de modifier les filtres des périphériques, contactez l'équipe de support de VMware.

Procédure

- 1 Accédez à l'instance de vCenter Server.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Paramètres**, cliquez sur **Paramètres avancés**, puis sur **MODIFIER LES PARAMÈTRES**.

4 Indiquez le filtre à désactiver.

Dans les zones de texte **Nom** et **Valeur** en bas de la page, entrez les informations appropriées.

Nom	Valeur
config.vpxd.filter.vmfsFilter	False
config.vpxd.filter.rdmFilter	False
config.vpxd.filter.sameHostsAndTranportsFilter	False
config.vpxd.filter.hostRescanFilter	False
<p>Note Si vous désactivez ce filtre, vos hôtes continuent d'effectuer une réanalyse à chaque fois que vous présentez un nouveau LUN à un hôte ou un cluster.</p>	

5 Cliquez sur **AJOUTER**, puis sur **ENREGISTRER** pour enregistrer vos modifications.

Vous n'avez pas besoin de redémarrer le système vCenter Server.

Configuration de la mise en miroir des disques dynamiques

En général, vous ne pouvez pas utiliser de logiciel de gestion de LUN sur des machines virtuelles pour mettre en miroir des disques virtuels. Cependant, si vos machines virtuelles Microsoft Windows prennent en charge les disques dynamiques, vous pouvez mettre en miroir des disques virtuels sur deux LUN SAN. La mise en miroir vous permet de protéger les machines virtuelles d'une perte imprévue de périphérique de stockage.

Conditions préalables

- Utilisez une machine virtuelle Windows qui prend en charge les disques dynamiques.
- Privilège requis : **Machine virtuelle. Configuration. Paramètres**

Procédure

- 1 Création d'une machine virtuelle disposant de deux disques virtuels.
Placez les disques sur différentes banques de données.
- 2 Connectez-vous à votre machine virtuelle et configurez les disques en tant que disques dynamiques mis en miroir.
Consultez la documentation de Microsoft.
- 3 Après la synchronisation des disques, mettez la machine virtuelle hors tension.

- 4 Modifiez les paramètres de la machine virtuelle pour activer la mise en miroir des disques dynamiques.
 - a Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
 - b Cliquez sur l'onglet **Options VM** et développez le menu **Avancé**.
 - c Cliquez sur **Modifier la configuration** en regard de Paramètres de configuration.
 - d Cliquez sur **Ajouter des paramètres de configuration** et ajoutez les paramètres suivants :

Remplacez # par l'ID du contrôleur de bus SCSI du périphérique de démarrage. Par défaut, il est défini sur 0.

Nom	Valeur
scsi#.returnNoConnectDuringAPD	True
scsi#.returnBusyOnNoConnectStatus	False

- e Si vous utilisez ESXi 6.7 ou version ultérieure, incluez un paramètre supplémentaire pour chaque disque virtuel participant à la configuration du logiciel RAID-1.

Le paramètre empêche les échecs d'E/S du système d'exploitation invité lorsqu'un périphérique de stockage échoue.

Remplacez # par l'ID du contrôleur de bus SCSI du périphérique de démarrage. Par défaut, il est défini sur 0.

Nom	Valeur
scsi#:1.passthruTransientErrors	True
scsi#:2.passthruTransientErrors	True

- f Cliquez sur **OK**.

Collecte d'informations de diagnostic pour les hôtes ESXi sur une banque de données VMFS

Pendant une panne d'hôte, ESXi doit pouvoir enregistrer des informations de diagnostic dans un emplacement préconfiguré à des fins de diagnostic et de support technique.

Généralement, une partition destinée à recueillir des informations de diagnostic, également nommée vidage de mémoire, est créée sur un périphérique de stockage local pendant l'installation d'ESXi. Vous pouvez également configurer ESXi Dump Collector pour conserver les vidages de mémoire sur un serveur réseau. Pour plus d'informations sur la configuration de ESXi Dump Collector, reportez-vous à la documentation *Installation et configuration de VMware ESXi*.

Une autre option consiste à utiliser un fichier sur une banque de données VMFS pour collecter les informations de diagnostic.

Configurer un fichier comme emplacement du vidage de mémoire

Si la taille de votre partition de vidage de mémoire disponible est insuffisante, vous pouvez configurer ESXi afin d'utiliser un fichier sur une banque de données VMFS pour les informations de diagnostic.

Note Les banques de données VMFS sur le logiciel iSCSI ne prennent pas en charge les fichiers de vidage de mémoire.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes esxcli dans ESXi Shell.

Procédure

- Créez un fichier de vidage de mémoire de banque de données VMFS en exécutant la commande suivante :

```
esxcli system coredump file add
```

La commande prend les options suivante, mais elles ne sont pas obligatoires et peuvent être omises :

Option	Description
<code>--datastore -d datastore_UUID or datastore_name</code>	Spécifiez la banque de données pour le fichier de vidage. Si la banque de données n'est pas indiquée, le système sélectionne une banque de données d'une taille suffisante.
<code>--file -f file_name</code>	Spécifiez le nom du fichier de vidage mémoire. Si le fichier n'est pas indiqué, le système spécifie un nom unique pour le fichier.
<code>--size -s file_size_MB</code>	Définissez la taille en Mo du fichier de vidage. Si la taille n'est pas indiquée, le système crée un fichier de la taille appropriée pour la mémoire installée dans l'hôte.

- Assurez-vous que le fichier a bien été créé :

```
esxcli system coredump file list
```

Vous pouvez obtenir un résultat semblable à ce qui suit :

Path	Active	Configured	Size
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile	false	false	104857600

- Activez le fichier de vidage de mémoire pour l'hôte :

```
esxcli system coredump file set
```

La commande accepte les options suivantes :

Option	Description
<code>--enable -e</code>	Activez ou désactivez le fichier de vidage mémoire. Cette option ne peut pas être spécifiée lors de l'annulation de la configuration du fichier de vidage.
<code>--path -p</code>	Chemin du fichier de vidage de mémoire à utiliser. Le fichier doit être pré-alloué.
<code>--smart -s</code>	Cet indicateur peut être utilisé uniquement avec <code>--enable -e=true</code> . Le fichier sera ainsi sélectionné en utilisant l'algorithme de sélection intelligente. Par exemple, <code>esxcli system coredump file set --smart --enable true</code>
<code>--unconfigure -u</code>	Annulez la configuration du fichier de vidage VMFS actuel.

- 4 Assurez-vous que le fichier de vidage de mémoire est activé et configuré :

```
esxcli system coredump file list
```

Un résultat semblable à ce qui suit indique que le fichier de vidage de mémoire est activé et configuré :

Path	Active	Configured	Size
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile	True	True	104857600

Étape suivante

Pour obtenir des informations sur les autres commandes que vous pouvez utiliser pour gérer les fichiers de vidage de mémoire, consultez la documentation *Référence d'ESXCLI*.

Désactiver et supprimer un fichier de vidage de mémoire

Désactivez un fichier de vidage de mémoire configuré et, si nécessaire, supprimez-le de la banque de données VMFS.

Vous pouvez désactiver temporairement le fichier de vidage de mémoire. Si vous ne prévoyez pas d'utiliser le fichier désactivé, vous pouvez le supprimer de la banque de données VMFS. Pour supprimer le fichier qui n'a pas été désactivé, vous pouvez utiliser la commande `esxcli system coredump file remove` avec le paramètre `--force | -F`.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- 1 Répertoriez les fichiers de vidage de mémoire :

```
esxcli system coredump file list
```

- 2 Désactivez le fichier de vidage de mémoire en utilisant la commande suivante :

```
esxcli system coredump file set --unconfigure | -u
```

- 3 Supprimez le fichier de la banque de données VMFS :

```
esxcli system coredump file remove --file | -f file_name
```

La commande accepte les options suivantes :

Option	Description
--file -f	Entrez le nom du fichier de vidage à supprimer. Si vous n'entrez pas de nom, la commande supprime le fichier de vidage de mémoire configuré par défaut.
--force -F	Désactivez et annulez la configuration du fichier de vidage supprimé. Cette option est requise si le fichier n'a pas été désactivé auparavant et est actif.

Résultats

Le fichier de vidage de mémoire est supprimé de la banque de données VMFS.

Vérification de la cohérence des métadonnées avec VOMA

Utilisez vSphere On-disk Metadata Analyser (VOMA) pour identifier et corriger les incidents d'altération des métadonnées qui affectent les systèmes de fichiers ou les volumes logiques sous-jacents.

Problème

Vous pouvez vérifier la cohérence des métadonnées lorsque vous rencontrez des problèmes avec une banque de données VMFS ou une ressource Virtual Flash. Par exemple, effectuez une vérification des métadonnées si l'un des incidents suivants se produit :

- Vous rencontrez des pannes de stockage.
- Après avoir reconstruit RAID ou effectué un remplacement de disque.
- Le fichier `vmkernel.log` présente des erreurs de métadonnées similaires aux suivantes :

```
cpu11:268057)WARNING: HBX: 599: Volume 50fd60a3-3aae1ae2-3347-0017a4770402
("<Datastore_name>") may be damaged on disk. Corrupt heartbeat detected at offset 3305472:
[HB state 0 offset 6052837899185946624 gen 15439450 stampUS 5 $
```

- Vous ne pouvez pas accéder aux fichiers sur un système VMFS.
- Un rapport de corruption s'affiche pour une banque de données dans les onglets d'événements de vCenter Server.

Solution

Pour vérifier la cohérence des métadonnées, exécutez VOMA à partir de l'interface de ligne de commande d'un hôte ESXi. VOMA peut être utilisé pour vérifier et corriger les problèmes d'incohérence mineurs d'une banque de données VMFS ou des volumes logiques soutenant la banque de données VMFS.

VOMA peut vérifier et corriger les éléments suivants.

Tableau 9-5. Fonctions VOMA

Fonctions VOMA	Description
Correctif et vérification des métadonnées	<p>Voici quelques exemples de vérification et de correctif des métadonnées :</p> <ul style="list-style-type: none"> ■ Validation d'un en-tête de volume VMFS pour la cohérence des métadonnées de base. ■ Vérification de la cohérence des fichiers de ressources VMFS (fichier système). ■ Vérification du chemin d'accès et la connectivité de tous les fichiers.
Correctif et vérification des métadonnées d'affinité	<p>Pour activer la vérification d'affinité pour VMFS6, utilisez l'option <code>-a --affinityChk</code>.</p> <p>Voici quelques exemples de vérification et de correctif des métadonnées d'affinité :</p> <ul style="list-style-type: none"> ■ Indicateurs d'affinité dans les types de ressources et FS3_ResFileMetadata. ■ Validation des indicateurs d'affinité dans SFB RC méta (FS3_ResourceClusterMDVMFS6). ■ Validation de toutes les entrées affinityInfo rcMeta rc, y compris la clé de dépassement de capacité, pour vérifier l'absence d'entrée non valide. Vérification d'entrées manquantes.
Validation du répertoire	<p>VOMA peut détecter et corriger les erreurs suivantes :</p> <ul style="list-style-type: none"> ■ Altération de bloc de hachage de répertoire. ■ Altération de mappage d'allocation. ■ Altérations des blocs de liaison. ■ Altérations de blocs d'entrée de répertoire. <p>En fonction de la nature de l'altération des données, VOMA peut corriger uniquement les entrées altérées ou entièrement reconstruire le bloc de hachage, les blocs de mappage d'allocation et les blocs de liaison.</p>
Fichiers perdus et trouvés	<p>Lors d'une vérification du système de fichiers, VOMA peut rechercher des fichiers qui ne sont pas référencés dans le système de fichiers. Ces fichiers inactifs sont valides et complets, mais vous ne disposez pas d'une entrée de nom ou de répertoire sur le système.</p> <p>Si VOMA rencontre des fichiers inactifs lors de l'analyse, il crée un répertoire nommé <code>lost+found</code> à la racine du volume pour stocker les fichiers inactifs. Les noms des fichiers utilisent le format <code>Filesequence-number</code>.</p>

Les options de commande utilisées par l'outil de VOMA comprennent les éléments suivants.

Tableau 9-6. Options de commande VOMA

Option de commande	Description
-m --module	<p>Les modules à exécuter sont notamment les suivants :</p> <ul style="list-style-type: none"> vmfs lvm ptbl
-f --func	<p>Les fonctions à exécuter sont notamment les suivantes :</p> <ul style="list-style-type: none"> query check fix dump
-a --affinityChk	Incluez la vérification et le correctif associé à l'affinité pour VMFS6.
-d --device	<p>Indiquez le périphérique ou le disque à inspecter. Assurez-vous de fournir le chemin absolu de la partition du périphérique qui prend en charge la banque de données VMFS. Si la banque de données s'étend sur plusieurs périphériques, fournissez l'UUID de l'extension de tête.</p> <p>Par exemple, <code>voma -m vmfs -f check -d /vmfs/devices/disks/naa.xxxxx:*</code></p> <p>Si vous utilisez la commande <code>-x --extractDump</code>, entrez plusieurs chemins de périphérique, avec un qualificateur de partition, séparés par une virgule. Le nombre de chemins de périphérique que vous entrez est égal au nombre de périphériques couverts.</p>
-b --blockSize	Indiquez la taille du bloc de disque.
-s --logfile	Spécifiez le chemin d'accès au fichier journal pour obtenir les résultats.
-x --extractDump	Extrayez le vidage de mémoire collecté à l'aide de VOMA.

Tableau 9-6. Options de commande VOMA (suite)

Option de commande	Description
<code>-D --dumpfile</code>	Indiquez le fichier de vidage pour enregistrer le vidage de métadonnées collecté.
<code>-v --version</code>	Afficher la version de VOMA.
<code>-h --help</code>	Afficher le message d'aide de la commande VOMA.
<code>-Y</code>	Indiquez que vous exécutez VOMA sans utiliser les tables PE pour la résolution d'adresses.
<code>-Z --file</code>	Indiquez que vous exécutez VOMA sur des fichiers de périphérique extraits.

Exemple

Collectez le vidage des métadonnées à partir d'un volume couvert :

```
voma -m vmfs -f dump -d head_extent -D dump_filename
```

Extrayez le vidage collecté sur les périphériques d'un volume couvert :

```
voma -x dump_filename -d head_extent,extent_2,extent_3...extent_n
```

Utiliser VOMA pour vérifier la cohérence des métadonnées

La tâche explique comment utiliser VOMA pour vérifier la cohérence des métadonnées VMFS. VOMA peut être utilisé pour vérifier et corriger les problèmes d'incohérence mineurs concernant une banque de données VMFS ou une ressource Virtual Flash. Exécutez VOMA depuis l'interface de ligne de commande d'un hôte d'ESXi.

Conditions préalables

Mettez hors tension les machines virtuelles en cours d'exécution ou déplacez-les vers une autre banque de données.

Procédure

- Obtenez le nom et le numéro de la partition du périphérique qui prend en charge la banque de données VMFS que vous souhaitez vérifier.

```
#esxcli storage vmfs extent list
```

Les colonnes Nom périphérique et Partition dans la sortie identifient le périphérique. Par exemple :

Volume Name	Device Name	Partition
1TB_VMFS6	naa.xxxx	3

- Recherchez les erreurs VMFS.

Indiquez le chemin absolu de la partition du périphérique qui prend en charge la banque de données VMFS et entrez un numéro de partition avec le nom du périphérique. Par exemple :

```
# voma -m vmfs -f check -d /vmfs/devices/disks/naa.xxxx:x
```

La sortie répertorie les erreurs possibles. Par exemple, la sortie suivante indique que l'adresse de signal de pulsation n'est pas valide.

```
XXXXXXXXXXXXXXXXXXXXXX
Phase 2: Checking VMFS heartbeat region
ON-DISK ERROR: Invalid HB address
Phase 3: Checking all file descriptors.
Phase 4: Checking pathname and connectivity.
Phase 5: Checking resource reference counts.

Total Errors Found:           1
```

Configuration du cache de blocs de pointage VMFS

Les blocs de pointage, également appelés blocs d'indirection, sont les ressources du système de fichiers qui contiennent les adresses vers les blocs de fichiers VMFS. Lorsque vous ouvrez un fichier `vmdk` sur un hôte ESXi, les blocs de pointage associés à ce fichier sont stockés dans le cache de blocs de pointage. La taille du cache de blocs de pointage est un paramètre configurable.

Le cache de blocs de pointage est un cache s'appliquant à tout l'hôte qui est indépendant du VMFS. Le cache est partagé entre toutes les banques de données qui sont accessibles depuis le même hôte ESXi.

La taille du cache de blocs de pointage est contrôlée par `/VMFS3/MinAddressableSpaceTB` et `/VMFS3/MaxAddressableSpaceTB`. Vous pouvez configurer la taille minimale et la taille maximale sur chaque hôte ESXi.

/VMFS3/MinAddressableSpaceTB

La valeur minimale est la quantité minimale de mémoire garantie par le système au cache de blocs de pointage. Par exemple, 1 To d'espace pour les fichiers ouverts exige environ 4 Mo de mémoire. La valeur par défaut est 10 To.

/VMFS3/MaxAddressableSpaceTB

Ce paramètre définit la limite maximale des blocs de pointage qu'il est possible de mettre en cache dans la mémoire. La valeur par défaut est 32 To. La valeur maximale est 128 To. En général, la valeur par défaut du paramètre `/VMFS3/MaxAddressableSpaceTB` est suffisante.

Toutefois, à mesure que la taille des fichiers `vmdk` ouverts augmente, le nombre de blocs de pointage associés à ces fichiers augmente également. Si l'augmentation entraîne une dégradation des performances, vous pouvez ajuster le paramètre à sa valeur maximale pour fournir davantage d'espace au cache de blocs de pointage. Basez la taille maximale du cache de blocs de pointage sur l'ensemble de travail ou sur les blocs de pointage actifs requis.

Éviction de blocs de pointage

Le paramètre `/VMFS3/MaxAddressableSpaceTB` contrôle également la croissance du cache de blocs de pointage. Lorsque la taille du cache de blocs de pointage s'approche de la taille maximale configurée, un processus d'éviction de blocs de pointage démarre. Le mécanisme conserve les blocs de pointage actifs, mais il supprime les blocs non actifs ou moins actifs du cache afin que l'espace puisse être réutilisé.

Pour modifier les valeurs du cache de blocs de pointage, utilisez la boîte de dialogue **Paramètres système avancés** de vSphere Client ou la commande `esxcli system settings advanced set -o`.

Vous pouvez utiliser la commande `esxcli storage vmfs pbcache` pour obtenir des informations sur la taille du cache de blocs de pointage et d'autres statistiques. Ces informations vous aident à ajuster les tailles minimale et maximale du cache de blocs de pointage afin d'optimiser les performances.

Obtenir des informations sur le cache de blocs de pointage VMFS

Vous pouvez obtenir des informations sur l'utilisation du cache de blocs de pointage VMFS. Ces informations vous aident à comprendre combien d'espace consomme le cache de blocs de pointage. Vous pouvez également déterminer si vous devez ajuster les tailles minimales et maximales du cache de blocs de pointage.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Pour obtenir ou réinitialiser les statistiques du cache de blocs de pointage, utilisez la commande suivante :

```
esxcli storage vmfs pbcache
```

Option	Description
<code>get</code>	Obtenez les statistiques du cache de blocs de pointage VMFS.
<code>reset</code>	Réinitialisez les statistiques du cache de blocs de pointage VMFS.

Exemple : Obtention de statistiques pour le cache de blocs de pointage

```
#esxcli storage vmfs pbcache get
Cache Capacity Miss Ratio: 0 %
Cache Size: 0 MiB
Cache Size Max: 132 MiB
Cache Usage: 0 %
Cache Working Set: 0 TiB
Cache Working Set Max: 32 TiB
Vmfs Heap Overhead: 0 KiB
Vmfs Heap Size: 23 MiB
Vmfs Heap Size Max: 256 MiB
```

Modifier la taille du cache de blocs de pointage

Vous pouvez ajuster la taille minimale et la taille maximale du cache de blocs de pointage.

Attention La modification des options avancées est considérée comme non prise en charge. En général, les paramètres par défaut donnent un résultat optimal. Modifiez les options avancées uniquement lorsque vous recevez des instructions spécifiques du support technique de VMware ou d'un article de la base de connaissances.

Procédure

- 1 Accédez à l'hôte.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Système**, cliquez sur **Paramètres système avancés**.
- 4 Dans Paramètres système avancés, sélectionnez l'élément approprié.

Option	Description
<code>VMFS3.MinAddressableSpaceTB</code>	Taille minimale de tous les fichiers ouverts que le cache VMFS garantit de prendre en charge.
<code>VMFS3.MaxAddressableSpaceTB</code>	Taille maximale de tous les fichiers ouverts que le cache VMFS prend en charge avant le démarrage de l'éviction.

- 5 Cliquez sur le bouton **Modifier** et modifiez la valeur.
- 6 Cliquez sur **OK**.

Exemple : Utiliser la commande esxcli pour modifier le cache de blocs de pointage

Vous pouvez également utiliser `esxcli system settings advanced set -o` pour modifier la taille du cache de blocs de pointage. L'exemple suivant explique comment définir la taille sur sa valeur maximale de 128 To.

- 1 Pour remplacer la valeur de `/VMFS3/MaxAddressableSpaceTB` par 128 To, entrez la commande suivante :

```
# esxcli system settings advanced set -i 128 -o /VMFS3/
MaxAddressableSpaceTB
```

- 2 Pour confirmer que la valeur définie est correcte, entrez cette commande :

```
# esxcli system settings advanced list -o /VMFS3/MaxAddressableSpaceTB
```

Concepts et opérations de banque de données NFS

Un client NFS intégré dans ESXi utilise le protocole NFS (Network File System) sur TCP/IP pour accéder à un volume NFS désigné qui se trouve sur un serveur NAS. L'hôte ESXi peut monter le volume et l'utiliser pour ses besoins en stockage. vSphere prend en charge les versions 3 et 4.1 du protocole NFS.

En général, le volume ou le répertoire NFS est créé par un administrateur de stockage et exporté depuis le serveur NFS. Vous n'avez pas besoin de formater le volume NFS avec un système de fichiers local tel que VMFS. Vous pouvez plutôt monter le volume directement sur les hôtes ESXi et l'utiliser pour stocker et démarrer les machines virtuelles de la même manière que vous utilisez les banques de données VMFS.

Outre le stockage des disques virtuels sur les banques de données NFS, vous pouvez employer NFS comme référentiel central pour les images ISO, les modèles de machine virtuelle, etc. Si vous utilisez la banque de données pour les images ISO, vous pouvez connecter le périphérique CD-ROM de la machine virtuelle à un fichier ISO sur la banque de données. Vous pouvez ensuite installer un système d'exploitation invité à partir du fichier ISO.

Après avoir configuré l'environnement de stockage NFS, reportez-vous aux rubriques suivantes pour créer et gérer des banques de données NFS :

- [Créer une banque de données NFS](#)
- [Opérations administratives de base pour les banques de données](#)

Protocoles NFS et ESXi

ESXi prend en charge les protocoles NFS version 3 et 4.1. Pour prendre en charge les deux versions, ESXi utilise deux clients NFS différents.

Comparaison des versions des clients NFS

Le tableau suivant répertorie les fonctionnalités prises en charge par les versions 3 et 4.1 de NFS.

Caractéristiques	NFS version 3	NFS version 4.1
Mécanismes de sécurité	AUTH_SYS	AUTH_SYS et Kerberos (krb5 et krb5i)
Algorithmes de chiffrement avec Kerberos	S.O.	AES256-CTS-HMAC-SHA1-96 et AES128-CTS-HMAC-SHA1-96
Gestion multivoie	Non pris en charge	Pris en charge via la jonction de sessions
Mécanismes de verrouillage	Verrouillage des propriétés côté client	Verrouillage côté serveur
Accélération matérielle	Pris en charge	Pris en charge
Disques virtuels statiques	Pris en charge	Pris en charge
IPv6	Pris en charge	Pris en charge pour AUTH_SYS et Kerberos
Images ISO présentées en tant que CD-ROM aux machines virtuelles	Pris en charge	Pris en charge

Caractéristiques	NFS version 3	NFS version 4.1
Snapshots de machine virtuelle	Pris en charge	Pris en charge
Machines virtuelles disposant de disques virtuels d'une capacité supérieure à 2 To	Pris en charge	Pris en charge

Protocoles NFS et solutions vSphere

Le tableau suivant répertorie les principales solutions vSphere prises en charge par les versions de NFS.

Fonctionnalités de vSphere	NFS version 3	NFS version 4.1
vMotion et Storage vMotion	Oui	Oui
Haute disponibilité (HA)	Oui	Oui
Fault Tolerance (FT)	Oui	Oui
Distributed Resource Scheduler (DRS)	Oui	Oui
Profils d'hôte	Oui	Oui
Storage DRS	Oui	Non
Storage I/O Control	Oui	Non
Site Recovery Manager	Oui	Site Recovery Manager ne prend pas en charge les banques de données NFS 4.1 pour la réplication basée sur la baie et la réplication de Virtual Volumes. Vous pouvez utiliser Site Recovery Manager avec des banques de données NFS v4.1 pour vSphere Replication.
Virtual Volumes	Oui	Oui
vSphere Replication	Oui	Oui
VMware Aria Operations	Oui	Oui

NFS 4.1 et Fault Tolerance

Les machines virtuelles sur NFS 4.1 prennent en charge le nouveau mécanisme de tolérance de panne qui a été introduit dans vSphere 6.0. Ce mécanisme peut accueillir des machines virtuelles à multiprocesseur symétrique (SMP) pouvant contenir jusqu'à quatre vCPU.

Les machines virtuelles NFS 4.1 ne prennent pas en charge le mécanisme de tolérance de panne hérité.

Mises à niveau de NFS

Lorsque vous mettez à niveau ESXi à partir d'une version antérieure à la version 6.5, les banques de données NFS 4.1 existantes commencent automatiquement la prise en charge de fonctionnalités qui n'étaient pas disponibles dans la version précédente d'ESXi. Ces fonctionnalités sont notamment Virtual Volumes, l'accélération matérielle, etc.

ESXi ne prend pas en charge les conversions automatiques de banques de données de NFS version 3 vers NFS 4.1.

Si vous souhaitez mettre à niveau votre banque de données NFS 3, les options suivantes sont disponibles :

- Créez la banque de données NFS 4.1, puis utilisez Storage vMotion pour migrer des machines virtuelles de l'ancienne banque de données vers la nouvelle.
- Utilisez les méthodes de conversion fournies par votre serveur de stockage NFS. Pour plus d'informations, contactez votre fournisseur de stockage.
- Démontez la banque de données NFS 3, puis montez-la comme une banque de données NFS 4.1.

Attention Si vous utilisez cette option, assurez-vous de démonter la banque de données de tous les hôtes ayant accès à la banque de données. La banque de données ne peut jamais être montée en utilisant les deux protocoles simultanément.

Directives et configuration requise du stockage NFS

Lorsque vous utilisez un stockage NFS, suivez les directives spécifiques associées à la configuration du serveur NFS, à la mise en réseau, aux banques de données NFS, etc.

■ Configuration des serveurs NFS

Lorsque vous configurez des serveurs NFS pour utiliser ESXi, suivez les recommandations de votre fournisseur de stockage. Outre ces recommandations générales, utilisez les directives spécifiques qui s'appliquent à NFS dans l'environnement vSphere.

■ Mise en réseau NFS

Un hôte ESXi utilise une connexion réseau TCP/IP pour accéder à un serveur NAS distant. Certaines directives et meilleures pratiques permettent de configurer la mise en réseau lorsque vous utilisez le stockage NFS.

■ Verrouillage des fichiers NFS

Des mécanismes de verrouillage de fichiers sont utilisés pour restreindre l'accès aux données stockées sur un serveur à un seul utilisateur ou processus à la fois. Les mécanismes de verrouillage des deux versions de NFS ne sont pas compatibles. NFS 3 utilise le verrouillage propriétaire et NFS 4.1 utilise le verrouillage spécifié du protocole natif.

- **Sécurité NFS**

Avec NFS 3 et NFS 4.1, ESXi prend en charge la sécurité AUTH_SYS. En outre, pour NFS 4.1, le mécanisme de sécurité Kerberos est pris en charge.

- **Gestion de chemins multiples NFS**

NFS 4.1 prend en charge la gestion multivoie selon les spécifications du protocole. Pour NFS 3, la gestion multivoie n'est pas applicable.

- **NFS et accélération matérielle**

Les disques virtuels créés sur des banques de données NFS sont provisionnés dynamiquement par défaut. Pour pouvoir créer des disques virtuels à provisionnement statique, vous devez utiliser une accélération matérielle prenant en charge l'opération de réserve d'espace.

- **Banques de données NFS**

Lorsque vous créez une banque de données NFS, suivez les directives spécifiques.

Configuration des serveurs NFS

Lorsque vous configurez des serveurs NFS pour utiliser ESXi, suivez les recommandations de votre fournisseur de stockage. Outre ces recommandations générales, utilisez les directives spécifiques qui s'appliquent à NFS dans l'environnement vSphere.

Les directives incluent les éléments suivants.

- Assurez-vous que les serveurs NAS que vous utilisez sont répertoriés dans *VMware HCL*. Utilisez la bonne version du microprogramme du serveur.
- Assurez-vous que le volume NFS est exporté en utilisant NFS sur TCP.
- Assurez-vous que le serveur NAS exporte un partage particulier en tant que NFS 3 ou NFS 4.1. Le serveur NAS ne doit pas fournir deux versions de protocole pour le même partage. Le serveur NAS doit appliquer cette stratégie, car ESXi n'empêche pas le montage du même partage avec différentes versions de NFS.
- NFS 3 et NFS 4.1 non Kerberos (AUTH_SYS) ne prennent pas en charge la fonctionnalité d'utilisateur délégué qui permet d'accéder aux volumes NFS en utilisant des informations d'identification non racine. Si vous utilisez NFS 3 ou NFS 4.1 non-Kerberos, assurez-vous que chaque hôte a un accès racine au volume. Différents fournisseurs de stockage ont différentes méthodes d'activation de cette fonctionnalité, mais les serveurs NAS utilisent généralement l'option `no_root_squash`. Si le serveur NAS n'accorde pas un accès racine, vous pourrez quand même monter la banque de données NFS sur l'hôte. Cependant, vous ne pouvez pas créer de machines virtuelles sur la banque de données.
- Si le volume NFS sous-jacent est en lecture seule, assurez-vous que le volume est exporté sous forme de partage en lecture seule par le serveur NFS. Vous pouvez également monter le volume sous forme de banque de données en lecture seule sur l'hôte ESXi. Sinon, l'hôte considère que la banque de données est en lecture et en écriture et peut ne pas ouvrir les fichiers.

Mise en réseau NFS

Un hôte ESXi utilise une connexion réseau TCP/IP pour accéder à un serveur NAS distant. Certaines directives et meilleures pratiques permettent de configurer la mise en réseau lorsque vous utilisez le stockage NFS.

Pour plus d'informations, consultez la documentation *Mise en réseau vSphere*.

- Pour la connectivité réseau, utilisez un adaptateur réseau standard dans votre hôte ESXi.
- ESXi prend en charge les commutateurs réseau de niveau 2 et de niveau 3. Si vous utilisez des commutateurs de niveau 3, les hôtes ESXi et les baies de stockage NFS doivent être sur des sous-réseaux différents et le commutateur réseau doit traiter les informations de routage.
- Configurez un groupe de ports VMkernel pour le stockage NFS. Vous pouvez créer le groupe de ports VMkernel pour un stockage IP sur un commutateur virtuel existant (vSwitch) ou sur un nouveau vSwitch. Le vSwitch peut être un commutateur standard vSphere (VSS) ou un vSphere Distributed Switch (VDS).
- Si vous utilisez plusieurs ports pour le trafic NFS, assurez-vous de correctement configurer vos commutateurs virtuels et vos commutateurs physiques.
- NFS 3 et NFS 4.1 prennent en charge IPv6.

Verrouillage des fichiers NFS

Des mécanismes de verrouillage de fichiers sont utilisés pour restreindre l'accès aux données stockées sur un serveur à un seul utilisateur ou processus à la fois. Les mécanismes de verrouillage des deux versions de NFS ne sont pas compatibles. NFS 3 utilise le verrouillage propriétaire et NFS 4.1 utilise le verrouillage spécifié du protocole natif.

Le verrouillage NFS 3 sur ESXi n'utilise pas le protocole NLM (Network Lock Manager). VMware fournit plutôt son propre protocole de verrouillage. Les verrouillages NFS 3 sont mis en œuvre en créant des fichiers de verrouillage sur le serveur NFS. Les fichiers de verrouillage se nomment `.lck-file_id..`

NFS 4.1 utilise des réservations de partages comme mécanisme de verrouillage.

Comme les clients NFS 3 et NFS 4.1 n'utilisent pas le même protocole de verrouillage, vous ne pouvez pas utiliser différentes versions de NFS pour monter la même banque de données sur plusieurs hôtes. L'accès aux mêmes disques virtuels à partir de deux clients incompatibles peut provoquer un comportement incorrect et entraîner l'altération des données.

Sécurité NFS

Avec NFS 3 et NFS 4.1, ESXi prend en charge la sécurité AUTH_SYS. En outre, pour NFS 4.1, le mécanisme de sécurité Kerberos est pris en charge.

NFS 3 prend en charge le mécanisme de sécurité AUTH_SYS. Avec ce mécanisme, le trafic de stockage est transmis dans un format non chiffré sur le réseau local. En raison de cette sécurité limitée, utilisez le stockage NFS uniquement sur des réseaux approuvés et isolez le trafic sur des commutateurs physiques séparés. Vous pouvez également utiliser un VLAN privé.

NFS 4.1 prend en charge le protocole d'authentification Kerberos pour sécuriser les communications avec le serveur NFS. Les utilisateurs autres que l'utilisateur racine peuvent accéder aux fichiers lorsque Kerberos est utilisé. Pour plus d'informations, consultez [Utilisation de Kerberos pour NFS 4.1](#).

Outre Kerberos, NFS 4.1 prend en charge les montages traditionnels non Kerberos avec la sécurité AUTH_SYS. Dans ce cas, utilisez les directives d'accès racine pour NFS version 3.

Note Vous ne pouvez pas utiliser deux mécanismes de sécurité, AUTH_SYS et Kerberos, pour la même banque de données NFS 4.1 partagée par plusieurs hôtes.

Gestion de chemins multiples NFS

NFS 4.1 prend en charge la gestion multivoie selon les spécifications du protocole. Pour NFS 3, la gestion multivoie n'est pas applicable.

NFS 3 utilise une connexion TCP pour l'E/S. Par conséquent, ESXi prend en charge l'E/S uniquement sur une adresse IP et un nom d'hôte pour le serveur NFS et ne prend pas en charge les chemins multiples. Selon l'infrastructure et la configuration de votre réseau, vous pouvez utiliser la pile réseau pour configurer plusieurs connexions aux cibles de stockage. Dans ce cas, vous devez disposer de plusieurs banques de données, chaque banque de données utilisant alors des connexions réseau séparées entre l'hôte et le stockage.

NFS 4.1 assure la gestion des chemins multiples pour les serveurs prenant en charge la jonction de sessions. Lorsque la jonction est disponible, vous pouvez utiliser plusieurs adresses IP pour accéder à un volume NFS spécifique. La jonction d'ID de client n'est pas prise en charge.

NFS et accélération matérielle

Les disques virtuels créés sur des banques de données NFS sont provisionnés dynamiquement par défaut. Pour pouvoir créer des disques virtuels à provisionnement statique, vous devez utiliser une accélération matérielle prenant en charge l'opération de réserve d'espace.

NFS 3 et NFS 4.1 prennent en charge l'accélération matérielle permettant à votre hôte d'intégrer des périphériques NAS et d'utiliser plusieurs opérations matérielles fournies par le stockage NAS. Pour plus d'informations, consultez [Accélération matérielle sur les périphériques NAS](#).

Banques de données NFS

Lorsque vous créez une banque de données NFS, suivez les directives spécifiques.

Les directives et meilleures pratiques concernant la banque de données NFS sont notamment les éléments suivants :

- Vous ne pouvez pas utiliser des versions NFS différentes pour monter la même banque de données sur des hôtes différents. Les clients NFS 3 et NFS 4.1 ne sont pas compatibles et n'utilisent pas le même protocole de verrouillage. Par conséquent, l'accès aux mêmes disques virtuels à partir de deux clients incompatibles peut provoquer un comportement incorrect et entraîner l'altération des données.
- Des banques de données NFS 3 et NFS 4.1 peuvent coexister sur le même hôte.

- ESXi ne peut pas automatiquement mettre à niveau NFS version 3 vers la version 4.1, mais vous pouvez utiliser d'autres méthodes de conversion. Pour plus d'informations, consultez [Concepts et opérations de banque de données NFS](#).
- Lorsque vous montez le même volume NFS 3 sur des hôtes différents, assurez-vous que les noms de serveurs et de dossiers sont identiques sur les hôtes. Si les noms ne correspondent pas, les hôtes voient le même volume NFS version 3 sous la forme de deux banques de données différentes. Cette erreur peut provoquer une défaillance de certaines fonctions, telles que vMotion. Un exemple d'un tel écart d'utilisation serait d'entrer `filer` comme nom de serveur sur un hôte et `filer.domain.com` sur l'autre. Cette directive ne s'applique pas à NFS version 4.1.
- Si vous utilisez des caractères non-ASCII pour nommer des banques de données et des machines virtuelles, veillez à ce que le serveur NFS sous-jacent offre une prise en charge de l'internationalisation. Si le serveur ne prend pas en charge les caractères internationaux, utilisez uniquement des caractères ASCII, sinon des incidents imprévisibles peuvent se produire.

Configurations de pare-feu pour le stockage NFS

ESXi contient un pare-feu situé entre l'interface de gestion et le réseau. Le pare-feu est activé par défaut. Au moment de l'installation, le pare-feu ESXi est configuré pour bloquer le trafic entrant et sortant, à l'exception du trafic des services par défaut, tels que NFS.

Les services pris en charge, notamment NFS, sont décrits dans un fichier de configuration de groupe de règles dans le répertoire du pare-feu ESXi `/etc/vmware/firewall/`. Le fichier contient les règles de pare-feu et leurs relations avec les ports et les protocoles.

Le comportement de l'ensemble de règles du client NFS (`nfsClient`) diffère de celui des autres ensembles de règles.

Pour plus d'informations sur les configurations de pare-feu, reportez-vous à la documentation de *Sécurité vSphere*.

Comportement du pare-feu client NFS

L'ensemble de règles de pare-feu du client NFS ne se comporte pas comme les ensembles de règles de pare-feu ESXi. ESXi configure les paramètres du client NFS lorsque vous montez ou démontez une banque de données NFS. Le comportement dépend de la version de NFS.

Lorsque vous ajoutez, montez ou démontez une banque de données NFS, le comportement obtenu dépend de la version de NFS.

Comportement du pare-feu NFS v3

Lorsque vous ajoutez ou montez une banque de données NFS v3, ESXi vérifie l'état de l'ensemble de règles de pare-feu du client NFS (`nfsClient`).

- Si l'ensemble de règles `nfsClient` est désactivé, ESXi active l'ensemble de règles et désactive la stratégie Autoriser toutes les adresses IP en définissant l'indicateur `allowedAll` sur FALSE. L'adresse IP du serveur NFS est ajoutée à la liste des adresses IP sortantes autorisées.
- Si l'ensemble de règles `nfsClient` est activé, l'état de l'ensemble de règles et la stratégie d'adresse IP autorisée ne sont pas modifiés. L'adresse IP du serveur NFS est ajoutée à la liste des adresses IP sortantes autorisées.

Note Si vous activez manuellement l'ensemble de règles `nfsClient` ou configurez manuellement la stratégie Autoriser toutes les adresses IP, avant ou après avoir ajouté une banque de données NFS v3 dans le système, vos paramètres sont remplacés lorsque la dernière banque de données NFS v3 est démontée. L'ensemble de règles `nfsClient` est désactivé lorsque toutes les banques de données NFS v3 sont démontées.

Lorsque vous supprimez ou démontez une banque de données NFS v3, ESXi réalise l'une des actions suivantes.

- Si aucune des banques de données NFS v3 restantes n'est montée à partir du serveur de la banque de données que vous êtes en train de démonter, ESXi supprime l'adresse IP du serveur dans la liste des adresses IP sortantes.
- S'il ne reste aucune banque de données NFS v3 montée une fois l'opération de démontage terminée, ESXi désactive l'ensemble de règles de pare-feu `nfsClient`.

Comportement du pare-feu NFS v4.1

Lorsque vous montez la première banque de données NFS v4.1, ESXi active l'ensemble de règles `nfs41client` et définit son indicateur `allowedAll` sur TRUE. Cette action ouvre le port 2049 pour toutes les adresses IP. Le démontage d'une banque de données NFS v4.1 n'a pas d'impact sur l'état du pare-feu. En d'autres termes, le port 2049 s'ouvre la première fois que vous montez une banque de données NFS v4.1 et reste ouvert jusqu'à ce que vous le fermiez explicitement.

Vérifier les ports de pare-feu pour des clients NFS

Pour activer l'accès à un stockage NFS, ESXi ouvre automatiquement des ports de pare-feu pour les clients NFS lorsque vous montez une banque de données NFS. À des fins de dépannage, vous devrez éventuellement vérifier que les ports sont ouverts.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Système**, cliquez sur **Pare-feu**, puis sur **Modifier**.

- 4 Faites défiler les informations vers le bas jusqu'à une version appropriée de NFS pour vous assurer que le port est ouvert.

Utiliser des connexions routées L3 pour accéder à un stockage NFS

Lorsque vous utilisez des connexions routées L3 pour accéder à du stockage NFS, il vous faut prendre en compte un certain nombre d'exigences et de restrictions.

Assurez-vous que votre environnement répond aux exigences suivantes :

- Utiliser le protocole Hot Standby Router (HSRP) de Cisco dans le routeur IP. Si vous utilisez un routeur non-Cisco, utilisez à la place le protocole Virtual Router Redundancy Protocol (VRRP).
- Pour hiérarchiser le trafic NFS L3 sur les réseaux avec des bandes passantes limitées ou les réseaux encombrés, utilisez QoS (Quality of Service). Consultez la documentation de votre routeur pour de plus amples détails.
- Suivez les recommandations sur les connexions routées NFS L3 proposées par le fournisseur de stockage. Contactez votre fournisseur de stockage pour plus d'informations.
- Désactivez Network I/O Resource Management (NetIORM).
- Si vous prévoyez d'utiliser des systèmes avec des commutateurs en haut de baie ou un partitionnement de périphérique d'E/S dépendant d'un commutateur, contactez le fournisseur du système pour la compatibilité et la prise en charge.

Dans un environnement L3, les restrictions suivantes s'appliquent :

- L'environnement ne prend pas en charge VMware Site Recovery Manager.
- L'environnement prend uniquement en charge le protocole NFS. N'utilisez pas d'autres protocoles de stockage comme FCoE sur le même réseau physique.
- Le trafic NFS dans cet environnement ne prend pas en charge IPv6.
- Le trafic NFS dans cet environnement peut être routé uniquement sur un réseau local. Les autres environnements comme les réseaux WAN ne sont pas pris en charge.

Utilisation de Kerberos pour NFS 4.1

Avec NFS version 4.1, ESXi prend en charge le mécanisme d'authentification Kerberos.

Le mécanisme Kerberos RPCSEC_GSS est un service d'authentification. Il permet à un client NFS 4.1 installé sur ESXi de justifier son identité à un serveur NFS, préalablement au montage d'un partage NFS. Grâce au chiffrement, la sécurité Kerberos permet de travailler sur une connexion réseau non sécurisée.

La mise en œuvre ESXi de Kerberos pour NFS 4.1 fournit deux modèles de sécurité, krb5 et krb5i, qui offrent deux niveaux de sécurité différents.

- Kerberos pour l'authentification uniquement (krb5) prend en charge la vérification de l'identité.

- Kerberos pour l'authentification et l'intégrité des données (krb5i), en plus de la vérification de l'identité, fournit des services d'intégrité des données. Ces services permettent de protéger le trafic NFS contre la falsification en vérifiant les modifications potentielles des paquets de données.

Kerberos prend en charge des algorithmes de chiffrement qui empêchent les utilisateurs non autorisés d'obtenir l'accès au trafic NFS. Le client NFS 4.1 sur ESXi tente d'utiliser l'algorithme AES256-CTS-HMAC-SHA1-96 ou AES128-CTS-HMAC-SHA1-96 pour accéder à un partage sur le serveur NAS. Avant d'utiliser vos banques de données NFS 4.1, assurez-vous que l'algorithme AES256-CTS-HMAC-SHA1-96 ou AES128-CTS-HMAC-SHA1-96 est activé sur le serveur NAS.

Le tableau suivant compare les niveaux de sécurité Kerberos pris en charge par ESXi.

Tableau 9-7. Types de sécurité Kerberos

	ESXi 6.0	ESXi 6.5 et versions ultérieures
Kerberos pour l'authentification uniquement (krb5)	Total de contrôle d'intégrité pour l'en-tête RPC	Oui avec DES
	Total de contrôle d'intégrité pour les données RPC	Non
Kerberos pour l'authentification et l'intégrité des données (krb5i)	Total de contrôle d'intégrité pour l'en-tête RPC	Pas de krb5i
	Total de contrôle d'intégrité pour les données RPC	Oui avec AES

Lorsque vous utilisez l'authentification Kerberos, les considérations suivantes s'appliquent :

- ESXi utilise Kerberos avec le domaine Active Directory.
- En tant qu'administrateur de vSphere, vous devez spécifier les informations d'identification Active Directory requises pour octroyer l'accès aux banques de données Kerberos NFS 4.1 à un utilisateur NFS. Le même ensemble d'informations d'identification est utilisé pour accéder à toutes les banques de données Kerberos montées sur cet hôte.
- Lorsque plusieurs hôtes ESXi partagent la même banque de données NFS 4.1, vous devez utiliser les mêmes informations d'identification Active Directory pour tous les hôtes qui accèdent à la banque de données partagée. Pour automatiser le processus d'attribution, définissez l'utilisateur dans un profil d'hôte et appliquez le profil à tous les hôtes ESXi.
- Vous ne pouvez pas utiliser deux mécanismes de sécurité, AUTH_SYS et Kerberos, pour la même banque de données NFS 4.1 partagée par plusieurs hôtes.

Pour des instructions détaillées, reportez-vous à la documentation *Stockage vSphere*.

Configurer un environnement de stockage NFS

Vous devez effectuer plusieurs opérations de configuration avant de monter une banque de données NFS dans vSphere.

Conditions préalables

- Familiarisez-vous avec les directives de la section [Directives et configuration requise du stockage NFS](#).
- Pour obtenir plus de détails sur la configuration du stockage NFS, reportez-vous à la documentation du fournisseur de votre stockage.
- Si vous utilisez Kerberos, assurez-vous que AES256-CTS-HMAC-SHA1-96 ou AES128-CTS-HMAC-SHA1-96 sont activés sur le serveur NAS.

Procédure

- 1 Sur le serveur NFS, configurez un volume NFS et exportez-le pour le monter sur les hôtes ESXi.
 - a Notez l'adresse IP ou le nom DNS du serveur NFS, ainsi que le chemin d'accès complet, ou le nom de dossier, du partage NFS.
Pour NFS 4.1, vous pouvez collecter plusieurs adresses IP ou noms DNS pour utiliser la prise en charge de la gestion de chemins multiples fournie par la banque de données NFS 4.1.
 - b Si vous prévoyez utiliser l'authentification Kerberos avec NFS 4.1, spécifiez les informations d'identification Kerberos à utiliser par ESXi pour l'authentification.
- 2 Sur chaque hôte ESXi, configurez un port réseau VMkernel dédié au trafic NFS.
Pour plus d'informations, consultez la documentation *Mise en réseau vSphere*.
- 3 Si vous prévoyez utiliser l'authentification Kerberos avec la banque de données NFS 4.1, configurez les hôtes ESXi pour l'authentification Kerberos.
Reportez-vous à [Configurer les hôtes ESXi pour l'authentification Kerberos](#).

Étape suivante

Vous pouvez maintenant créer une banque de données NFS sur les hôtes ESXi.

Configurer les hôtes ESXi pour l'authentification Kerberos

Si vous utilisez NFS 4.1 avec Kerberos, vous devez effectuer différentes tâches afin de configurer vos hôtes pour l'authentification Kerberos.

Lorsque plusieurs hôtes ESXi partagent la même banque de données NFS 4.1, vous devez utiliser les mêmes informations d'identification Active Directory pour tous les hôtes qui accèdent à la banque de données partagée. Vous pouvez automatiser le processus d'attribution en définissant l'utilisateur dans les profils d'hôte et en appliquant le profil à tous les hôtes ESXi.

Conditions préalables

- Assurez-vous que les serveurs NFS et Microsoft Active Directory (AD) sont configurés de manière à utiliser Kerberos.

- Activez les modes de chiffrement AES256-CTS-HMAC-SHA1-96 ou AES128-CTS-HMAC-SHA1-96 sur AD. Le client NFS 4.1 ne prend pas en charge le mode de chiffrement DES-CBC-MD5.
- Assurez-vous que les exportations du serveur NFS sont configurées de manière à octroyer les droits d'accès complets à l'utilisateur Kerberos.

Procédure

1 Configurer DNS pour NFS 4.1 avec Kerberos

Lorsque vous utilisez NFS 4.1 avec Kerberos, vous devez modifier les paramètres DNS sur les hôtes ESXi. Les paramètres doivent pointer vers le serveur DNS configuré pour distribuer les enregistrements DNS dans le centre de distribution de clés Kerberos. Par exemple, utilisez l'adresse de serveur Active Directory, si Active Directory est utilisé comme serveur DNS.

2 Configurer le protocole NTP (Network Time Protocol) pour NFS 4.1 avec Kerberos

Si vous utilisez NFS 4.1 avec Kerberos, les hôtes ESXi, le serveur NFS et le serveur Active Domain doivent être synchronisés. En général, dans la configuration, le serveur Active Domain est utilisé comme serveur NTP (Network Time Protocol).

3 Activer l'authentification Kerberos dans Active Directory

Si vous utilisez le stockage NFS 4.1 avec Kerberos, vous devez ajouter chaque hôte ESXi à un domaine Active Directory et activer l'authentification Kerberos. Kerberos s'intègre à Active Directory pour permettre la fonctionnalité Single Sign-On et offrir une couche supplémentaire de sécurité en cas d'utilisation via une connexion réseau non sécurisée.

Configurer DNS pour NFS 4.1 avec Kerberos

Lorsque vous utilisez NFS 4.1 avec Kerberos, vous devez modifier les paramètres DNS sur les hôtes ESXi. Les paramètres doivent pointer vers le serveur DNS configuré pour distribuer les enregistrements DNS dans le centre de distribution de clés Kerberos. Par exemple, utilisez l'adresse de serveur Active Directory, si Active Directory est utilisé comme serveur DNS.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Mise en réseau**, cliquez sur **Configuration TCP/IP**.
- 4 Sélectionnez **Par défaut**, puis cliquez sur l'icône **Modifier**.
- 5 Entrez manuellement les paramètres DNS.

Option	Description
Domaine	<i>Nom de domaine AD</i>
Serveur DNS favori	<i>Adresse IP du serveur AD</i>
Rechercher dans les domaines	<i>Nom de domaine AD</i>

Configurer le protocole NTP (Network Time Protocol) pour NFS 4.1 avec Kerberos

Si vous utilisez NFS 4.1 avec Kerberos, les hôtes ESXi, le serveur NFS et le serveur Active Domain doivent être synchronisés. En général, dans la configuration, le serveur Active Domain est utilisé comme serveur NTP (Network Time Protocol).

La tâche suivante décrit comment synchroniser l'hôte ESXi avec le serveur NTP.

La meilleure pratique consiste à utiliser le serveur Active Domain comme serveur NTP.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Système**, sélectionnez **Configuration de temps**.
- 4 Cliquez sur **Modifier** et configurez le serveur NTP.
 - a Sélectionnez **Utiliser le protocole de temps du réseau (activer le client NTP)**.
 - b Pour procéder à une synchronisation avec le serveur NTP, entrez ses adresses IP.
 - c Sélectionnez **Démarrer le Service NTP**.
 - d Définissez la stratégie de démarrage du service NTP.
- 5 Cliquez sur **OK**.

L'hôte se synchronise avec le serveur NTP.

Activer l'authentification Kerberos dans Active Directory

Si vous utilisez le stockage NFS 4.1 avec Kerberos, vous devez ajouter chaque hôte ESXi à un domaine Active Directory et activer l'authentification Kerberos. Kerberos s'intègre à Active Directory pour permettre la fonctionnalité Single Sign-On et offrir une couche supplémentaire de sécurité en cas d'utilisation via une connexion réseau non sécurisée.

Conditions préalables

Configurez un domaine AD et un compte d'administrateur de domaine possédant les droits pertinents pour pouvoir ajouter des hôtes au domaine.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Système**, cliquez sur **Services d'authentification**.

- 4 Ajoutez l'hôte ESXi au domaine Active Directory.
 - a Dans le volet Services d'authentification, cliquez sur **Joindre le domaine**.
 - b Fournissez les paramètres du domaine, puis cliquez sur **OK**.

Le type des services d'annuaire devient Active Directory.
- 5 Configurez ou modifiez les informations d'identification d'un utilisateur NFS Kerberos.
 - a Dans le volet Informations d'identification NFS Kerberos, cliquez sur **Modifier**.
 - b Tapez un nom d'utilisateur et un mot de passe.

Ces informations d'identification permettront d'accéder aux fichiers stockés dans toutes les banques de données Kerberos.

L'état des informations d'identification NFS Kerberos devient Activé.

Étape suivante

Après avoir configuré l'hôte pour Kerberos, vous pouvez créer une banque de données NFS 4.1 avec Kerberos activé.

Configurer la liaison VMkernel pour la banque de données NFS 3

La liaison de port VMkernel pour la banque de données NFS 3 vous permet de lier un volume NFS à un adaptateur VMkernel spécifique pour établir la connexion avec un serveur NFS. Avec les banques de données NFS 3, vous pouvez isoler le trafic NFS et le lier à un adaptateur VMkernel spécifique. Pour acheminer le trafic vers cet adaptateur, connectez la banque de données à l'adaptateur.

Note Sans liaison, en cas de défaillance de l'adaptateur VMkernel que ESXi utilise pour le trafic NFS, l'infrastructure réseau redirige le trafic sur une autre route. De ce fait, le trafic NFS risque de passer involontairement par un adaptateur VMkernel aléatoire.

Conditions préalables

- Configurez l'environnement de stockage NFS.
- Créez et configurez un adaptateur VMkernel sur la pile TCP/IP par défaut.

Procédure

- 1 Liez une banque de données NFS 3 à un adaptateur VMkernel.
 - a Dans le navigateur d'objets vSphere Client, accédez à un hôte, un cluster ou un centre de données.
 - b Dans le menu contextuel, sélectionnez **Stockage > Nouvelle banque de données**.
 - c Choisissez **NFS** comme type de banque de données et sélectionnez **NFS 3**.
 - d Entrez les paramètres de banque de données. Pour plus d'informations, consultez [Créer une banque de données NFS](#).

- e Sélectionnez **Lier à vmknic**.
- f Si vous créez une banque de données au niveau du centre de données ou du cluster, sélectionnez les hôtes qui assurent le montage de la banque de données.
- g Pour la banque de données au niveau du centre de données ou du cluster, sélectionnez l'une des options suivantes.
 - Sélectionnez **Vmknics sur tous les hôtes**. Avec cette option, des adaptateurs VMkernel sélectionnables sont disponibles sur tous les hôtes sur lesquels vous montez votre banque de données.
 - Sélectionnez **Vmknic par hôte**. Avec cette option, vous pouvez spécifier un adaptateur VMkernel par hôte.

Note Vous ne pouvez effectuer qu'une sélection à la fois.

- h Passez en revue les options de configuration que vous avez choisies puis cliquez sur **Terminer**.
- 2 Vérifiez les hôtes connectés à la banque de données NFS 3.

- a Dans la vSphere Client, sélectionnez la banque de données NFS 3 avec liaison d'adaptateur VMkernel.
- b Cliquez sur l'onglet **Configurer**, puis sur **Connectivité avec les hôtes**.

Vous pouvez afficher tous les hôtes connectés à la banque de données NFS 3. La colonne **Liaison Vmknic** affiche les adaptateurs VMkernel connectés à la banque de données

The screenshot shows the vSphere Client interface for managing a datastore. The left sidebar shows a tree view with nodes like '10.196.138.', 'vcqaDC', and 'Datastore_15'. The 'Datastore_15' node is selected. The main pane has tabs for 'Summary', 'Monitor', 'Configure', 'Permissions', 'Files', 'Hosts', and 'VMs'. The 'Configure' tab is active, and the 'Connectivity with Hosts' section is selected. A table titled 'Connectivity with Hosts' lists two hosts: '10.196.138....' which is connected with 'Read-write' access mode and 'vmk1' binding, and another entry for '10.196.138....' which is also connected with 'Read-write' access mode and 'vmk1' binding. The table has columns for Host, Datastore Connectivity, Access Mode, Vmknic Binding, and Mount Point.

Host	Datastore Connectivity	Access Mode	Vmknic Binding	Mount Point
10.196.138....	Connected	Read-write	vmk1	/vmfs/volumes/d40c67cc-3ca9a6...
10.196.138....	Connected	Read-write	vmk1	/vmfs/volumes/d40c67cc-3ca9a6...

Note Si vous supprimez l'adaptateur VMkernel associé à la banque de données NFS 3, la banque de données devient inaccessible, ce qui déclenche un avertissement. L'avertissement affiche le texte dans l'écran **Événements**, semblable au suivant.

```
vmknic vmkX removed, NFSv3 datastore datastore_name configured with the vmknic will
be inaccessible.
```

Collecte d'informations statistiques pour le stockage NFS

Vous pouvez utiliser l'outil `nfsStats` de votre hôte ESXi pour afficher des informations statistiques sur les appels NFS et les appels de procédure distante (RPC). La commande affiche des informations statistiques pour les montages NFS 3 et NFS 4.1 sur l'hôte ESXi.

L'outil `nfsStats` effectue généralement les tâches suivantes.

- Rassemble les statistiques NFS pour examiner les problèmes survenant lors du déploiement d'une nouvelle configuration (par exemple, un nouveau serveur ou réseau NFS) dans l'environnement NFS.
- Fournit des statistiques sur la réussite et l'échec des opérations NFS.
- Publie des statistiques de latence sur la réussite et l'échec des opérations NFS.
- Corrige les problèmes de performances NFS.

La syntaxe de la commande est `nfsStats options`.

Les options de commande suivantes sont disponibles.

Tableau 9-8. Commandes `nfsStats`

Option de commande	Description
No option	Obtenir les statistiques NFS et RPC pour toutes les banques de données NFS.
-3	N'afficher que les statistiques NFS 3.
-4	N'afficher que les statistiques NFS 4.1.
-n	N'afficher que les statistiques NFS 3 et NFS 4.1.
-r	Afficher les statistiques RPC.
<code>-i interval</code>	Afficher les statistiques NFS et RPC à un intervalle égal à la valeur spécifiée en secondes. Par exemple, si la valeur que vous entrez est 10, les statistiques sont actualisées toutes les 10 secondes.
-j	Afficher les statistiques au format JSON.
-e	Affichez les statistiques d'erreur pour les protocoles NFS 3, NFS 4.1 et RPC.
<code>-d, --datastore-name DSNAME1, DSNAME2, ...</code>	Afficher les statistiques NFS et RPC pour les banques de données NFS spécifiées. Utilisez cette option en conjonction avec le type de la banque de données NFS (par exemple, -3 ou -4).

Présentation de la gestion multivoie et du basculement

10

Pour assurer une connexion constante entre un hôte et son stockage, ESXi prend en charge le chemins multiples. La gestion multivoie vous permet d'utiliser plusieurs chemins physiques qui transfèrent les données entre l'hôte et un périphérique de stockage externe.

En cas de panne d'un élément dans le réseau SAN, tel qu'un adaptateur, un commutateur ou un câble, l'ESXi peut basculer vers un autre chemin physique viable. Ce processus de basculement du chemin afin d'éviter des composants défaillants est connu sous le nom de basculement de chemin.

En plus du basculement de chemin, le chemins multiples permet d'équilibrer les charges. L'équilibrage de charge est le procédé qui consiste à distribuer les charges E/S sur différents chemins d'accès physiques. L'équilibrage de charge réduit, voire supprime, les goulets d'étranglement potentiels.

Note Les E/S d'une machine virtuelle peuvent être retardées de 60 secondes maximum lors du basculement de chemin. Ces délais permettent au SAN de stabiliser sa configuration après les modifications de topologie. En général, les délais d'E/S peuvent s'avérer plus longs sur les baies actives/passives et plus courts sur les baies actives/actives.

Ce chapitre contient les rubriques suivantes :

- Basculements avec Fibre Channel
- Basculement basé sur hôte avec iSCSI
- Basculement à base de baie avec iSCSI
- Basculement de chemin et machines virtuelles
- Architecture de stockage enfichable et gestion des chemins
- Affichage et gestion des chemins
- Utilisation des règles de réclamation
- Files d'attente de planification pour les E/S de machines virtuelles

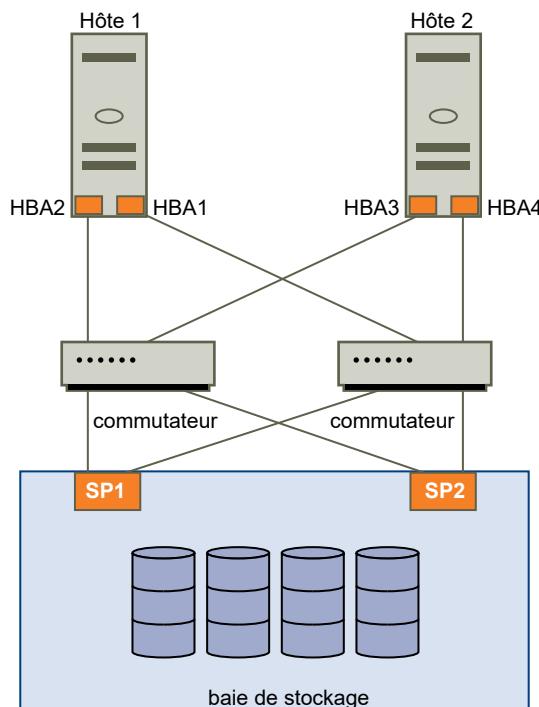
Basculements avec Fibre Channel

Afin de prendre en charge la gestion multivoie, de façon classique votre hôte dispose de deux ou plusieurs HBA disponibles. Cette configuration complète la configuration de gestion multivoie

SAN. De manière générale, la gestion multivoie SAN fournit un ou plusieurs commutateurs dans la production SAN et un ou plusieurs processeurs de stockage sur la baie de stockage elle-même.

Dans l'illustration suivante, les chemins multiples physiques connectent chaque serveur au périphérique de stockage. Par exemple, si HBA1 ou le lien entre HBA1 et le commutateur FC tombe en panne, HBA2 reprend la fonction et fournit la connexion. Le processus de reprise par un HBA pour un autre est appelé basculement HBA.

Figure 10-1. Gestion multivoie et basculement avec Fibre Channel



De même, si SP1 tombe en panne ou que les liens entre SP1 et les commutateurs sont brisés, SP2 reprend la main. SP2 fournit la connexion entre le commutateur et le périphérique de stockage. Ce processus est appelé basculement SP. VMware ESXi prend en charge les basculements HBA et SP.

Basculement basé sur hôte avec iSCSI

Lorsque vous configurez votre hôte ESXi pour la gestion multivoie et le basculement, vous pouvez utiliser plusieurs HBA iSCSI ou combiner plusieurs cartes réseau avec l'adaptateur iSCSI logiciel.

Pour plus d'informations sur les différents types d'adaptateurs iSCSI, consultez [Initiateurs iSCSI](#).

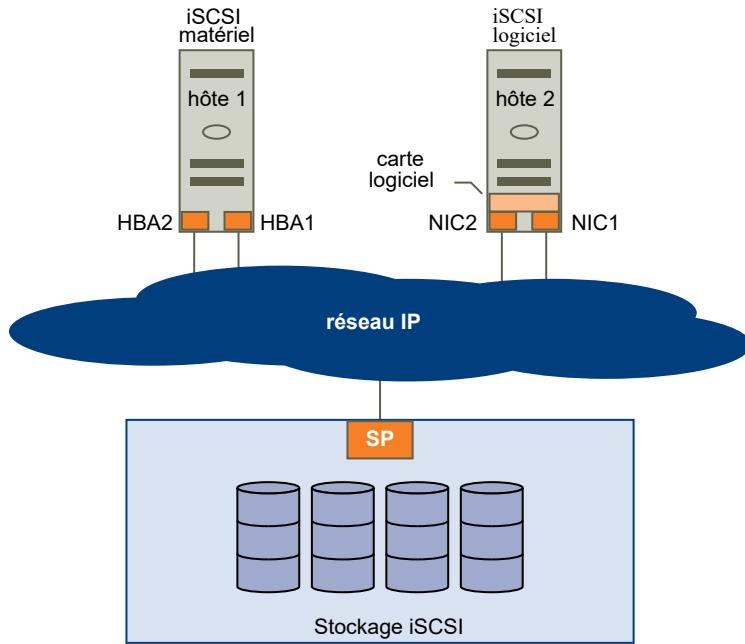
Lorsque vous utilisez la gestion multivoie, certaines considérations spécifiques s'appliquent.

- ESXi ne prend pas en charge la gestion multivoie lorsque vous combinez des adaptateurs de matériel indépendant à des adaptateurs logiciels ou de matériel dépendant dans le même hôte.

- La gestion des chemins multiples entre les adaptateurs logiciels et dépendants dans le même hôte est prise en charge.
- Vous pouvez mélanger les adaptateurs dépendants et indépendants, sur différents hôtes.

L'illustration suivante montre les configurations à chemins multiples possibles avec différents types d'initiateurs iSCSI.

Figure 10-2. Basculement de chemin basé sur hôte



iSCSI matériel et basculement

Avec iSCSI matériel, l'hôte dispose généralement de plusieurs adaptateurs iSCSI matériels. L'hôte utilise les adaptateurs pour atteindre le système de stockage via un ou plusieurs commutateurs. La configuration peut également inclure un adaptateur et deux processeurs de stockage afin que l'adaptateur utilise des chemins différents pour atteindre le système de stockage.

Sur l'illustration, Host1 possède deux adaptateurs iSCSI matériels, HBA1 et HBA2, qui fournissent deux chemins physiques vers le système de stockage. Les plug-ins de gestion multivoie sur votre hôte, qu'il s'agisse du NMP VMkernel ou de MPP tiers, ont accès aux chemins par défaut. Les plug-ins peuvent surveiller la santé de chaque chemin physique. Si, par exemple, le HBA1 ou la liaison entre le HBA1 et le réseau échoue, les plug-ins de chemins multiples peuvent basculer le chemin sur le HBA2.

iSCSI logiciel et basculement

Avec iSCSI logiciel, comme indiqué sur l'hôte 2 de l'illustration, vous pouvez utiliser plusieurs cartes réseau qui fournissent des capacités d'équilibrage de charge et de basculement pour les connexions iSCSI.

Les plug-ins de gestion multivoie n'ont pas un accès direct aux cartes réseau physiques de votre hôte. Par conséquent, pour cette configuration, vous devez d'abord connecter chaque carte réseau physique à un port VMkernel distinct. Vous associez ensuite tous les ports VMkernel à l'initiateur iSCSI logiciel à l'aide d'une technique de liaison de port. Chaque port VMkernel connecté à une carte réseau séparée devient un chemin différent que la pile de stockage iSCSI et ses plug-ins de gestion multivoie prenant en charge le stockage peuvent utiliser.

Pour plus d'informations sur la configuration de la gestion multivoie pour iSCSI logiciel, consultez [Configuration du réseau pour iSCSI et iSER](#).

Basculement à base de baie avec iSCSI

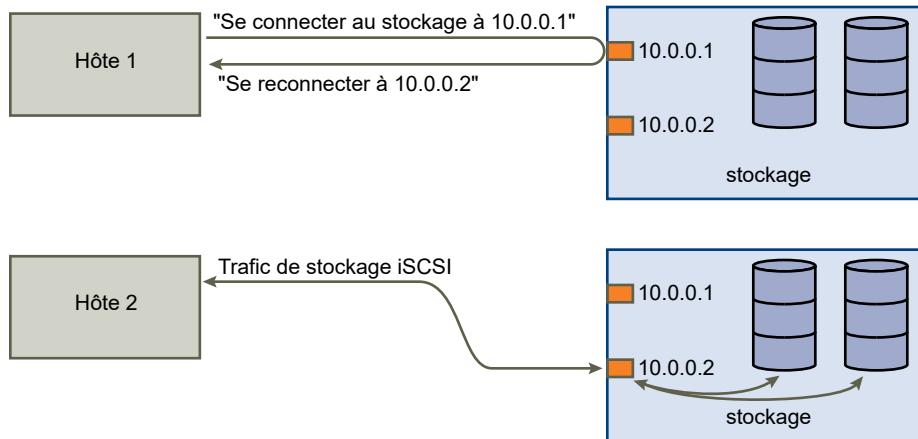
Certains systèmes de stockage iSCSI gèrent l'utilisation des chemins de leurs ports de manière automatique et transparente vers ESXi.

Lorsque vous utilisez l'un de ces systèmes de stockage, votre hôte ne voit pas plusieurs ports sur le stockage et ne peut pas choisir le port de stockage auquel se connecter. Ces systèmes disposent d'une seule adresse de port virtuel que votre hôte utilise au départ pour communiquer. Pendant cette communication initiale, le système de stockage peut rediriger l'hôte pour qu'il communique avec un autre port sur le système de stockage. Les initiateurs iSCSI dans l'hôte obéissent à cette demande de reconnexion et se connectent à un autre port sur le système. Le système de stockage utilise cette technique pour répartir la charge sur les différents ports disponibles.

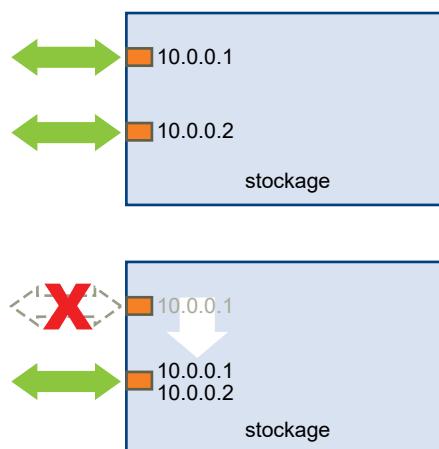
Si l'hôte ESXi perd sa connexion à l'un de ces ports, il tente automatiquement de se reconnecter au port virtuel du système de stockage et doit être redirigé vers un port utilisable actif. Cette reconnexion et redirection se produit rapidement et n'interrompt généralement pas l'exécution des machines virtuelles. Ces systèmes de stockage peuvent également demander que les initiateurs iSCSI se reconnectent au système pour modifier le port de stockage auquel ils sont connectés. Cela permet une utilisation plus efficace des différents ports.

L'illustration Redirection de port montre un exemple de redirection de port. L'hôte tente de se connecter au port virtuel 10.0.0.1. Le système de stockage redirige cette demande vers le port 10.0.0.2. L'hôte se connecte au port 10.0.0.2 et l'utilise pour la communication E/S.

Note Le système de stockage ne redirige pas toujours les connexions. Le port 10.0.0.1 peut également être utilisé pour le trafic.

Figure 10-3. Redirection de port

Si le port du système de stockage qui agit en tant que port virtuel devient indisponible, le système de stockage réattribue l'adresse du port virtuel à un autre port du système. L'illustration Réattribution de port montre un exemple de ce type de réattribution de port. Dans ce cas, le port virtuel 10.0.0.1 devient indisponible et le système de stockage réattribue l'adresse IP du port virtuel à un autre port. Le second port répond aux deux adresses.

Figure 10-4. Réattribution de port

Avec cette forme de basculement basé sur baie, vous pouvez avoir plusieurs chemins d'accès au stockage uniquement si vous utilisez plusieurs ports sur l'hôte ESXi. Ces chemins sont actifs-actifs. Pour plus d'informations, reportez-vous à la section [Gestion des sessions iSCSI](#).

Basculement de chemin et machines virtuelles

Un basculement de chemin se produit lorsque le chemin actif vers un LUN est remplacé par un autre chemin. En général, le basculement de chemin se produit suite à une panne de composant SAN sur le chemin actuel.

En cas de défaillance d'un chemin, l'E/S de stockage peut s'interrompre pendant 30 à 60 secondes jusqu'à ce que votre hôte détermine que ce lien est indisponible et effectue le basculement. Si vous essayez d'afficher l'hôte, ses périphériques de stockage ou ses adaptateurs, le fonctionnement peut apparaître figé. Les machines virtuelles avec leurs disques installés sur le stockage SAN peuvent apparaître comme ne répondant plus. Après le basculement, l'E/S reprend normalement et les machines virtuelles continuent à fonctionner.

Une machine virtuelle Windows peut interrompre l'E/S et peut finalement échouer si les basculements prennent trop de temps. Pour éviter la panne, définissez le délai du disque pour la machine virtuelle Windows à au moins 60 secondes.

Définir le délai d'expiration du SE invité Windows

Pour éviter les interruptions pendant un basculement de chemin, augmentez la valeur de délai d'expiration de disque standard sur un système d'exploitation invité Windows.

Cette procédure explique comment changer le délai d'expiration en utilisant le registre de Windows.

Conditions préalables

Sauvegarde du registre Windows.

Procédure

- 1 Sélectionnez **Démarrer > Exécuter**.
- 2 Tapez **regedit.exe**, et cliquez sur **OK**.
- 3 Dans la vue hiérarchique du panneau de gauche, double-cliquez sur **HKEY_LOCAL_MACHINE > System > CurrentControlSet > Services > Disk**.
- 4 Faites un double clic sur **TimeOutValue**.
- 5 Définissez la valeur sur 0x3c (hexadécimal) ou 60 (décimal) et cliquez sur **OK**.

Après avoir effectué cette modification, Windows attend au moins 60 secondes pour que les opérations de disque puissent se terminer avant de générer des erreurs.

- 6 Redémarrez le SE invité pour appliquer la modification.

Architecture de stockage enfichable et gestion des chemins

Cette rubrique présente les principaux concepts qui sous-tendent la gestion multivoie du stockage d'ESXi.

Architecture de stockage enfichable (PSA)

Pour gérer la gestion multivoie, ESXi utilise une couche VMkernel spéciale appelée Architecture de stockage enfichable (PSA). La PSA est une structure modulaire et ouverte qui coordonne les divers modules logiciels responsables des opérations de gestion multivoie.

Ces modules incluent des modules de gestion multivoie génériques fournis par VMware, NMP et HPP, ainsi que des MPP tiers.

Native Multipathing Plug-in (NMP)

Le NMP est le module de gestion multivoie VMkernel que ESXi fournit par défaut. Le NMP associe des chemins physiques à un périphérique de stockage spécifique et fournit un algorithme de sélection de chemin par défaut qui repose sur le type de la baie. Le NMP est extensible et gère des sous-modules supplémentaires, appelés Règles de sélection de chemin (PSP) et Stratégie du type de baie de stockage (SATP). Les PSP et les SATP peuvent être fournis par VMware ou par un tiers.

Path Selection Plug-ins (PSP)

Les PSP sont des sous-modules du VMware NMP. Ils sont responsables de la sélection d'un chemin physique pour des demandes d'E/S.

Storage Array Type Plug-ins (SATP)

Les SATP sont des sous-modules du VMware NMP. Les SATP sont responsables des opérations spécifiques des baies. Le SATP peut déterminer l'état d'un chemin particulier spécifique d'une baie, activer un chemin et détecter les erreurs de chemin.

Multipathing Plug-ins (MPP)

Le PSA propose une collection d'API VMkernel que les tiers peuvent utiliser pour créer leurs propres plug-ins de gestion multivoie (MPP). Les modules fournissent des fonctionnalités d'équilibrage de charge et de basculement spécifiques pour une baie de stockage particulière. Les MPP peuvent être installés sur l'hôte ESXi. Ils peuvent s'exécuter en plus des modules VMware natifs, ou les remplacer.

VMware High-Performance Plug-in (HPP)

Le HPP remplace le NMP pour les périphériques à haute vitesse, tels que les dispositifs NVMe. Le HPP peut améliorer les performances des périphériques flash ultra-rapides installés localement sur votre hôte ESXi et est le plug-in par défaut qui récupère les NVMe cibles. Pour prendre en charge la gestion multivoie, le HPP utilise les schémas PSS (Path Selection Schemes). Un PSS particulier est responsable de la sélection des chemins physiques pour les demandes d'E/S.

Pour plus d'informations, consultez [VMware High Performance Plug-In et Path Selection Schemes](#).

Règles de réclamation

Le PSA utilise des règles de réclamation pour déterminer quel plug-in possède les chemins d'accès à un périphérique de stockage particulier.

Tableau 10-1. Acronymes relatifs à la gestion des chemins

Acronyme	Définition
PSA	Architecture de stockage enfichable
NMP	Native Multipathing Plug-in. Module de gestion multivoie VMware générique utilisé par des périphériques de stockage SCSI.
PSP	Path Selection Plug-in. Gère la sélection de chemin d'un périphérique de stockage SCSI.
SATP	Storage Array Type Plug-in. Gère le basculement de chemin d'une baie de stockage SCSI.
MPP (tiers)	Multipathing Plug-in. Module de gestion multivoie développé et fourni par un tiers.
HPP	Native High-Performance Plug-in fourni par VMware. Il est utilisé avec des périphériques flash ultra-rapides, locaux et en réseau, tels que NVMe.
PSS	Schéma de sélection de chemin Gère la gestion multivoie pour les périphériques de stockage NVMe.

À propos de l'architecture de stockage enfichable

L'architecture de stockage enfichable (PSA) est une structure modulaire et ouverte qui coordonne divers modules logiciels responsables des opérations de gestion multivoie.

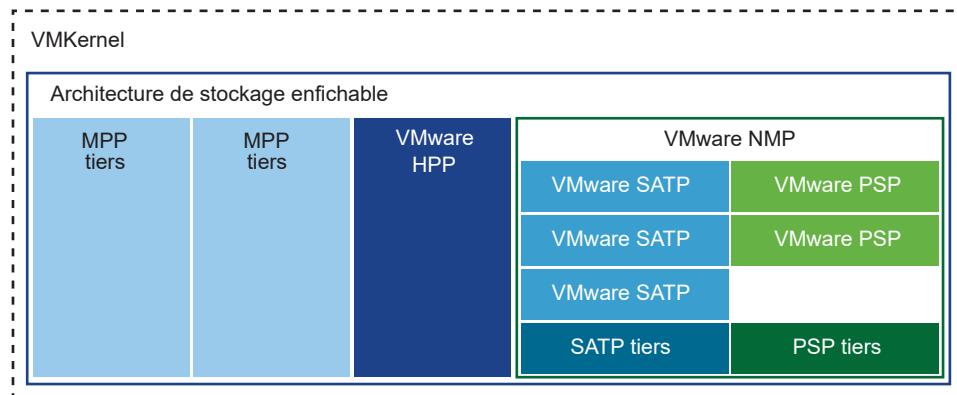
VMware fournit des modules de gestion multivoie natifs génériques, appelés VMware NMP et VMware HPP. En outre, la PSA propose une collection d'API VMkernel destinée aux développeurs tiers. Les développeurs de logiciels peuvent créer leurs propres modules d'équilibrage de charge et de basculement pour une baie de stockage en particulier. Ces modules de gestion multivoie tiers (MPP) peuvent être installés sur l'hôte ESXi et s'exécuter en complément des modules VMware natifs ou en les remplaçant.

Lors de la coordination des modules VMware natifs et de tous les MPP tiers installés, la PSA effectue les tâches suivantes :

- Chargement et déchargement des plug-ins gestion multivoie.
- Dissimulation des informations détaillées sur la machine virtuelle à un plug-in particulier.
- Routage des demandes d'E/S pour un périphérique logique spécifique vers le MPP qui gère ce périphérique.
- Traitement des files d'attente d'E/S vers les périphériques logiques.
- Mise en place du partage de la bande passante du périphérique logique entre les machines virtuelles.
- Traitement des files d'attente d'E/S vers les HBA de stockage physiques.
- Traitement de la détection et de la suppression des chemins physiques.
- Mise à disposition des statistiques d'E/S du périphérique logique et du chemin physique.

Comme l'illustration de l'architecture de stockage enfichable le montre, de multiples MPP tiers peuvent s'exécuter parallèlement au NMP ou HPP VMware. Lorsqu'ils sont installés, les MPP tiers peuvent remplacer le comportement des modules natifs. Les MPP peuvent prendre le contrôle des opérations de basculement de chemin et d'équilibrage de charge pour les périphériques de stockage spécifiés.

Figure 10-5. Architecture de stockage enfichable



VMware Native Multipathing Plug-In

Par défaut, ESXi offre un module de gestion multivoie extensible appelé NMP (Native Multipathing Plug-In).

De manière générale, le VMware NMP prend en charge toutes les baies de stockage répertoriées sur la liste de compatibilité matérielle (HCL) de stockage de VMware et fournit un algorithme de sélection de chemin par défaut reposant sur le type de baie. Le NMP associe une série de chemins physiques à un périphérique de stockage spécifique ou à une LUN.

Pour toute opération de gestion multivoie supplémentaire, le NMP utilise des sous-modules appelés SATP et PSP. Le NMP délègue au SATP les détails spécifiques de la gestion du basculement de chemin pour le périphérique. Le PSP gère la sélection de chemin pour le périphérique.

En général, le NMP effectue les opérations suivantes :

- Gère les réclamations et les non-réclamations de chemins physiques.
- Enregistre et annule l'enregistrement des périphériques logiques.
- Associe les chemins physiques aux périphériques logiques.
- Prend en charge la détection et la correction des pannes de chemin.
- Traite les demandes d'E/S vers les périphériques logiques :
 - Sélectionne un chemin physique optimal pour la demande.
 - Effectue les actions nécessaires à la gestion des pannes de chemin et des nouvelles tentatives de commande d'E/S.
- Prend en charge les tâches de gestion, telles que la réinitialisation des périphériques logiques.

ESXi installe automatiquement un SATP approprié pour une baie que vous utilisez. Il n'est pas nécessaire d'obtenir ou de télécharger de SATP.

Flux d'E/S de VMware NMP

Lorsqu'une machine virtuelle envoie une demande d'E/S à un périphérique de stockage géré par le NMP, le processus suivant a lieu :

- 1 Le NMP appelle le PSP assigné à ce périphérique de stockage.
- 2 Le PSP sélectionne le chemin physique approprié sur lequel il peut envoyer l'E/S.
- 3 Le NMP envoie la requête d'E/S sur le chemin sélectionné par le PSP.
- 4 Si l'opération d'E/S réussie, le NMP signale qu'elle est terminée.
- 5 Si l'opération d'E/S échoue, le NMP appelle le SATP approprié.
- 6 Le SATP interprète les erreurs de commande d'E/S et, si nécessaire, active les chemins inactifs.
- 7 Le PSP est appelé et sélectionne un nouveau chemin sur lequel il peut envoyer l'E/S.

Affichage des modules de gestion multivoie

Utilisez la commande `esxcli` pour répertorier tous les modules de gestion multivoie chargés sur le système. Les modules de gestion multivoie gèrent les chemins physiques qui connectent votre hôte au stockage. Les modules incluent le NMP et HPP VMware natifs et des MPP tiers.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Pour afficher les modules de gestion multivoie, exécutez la commande suivante :

```
esxcli storage core plugin list --plugin-class=MP
```

Résultats

Cette commande montre généralement le NMP, le HPP et le module MASK_PATH, s'il est chargé. Si des MPP tiers ont été chargés, ils sont également répertoriés.

Plugin name	Plugin class
NMP	MP

Pour plus d'informations sur cette commande, consultez la documentation *Concepts et exemples d'ESXCLI et Référence d'ESXCLI*.

Affichage des périphériques de stockage NMP

Utilisez la commande `esxcli` pour répertorier tous les périphériques de stockage contrôlés par le VMware NMP et afficher les informations sur le SATP et le PSP correspondant à chaque périphérique.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Pour répertorier tous les périphériques de stockage, exécutez la commande suivante :

```
esxcli storage nmp device list
```

Utilisez le paramètre `--device | -d=device_ID` pour filtrer le résultat de cette commande et afficher un seul périphérique.

Exemple : Affichage des périphériques de stockage NMP

```
# esxcli storage nmp device list
mpx.vmhba1:C0:T2:L0
  Device Display Name: Local VMware Disk (mpx.vmhba1:C0:T2:L0)
  Storage Array Type: VMW_SATP_LOCAL
  Storage Array Type Device Config: SATP VMW_SATP_LOCAL does not support device
configuration.
  Path Selection Policy: VMW_PSP_FIXED
  Path Selection Policy Device Config: {preferred=vmhba1:C0:T2:L0;current=vmhba1:C0:T2:L0}
  Path Selection Policy Device Custom Config:
  Working Paths: vmhba1:C0:T2:L0
  Is USB: false

.....
eui.6238666462643332
  Device Display Name: SCST_BIO iSCSI Disk (eui.6238666462643332)
  Storage Array Type: VMW_SATP_DEFAULT_AA
  Storage Array Type Device Config: {action_OnRetryErrors=off}
  Path Selection Policy: VMW_PSP_FIXED
  Path Selection Policy Device Config: {preferred=vmhba65:C0:T0:L0;current=vmhba65:C0:T0:L0}
  Path Selection Policy Device Custom Config:
  Working Paths: vmhba65:C0:T0:L0
  Is USB: false
```

Pour plus d'informations sur cette commande, consultez la documentation *Concepts et exemples d'ESXCLI* et *Référence d'ESXCLI*.

Path Selection Plug-Ins et règles

Les plug-ins VMware Path Selection Plug-ins (PSP) sont responsables de la sélection d'un chemin physique pour les demandes d'E/S.

Les plug-ins sont des sous-modules du VMware NMP. Le NMP attribue un PSP par défaut pour chaque périphérique logique en fonction du type de périphérique. Vous pouvez remplacer le PSP par défaut. Pour plus d'informations, consultez [Modification de la stratégie de sélection de chemin d'accès](#).

Chaque PSP active et applique une stratégie de sélection de chemin correspondante.

VMW_PSP_MRU - Plus récemment utilisé (VMware)

La stratégie Plus fréquemment utilisé (VMware) est appliquée par VMW_PSP_MRU. Elle sélectionne le premier chemin opérationnel détecté au moment du démarrage du système. Quand le chemin d'accès devient non disponible, l'hôte sélectionne un autre chemin d'accès. L'hôte ne restaure pas le chemin d'accès d'origine quand ce chemin devient disponible. La stratégie Plus fréquemment utilisé n'utilise pas le paramètre de chemin préféré. Plus fréquemment utilisé est la stratégie par défaut pour la plupart des périphériques de stockage actifs-passifs.

VMW_PSP_MRU prend en charge le classement des chemins. Pour définir les rangs des chemins individuels, utilisez la commande `esxcli storage nmp psp generic pathconfig set`. Pour plus d'informations, consultez l'article de la base de connaissances VMware à l'adresse <http://kb.vmware.com/kb/2003468> et la documentation *Référence d'ESXCLI*.

VMW_PSP_FIXED - Corrigé (VMware)

La stratégie Fixe (VMware) est mise en œuvre par VMW_PSP_FIXED. Elle utilise le chemin préféré désigné. Si le chemin préféré n'est pas attribué, la stratégie sélectionne le premier chemin opérationnel détecté au moment du démarrage du système. Si le chemin préféré devient non disponible, l'hôte sélectionne un autre chemin disponible. L'hôte renvoie le chemin préféré précédemment défini lorsqu'il devient à nouveau disponible.

Fixe est la stratégie par défaut pour la plupart des baies actives/actives.

VMW_PSP_RR - Circulaire (VMware)

VMW_PSP_RR active la stratégie Répétition alternée (VMware). Répétition alternée est la stratégie par défaut pour de nombreuses baies. Elle emploie un algorithme de sélection automatique de chemin qui effectue une permutation circulaire sur tous les chemins configurés.

Les baies actives-actives et actives-passives utilisent la stratégie pour mettre en œuvre l'équilibrage de charge sur les chemins pour différents LUN. Avec les baies actives-passives, la stratégie utilise les chemins actifs. Avec les baies actives-actives, la stratégie utilise tous les chemins disponibles.

Le mécanisme de latence qui peut être activé pour la stratégie la rend plus adaptative. Pour atteindre de meilleurs résultats d'équilibrage de charge, le mécanisme sélectionne dynamiquement un chemin d'accès optimal en tenant compte des caractéristiques de chemin d'accès suivants :

- Bande passante d'E/S

- Latence de chemin d'accès

Pour modifier les paramètres par défaut de la stratégie circulaire à latence adaptative, ou pour désactiver le mécanisme de latence, consultez la section [Modifier les paramètres par défaut pour la latence circulaire](#).

Pour définir d'autres paramètres configurables pour VMW_PSP_RR, utilisez la commande `esxcli storage nmp psp roundrobin`. Pour plus d'informations, voir la documentation [Référence d'ESXCLI](#).

SATP de VMware

Les SATP (Storage Array Type Plug-in) sont responsables des opérations spécifiques aux baies. Les SATP sont des sous-modules du module VMware NMP.

ESXi offre un SATP pour chaque type de baie pris en charge par VMware. ESXi fournit également des SATP par défaut qui prennent en charge des périphériques actifs-actifs, actifs-passifs, ALUA et locaux non spécifiques.

Chaque SATP contient des caractéristiques spéciales d'une certaine classe de baie de stockage. Un SATP peut effectuer les opérations spécifiques à une baie nécessaires pour détecter l'état du chemin d'accès et activer un chemin inactif. Par conséquent, le module NMP peut fonctionner avec de nombreuses baies de stockage sans avoir à connaître les informations détaillées du périphérique de stockage.

En règle générale, le module NMP détermine le SATP à utiliser pour un périphérique de stockage spécifique et l'associe aux chemins physiques de ce périphérique de stockage. Le SATP effectue notamment les tâches suivantes :

- Surveillance du bon fonctionnement de chaque chemin physique.
- Rapports sur les modifications d'état de chaque chemin physique.
- Exécution d'actions spécifiques à la baie nécessaires pour le basculement du stockage. Par exemple, pour les périphériques actifs-passifs, il peut activer les chemins passifs.

ESXi inclut plusieurs modules SATP génériques pour les baies de stockage.

VMW_SATP_LOCAL

SATP pour les périphériques locaux directement reliés.

À compter de la version vSphere 6.5 Update 2, VMW_SATP_LOCAL prend en charge les chemins multiples pour les périphériques locaux, sauf les périphériques au format natif 4K. Pour réclamer des chemins multiples vers les périphériques locaux, vous n'êtes plus obligé d'utiliser d'autres SATP, comme dans les versions antérieures de vSphere.

VMW_SATP_LOCAL prend en charge les plug-ins de sélection de chemin VMW_PSP_MRU et VMW_PSP_FIXED, mais ne prend pas en charge le plug-in VMW_PSP_RR.

VMW_SATP_DEFAULT_AA

SATP générique pour les baies actives-actives.

VMW_SATP_DEFAULT_AP

SATP générique pour les baies actives-passives.

VMW_SATP_ALUA

SATP pour les baies ALUA.

Pour plus d'informations, reportez-vous au *Guide de compatibilité VMware* et à la documentation *Référence d'ESXCLI*.

Affichage des SATP pour l'hôte

Utilisez la commande `esxcli` pour répertorier les SATP NMP de VMware chargés sur le système. Affichez les informations sur les SATP.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Pour répertorier les SATP de VMware, exécutez la commande suivante :

```
esxcli storage nmp satp list
```

Résultats

Pour chaque SATP, la sortie affiche les informations indiquant le type de baie de stockage ou de système pris en charge par le SATP. Le résultat indique également le PSP par défaut pour tous les LUN qui utilisent ce SATP. Placeholder (plugin not loaded) dans la colonne Description indique que le SATP n'est pas chargé.

Exemple : Affichage des SATP pour l'hôte

```
# esxcli storage nmp satp list
Name          Default PSP    Description
VMW_SATP_MSA   VMW_PSP_MRU  Placeholder (plugin not loaded)
VMW_SATP_ALUA  VMW_PSP_MRU  Placeholder (plugin not loaded)
VMW_SATP_DEFAULT_AP VMW_PSP_MRU Placeholder (plugin not loaded)
VMW_SATP_SVC    VMW_PSP_FIXED Placeholder (plugin not loaded)
VMW_SATP_EQL    VMW_PSP_FIXED Placeholder (plugin not loaded)
VMW_SATP_INV    VMW_PSP_FIXED Placeholder (plugin not loaded)
VMW_SATP_EVA    VMW_PSP_FIXED Placeholder (plugin not loaded)
VMW_SATP_ALUA_CX VMW_PSP_RR   Placeholder (plugin not loaded)
VMW_SATP_SYMM   VMW_PSP_RR   Placeholder (plugin not loaded)
VMW_SATP_CX     VMW_PSP_MRU  Placeholder (plugin not loaded)
VMW_SATP_LSI    VMW_PSP_MRU  Placeholder (plugin not loaded)
VMW_SATP_DEFAULT_AA VMW_PSP_FIXED Supports non-specific active/active arrays
VMW_SATP_LOCAL   VMW_PSP_FIXED Supports direct attached devices
```

Pour plus d'informations sur cette commande, consultez la documentation *Concepts et exemples d'ESXCLI* et *Référence d'ESXCLI*.

VMware High Performance Plug-In et Path Selection Schemes

VMware fournit High Performance Plug-In (HPP) pour améliorer les performances des périphériques de stockage sur les hôtes ESXi.

Le HPP remplace le NMP pour les périphériques à haute vitesse, tels que les dispositifs NVMe. Le plug-in HPP est le plug-in par défaut qui réclame les cibles NVMe-oF. ESXi prend en charge l'émulation *de bout en bout NVMe sans et SCSI vers NVMe*. Le HPP prend uniquement en charge les cibles ALUA actives/actives et implicites.

À partir de vSphere 7.0 Update 2, HPP devient le plug-in par défaut pour les périphériques NVMe et SCSI locaux, mais vous pouvez le remplacer par NMP.

Prise en charge de HPP	vSphere 7.0 Update 2 et versions ultérieures
Périphériques de stockage	NVMe et SCSI locaux NVMe-oF partagé (cibles ALUA actives/actives et implicites uniquement)
Gestion multivoie	Oui
Plug-ins de second niveau	Non
Réservations persistantes SCSI-3	Non
Périphériques 4Kn avec émulation logicielle	Oui

Path Selection Schemes

Pour prendre en charge la gestion multivoie, le HPP utilise les schémas PSS (Path Selection Schemes) lors de la sélection de chemins physiques pour les demandes d'E/S.

Vous pouvez utiliser vSphere Client ou la commande `esxcli` pour modifier le mécanisme de sélection de chemin par défaut.

Pour plus d'informations sur la configuration des mécanismes de chemin d'accès dans vSphere Client, reportez-vous à [Modification de la stratégie de sélection de chemin d'accès](#). Pour la configuration avec la commande `esxcli`, reportez-vous à [Commandes esxcli HPP d'ESXi](#).

ESXi prend en charge les mécanismes de sélection de chemin d'accès suivants.

FIXE

Avec ce schéma, un chemin préféré désigné est utilisé pour les demandes d'E/S. Si le chemin préféré n'est pas attribué, l'hôte sélectionne le premier chemin opérationnel détecté au moment du démarrage. Si le chemin préféré devient non disponible, l'hôte sélectionne un autre chemin disponible. L'hôte renvoie le chemin préféré précédemment défini lorsqu'il devient à nouveau disponible.

Lorsque vous configurez **FIXED** en tant que mécanisme de sélection de chemin d'accès, sélectionnez le chemin préféré.

LB-RR (Load Balance - Round Robin)

Il s'agit du schéma par défaut pour les périphériques revendiqués par HPP. Après le transfert d'un nombre spécifié d'octets ou d'E/S sur un chemin actuel, le schéma sélectionne le chemin d'accès à l'aide de l'algorithme de répétition alternée.

Pour configurer le mécanisme de sélection de chemin d'accès **LB-RR**, spécifiez les propriétés suivantes :

- **IOPS** indique le nombre d'E/S sur le chemin à utiliser comme critère de basculement d'un chemin d'accès pour le périphérique.
- **Octets** indique le nombre d'octets sur le chemin à utiliser comme critère de basculement d'un chemin d'accès pour le périphérique.

LB-IOPS (Load Balance - IOPs)

Après le transfert d'un nombre spécifié d'E/S sur un chemin actuel, la valeur par défaut est 1000, le système sélectionne un chemin optimal ayant le moins d'E/S en attente.

Lors de la configuration de ce mécanisme, spécifiez le paramètre **IOPS** pour indiquer le nombre d'E/S sur le chemin à utiliser comme critère de basculement d'un chemin d'accès pour le périphérique.

LB-BYTES (Load Balance - Bytes)

Après le transfert d'un nombre spécifié d'octets sur un chemin actuel, la valeur par défaut est 10 Mo, le système sélectionne un chemin optimal ayant le moins d'octets en attente.

Pour configurer ce mécanisme, utilisez le paramètre **Octets** pour indiquer le nombre d'octets sur le chemin à utiliser comme critère de basculement d'un chemin d'accès pour le périphérique.

Load Balance - Latency (LB-Latency)

Pour atteindre de meilleurs résultats d'équilibrage de charge, le mécanisme sélectionne dynamiquement un chemin d'accès optimal en tenant compte des caractéristiques de chemin d'accès suivants :

- Le paramètre **Durée d'évaluation de la latence** indique à quel intervalle de temps, en millisecondes, la latence des chemins d'accès doit être évaluée.
- Le paramètre **Exemple d'E/S par chemin** contrôle le nombre d'exemples d'E/S qui doivent être émis sur chaque chemin pour calculer la latence du chemin d'accès.

Meilleures pratiques liées au HPP

Pour obtenir le débit le plus rapide d'un périphérique de stockage à haute vitesse, suivez ces recommandations.

- Utilisez la version vSphere qui prend en charge le HPP.

- Utilisez HPP pour les périphériques NVMe et SCSI locaux, et les périphériques NVMe-oF.
 - Si vous utilisez des périphériques NVMe over Fibre Channel, suivez les recommandations générales pour le stockage Fibre Channel. Reportez-vous à la section [Chapitre 3 Utilisation d'ESXi avec un SAN Fibre Channel](#).
 - Si vous utilisez NVMe-oF, ne mélangez pas les types de transport pour accéder au même espace de noms.
 - Lors de l'utilisation d'espaces de noms NVMe-oF, assurez-vous que les chemins actifs sont présentés à l'hôte. Les espaces de noms ne peuvent pas être enregistrés tant que le chemin actif n'est pas découvert.
 - Lorsque vous configurez vos machines virtuelles, vous pouvez utiliser des contrôleurs paravirtuels VMware ou ajouter des contrôleurs NVMe. Les deux types ont leurs avantages et leurs inconvénients. Pour vérifier ce qui convient le mieux à votre environnement, reportez-vous à la section [Conditions, limitations et compatibilité des contrôleurs de stockage SCSI, SATA et NVMe](#) dans la documentation *Administration d'une machine virtuelle vSphere*.
 - Définissez le seuil sensible de latence.
 - Si une seule machine virtuelle effectue une part importante de la charge de travail d'E/S du périphérique, envisagez de répartir les E/S sur plusieurs disques virtuels. Attachez les disques à des contrôleurs virtuels séparés de la machine virtuelle.
- Sinon, le débit d'E/S pourrait être limité en raison de la saturation du processeur principal responsable du traitement des E/S sur un contrôleur de stockage virtuel particulier.

Pour plus d'informations sur les identifiants de périphérique pour les périphériques NVMe qui prennent uniquement en charge le format d'ID NGUID, reportez-vous à la section [Périphériques NVMe avec identifiants de périphérique NGUID](#).

Activer High-Performance Plug-In et Path Selection Schemes

Le plug-in haute performance (HPP) est le plug-in par défaut qui réclame des périphériques NVMe et SCSI locaux, ainsi que des cibles NVMe-oF. Si nécessaire, vous pouvez le remplacer par NMP. Dans vSphere version 7.0 Update 1 et antérieures, NMP reste le plug-in par défaut pour les périphériques NVMe et SCSI locaux, mais vous pouvez le remplacer par HPP.

Utilisez la commande `esxcli storage core claimrule add` pour activer HPP ou NMP sur votre hôte ESXi.

Pour exécuter la commande `esxcli storage core claimrule add`, vous pouvez utiliser ESXi Shell ou vSphere CLI. Pour plus d'informations, reportez-vous à *Démarrage avec ESXCLI et Référence d'ESXCLI*.

Les exemples de cette rubrique montrent comment activer HPP et configurer les schémas PSS.

Note L'activation du HPP n'est pas prise en charge sur les hôtes ESXi démarrés par PXE.

Conditions préalables

Configurez votre environnement de stockage VMware NVMe. Pour plus d'informations, consultez [Chapitre 8 À propos du stockage VMware NVMe](#).

Procédure

- Créez une règle de réclamation HPP en exécutant la commande `esxcli storage core claimrule add`.

Utilisez une des méthodes suivantes pour ajouter la règle de réclamation.

Méthode	Description
Selon le modèle de contrôleur NVMe	<code>esxcli storage core claimrule add --type vendor --nvme-controller-model</code> Par exemple, <code>esxcli storage core claimrule add --rule 429 --type vendor --nvme-controller-model "ABCD*" --plugin HPP</code>
Selon l'ID de fournisseur et l'ID de sous-fournisseur PCI	<code>esxcli storage core claimrule add --type vendor --pci-vendor-id --pci-sub-vendor-id</code> Par exemple, <code>esxcli storage core claimrule add --rule 429 --type vendor --pci-vendor-id 8086 --pci-sub-vendor-id 8086 --plugin HPP.</code>

- Configurez les schémas PSS.

Sélectionnez l'une des méthodes suivantes.

Méthode	Description
Définir les schémas PSS selon l'ID de périphérique	<code>esxcli storage hpp device set</code> Par exemple, <code>esxcli storage hpp device set --device=device --pss=FIXED --path=preferred path</code>
Définir les schémas PSS selon la paire fournisseur/modèle	Utilisez l'option <code>--config-string</code> avec la commande <code>esxcli storage core claimrule add</code> . Par exemple, <code>esxcli storage core claimrule add -r 914 -t vendor -V vendor -M model -P HPP --config-string "pss=LB-Latency,latency-eval-time=40000"</code>

- Redémarrez votre hôte pour appliquer les modifications

Définir le seuil sensible de latence

Lorsque vous utilisez le HPP pour vos périphériques de stockage, définissez le seuil sensible de latence du périphérique afin que les E/S puissent contourner le planificateur d'E/S.

Par défaut, ESXi transmet chaque E/S via le planificateur d'E/S. Cependant, l'utilisation du planificateur peut créer des files d'attente internes, ce qui n'est pas efficace avec les périphériques de stockage à haute vitesse.

Vous pouvez configurer le seuil sensible de latence et activer le mécanisme d'envoi direct qui permet à l'E/S de contourner le planificateur. Lorsque ce mécanisme est activé, l'E/S est transmise directement du PSA au pilote de périphérique via le HPP.

Pour que l'envoi direct fonctionne correctement, la latence d'E/S moyenne observée doit être inférieure au seuil de latence que vous spécifiez. Si la latence d'E/S dépasse le seuil de latence spécifié, le système arrête l'envoi direct et réutilise temporairement le planificateur d'E/S. L'envoi direct reprend lorsque la latence d'E/S moyenne descend à nouveau au-dessous du seuil de latence.

Vous pouvez définir le seuil de latence pour une famille de périphériques réclamés par HPP. Définissez le seuil de latence à l'aide de la paire fournisseur et modèle, du modèle de contrôleur ou de la paire ID de fournisseur PCIe et ID de sous-fournisseur.

Procédure

- Pour définir le seuil sensible de latence pour le périphérique, exécutez la commande suivante :

```
esxcli storage core device latencythreshold set -t valeur en millisecondes
```

Sélectionnez l'une des options suivantes.

Option	Exemple
Fournisseur/modèle	Définissez le paramètre de seuil sensible à la latence pour tous les périphériques avec le fournisseur et le modèle indiqués : esxcli storage core device latencythreshold set -v 'vendor1' -m 'model1' -t 10
Modèle de contrôleur NVMe	Définissez le seuil sensible à la latence pour tous les périphériques NVMe avec le modèle de contrôleur indiqué : esxcli storage core device latencythreshold set -c 'controller_model1' -t 10
ID de fournisseur/sous-fournisseur PCIe	Définissez le seuil sensible à la latence pour les périphériques avec 0x8086 comme ID de fournisseur PCIe et 0x8086 comme ID de sous-fournisseur PCIe. esxcli storage core device latencythreshold set -p '8086' -s '8086' -t 10

- Vérifiez que le seuil de latence est défini :

```
esxcli storage core device latencythreshold list
```

Device	Latency Sensitive Threshold
naa.55cd2e404c1728aa	0 milliseconds
naa.500056b34036cdfd	0 milliseconds
naa.55cd2e404c172bd6	50 milliseconds

- Surveillez l'état du seuil sensible de latence. Vérifiez les entrées suivantes dans les journaux de VMkernel :

- Latency Sensitive Gatekeeper turned on for device device. Threshold of XX msec is larger than max completion time of YYY msec

- Latency Sensitive Gatekeeper turned off for device *device*. Threshold of *XX* msec is exceeded by command completed in *YYY* msec

Commandes esxcli HPP d'ESXi

Vous pouvez utiliser les commandes ESXi Shell ou vSphere CLI pour configurer et surveiller HPP (High-Performance Plug-in).

Consultez *Démarrage avec ESXCL* pour une introduction, et *Référence d'ESXCL* pour obtenir des détails sur l'utilisation de la commande `esxcli`.

Commande	Description	Options
<code>esxcli storage hpp path list</code>	Répertorie les chemins actuellement réclamés par HPP.	<code>-d --device=device</code> Affiche les informations relatives à un périphérique spécifique. <code>-p --path=path</code> Limite la sortie à un chemin spécifique.
<code>esxcli storage hpp device list</code>	Répertorie les périphériques actuellement contrôlés par HPP.	<code>-d --device=device</code> Affiche un périphérique spécifique.

Commande	Description	Options
<code>esxcli storage hpp device set</code>	Configure les paramètres pour un périphérique HPP.	<p><code>-B --bytes=long</code> Nombre maximal d'octets dans le chemin, après lequel le chemin est basculé.</p> <p><code>--cfg-file</code> Mettre à jour le fichier de configuration et l'exécution avec le nouveau paramètre. Si le périphérique est réclamé par un autre PSS, ignorez les erreurs lors de l'application de la configuration d'exécution.</p> <p><code>-d --device=device</code> Spécifie le périphérique HPP utilisé. Utilise n'importe quel UID signalé par le périphérique. Requis.</p> <p><code>-I --iops=long</code> Nombre maximal d'IOPS dans le chemin, après lequel le chemin est basculé.</p> <p><code>-T --latency-eval-time=long</code> Contrôle à quel intervalle (en ms) la latence des chemins doit être évaluée.</p> <p><code>-L --mark-device-local=bool</code> Indique à HPP de traiter le terminal comme étant local ou non.</p> <p><code>-M --mark-device-ssd=bool</code> Indique si HPP traite le périphérique comme un disque SSD ou non.</p> <p><code>-p --path=str</code> Le chemin d'accès à définir comme chemin préféré pour le périphérique.</p> <p><code>-P --pss=pss_name</code> Le schéma PSS à attribuer au périphérique. Si vous ne spécifiez pas la valeur, le système sélectionne la valeur par défaut. Pour la description des schémas PSS, reportez-vous à VMware High Performance Plug-In et Path Selection Schemes. Voici les options possibles :</p> <ul style="list-style-type: none"> ■ FIXED Utilisez la sous-option <code>-p --path=str</code> pour définir le chemin préféré. ■ LB-Bytes Utilisez la sous-option <code>-B --bytes=long</code> pour spécifier l'entrée. ■ LB-IOPS Utilisez la sous-option <code>-I --iops=long</code> pour spécifier l'entrée. ■ LB-Latency Voici les sous-options possibles : <ul style="list-style-type: none"> <code>-T --latency-eval-time=long</code> <code>-S --sampling-ios-per-path=long</code> ■ LB-RR (par défaut)

Commande	Description	Options
		<p>Voici les sous-options possibles :</p> <p>-B --bytes=<i>long</i></p> <p>-I --iops=<i>long</i></p> <p>-S --sampling-ios-per-path=<i>long</i> Contrôle le nombre d'exemples d'E/S qui doivent être émis sur chaque chemin pour calculer la latence du chemin d'accès.</p> <p>-U --use-ano=<i>bool</i> Définissez l'option sur <i>true</i> pour inclure des chemins non optimisés dans l'ensemble de chemins actifs utilisés pour émettre des E/S sur ce périphérique. Sinon, définissez l'option sur <i>false</i>.</p>
<code>esxcli storage hpp device usermarkedssd list</code>	Répertorie les périphériques qui ont été marqués ou démarqués comme SSD par l'utilisateur.	<code>-d --device=device</code> Limite la sortie à un périphérique spécifique.

Affichage et gestion des chemins

Lorsque vous démarrez votre hôte ESXi ou réanalysez votre adaptateur de stockage, l'hôte détecte tous les chemins physiques vers les périphériques de stockage disponibles sur l'hôte. Sur la base d'un ensemble de règles de réclamation, l'hôte détermine quel module de gestion multivoie (NMP, HPP ou MPP) possède les chemins menant à un périphérique particulier.

Le module qui possède le périphérique devient responsable de la gestion de la prise en charge de gestion multivoie pour le périphérique. Par défaut, l'hôte exécute une évaluation périodique des chemins toutes les cinq minutes et attribue les chemins non réclamés au module approprié.

Pour les chemins administrés par le module NMP, un second ensemble de règles de réclamation est utilisé. Ces règles attribuent un module SATP et un module PSP à chaque périphérique de stockage et déterminent la stratégie du type de baie de stockage et la stratégie de sélection de chemin qui s'applique.

Utilisez vSphere Client pour afficher la stratégie du type de baie de stockage et la stratégie de sélection de chemin attribuées à un périphérique de stockage spécifique. Vous pouvez également vérifier l'état de tous les chemins disponibles pour ce périphérique de stockage. Au besoin, vous pouvez modifier la stratégie de sélection de chemin par défaut à l'aide du client.

Pour modifier le module de gestion multivoie par défaut ou le SATP, modifiez les règles de réclamation à l'aide de vSphere CLI.

Vous pourrez trouver des informations sur la modification des règles de réclamation dans [Utilisation des règles de réclamation](#).

Affichage des chemins d'accès aux périphériques de stockage

Vous pouvez afficher les règles multivoie qu'utilise l'hôte pour un périphérique de stockage spécifique, ainsi que l'état de tous les chemins disponibles pour ce périphérique de stockage.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Périphériques de stockage**.
- 4 Sélectionnez le périphérique de stockage dont vous voulez afficher les chemins d'accès.
- 5 Cliquez sur l'onglet **Propriétés** et vérifiez le module qui possède le périphérique, par exemple NMP ou HPP.
Sous Stratégies de gestion multivoie, vous pouvez également afficher la stratégie de sélection de chemin et, le cas échéant, la stratégie du type de baie de stockage attribuées au périphérique.
- 6 Cliquez sur l'onglet **Chemins** pour vérifier tous les chemins disponibles pour le périphérique de stockage et l'état de chaque chemin. Les informations de l'état du chemin suivantes peuvent s'afficher :

État	Description
Actif (E/S)	Chemin opérationnel ou chemins multiples qui transfèrent actuellement des données.
En attente	Chemins qui sont inactifs. En cas d'échec du chemin actif, les chemins peuvent devenir opérationnels et commencer le transfert des E/S.
Désactivé	Chemins désactivés par l'administrateur.
Mort	Chemins qui ne sont plus disponibles pour le traitement des E/S. Une défaillance du support physique ou une baie mal configurée peut être à l'origine de cet état.

Si vous utilisez la politique de chemin **Fixe**, vous pouvez voir quel est le chemin préféré. Le chemin préféré est marqué par une astérisque (*) dans la colonne Préféré.

Affichage des chemins d'accès aux banques de données

Vérifiez les chemins d'accès qui assurent la connexion aux périphériques de stockage utilisés pour sauvegarder vos banques de données VMFS.

Procédure

- 1 Dans vSphere Client, accédez à la banque de données.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Cliquez sur **Connectivité et chemins multiples**.
- 4 Sélectionnez un hôte pour afficher les détails de gestion multivoie de ses périphériques.

- 5 Sous Règles de gestion multivoie, vérifiez le module qui possède le périphérique, par exemple NMP. Vous pouvez également afficher la stratégie de sélection de chemin et la stratégie du type de baie de stockage attribuées au périphérique.

Par exemple, vous pouvez afficher les éléments suivants :

Stratégie de sélection de chemin	Chemin préféré
Stratégie du type de baie de stockage	VMW_SATP_LOCAL
Plugin propriétaire	NMP

- 6 Sous Chemins, vérifiez les chemins des périphériques et l'état de chaque chemin. Les informations de l'état du chemin suivantes peuvent s'afficher :

État	Description
Actif (E/S)	Chemin opérationnel ou chemins multiples qui transfèrent actuellement des données.
En attente	Chemins qui sont inactifs. En cas d'échec du chemin actif, les chemins peuvent devenir opérationnels et commencer le transfert des E/S.
Désactivé	Chemins désactivés par l'administrateur.
Mort	Chemins qui ne sont plus disponibles pour le traitement des E/S. Une défaillance du support physique ou une baie mal configurée peut être à l'origine de cet état.

Si vous utilisez la politique de chemin **Fixe**, vous pouvez voir quel est le chemin préféré. Le chemin préféré est marqué par une astérisque (*) dans la colonne Préféré.

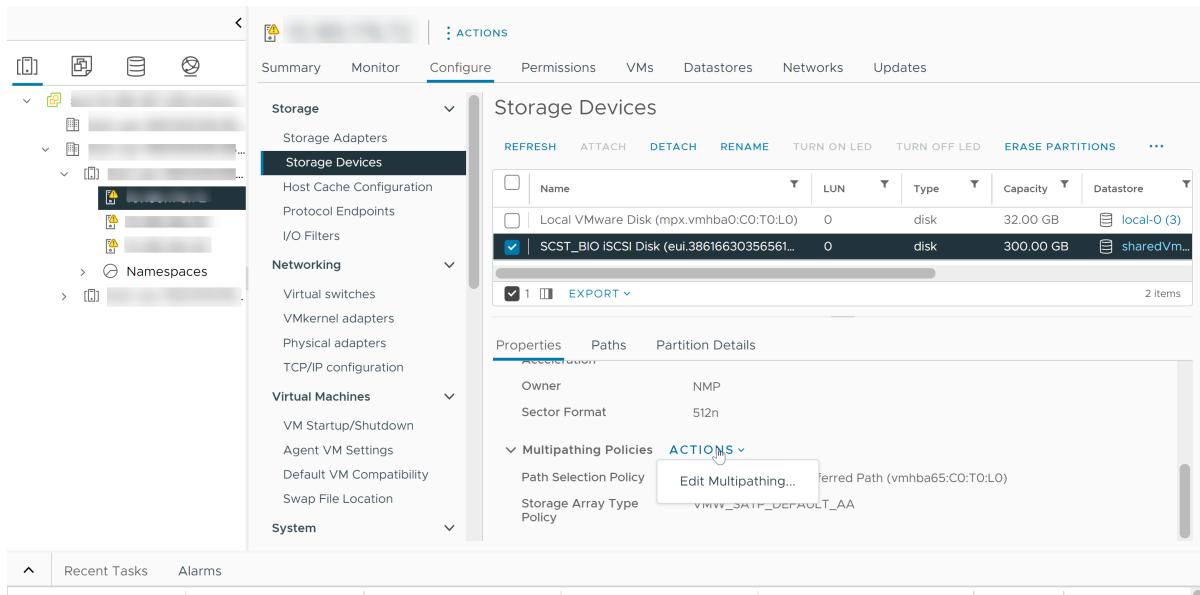
Modification de la stratégie de sélection de chemin d'accès

En général, il n'est pas nécessaire de modifier les paramètres de gestion multivoie par défaut utilisés par votre hôte ESXi pour un périphérique de stockage spécifique. Si vous souhaitez apporter des modifications, vous pouvez utiliser la boîte de dialogue **Modifier les stratégies de gestion multivoie** pour modifier la stratégie de sélection de chemin d'accès. Dans cette boîte de dialogue, vous pouvez également modifier les chemins multiples correspondant aux points de terminaison de protocole SCSI.

Procédure

- Dans vSphere Client, accédez à l'hôte ESXi.
- Cliquez sur l'onglet **Configurer**.
- Sous **Stockage**, cliquez sur **Périphériques de stockage** ou **Points de terminaison de protocole**.
- Selectionnez l'élément de protocole dont vous voulez modifier les chemins et cliquez sur l'onglet **Propriétés**.

- 5 Sous Règles de gestion multivoie, sélectionnez **Modifier la gestion multivoie** dans le menu **Actions**.



- 6 Sélectionnez une stratégie de chemin d'accès et configurez ses paramètres. Vos options changent en fonction du type de périphérique de stockage utilisé.
- Pour plus d'informations sur les stratégies de chemin d'accès pour les périphériques SCSI, reportez-vous à [Path Selection Plug-Ins et règles](#).
 - Pour plus d'informations sur les mécanismes de chemin d'accès pour les périphériques NVMe, reportez-vous à [VMware High Performance Plug-In et Path Selection Schemes](#).
- 7 Pour enregistrer vos paramètres et quitter la boîte de dialogue, cliquez sur **OK**.

Modifier les paramètres par défaut pour la latence circulaire

Sur l'hôte ESXi, vous pouvez activer le mécanisme de latence pour la stratégie de sélection de chemin d'accès circulaire. Le mécanisme prend en compte la bande passante d'E/S et la latence de sélection de chemin pour sélectionner un chemin optimal pour les E/S. Lors de l'utilisation du mécanisme de latence, la stratégie circulaire peut dynamiquement sélectionner le chemin optimal et obtenir de meilleurs résultats d'équilibre de charge.

Lorsque la latence est activée, l'utilisation des chemins d'accès pour les E/S dépend de la charge de travail. Lorsqu'un grand nombre de chemins est disponible, mais que la charge de travail n'est pas suffisamment élevée, le système peut ne pas utiliser certains chemins d'accès pour les E/S.

Utilisez la commande `esxcli` pour modifier les paramètres par défaut du mécanisme de latence, ou pour désactiver le mécanisme.

Conditions préalables

Définissez la stratégie de sélection de chemin sur Circulaire. Reportez-vous à la section [Modification de la stratégie de sélection de chemin d'accès](#).

Procédure

- Configurez le mécanisme de latence à l'aide de la commande suivante.

```
esxcli storage nmp psp roundrobin deviceconfig set --type=latency --device=device ID
```

La commande prend les paramètres suivants :

Paramètre	Description
-S --num-sampling-cycles=sampling value	Lorsque --type est défini sur latency, ce paramètre contrôle combien d'E/S utiliser pour calculer la latence moyenne de chaque chemin. La valeur par défaut de ce paramètre est 16.
-T --latency-eval-time=time in ms	Lorsque --type est défini sur latency, ce paramètre contrôle la fréquence à laquelle la latence des chemins d'accès est mise à jour. La valeur par défaut est de 3 minutes.

- Vérifiez si la latence circulaire et ses paramètres sont correctement configurés.

```
esxcli storage nmp psp roundrobin deviceconfig get --device=device ID
```

ou

```
esxcli storage nmp device list --device=device ID
```

L'exemple de sortie suivant illustre la configuration du chemin d'accès :

```
Path Selection Policy: VMW_PSP_RR
Path Selection Policy Device Config:
{policy=latency,latencyEvalTime=180000,samplingCycles=16,curSamplingCycle=16,useANO=0;
CurrentPath=vmhba1:C0:T0:L0: NumIosPending=0,latency=0}
```

Étape suivante

Pour désactiver le mécanisme de latence, remplacez le paramètre `Misc.EnablePSPLatencyPolicy` par 0 dans les paramètres système avancés de votre hôte.

Désactiver les chemins de stockage

Vous pouvez désactiver temporairement les chemins d'accès pour des raisons de maintenance ou pour d'autres raisons.

Pour désactiver un chemin d'accès, vous devez utiliser le panneau Chemins. Il existe plusieurs façons d'accéder au panneau Chemins : depuis une banque de données, un périphérique de stockage, un adaptateur ou une vue de points de terminaison de protocole Virtual Volumes.

Procédure

- Dans vSphere Client, accédez à l'hôte ESXi.
- Cliquez sur l'onglet **Configurer**.

- 3 Sous **Stockage**, cliquez sur l'un des éléments suivants :
 - **Adaptateurs de stockage**
 - **Périphériques de stockage**
 - **Points d'accès de protocole**
- 4 Dans le volet de droite, sélectionnez l'élément dont vous souhaitez désactiver les chemins, un adaptateur, un périphérique de stockage ou un point de terminaison de protocole, puis cliquez sur l'onglet **Chemins**.
- 5 Sélectionnez le chemin à désactiver et cliquez sur **Désactiver**.
L'état du chemin devient Désactivé.

Utilisation des règles de réclamation

Les règles de réclamation déterminent quel module de gestion multivoie possède les chemins menant à un périphérique de stockage particulier. Elles définissent également le type de prise en charge de la gestion multivoie que l'hôte fournit au périphérique.

Les règles de réclamation sont répertoriées dans le fichier `/etc/vmware/esx.conf` de l'hôte.

Elles entrent dans les catégories suivantes :

Règles de réclamation de base

Ces règles déterminent quel module de gestion multivoie, NMP, HPP ou un MPP tiers, réclame le périphérique spécifique.

Règles de réclamation SATP

Selon le type de périphérique, ces règles attribuent un sous-module SATP particulier qui fournit au périphérique la gestion multivoie spécifique du fournisseur.

Vous pouvez utiliser les commandes `esxcli` pour modifier les règles de réclamation de base et SATP ou en ajouter. En général, vous ajoutez des règles de réclamation pour charger un MPP tiers ou pour masquer un LUN de votre hôte. La modification des règles de réclamation peut s'avérer nécessaire lorsque les paramètres par défaut appliqués à un périphérique spécifique ne suffisent pas.

Pour plus d'informations sur les commandes disponibles pour gérer les règles de réclamation PSA, consultez *Démarrage avec ESXCLI*.

Pour une liste des baies de stockage et des SATP et PSP correspondants, consultez la section Stockage/SAN du *vSphere Compatibility Guide*.

Considérations concernant la gestion multivoie

Des considérations spécifiques s'appliquent lorsque vous gérez des plug-ins gestion multivoie de stockage et des règles de réclamation.

Les considérations suivantes sont destinées à vous aider à utiliser la gestion multivoie :

- Si les règles de réclamation n'ont pas alloué de SATP au périphérique, le SATP par défaut pour iSCSI ou pour les périphériques FC est VMW_SATP_DEFAULT_AA. Le PSP par défaut est VMW_PSP_FIXED.
- Lorsque le système recherche les règles SATP pour localiser un SATP pour un périphérique donné, il recherche les règles du pilote en premier. En cas de non correspondance, les règles du fournisseur/modèle sont recherchées, et pour finir, les règles de transport sont recherchées. En cas de non correspondance, NMP sélectionne un SATP par défaut pour le périphérique.
- Si VMW_SATP_ALUA est attribué à un périphérique de stockage spécifique mais le périphérique ne prend pas en charge ALUA, il n'y a aucune correspondance à la règle de réclamation pour ce périphérique. Le périphérique est réclamé par le SATP par défaut selon le type de transport du périphérique.
- Le PSP par défaut de tous les périphériques réclamés par VMW_SATP_ALUA est VMW_PSP_MRU. VMW_PSP_MRU sélectionne un chemin actif/optimisé que lui a indiqué VMW_SATP_ALUA, ou un chemin actif/non optimisé s'il n'y a pas de chemin actif/optimisé. Ce chemin est utilisé jusqu'à ce qu'un meilleur chemin soit disponible (MRU). Par exemple, si VMW_PSP_MRU utilise un chemin actif/non optimisé et qu'un chemin actif/optimisé est disponible, VMW_PSP_MRU change de chemin pour utiliser le chemin actif/optimisé.
- Bien que VMW_PSP_MRU soit généralement sélectionné par défaut pour les baies ALUA, certaines baies de stockage ALUA nécessitent d'utiliser VMW_PSP_FIXED. Pour vérifier si votre baie de stockage nécessite VMW_PSP_FIXED, consultez le *Guide de compatibilité VMware* ou contactez votre fournisseur de baies. Lorsque vous utilisez VMW_PSP_FIXED avec des baies ALUA, et à moins que vous ne spécifiez explicitement un chemin préféré, l'hôte ESXi sélectionne le chemin actif optimal et le désigne comme chemin préféré par défaut. Si le chemin sélectionné par l'hôte devient indisponible, l'hôte sélectionne un chemin de substitution disponible. Toutefois, si vous désignez explicitement le chemin préféré, celui-ci restera le chemin préféré quel que soit son état.
- Par défaut, la règle de réclamation 101 du PSA masque les périphériques pseudo de baie Dell. Ne supprimez pas cette règle sauf si vous voulez afficher ces périphériques.

Liste de règles de réclamation de gestion multivoie pour l'hôte

Utilisez la commande esxcli pour répertorier les règles de réclamation de gestion multivoie disponibles.

Les règles de réclamation indiquent si le NMP, le HPP ou un MPP tiers gère un chemin physique donné. Chaque règle de réclamation identifie une série de chemins selon les paramètres suivants :

- Chaînes d'éditeur/modèle
- Transport, tel que SATA, IDE ou Fibre Channel

- Adaptateur, cible ou emplacement de la LUN
- Pilote du périphérique, par exemple, Mega-RAID

Procédure

- ◆ Pour répertorier les règles de réclamation de gestion multivoie, exécutez la commande **esxcli storage core claimrule list --claimrule-class=MP**.

Si vous n'utilisez pas l'option `claimrule-class`, la classe de règle MP est implicite.

Exemple : Exemple de résultat de la commande esxcli storage core claimrule list

Rule Class	Rule	Class	Type	Plugin	Matches
MP	10	runtime	vendor	HPP	vendor=NVMe model=*
MP	10	file	vendor	HPP	vendor=NVMe model=*
MP	50	runtime	transport	NMP	transport=usb
MP	51	runtime	transport	NMP	transport=sata
MP	52	runtime	transport	NMP	transport=ide
MP	53	runtime	transport	NMP	transport=block
MP	54	runtime	transport	NMP	transport=unknown
MP	101	runtime	vendor	MASK_PATH	vendor=DELL model=Universal Xport
MP	101	file	vendor	MASK_PATH	vendor=DELL model=Universal Xport
MP	200	runtime	vendor	MPP_1	vendor>NewVend model=*
MP	200	file	vendor	MPP_1	vendor>NewVend model=*
MP	201	runtime	location	MPP_2	adapter=vhba41 channel=* target=* lun=*
MP	201	file	location	MPP_2	adapter=vhba41 channel=* target=* lun=*
MP	202	runtime	driver	MPP_3	driver=megaraid
MP	202	file	driver	MPP_3	driver=megaraid
MP	65535	runtime	vendor	NMP	vendor=* model=*

Cet exemple indique :

- Le NMP réclame tous les chemins connectés aux périphériques de stockage qui utilisent le transport USB, SATA, IDE et Block SCSI.
- Les règles pour HPP, MPP_1, MPP_2 et MPP_3 ont été ajoutées, afin que les modules puissent réclamer des périphériques spécifiés. Par exemple, le HPP réclame tous les périphériques avec le fournisseur NVMe. Tous les périphériques gérés par le pilote nvme de la boîte de réception sont réclamés, quel que soit le fournisseur réel. Le module MPP_1 réclame tous les chemins connectés à tout modèle de baie de stockage NewVend.
- Vous pouvez utiliser le module MASK_PATH pour masquer les périphériques inutilisés de votre hôte. Par défaut, la règle de réclamation 101 du PSA masque les périphériques pseudo de baie Dell avec une chaîne de fournisseur DELL et une chaîne de modèle Universal Xport.
- La colonne Classe de règles dans la sortie décrit la catégorie de règle de réclamation. Elle peut être MP (plug-in gestion multivoie), Filtre ou VAAI.

- La colonne Classe montre les règles qui sont définies et celles qui sont chargées. Le paramètre `file` dans la colonne Class indique que la règle est définie. Le paramètre `runtime` indique que la règle a été chargée sur votre système. Pour activer une règle de réclamation définie par l'utilisateur, il faut que deux lignes ayant le même nombre de règles soient présentes. Une ligne pour la règle avec le paramètre `file` et une autre ligne avec le paramètre `runtime`. Plusieurs règles de réclamation définies par défaut par le système ont une seule ligne avec la classe `runtime`. Vous ne pouvez pas modifier ces règles.
- La règle par défaut 65535 attribue tous les chemins non réclamés au NMP. Ne supprimez pas cette règle.

Ajout de règles de réclamation de gestion multivoie

Utilisez les commandes `esxcli` pour ajouter une règle de réclamation de gestion multivoie PSA à l'ensemble de stratégies de réclamation sur le système. Pour activer la nouvelle règle de réclamation, définissez d'abord la règle puis chargez-la sur votre système.

Exemples d'ajout d'une règle de réclamation PSA :

- Vous chargez un nouveau MPP tiers et vous devez définir les chemins que ce module réclame.
- Vous devez activer le HPP natif.

Avertissement Vous ne pouvez pas créer de règles pour lesquelles deux plug-ins différents réclament des chemins vers le même périphérique. Vos tentatives de création de ces règles de réclamation échouent avec un message d'avertissement dans le fichier `vmkernel.log`.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- 1 Pour définir une nouvelle règle de réclamation, utilisez la commande suivante :

```
esxcli storage core claimrule add
```

La commande accepte les options suivantes :

Option	Description
<code>-A --adapter=<adapter></code>	Adaptateur des chemins d'accès à utiliser. Valide uniquement si <code>--type</code> est <code>location</code> .
<code>-u --autoassign</code>	Permet d'ajouter une règle de réclamation selon ses caractéristiques. Le numéro de règle n'est pas nécessaire.
<code>-C --channel=<channel></code>	Canal des chemins d'accès à utiliser. Valide uniquement si <code>--type</code> est <code>location</code> .

Option	Description
-c --claimrule-class=<cl>	Classe des règles de réclamation à utiliser pour cette opération. Vous pouvez spécifier MP (par défaut), Filter ou VAAI.
	Pour configurer l'accélération matérielle pour une nouvelle baie, ajoutez deux règles de réclamation, une pour le filtre VAAI et une autre pour le plug-in VAAI. Reportez-vous à Ajout de règles de réclamation d'accélération matérielle pour obtenir des instructions détaillées.
-d --device=<device_uid>	UID du périphérique. Valide uniquement lorsque --type est device.
-D --driver=<driver>	Pilote pour l'adaptateur HBA des chemins d'accès à utiliser. Valide uniquement si --type est driver.
-f --force	Forcez les règles de réclamation à ignorer les vérifications de validité et à installer la règle.
--force-reserved	Remplacez la protection des plages d'ID de règle réservées. Les règles de réclamation réservées sont les règles dont l'ID est inférieur à 100. Vous pouvez les utiliser pour réattribuer les périphériques locaux aux plug-ins spécifiques (par exemple, le périphérique NVMe au HPP).
--if-unset=<str>	Exécutez cette commande si cette variable d'utilisateur avancé n'est pas définie sur la valeur 1.
-i --iqn=<iscsi_name>	Nom complet iSCSI de la cible. Valide uniquement lorsque --type est target.
-L --lun=<lun_id>	LUN des chemins d'accès. Valide uniquement si --type est location. L'ID de LUN ne doit pas être supérieur à la valeur de l'option de configuration avancée /Disk/MaxLUN.
-M --model=<model>	Modèle des chemins d'accès à utiliser. Valide uniquement si --type est vendor. Les valeurs valides sont les valeurs de la chaîne de modèle à partir de la chaîne SCSI INQUIRY. Exécutez <code>vicfg-scsidevs <conn_options> -l</code> sur chaque périphérique pour afficher les valeurs de la chaîne de modèle.
-P --plugin=<plugin>	Plug-in PSA à utiliser. Les valeurs sont NMP, MASK_PATH ou HPP. Des développeurs tiers peuvent également fournir leurs propres plug-ins PSA. Requis.
-r --rule=<rule_ID>	ID de règle à utiliser. L'ID de règle indique l'ordre dans lequel la règle de réclamation doit être évaluée. Les règles de réclamation définies par l'utilisateur sont évaluées dans l'ordre numérique à partir de 101. Vous pouvez exécuter <code>esxcli storage core claimrule list</code> pour déterminer les ID de règle disponibles.
-T --target=<target>	Cible des chemins d'accès à utiliser. Valide uniquement si --type est location.

Option	Description
-R --transport=<transport>	Transport des chemins d'accès à utiliser. Valide uniquement si --type est transport . Les valeurs suivantes sont prises en charge. <ul style="list-style-type: none"> ■ block — Stockage des blocs ■ fc — Fibre Channel ■ iscsivendor — iSCSI ■ iscsi — Actuellement inutilisé ■ ide — Stockage IDE ■ sas — Stockage SAS ■ sata — Stockage SATA ■ usb — Stockage USB ■ parallel — Parallèle ■ fcoe — FCoE ■ unknown
-t --type=<type>	Type de correspondance à utiliser pour l'opération. Les valeurs valides sont les suivantes : Requis. <ul style="list-style-type: none"> ■ vendor ■ location ■ driver ■ transport ■ device ■ target
-v --vendor=<vendor>	Fournisseur des chemins d'accès à utiliser. Valide uniquement si --type est vendor . <p>Les valeurs valides sont les valeurs de la chaîne de fournisseur à partir de la chaîne SCSI INQUIRY. Exécutez <code>vicfg-scsidevs <conn_options> -l</code> sur chaque périphérique pour afficher les valeurs de la chaîne de fournisseur.</p>
--wwnn=<wwnn>	Numéro de nœud mondial (WWNN) pour la cible.
--wwpn=<wwpn>	Numéro de port mondial (WWPN) pour la cible.
-a --xcopy-use-array-values	Utilisez les valeurs indiquées par la baie pour construire la commande XCOPY à envoyer à la baie de stockage. Cela s'applique aux règles de réclamation VAAI uniquement.
-s --xcopy-use-multi-segs	Utilisez plusieurs segments lors de l'émission d'une demande XCOPY. Valide uniquement si --xcopy-use-array-values est spécifié.
-m --xcopy-max-transfer-size-	Taille maximale en Mo de transfert de données lorsque vous utilisez une taille de transfert différente de celle indiquée par la baie. Valide uniquement si --xcopy-use-array-values est spécifié.
-k --xcopy-max-transfer-size-kib	Taille maximale en Kio de transfert pour les commandes XCOPY lorsque vous utilisez une taille de transfert différente de celle indiquée par la baie. Valide uniquement si --xcopy-use-array-values est spécifié.

- 2 Pour charger la nouvelle règle de réclamation sur votre système, utilisez la commande suivante :

```
esxcli storage core claimrule load
```

Cette commande charge toutes les nouvelles règles de réclamation de gestion multivoie à partir du fichier de configuration `esx.conf` dans le noyau VMkernel. La commande ne se compose d'aucune option.

- 3 Pour appliquer des règles de réclamation qui sont chargées, utilisez la commande suivante :

```
esxcli storage core claimrule run
```

La commande accepte les options suivantes :

Option	Description
-A --adapter=<adapter>	Si <code>--type</code> est <code>location</code> , il s'agit du nom de l'adaptateur HBA pour les chemins d'accès sur lesquels les règles de réclamation doivent être exécutées. Pour exécuter des règles de réclamation sur les chemins d'accès pour tous les adaptateurs, omettez cette option.
-C --channel=<channel>	Si <code>--type</code> est <code>location</code> , indiquez le canal des chemins à utiliser pour cette opération. Pour exécuter des règles de réclamation sur les chemins d'accès pour tout numéro de canal, omettez cette option.
-c --claimrule-class=<cl>	Classe des règles de réclamation à utiliser pour cette opération.
-d --device=<device_uid>	UID du périphérique.
-L --lun=<lun_id>	Si <code>--type</code> est <code>location</code> , indiquez la valeur du LUN pour les chemins sur lesquels les règles de réclamation doivent être exécutées. Pour exécuter des règles de réclamation sur les chemins d'accès pour tout LUN, omettez cette option.
-p --path=<path_uid>	Si <code>--type</code> est <code>path</code> , cette option indique l'identifiant de chemin d'accès unique (UID) ou le nom d'exécution d'un chemin d'accès sur lequel les règles de réclamation doivent être exécutées.
-T --target=<target>	Si <code>--type</code> est <code>location</code> , indiquez la cible des chemins sur lesquels les règles de réclamation doivent être exécutées. Pour exécuter des règles de réclamation sur les chemins d'accès pour tout numéro cible, omettez cette option.
-t --type=<location path all>	Type de réclamation à effectuer. Par défaut, utilise <code>all</code> , ce qui signifie que des règles de réclamation s'exécutent sans restriction pour les chemins. Les valeurs valides sont <code>location</code> , <code>path</code> et <code>all</code> .
-w --wait	<p>Vous ne pouvez utiliser cette option que si vous utilisez également <code>--type all</code>.</p> <p>Si cette option est incluse, la réclamation attend que le réglage des chemins d'accès soit effectué avant l'exécution de l'opération de réclamation. Dans ce cas, le système ne démarre le processus de réclamation que lorsqu'il est probable que tous les chemins d'accès au système sont apparus.</p> <p>Lorsque le processus de réclamation est démarré, la commande ne renvoie rien jusqu'à ce que l'enregistrement du périphérique soit effectué.</p> <p>Si vous ajoutez ou supprimez des chemins d'accès au cours du processus de réclamation ou de détection, cette option peut ne pas fonctionner correctement.</p>

Exemple : Définition des règles de réclamation de gestion multivoie

Dans l'exemple suivant, vous ajoutez et chargez la règle #500. La règle réclame tous les chemins avec la chaîne de modèle NewMod et la chaîne de fournisseur NewVend pour le plug-in NMP.

```
# esxcli storage core claimrule add -r 500 -t vendor -V NewVend -M NewMod -P
NMP
```

```
# esxcli storage core claimrule load
```

Après avoir exécuté la commande `esxcli storage core claimrule list`, vous pouvez voir apparaître la nouvelle règle de réclamations sur la liste.

La sortie suivante indique que la règle de réclamation 500 a été chargée dans le système et est active.

Rule	Class	Rule	Class	Type	Plugin	Matches
...
MP		500	runtime	vendor	NMP	vendor=NewVend model>NewMod
MP		500	file	vendor	NMP	vendor=NewVend model>NewMod

Suppression de règles de réclamation de gestion multivoie

Utilisez les commandes `esxcli` pour supprimer une règle de réclamation PSA de gestion multivoie de la série de règles de réclamation sur le système.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- Supprimez une règle de réclamation d'une série de règles de réclamation.

```
esxcli storage core claimrule remove
```

Note Par défaut, la règle de réclamation 101 du PSA masque les périphériques pseudo de baie Dell. Ne supprimez pas cette règle sauf si vous voulez afficher ces périphériques.

La commande accepte les options suivantes :

Option	Description
<code>-c --claimrule-class=<str></code>	Indiquez la classe de règle de réclamation (MP, Filtre, VAAI).
<code>-P --plugin=<str></code>	Indiquez le plug-in.
<code>-r --rule=<long></code>	Indiquez l'ID de règle.

Cette étape supprime la règle de réclamation de la classe de fichiers.

- 2 Supprimez la règle de réclamation du système.

```
esxcli storage core claimrule load
```

Cette étape supprime la règle de réclamation de la classe Runtime.

Masquage des chemins

Vous pouvez empêcher l'hôte d'accéder aux périphériques de stockage ou aux LUN, ou encore l'empêcher d'utiliser certains chemins d'accès à un LUN. Pour masquer les chemins d'accès, utilisez les commandes `esxcli`. Lorsque vous masquez des chemins d'accès, vous créez des règles de réclamation qui affectent le plug-in `MASK_PATH` aux chemins spécifiés.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- 1 Vérifiez l'ID de règle disponible suivant

```
esxcli storage core claimrule list
```

Les règles de réclamation qui vous permettent de masquer les chemins possèdent des ID de règle compris entre 101 et 200. Si cette commande indique que les règles 101 et 102 existent, vous pouvez utiliser 103 pour la règle à ajouter.

- 2 Affectez le plug-in `MASK_PATH` à un chemin d'accès : pour cela, créez une nouvelle règle de réclamation à associer au plug-in.

```
esxcli storage core claimrule add -P MASK_PATH
```

- 3 Chargez la règle de réclamation du plug-in `MASK_PATH` dans votre système.

```
esxcli storage core claimrule load
```

- 4 Vérifiez que cette règle a bien été ajoutée.

```
esxcli storage core claimrule list
```

- 5 Si une règle de réclamation existe déjà pour le chemin d'accès masqué, supprimez-la.

```
esxcli storage core claiming unclaim
```

- 6 Exécutez les règles de réclamation de chemin d'accès.

```
esxcli storage core claimrule run
```

Résultats

Une fois que vous avez affecté le plug-in `MASK_PATH` à un chemin d'accès, l'état de l'état de ce dernier devient non pertinent et n'est plus géré par l'hôte. Par conséquent, les commandes qui affichent les informations de chemin masqué peuvent indiquer que ce chemin est mort.

Exemple : Masquage d'un LUN

Dans cet exemple, vous masquez le LUN 20 pour les cibles T1 et T2, dont l'accès s'effectue via les adaptateurs de stockage vmhba2 et vmhba3.

```

1 #esxcli storage core claimrule list

2 #esxcli storage core claimrule add -P MASK_PATH -r 109 -t location -A vmhba2 -C 0 -T 1 -L
20
#esxcli storage core claimrule add -P MASK_PATH -r 110 -t location -A vmhba3 -C 0 -T 1 -L
20
#esxcli storage core claimrule add -P MASK_PATH -r 111 -t location -A vmhba2 -C 0 -T 2 -L
20
#esxcli storage core claimrule add -P MASK_PATH -r 112 -t location -A vmhba3 -C 0 -T 2 -L
20

3 #esxcli storage core claimrule load

4 #esxcli storage core claimrule list

5 #esxcli storage core claiming unclaim -t location -A vmhba2
#esxcli storage core claiming unclaim -t location -A vmhba3

6 #esxcli storage core claimrule run

```

Démasquage des chemins

Si vous souhaitez que l'hôte accède au périphérique de stockage masqué, démasquez les chemins menant à ce périphérique.

Note Lorsque vous exécutez une opération de non-réclamation à l'aide d'une propriété de périphérique (comme ID de périphérique ou fournisseur), les chemins réclamés par le plug-in MASK_PATH ne sont pas non réclamés. Le plug-in MASK_PATH n'effectue aucun suivi des propriétés de périphérique des chemins qu'il réclame.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes esxcli dans ESXi Shell.

Procédure

- Supprimez la règle de réclamation MASK_PATH.

```
esxcli storage core claimrule remove -r rule#
```

- Vérifiez que la règle de réclamation a été supprimée correctement.

```
esxcli storage core claimrule list
```

- 3 Rechargez les règles de réclamation du chemin à partir du fichier de configuration dans le VMkernel.

```
esxcli storage core claimrule load
```

- 4 Exécutez la commande **esxcli storage core claiming unclaim** pour chaque chemin vers le périphérique de stockage masqué.

Par exemple :

```
esxcli storage core claiming unclaim -t location -A vmhba0 -C 0 -T 0 -L  
149
```

- 5 Exécutez les règles de réclamation de chemin d'accès.

```
esxcli storage core claimrule run
```

Résultats

Votre hôte peut désormais accéder au périphérique de stockage qui a été masqué.

Définition des règles SATP de NMP

Les règles de réclamation NMP SATP définissent le SATP qui gère un périphérique de stockage. En règle générale, vous pouvez utiliser les SATP par défaut fournis pour les périphériques de stockage. Si les paramètres par défaut ne suffisent pas, utilisez les commandes **esxcli** pour modifier le SATP pour un périphérique spécifique.

Vous devrez éventuellement créer une règle SATP lors de l'installation d'un SATP tiers pour une baie de stockage spécifique.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes **esxcli** dans ESXi Shell.

Procédure

- 1 Pour ajouter une règle de réclamation à un SATP spécifique, exécutez la commande **esxcli storage nmp satp rule add**. La commande accepte les options suivantes.

Option	Description
-b --boot	Il s'agit d'une règle par défaut du système ajoutée au moment du démarrage. Ne modifiez pas <code>esx.conf</code> ou ne l'ajoutez pas au profil d'un hôte.
-c --claim-option=<i>string</i>	Définissez la chaîne d'option de réclamation lors de l'ajout d'une règle de réclamation SATP.
-e --description=<i>string</i>	Définissez la description de la règle de réclamation lors de l'ajout d'une règle de réclamation SATP.
-d --device=<i>string</i>	Définissez le périphérique lors de l'ajout de règles de réclamation SATP. Les règles de périphérique sont mutuellement exclusives aux règles d'éiteur/modèle et de pilote.

Option	Description
-D --driver=string	Définissez la chaîne de pilote lors de l'ajout d'une règle de réclamation SATP. Les règles de pilote sont mutuellement exclusives aux règles d'éditeur/modèle.
-f --force	Forcez les règles de réclamation à ignorer les vérifications de validité et à installer la règle.
-h --help	Affichez le message d'aide.
-M --model=string	Définissez la chaîne de modèle lors de l'ajout d'une règle de réclamation SATP. Les règles d'éditeur/modèle sont mutuellement exclusives aux règles de pilote.
-o --option=string	Définissez la chaîne d'option lors de l'ajout d'une règle de réclamation SATP.
-P --psp=string	Définissez le PSP par défaut pour la règle de réclamation SATP.
-O --psp-option=string	Définissez les options du PSP pour la règle de réclamation SATP.
-s --satp=string	Le SATP pour lequel une nouvelle règle est ajoutée.
-R --transport=string	Définissez la chaîne du type de transport lors de l'ajout d'une règle de réclamation SATP.
-t --type=string	Définissez le type de chaîne lors de l'ajout d'une règle de réclamation SATP.
-V --vendor=string	Définissez la chaîne de fournisseur lors de l'ajout de règles de réclamation SATP. Les règles d'éditeur/modèle sont mutuellement exclusives aux règles de pilote.

Note Lors de la recherche de règles SATP pour localiser le SATP d'un périphérique donné, le NMP commence par rechercher les règles de pilote. Si aucune correspondance n'est trouvée, les règles d'éditeur/modèle sont recherchées et finalement les règles de transport. Si aucune correspondance n'est trouvée cette fois encore, le NMP sélectionne un SATP par défaut pour le périphérique.

2 Redémarrez l'hôte.

Exemple : Définition d'une règle NMP SATP

L'exemple de commande suivant affecte le plug-in VMW_SATP_INV à la gestion des baies de stockage avec une chaîne de fournisseur NewVend et une chaîne de modèle NewMod.

```
# esxcli storage nmp satp rule add -V NewVend -M NewMod -s VMW_SATP_INV
```

Lorsque vous exécutez la commande `esxcli storage nmp satp list -s VMW_SATP_INV`, vous pouvez voir la nouvelle règle ajoutée à la liste de règles VMW_SATP_INV.

Files d'attente de planification pour les E/S de machines virtuelles

Par défaut, vSphere fournit un mécanisme qui crée des files d'attente de planification pour chaque fichier de machine virtuelle. Chaque fichier (.vmdk, par exemple) obtient ses propres contrôles de bande passante.

Ce mécanisme assure que les E/S associées à un fichier de machine virtuelle spécifique vont dans leur file d'attente individuelle et n'interfèrent pas avec les E/S des autres fichiers.

Cette capacité est activée par défaut. Vous pouvez utiliser vSphere Client ou les commandes esxcli pour désactiver la capacité.

Modifier la planification des E/S par fichier dans vSphere Client

Le paramètre `VMkernel.Boot.isPerFileSchedModelActive` avancé contrôle le mécanisme de planification des E/S par fichier sur les banques de données VMFS et NFS 3. Ce mécanisme est activé par défaut sur l'hôte ESXi. Vous pouvez le désactiver dans la boîte de dialogue **Paramètres système avancés**.

Si vous désactivez le modèle de planification des E/S par fichier, votre hôte reprend un mécanisme de planification hérité. La planification héritée gère une file d'attente d'E/S unique pour chaque paire de machine virtuelle et de périphérique de stockage. Toutes les E/S entre la machine virtuelle et ses disques virtuels sont déplacées vers cette file d'attente. Par conséquent, les E/S des différents disques virtuels peuvent interférer les unes avec les autres lorsqu'elles partagent la bande passante et affecter les performances les unes des autres.

Note Ne désactivez pas la planification par fichier si le plug-in HPP et le paramètre de seuil sensible à la latence sont configurés pour des périphériques locaux haute vitesse. La désactivation de la planification par fichier peut entraîner un comportement imprévisible.

Procédure

- Dans vSphere Client, accédez à l'hôte ESXi.
- Cliquez sur l'onglet **Configurer**.
- Sous **Système**, cliquez sur **Paramètres système avancés**.
- Modifiez la valeur du paramètre `VMkernel.Boot.isPerFileSchedModelActive`.

Option	Description
True	Activez le mécanisme de planification par fichier. Par défaut, le paramètre est activé.
False	Désactivez le mécanisme de planification par fichier.

- Redémarrez l'hôte pour que vos modifications puissent prendre effet.

Utiliser les commandes esxcli pour modifier la planification des E/S par fichier

Vous pouvez utiliser les commandes `esxcli` pour modifier la capacité de planification des E/S pour les banques de données VMFS, NFS 3 et NFS 4.1 sur votre hôte ESXi. Cette capacité est activée par défaut.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Pour définir ou modifier la planification des E/S par fichier, exécutez les commandes suivantes :

Option	Description
<code>esxcli system settings kernel set -s isPerFileSchedModelActive -v FALSE</code>	Désactivez la planification des E/S par fichier pour VMFS et NFS 3.
<code>esxcli system settings kernel set -s isPerFileSchedModelActive -v TRUE</code>	Activez la planification des E/S par fichier pour VMFS et NFS 3.
<code>esxcli system module parameters list -m nfs41client</code>	Affichez l'état actuel du planificateur basé sur les fichiers NFS 4.1.
<code>esxcli system module parameters set -m nfs41client -p fileBasedScheduler=0</code>	Désactivez le planificateur basé sur les fichiers pour NFS 4.1.
<code>esxcli system module parameters set -m nfs41client -p fileBasedScheduler=1</code>	Activez le planificateur basé sur les fichiers pour NFS 4.1.

Mappage de périphérique brut

11

La technologie RDM (Raw Device Mapping) fournit un mécanisme qui permet aux machines virtuelles d'accéder directement aux LUN du sous-système de stockage physique.

Les rubriques suivantes contiennent des informations sur les RDM et fournissent des instructions sur la manière de créer et de gérer des RDM.

Ce chapitre contient les rubriques suivantes :

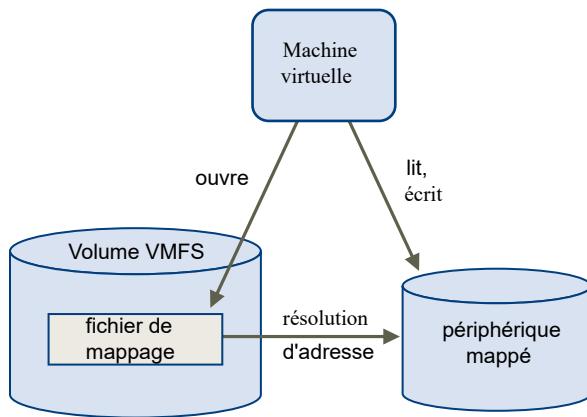
- À propos du mappage de périphérique brut
- Caractéristiques du mappage de périphérique brut
- Création de machines virtuelles avec des RDM
- Gérer les chemins pour un LUN mappé
- Les machines virtuelles dotées de RDM doivent ignorer le cache SCSI INQUIRY

À propos du mappage de périphérique brut

Un RDM est un fichier de mappage dans un volume VMFS séparé qui se comporte comme un proxy pour un périphérique physique brut. Avec le disque RDM, une machine virtuelle peut accéder au périphérique de stockage et l'utiliser directement. Le RDM contient des métadonnées pour la gestion et la redirection de l'accès au disque vers le périphérique physique.

Le fichier vous donne certains des avantages de l'accès direct au périphérique physique tout en conservant les avantages du disque virtuel dans VMFS. En conséquence, il associe la capacité de gestion de VMFS à l'accès au périphérique brut.

Figure 11-1. Mappage de périphérique brut



Généralement, vous utilisez les banques de données VMFS pour la plupart des opérations de stockage de disque virtuel. Dans certains cas, vous pouvez utiliser des LUN bruts ou des disques logiques situés sur un SAN.

Par exemple, vous pouvez utiliser des LUN bruts avec des RDM dans les situations suivantes :

- Lorsque le snapshot du SAN ou d'autres applications en couche sont exécutés dans la machine virtuelle. Le RDM active des systèmes de déchargement de sauvegarde à l'aide de fonctionnalités inhérentes au SAN.
- Dans tout scénario de mise en cluster MSCS s'étendant sur les hôtes physiques, comme des clusters virtuels à virtuels et des clusters physiques à virtuels. Dans ce cas, les données du cluster et les disques quorum sont configurés comme des RDM plutôt que comme des disques virtuels sur un VMFS partagé.

Considérez un RDM comme un lien symbolique d'un volume VMFS vers un LUN brut. Le mappage fait apparaître les LUN comme des fichiers dans un volume VMFS. LE RDM, et non le LUN brut, est référencé dans la configuration de la machine virtuelle. Le RDM contient une référence au LUN brut.

Deux modes de compatibilité sont disponibles pour les RDM :

- En mode de compatibilité virtuelle, le RDM agit comme un fichier de disque virtuel. Le RDM peut utiliser des snapshots.
- En mode de compatibilité physique, le RDM offre un accès direct au périphérique SCSI pour les applications qui requièrent un contrôle de niveau inférieur.

Avantages du mappage de périphérique brut

Un RDM fournit un certain nombre d'avantages, mais il ne doit pas être utilisé dans tous les cas. Généralement, les fichiers de disque virtuel sont préférables à la capacité de gestion du RDM. Cependant, si vous avez besoin de périphériques bruts, vous devez utiliser le RDM.

Le RDM offre plusieurs avantages.

Noms persistants conviviaux

Fournit un nom convivial pour un périphérique mappé. Lorsque vous utilisez un RDM, il est inutile de se rapporter au périphérique par son nom de périphérique. Vous lappelez par le nom du fichier de mappage, par exemple :

```
/vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk
```

Résolution dynamique de nom

Stocke des informations uniques d'identification pour chaque périphérique mappé. VMFS associe chaque RDM à son périphérique SCSI actuel, quelles que soient les modifications dans la configuration physique du serveur, en raison des modifications matérielles de l'adaptateur, des modifications de chemin, de la relocalisation du périphérique, etc.

Verrouillage des fichiers distribués

Permet d'utiliser le verrouillage distribué VMFS pour les périphériques SCSI bruts. Le verrouillage distribué sur un RDM permet d'utiliser en toute sécurité un LUN brut partagé sans perdre de données lorsque deux machines virtuelles sur des serveurs différents essaient d'accéder au même LUN.

Autorisations de fichier

Rend les autorisations de fichier possibles. Les autorisations de fichier de mappage sont appliquées au moment de l'ouverture du fichier pour protéger le volume mappé.

Opérations du système de fichiers

Permet d'utiliser les utilitaires du système de fichiers pour travailler avec un volume mappé à l'aide du fichier de mappage comme proxy. La plupart des opérations valides pour un fichier ordinaire peuvent être appliquées au fichier de mappage et sont redirigées pour fonctionner sur un périphérique mappé.

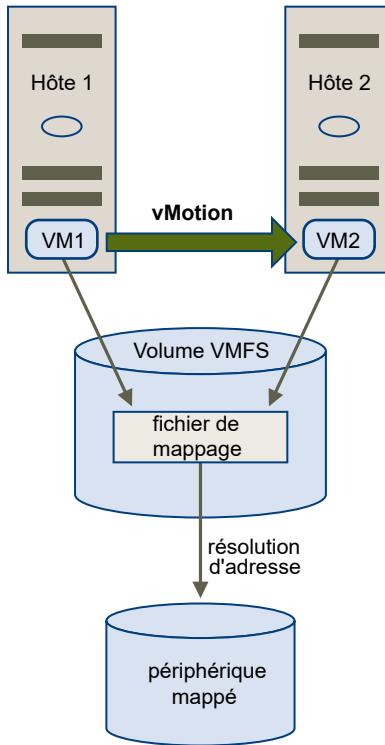
Snapshots

Permet d'utiliser des snapshots de machine virtuelle sur un volume mappé. Les snapshots ne sont pas disponibles lorsque le RDM est utilisé en mode de compatibilité physique.

vMotion

Vous permet de migrer une machine virtuelle avec vMotion. Le fichier de mappage agit comme un proxy pour permettre à vCenter Server de migrer la machine virtuelle à l'aide du même mécanisme que celui qui existe pour la migration des fichiers du disque.

Figure 11-2. vMotion pour une machine virtuelle utilisant le mappage de périphérique brut



Agents de gestion du SAN

Permet d'exécuter certains agents de gestion du SAN à l'intérieur d'une machine virtuelle. De même, tout logiciel ayant besoin d'accéder à un périphérique à l'aide de commandes SCSI spécifiques au matériel peut être exécuté dans une machine virtuelle. Ce type de logiciel est appelé logiciel basé sur cible SCSI. Lorsque vous utilisez les agents de gestion du SAN, sélectionnez un mode de compatibilité physique pour le RDM.

Virtualisation d'ID de port N (NPIV)

Permet d'utiliser la technologie NPIV qui autorise un port unique Fibre Channel HBA à s'enregistrer sur l'ensemble Fibre Channel à l'aide de plusieurs noms de port mondiaux (WWPN). Ainsi, le port HBA a la forme de ports virtuels multiples, chacun ayant son propre ID et un nom de port virtuel. Les machines virtuelles peuvent ensuite appeler chacun de ces ports virtuels et les utiliser pour tout le trafic RDM.

Note Vous ne pouvez utiliser le NPIV qu'avec les machines virtuelles dotées de disques RDM.

VMware travaille avec les fournisseurs de logiciel de gestion de stockage pour garantir que leur logiciel fonctionne correctement dans des environnements incluant ESXi. Certaines applications de ce type sont :

- Logiciel de gestion du SAN
- Logiciel de gestion des ressources de stockage (SRM)

- Logiciel de snapshot
- Logiciel de réPLICATION

De tels logiciels utilisent un mode de compatibilité physique pour les RDM afin que le logiciel puisse accéder aux périphériques directement.

Divers produits de gestion s'exécutent mieux de manière centralisée (non pas sur la machine ESXi, tandis que d'autres s'exécutent bien sur les machines virtuelles. VMware ne certifie pas ces applications ou ne fournit pas de matrice de compatibilité. Pour savoir si une application de gestion du SAN est prise en charge dans un environnement ESXi, contactez le fournisseur du logiciel de gestion du SAN.

Considérations et Limitations des RDM

Certaines considérations et limitations existent lorsque vous utilisez les RDM.

- Le RDM n'est pas disponible pour les périphériques de traitement par blocs ou certains périphériques RAID à connexion directe. Le RDM utilise un numéro série SCSI permettant d'identifier le périphérique mappé. Comme les périphériques de traitement par blocs et certains périphériques RAID à connexion directe n'exportent pas de numéros de série, ils ne peuvent pas être utilisés avec les RDM.
- Si vous utilisez le RDM en mode de compatibilité physique, vous ne pouvez pas utiliser un snapshot avec le disque. Le mode de compatibilité physique permet à la machine virtuelle de gérer son propre snapshot ou de mettre en miroir des opérations.

Les snapshots de machine virtuelle sont disponibles pour les RDM avec le mode de compatibilité virtuel.

- Vous ne pouvez pas mapper sur une partition de disque. Les RDM exigent que le périphérique mappé soit un LUN entier.
- Si vous utilisez vMotion pour migrer des machines virtuelles avec des RDM, assurez-vous de maintenir des ID de LUN cohérents pour les RDM, parmi tous les hôtes ESXi participant.

Caractéristiques du mappage de périphérique brut

Un RDM est un fichier de mappage spécial dans un volume VMFS qui gère les métadonnées pour son périphérique mappé. Le fichier de mappage est présenté au logiciel de gestion comme un fichier de disque ordinaire, disponible pour les opérations fichier-système habituelles. Pour la machine virtuelle, la couche de visualisation du stockage présente le périphérique mappé comme un périphérique SCSI.

Le contenu clé des métadonnées du fichier de mappage comprend l'emplacement du périphérique mappé (résolution de nom), l'état de verrouillage du périphérique mappé, les autorisations, etc.

Modes de compatibilité physique et virtuel du RDM

Vous pouvez utiliser les RDM en mode de compatibilité virtuelle ou en mode de compatibilité physique. Le mode virtuel spécifie la virtualisation totale du périphérique mappé. Le mode physique spécifie une virtualisation SCSI minimale du périphérique mappé, permettant une plus grande flexibilité pour le logiciel de gestion du réseau SAN.

En mode virtuel, VMkernel envoie uniquement READ et WRITE au périphérique mappé. Le périphérique mappé apparaît pour le système d'exploitation invité exactement comme un fichier de disque virtuel dans un volume VMFS. Les caractéristiques réelles du matériel sont masquées. Si vous utilisez un disque brut en mode virtuel, vous pouvez vous rendre compte des avantages du VMFS tels que le verrouillage avancé du fichier pour la protection des données et les snapshots pour la rationalisation des processus de développement. Le mode virtuel est également plus compatible au sein du matériel de stockage que le mode physique et présente le même comportement qu'un fichier de disque virtuel.

En mode physique, VMkernel transmet toutes les commandes SCSI au périphérique, sans aucune exception : la commande REPORT LUN est virtualisée afin que VMkernel puisse isoler le LUN pour la machine virtuelle propriétaire. Sinon, toutes les caractéristiques physiques du matériel sous-jacent sont exposées. Le mode physique est utilisé pour exécuter les agents de gestion du SAN et d'autres logiciels basés sur cible SCSI dans la machine virtuelle. Le mode physique permet également une mise en cluster virtuel à physique pour une disponibilité rentable.

VMFS5 et VMFS6 prennent en charge une taille de disque supérieure à 2 To pour les RDM en modes de compatibilité virtuelle et physique.

Résolution dynamique de nom

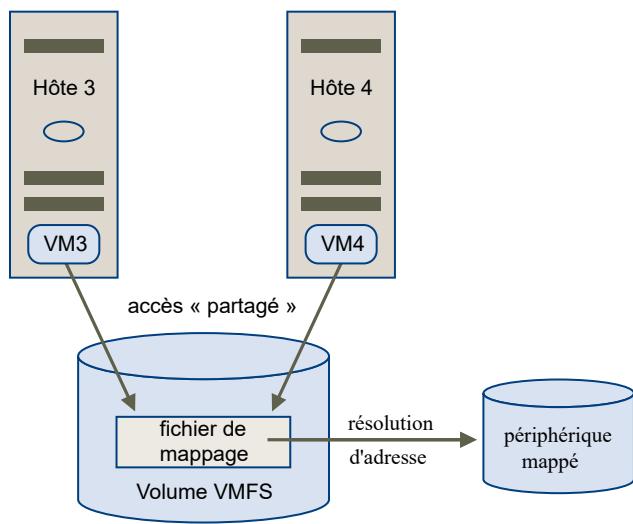
Le fichier RDM prend en charge la résolution dynamique de nom lorsqu'un chemin vers un périphérique brut change.

VMFS identifie de manière unique tous les périphériques de stockage mappés, et l'identification est stockée dans ses structures de données internes. Toute modification au chemin vers un périphérique brut, telle qu'une défaillance de commutateur Fibre Channel ou l'ajout d'un nouvel HBA, peut modifier le nom du périphérique. La résolution dynamique de nom résout ces modifications et associe automatiquement le périphérique d'origine à son nouveau nom.

Mappage de périphérique brut sur des clusters de machine virtuelle

Utilisez un RDM avec les clusters de machine virtuelle qui exigent l'accès au même LUN brut pour les scénarios de reprise. La configuration est identique à celle d'un cluster de machine virtuelle accédant au même fichier de disque virtuel, mais un RDM remplace le fichier de disque virtuel.

Figure 11-3. Accès à partir des machines virtuelles en clusters



Comparaison des modes d'accès disponibles du périphérique SCSI

Les méthodes d'accès à un périphérique de stockage SCSI comprennent un fichier de disque virtuel sur une banque de données VMFS, un RDM de mode virtuel et un RDM de mode physique.

Le tableau suivant fournit une comparaison des fonctions disponibles avec les différents modes.

Tableau 11-1. Fonctions disponibles dans les disques virtuels et les mappages de périphérique brut

Fonctions ESXi	Fichier de disque virtuel	RDM mode virtuel	RDM mode physique
Commandes SCSI transmises	Non	Non	Oui REPORT LUNs n'est pas transmis
Prise en charge vCenter Server	Oui	Oui	Oui
Snapshots	Oui	Oui	Non
Verrouillage distribué	Oui	Oui	Oui
Mettre en cluster	Cluster dans une boîte uniquement	Cluster dans une boîte cluster entre boîtes	Cluster physique à virtuel cluster entre boîtes
Logiciel basé sur cible SCSI	Non	Non	Oui

Utilisez les fichiers de disque virtuel pour le type Cluster dans une boîte. Si vous envisagez de reconfigurer vos clusters cluster dans une boîte en clusters cluster-across-the-box, utilisez les RDM de mode virtuel pour les clusters cluster dans une boîte.

Création de machines virtuelles avec des RDM

Quand vous donnez à votre machine virtuelle un accès direct à un LUN de réseau SAN brut, vous créez un disque RDM qui réside sur une banque de données VMFS et pointe vers le LUN. Vous

pouvez créer le RDM comme un disque initial pour une nouvelle machine virtuelle ou l'ajouter à une machine virtuelle existante. Lors de la création du RDM, vous spécifiez le LUN à mapper et la banque de données sur laquelle mettre le RDM.

Bien que le fichier du disque RDM ait la même extension `.vmdk` qu'un fichier de disque virtuel ordinaire, le RDM contient uniquement des informations de mappage. Les données réelles de disque virtuel sont stockées directement sur le LUN.

Cette procédure suppose que vous créez une nouvelle machine virtuelle. Pour plus d'informations, reportez-vous à la documentation *Administration d'une machine virtuelle vSphere*.

Procédure

1 Créez une machine virtuelle.

- a Cliquez avec le bouton droit sur n'importe quel objet de l'inventaire valide comme objet parent d'une machine virtuelle (un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, par exemple) et sélectionnez **Nouvelle machine virtuelle**.
- b Sélectionnez **Créer une nouvelle machine virtuelle** et cliquez sur **Suivant**.
- c Suivez les étapes requises pour créer une machine virtuelle.

2 Sur la page Personnaliser le matériel, cliquez sous l'onglet **Matériel virtuel**.

3 (Facultatif) Pour supprimer le disque dur virtuel par défaut créé par le système pour votre machine virtuelle, déplacez le curseur sur le disque et cliquez sur l'icône **Supprimer**.

4 Ajoutez un disque RDM.

- a Cliquez sur **Ajouter de nouveaux périphériques** et sélectionnez **Disque RDM** dans la liste.
- b Dans la liste des LUN, sélectionnez un LUN brut cible et cliquez sur **OK**.

Le système crée un disque RDM qui mappe votre machine virtuelle pour le LUN cible. Le disque RDM est affiché dans la liste des périphériques virtuels comme un nouveau disque dur.

5 Configurez le disque RDM.

- a Cliquez sur le triangle **Nouveau disque dur** pour développer les propriétés du disque RDM.
- b Sélectionnez un emplacement pour le RDM.

Vous pouvez placer le RDM sur la banque de données où résident vos fichiers de configuration de machine virtuelle ou en sélectionner une autre.

Note Pour utiliser vMotion pour les machines virtuelles avec NPIV activé, assurez-vous que les fichiers RDM et les fichiers des machines virtuelles sont situés dans la même banque de données. Vous ne pouvez pas effectuer des opérations Storage vMotion lorsque NPIV est activé.

- c Sélectionnez un mode de compatibilité.

Option	Description
Physique	Permet au système d'exploitation invité d'accéder directement au matériel. La compatibilité physique est utile si vous utilisez des applications prenant en charge les SAN sur la machine virtuelle. Toutefois, une machine virtuelle avec un RDM de compatibilité physique ne peut pas être clonée, convertie en modèle ou migrée si la migration implique de copier le disque.
Virtuel	Permet au RDM de se comporter comme un disque virtuel afin que vous puissiez utiliser des fonctions telles que la prise de snapshots, le clonage, etc. Quand vous clonez le disque ou en faites un modèle, le contenu du LUN est copié dans un fichier de disque virtuel .vmdk. Quand vous faites migrer un RDM en mode de compatibilité virtuelle, vous pouvez faire migrer le fichier de mappage ou copier le contenu du LUN dans un disque virtuel.

- d Si vous avez sélectionné un mode de compatibilité virtuel, sélectionnez un mode de disque.

Les modes de disque ne sont pas disponibles pour les disques RDM utilisant le mode de compatibilité physique.

Option	Description
Dépendant	Les disques dépendants sont inclus dans les snapshots.
Indépendant - Persistant	Les disques en mode persistant se comportent comme des disques normaux sur votre ordinateur physique. Toutes les données écrites sur un disque en mode persistant sont écrites de manière permanente sur le disque.
Indépendant - Non persistant	Les modifications des disques en mode de non-persistant sont supprimées lorsque vous mettez hors tension la machine virtuelle ou la réinitialisez. Avec non persistant, vous pouvez redémarrer la machine virtuelle avec un disque virtuel dans le même état chaque fois. Les modifications des disques sont écrites et lues dans un fichier journal de rétablissement qui est supprimé lorsque vous mettez hors tension ou réinitialisez.

- 6 Terminez la configuration de votre machine virtuelle.

Gérer les chemins pour un LUN mappé

Lorsque vous utilisez des machines virtuelles avec des RDM, vous pouvez gérer les chemins d'accès des LUN bruts mappés.

Procédure

- 1 Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.

- 2 Cliquez sur l'onglet **Appareil Virtuel**, puis sur **Disque dur** pour élargir le menu d'options de disque.
- 3 Cliquez sur l'ID de périphérique qui s'affiche en regard de **LUN physique** pour ouvrir la boîte de dialogue **Modifier les stratégies de gestion multivoie**.
- 4 Utilisez la boîte de dialogue **Modifier les stratégies de gestion multivoie** pour activer ou désactiver les chemins, définir la stratégie de gestion multivoie et indiquer le chemin préféré.

Pour plus d'informations sur la gestion des chemins, voir [Chapitre 10 Présentation de la gestion multivoie et du basculement](#).

Les machines virtuelles dotées de RDM doivent ignorer le cache SCSI INQUIRY

Certaines machines virtuelles dotées de RDM doivent obtenir les informations SCSI INQUIRY depuis le LUN plutôt qu'utiliser les données SCSI INQUIRY mises en cache par ESXi.

Problème

Certains systèmes d'exploitation invités ou certaines applications s'exécutant sur des machines virtuelles dotées de RDM ont un comportement imprévisible.

Cause

Ce comportement peut provenir des données SCSI INQUIRY mises en cache qui interfèrent avec les applications et les systèmes d'exploitation invités particuliers.

Lorsque l'hôte ESXi se connecte d'pour la première fois à un périphérique de stockage, il soumet la commande SCSI INQUIRY pour obtenir des données d'identification de base du périphérique. Par défaut ESXi met en cache les données SCSI INQUIRY reçues (Standard, page 80 et page 83) et les données restent par la suite inchangées. Les réponses aux commandes SCSI INQUIRY suivantes sont renvoyées à partir du cache.

Cependant, les systèmes d'exploitation invités particuliers s'exécutant sur des machines virtuelles dotées de RDM doivent interroger le LUN plutôt qu'utiliser les données SCSI INQUIRY mises en cache par ESXi. Dans ces cas, vous pouvez configurer la machine virtuelle afin d'ignorer le cache SCSI INQUIRY.

Solution

- ◆ Sélectionnez l'une des méthodes suivantes.

Option	Description
Modifier le fichier .vmx de la machine virtuelle avec le RDM	<p>Utilisez cette méthode pour les machines virtuelles disposant de la version matérielle 8 ou version ultérieure.</p> <p>a Ajoutez le paramètre suivant au fichier :</p> <pre>scsix:y.ignoreDeviceInquiryCache = "true"</pre> <p>où <i>x</i> est le nombre de contrôleurs SCSI et <i>y</i> le nombre cible SCSI du RDM.</p> <p>b Redémarrez la machine virtuelle.</p>
Utilisez la commande esxcli.	<p>Étant donné que vous configurez le paramètre au niveau de l'hôte, aucune limitation de version de matériel de machine virtuelle ne s'appliquent.</p> <pre>esxcli storage core device inquirecache set --device device_id --ignore true</pre> <p>Aucun redémarrage de machine virtuelle n'est nécessaire.</p>

Quelle que soit la méthode que vous utilisez pour définir le paramètre de cache SCSI INQUIRY sur true, la machine virtuelle démarre en contactant le LUN directement pour les données SCSI INQUIRY.

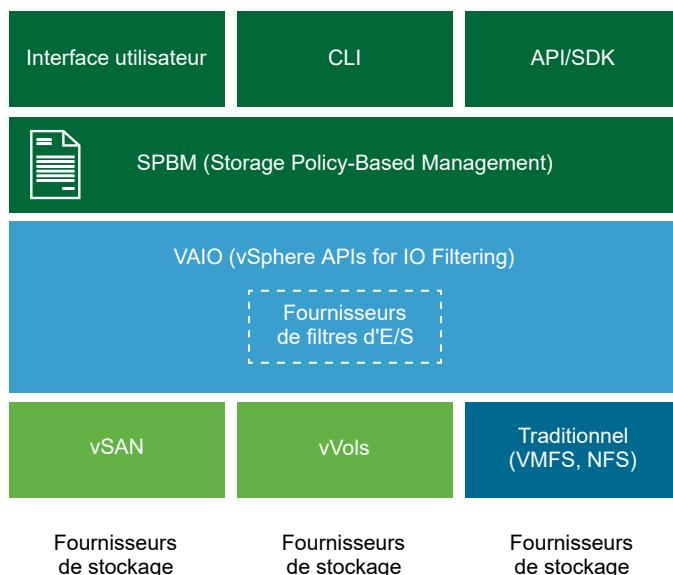
Paramètre ignoreDeviceInquiryCache dans vmx	Paramètres ignoreinquirycache dans esxcli	Demande d'interrogation traitée depuis
True	True	LUN
False (par défaut si le paramètre n'est pas présent)	True	LUN
True	False	LUN
False (par défaut si le paramètre n'est pas présent)	False	Cache

Gestion basée sur des stratégies de stockage (SPBM, Storage Policy Based Management)

Au sein d'un centre de données défini par logiciel, SPBM (Storage Policy Based Management) joue un rôle majeur en vous aidant à aligner le stockage sur les impératifs des applications de vos machines virtuelles. Ce mécanisme offre une infrastructure de stratégie de stockage qui fournit un panneau de contrôle unifié unique sur une large variété de services de données et de solutions de stockage.

En tant que couche d'abstraction, SPBM abstrait les services de stockage livrés par Virtual Volumes, vSAN, les filtres d'E/S ou d'autres entités de stockage.

Plutôt qu'une intégration avec chaque type de stockage et service de données, SPBM fournit une infrastructure universelle pour de nombreux types d'entités de stockage.



SPBM offre les mécanismes suivants :

- Annonce des capacités de stockage et des services de données que les baies de stockage et d'autres entités (par exemple, les filtres d'E/S) peuvent offrir.
- Communications bidirectionnelles entre ESXi et vCenter Server d'un côté, et les baies et les entités de stockage de l'autre.
- Provisionnement de machines virtuelles basé sur des stratégies de stockage de machine virtuelle.

Ce chapitre contient les rubriques suivantes :

- Stratégies de stockage de machine virtuelle
- Workflow pour les stratégies de stockage de machine virtuelle
- Remplissage de l'interface des stratégies de stockage de machine virtuelle
- À propos des règles et groupes de règles
- Création et gestion de stratégies de stockage de machine virtuelle
- À propos des composants de stratégie de stockage
- Stratégies de stockage et machines virtuelles
- Stratégies de stockage par défaut

Stratégies de stockage de machine virtuelle

Les stratégies de stockage de machine virtuelle sont essentielles pour le provisionnement des machines virtuelles via SPBM. Les stratégies déterminent le type de stockage fourni pour la machine virtuelle et comment cette dernière est placée dans le stockage. Elles déterminent également les services de données que la machine virtuelle peut utiliser.

vSphere propose des stratégies de stockage par défaut. Vous pouvez aussi en définir d'autres et les attribuer aux machines virtuelles.

Vous utilisez l'interface de stratégies de stockage de machine virtuelle pour créer une stratégie de stockage. Lorsque vous définissez la stratégie, vous spécifiez les différents besoins en stockage des applications qui s'exécutent sur les machines virtuelles. Vous pouvez également utiliser des stratégies de stockage pour demander des services de données spécifiques, comme la mise en cache ou la réplication, pour des disques virtuels.

Vous appliquez la stratégie de stockage lorsque vous créez, clonez ou migrez la machine virtuelle. Après l'application de la stratégie de stockage, le mécanisme SPBM vous aide à placer la machine virtuelle dans une banque de données correspondante. Dans certains environnements de stockage, SPBM détermine comment les objets de stockage de machine virtuelle sont provisionnés et alloués dans la ressource de stockage pour garantir le niveau de service requis. SPBM active aussi les services de données demandés pour la machine virtuelle et vous aide à surveiller la conformité de la stratégie.

Workflow pour les stratégies de stockage de machine virtuelle

En général, le processus de création et de gestion des stratégies de stockage est fragmenté en plusieurs étapes.

Une étape spécifique peut être requise ou non, selon le type de services de données ou de stockage offert par votre environnement.

Étape	Description
Remplissez l'interface des stratégies de stockage de machine virtuelle avec les données appropriées.	<p>Vérifiez que l'interface des stratégies de stockage de machine virtuelle contient les informations relatives aux banques de données et aux services de données disponibles dans votre environnement de stockage. Ces informations sont communiquées par des fournisseurs de stockage et des balises de banque de données.</p> <ul style="list-style-type: none"> ■ Pour les entités représentées par des fournisseurs de stockage, vérifiez qu'un fournisseur approprié est enregistré. Les entités qui utilisent le fournisseur de stockage sont notamment vSAN, Virtual Volumes et les filtres d'E/S. Selon le type de l'entité de stockage, certains fournisseurs sont automatiquement enregistrés. D'autres fournisseurs peuvent être manuellement enregistrés. Reportez-vous aux sections Utiliser des fournisseurs de stockage pour remplir l'interface des stratégies de stockage de machine virtuelle et Enregistrer des fournisseurs de stockage pour Virtual Volumes. ■ Balisez les banques de données qui ne sont pas représentées par des fournisseurs de stockage. Vous pouvez également utiliser les balises pour indiquer une propriété qui n'est pas communiquée via le fournisseur de stockage, par exemple un emplacement géographique ou un groupe administratif. Reportez-vous à la section Affecter des balises à des banques de données.
Créez des composants de stratégie de stockage prédéfinis.	<p>Un composant de stratégie de stockage décrit un service de données spécifique, tel que la réplication, qui doit être fourni pour la machine virtuelle. Vous pouvez définir le composant d'avance et l'associer à plusieurs stratégies de stockage de machine virtuelle. Les composants sont réutilisables et interchangeables.</p> <p>Reportez-vous à la section Créer des composants de stratégie de stockage.</p>
Créez des stratégies de stockage de machine virtuelle.	<p>Lorsque vous définissez des stratégies de stockage pour des machines virtuelles, vous spécifiez les besoins en stockage des applications qui s'exécutent sur les machines virtuelles.</p> <p>Reportez-vous à la section Création et gestion de stratégies de stockage de machine virtuelle.</p>
Appliquez la stratégie de stockage de machine virtuelle à la machine virtuelle.	<p>Vous pouvez appliquer la stratégie de stockage lorsque vous déployez la machine virtuelle ou lorsque vous configurez ses disques virtuels.</p> <p>Reportez-vous à la section Attribuer des stratégies de stockage à des machines virtuelles.</p>
Vérifiez la conformité de la stratégie de stockage de machine virtuelle.	<p>Vérifiez que la machine virtuelle utilise la banque de données conforme à la stratégie de stockage attribuée.</p> <p>Reportez-vous à la section Vérifier la conformité d'une stratégie de stockage de machine virtuelle.</p>

Pour créer et gérer vos stratégies de stockage, vous utilisez l'interface de stratégie de stockage de machine virtuelles de vSphere Client.

Remplissage de l'interface des stratégies de stockage de machine virtuelle

Avant de commencer à créer des stratégies de stockage de machine virtuelle, remplissez l'interface des stratégies de stockage de machine virtuelle avec des informations sur les entités de stockage et les services de données disponibles dans votre environnement de stockage.

Ces informations sont obtenues auprès de fournisseurs de stockage, également appelés fournisseurs VASA. Les balises de banque de données constituent une autre source.

Capacités et services de stockage

Certaines banques de données (par exemple, Virtual Volumes et vSAN) sont représentées par les fournisseurs de stockage. Via les fournisseurs de stockage, les banques de données peuvent annoncer leur capacité dans l'interface des stratégies de stockage de machine virtuelle. Ces capacités de banque de données, services de données et autres caractéristiques avec des plages de valeurs remplissent l'interface des stratégies de stockage de machine virtuelle.

Elles vous permettent de définir les règles de placement et de service basées sur la banque de données de votre stratégie de stockage.

Services de données

Les filtres d'E/S sur vos hôtes sont également représentés par les fournisseurs de stockage. Le fournisseur de stockage fournit les informations sur les services de données des filtres à l'interface des stratégies de stockage de machine virtuelle. Ces informations vous permettent de définir les règles des services de données basés sur un hôte, également appelées règles communes. Contrairement aux règles spécifiques au stockage, ces règles ne définissent pas les conditions requises pour le placement de stockage et le stockage de la machine virtuelle. Elles activent plutôt les services de données de filtre d'E/S demandés pour la machine virtuelle.

Balises

En règle générale, les banques de données VMFS et NFS ne sont pas représentées par un fournisseur de stockage. Leurs capacités et leurs services de données ne s'affichent pas dans l'interface des stratégies de stockage de machine virtuelle. Vous pouvez utiliser des balises pour coder des informations sur ces banques de données. Par exemple, vous pouvez baliser vos banques de données VMFS avec les balises VMFS-Gold et VMFS-Silver pour représenter différents niveaux de service.

Pour les banques de données Virtual Volumes et vSAN, vous pouvez utiliser des balises pour encoder des informations qui ne sont pas annoncées par le fournisseur de stockage, par exemple l'emplacement géographique (Palo Alto) ou le groupe administratif (Comptabilité).

Similaires aux capacités de stockage et aux caractéristiques, toutes les balises associées aux banques de données s'affichent dans l'interface des stratégies de stockage de machine virtuelle. Vous pouvez utiliser les balises lorsque vous définissez les règles de placement basé sur les balises.

Utiliser des fournisseurs de stockage pour remplir l'interface des stratégies de stockage de machine virtuelle

Pour les entités représentées par des fournisseurs de stockage (VASA), vérifiez qu'un fournisseur approprié est enregistré. Après l'enregistrement des fournisseurs de stockage, l'interface des

stratégies de stockage de machine virtuelle devient remplie avec des informations sur les banques de données et les services de données que les fournisseurs représentent.

Les entités qui utilisent le fournisseur de stockage sont notamment vSAN, Virtual Volumes et les filtres d'E/S. Selon le type de l'entité, certains fournisseurs sont automatiquement enregistrés. D'autres fournisseurs (par exemple, le fournisseur de stockage Virtual Volumes) doivent être manuellement enregistrés. Après l'enregistrement des fournisseurs de stockage, ces derniers livrent les données suivantes aux stratégies de stockage de machine virtuelle :

- Capacités de stockage et caractéristiques de banques de données telles que Virtual Volumes et vSAN.
- Services de données fournis par les filtres d'E/S.

Conditions préalables

Enregistrez les fournisseurs de stockage qui nécessitent un enregistrement manuel. Pour plus d'informations, consultez la documentation appropriée :

- *Administration de VMware vSAN*
- [Chapitre 14 Utilisation de VMware vSphere Virtual Volumes](#)
- [Chapitre 15 Filtrage des E/S de machines virtuelles](#)

Procédure

- 1 Accédez à l'instance de vCenter Server.
- 2 Cliquez sur l'onglet **Configurer**, puis cliquez sur **Fournisseurs de stockage**.
- 3 Dans la liste Fournisseurs de stockage, affichez les fournisseurs de stockage enregistrés dans vCenter Server.
La liste présente des informations générales, notamment le nom du fournisseur de stockage, son adresse URL et son état, les entités de stockage que le fournisseur représente, etc.
- 4 Pour afficher des informations plus détaillées, sélectionnez un fournisseur de stockage spécifique ou son composant dans la liste.

Affecter des balises à des banques de données

Utilisez des balises pour coder les informations sur une banque de données. Les balises sont utiles lorsque votre banque de données n'est pas représentée par un fournisseur de stockage et n'annonce pas ses services dans l'interface des stratégies de stockage de machine virtuelle. Vous pouvez également utiliser les balises pour indiquer une propriété qui n'est pas communiquée par un fournisseur de stockage, par exemple un emplacement géographique ou un groupe administratif.

Vous pouvez appliquer à une banque de données une nouvelle balise contenant des informations générales de stockage. Pour obtenir des informations plus détaillées sur les balises et leurs catégories et découvrir comment les gérer, reportez-vous à la documentation *Gestion de vCenter Server et des hôtes*.

Conditions préalables

Privilèges requis :

- **Balisage vSphere.**Créer une balise vSphere à la racine de l'instance de vCenter Server.
- **Balisage vSphere.**Créer une catégorie de balises vSphere à la racine de l'instance de vCenter Server.
- **Balisage vSphere.**Attribuer une balise vSphere ou en annuler l'attribution à la racine de l'instance de vCenter Server.

Procédure

1 Dans vSphere Client, créez une catégorie pour les balises de stockage.

- a Dans le menu Accueil, cliquez sur **Balises et attributs personnalisés**.
- b Cliquez sur l'onglet **Balises**, puis sur **Catégories**.
- c Cliquez sur l'icône **Ajouter une catégorie**.
- d Spécifiez les propriétés de la catégorie. Voir l'exemple suivant.

Propriété de la catégorie	Exemple
Nom catégorie	Emplacement de stockage
Description	Catégorie des balises relatives à l'emplacement de stockage
Balises par objet	Plusieurs balises
Types d'objets qui peuvent être liés	Banque de données et Cluster de banque de données

- e Cliquez sur **OK**.

2 Créez une balise de stockage.

- a Dans l'onglet **Balises**, cliquez sur **Balises**.
- b Cliquez sur l'icône **Ajouter une balise**.
- c Spécifiez les propriétés pour la balise. Voir l'exemple suivant.

Propriété de balise	Exemple
Nom	Texas
Description	Banque de données située au Texas
Catégorie	Emplacement de stockage

- d Cliquez sur **OK**.

- 3 Appliquez la balise à la banque de données.
 - a Accédez à la banque de données.
 - b Cliquez avec le bouton droit sur la banque de données, puis sélectionnez**Balises et attributs personnalisés > Affecter une balise**.
 - c Dans la liste de balises, sélectionnez une balise appropriée, par exemple, Texas dans la catégorie Emplacement de stockage et cliquez sur **Attribuer**.

Résultats

La nouvelle balise est attribuée à la banque de données et figure sur l'onglet **Résumé** du volet **Balises** de la banque de données.

Étape suivante

Lors de la création d'une stratégie de stockage de machine virtuelle, vous pouvez faire référence à la balise pour inclure la banque de données balisée dans la liste des ressources de stockage compatibles. Reportez-vous à la section [Créer une stratégie de stockage de machines virtuelles pour le placement basé sur des balises](#).

Vous pouvez également exclure la banque de données balisée de la stratégie de stockage de machine virtuelle. Par exemple, votre stratégie de stockage de VM peut inclure les banques de données Virtual Volumes situées au Texas et en Californie, mais exclure celles se trouvant au Nevada.

Pour en savoir plus sur l'utilisation de balises dans les stratégies de stockage de machine virtuelle, visionnez la vidéo suivante.



(Utilisation de balises dans les stratégies de stockage)

À propos des règles et groupes de règles

Lorsque l'interface des stratégies de stockage de machine virtuelle contient les données appropriées, vous pouvez commencer à créer vos stratégies de stockage. La création d'une stratégie consiste à définir des règles de placement pour le stockage spécifique et des règles pour configurer les services de données.

Règles

La règle est un élément de base de la stratégie de stockage de machine virtuelle. Chaque règle individuelle est une instruction qui décrit une exigence spécifique du stockage de machine virtuelle et des services de données.

Groupes de règles

Dans une stratégie de stockage, les règles individuelles sont organisées en collections de règles ou groupes de règles. Généralement, les règles sont réparties dans les catégories suivantes : règles pour les services basés sur l'hôte et règles spécifiques à une banque de données.

Groupes de règles spécifiques à une banque de données

Chaque groupe de règles doit inclure des règles de placement qui décrivent les exigences des ressources de stockage de machine virtuelle. Toutes les règles de placement au sein d'un groupe de règles spécifique représentent une entité de stockage unique. Ces règles peuvent être basées sur les capacités de stockage ou les balises.

En outre, le groupe de règles spécifique à une banque de données peut inclure des règles ou des composants de stratégie de stockage facultatifs qui décrivent les services de données à fournir pour la machine virtuelle. De manière générale, ces règles demandent des services tels que la mise en cache, la réPLICATION et d'autres services fournis par les systèmes de stockage.

Pour définir la stratégie de stockage, un groupe spécifique à la banque de données est requis. Les ensembles de règles supplémentaires sont facultatifs. Une stratégie spécifique peut utiliser plusieurs groupes de règles pour définir d'autres paramètres de placement de stockage, souvent à partir de plusieurs fournisseurs de stockage.

Règles de placement : basées sur la capacité

Les règles de placement spécifient une condition requise de stockage particulière pour la machine virtuelle et activent SPBM pour distinguer les banques de données compatibles parmi toutes les banques de données de l'inventaire. Ces règles décrivent également comment les objets de stockage de machine virtuelle sont alloués dans la banque de données pour recevoir le niveau de service requis. Par exemple, les règles peuvent répertorier Virtual Volumes comme destination et définir l'objectif de point de récupération (RPO) maximal pour les objets Virtual Volumes.

Lorsque vous provisionnez la machine virtuelle, ces règles déterminent la décision prise par SPBM concernant le placement de la machine virtuelle. SPBM trouve les banques de données Virtual Volumes pouvant correspondre aux règles et répondre aux conditions requises de stockage de la machine virtuelle. Reportez-vous à la section [Créer une stratégie de stockage de machine virtuelle pour Virtual Volumes](#).

Règles de placement : basées sur des balises

Les règles basées sur des balises font référence aux balises de la banque de données. Ces règles peuvent définir le placement de la machine virtuelle, par exemple, demander de choisir comme cible toutes les banques de données disposant de la balise VMFS-Gold. Vous pouvez utiliser les règles basées sur des balises pour ajuster votre demande de placement de machine virtuelle. Par exemple, exclure les banques de données comportant la balise Palo Alto de la liste de vos banques de données Virtual Volumes. Reportez-vous à la section [Créer une stratégie de stockage de machines virtuelles pour le placement basé sur des balises](#).

Règles pour les services basés sur l'hôte

Ce groupe de règles active les services de données fournis par l'hôte. Le groupe de services basés sur hôte peut inclure des règles ou des composants de stratégie de stockage qui décrivent certains services de données en particulier, tels que le chiffrement ou la réplication.

Contrairement aux règles spécifiques à une banque de données, ce groupe n'inclut pas les règles de placement. Les règles pour les services de données sont génériques (ils s'appliquent à tous les types de stockage) et ne dépendent pas de la banque de données.

Reportez-vous à la section [Créer une stratégie de stockage de machine virtuelle pour les services de données basés sur l'hôte](#).

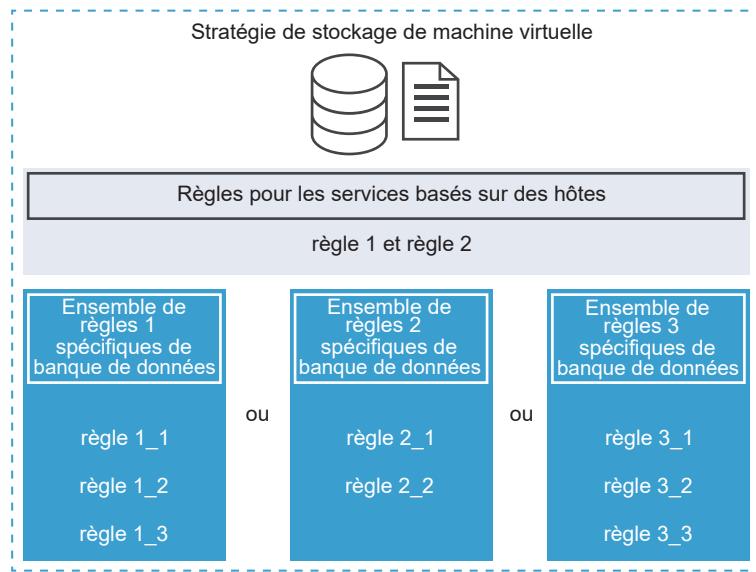
Tableau 12-1. Structure d'une stratégie de stockage de machine virtuelle

Règles pour les services basés sur l'hôte	Groupes de règles spécifiques à une banque de données
Règles ou composants de stratégie de stockage prédéfinis servant à activer les services de données installés sur des hôtes ESXi. Par exemple, réplication par filtres d'E/S.	Règles de placement basées sur la capacité ou des balises, qui décrivent les conditions requises pour les ressources de stockage de machine virtuelle. Par exemple, placement de Virtual Volumes. Règles ou composants de stratégie de stockage prédéfinis qui activent les services de données fournies par le stockage. Par exemple, mise en cache par Virtual Volumes.

Relation entre règles et groupes de règles

L'opérateur booléen OR définit la relation entre les groupes de règles spécifiques à une banque de données au sein de la stratégie. L'opérateur AND définit la relation entre toutes les règles au sein d'un groupe de règles spécifique. La stratégie peut contenir uniquement un groupe de règles pour les services basés sur l'hôte, uniquement un groupe de règles spécifique à une banque de données ou les deux.

Si le groupe de règles pour les services basés sur l'hôte n'est pas présent, le respect de toutes les règles d'un seul groupe de règles spécifiques à la banque de données suffit à satisfaire toute la stratégie. Si le groupe de règles pour les services basés sur l'hôte est présent, la stratégie correspond à la banque de données qui satisfait aux règles des services de l'hôte et à toutes les règles dans un des groupes spécifiques à une banque de données.



Création et gestion de stratégies de stockage de machine virtuelle

Pour créer et gérer des stratégies de stockage pour vos machines virtuelles, vous utilisez l'interface Stratégies de stockage VM.

Créer une stratégie de stockage de machine virtuelle pour les services de données basés sur l'hôte

Pour définir la stratégie de stockage VM dans vSphere Client, utilisez l'assistant **Créer une stratégie de stockage VM**. Dans cette tâche, vous créez des règles pour les services de données offerts par les hôtes ESXi. La stratégie de stockage VM qui inclut ces règles active les services de données spécifiés pour la machine virtuelle.

Les services de données disponibles incluent le chiffrement, le contrôle d'E/S, la mise en cache, etc. Certains services de données, tels que le chiffrement, sont fournis par VMware. D'autres peuvent être proposés par des filtres d'E/S tiers que vous installez sur votre hôte.

Les services de données sont généralement génériques pour tous les types de stockage et ne dépendent pas d'une banque de données. L'ajout de règles spécifiques à une banque de données à la stratégie de stockage est facultatif.

Si vous ajoutez des règles spécifiques à une banque de données, et que les filtres d'E/S sur l'hôte et le stockage proposent le même type de service, par exemple le chiffrement, votre stratégie peut demander ce service aux deux fournisseurs. Les données de la machine virtuelle sont donc chiffrées deux fois, par le filtre d'E/S et par votre stockage. Cependant, la réPLICATION fournie par Virtual Volumes et celle fournie par le filtre d'E/S ne peuvent pas coexister dans la même stratégie de stockage.

Conditions préalables

- Pour plus d'informations sur le chiffrement de vos machines virtuelles, reportez-vous à la documentation *Sécurité vSphere*.
- Pour plus d'informations sur les filtres d'E/S, reportez-vous au [Chapitre 15 Filtrage des E/S de machines virtuelles](#).
- Pour plus d'informations sur les composants de stratégie de stockage, reportez-vous à [À propos des composants de stratégie de stockage](#).
- Privilèges nécessaires : **Stratégies de stockage VM.Mettre à jour** et **Stratégies de stockage VM.Afficher**.

Procédure

- 1 Ouvrez l'assistant **Créer une stratégie de stockage VM**.
 - a Cliquez sur **Menu > Stratégies et profils**.
 - b Sous **Stratégies et profils**, cliquez sur **Stratégies de stockage VM**
 - c Cliquez sur **Créer**.
- 2 Entrez le nom de la stratégie et sa description, puis cliquez sur **Suivant**.

Option	Action
vCenter Server	Sélectionnez l'instance de vCenter Server.
Nom	Entrez le nom de la stratégie de stockage.
Description	Entrez la description de la stratégie de stockage.

- 3 Sur la page **Structure de la stratégie**, sous **Services basés sur l'hôte**, cliquez sur **Activer les règles basées sur l'hôte**.

- 4 Sur la page **Services basés sur l'hôte**, définissez des règles et configurez les services de données fournis par votre hôte.
 - a Cliquez sur l'onglet de la catégorie de service de données, par exemple **Chiffrement**.
 - b Définissez des règles personnalisées pour la catégorie de service de données ou utilisez des composants prédéfinis.

Option	Description
Désactivé	Il s'agit d'un paramètre par défaut.
Utiliser le composant de stratégie de stockage	Sélectionnez un composant de stratégie de stockage dans le menu déroulant. Cette option est disponible uniquement si vous disposez dans votre base de données de composants prédéfinis.
Personnalisé	Définissez des règles personnalisées pour la catégorie de service de données en spécifiant un fournisseur approprié et des valeurs pour ces règles.

Note Vous pouvez activer plusieurs services de données. Si vous utilisez le chiffrement avec d'autres services de données, utilisez l'option de chiffrement personnalisé et définissez le paramètre **Autoriser les filtres d'E/S avant le chiffrement** sur **True**. Ce paramètre permet à d'autres services tels que la réPLICATION d'analyser les données de texte clair avant leur chiffrement.

- 5 Sur la page **Compatibilité de stockage**, vérifiez la liste des banques de données qui correspondent à cette stratégie.
Pour être compatible avec la stratégie pour les services basés sur l'hôte, les banques de données doivent être connectées à l'hôte qui fournit ces services. Si vous ajoutez des ensembles de règles spécifiques à la banque de données, les banques de données compatibles doivent également remplir les exigences de la stratégie.
- 6 Sur la page **Vérifier et terminer**, vérifiez les paramètres de la stratégie de stockage, puis cliquez sur **Terminer**.

Pour modifier des paramètres, cliquez sur **Précédent** afin de revenir à la page concernée.

Résultats

La nouvelle stratégie de stockage VM pour les services de données basés sur l'hôte figure dans la liste.

Créer une stratégie de stockage de machine virtuelle pour Virtual Volumes

Pour définir la stratégie de stockage VM dans vSphere Client, utilisez l'assistant **Créer une stratégie de stockage VM**. Dans cette tâche, vous créez une stratégie de stockage personnalisée compatible avec Virtual Volumes. Lorsque vous définissez la stratégie de stockage VM pour Virtual Volumes, vous créez des règles pour configurer les services de stockage et de données fournis par la banque de données Virtual Volumes. Les règles sont appliquées lorsque la

machine virtuelle est placée sur la banque de données Virtual Volumes. La stratégie de stockage personnalisée peut remplacer la stratégie de stockage par défaut. Aucune condition requise pour Virtual Volumes est fournie par VMware.

La procédure part du principe que vous créez la stratégie de stockage VM pour Virtual Volumes. Pour plus d'informations sur la stratégie de stockage vSAN, reportez-vous à la documentation *Administration de VMware vSAN*.

Conditions préalables

- Vérifiez que le fournisseur de stockage Virtual Volumes est disponible et actif. Reportez-vous à la section [Enregistrer des fournisseurs de stockage pour Virtual Volumes](#).
- Vérifiez que l'interface des stratégies de stockage VM contient les informations relatives aux entités de stockage et aux services de données qui sont disponibles dans votre environnement de stockage. Reportez-vous à la section [Remplissage de l'interface des stratégies de stockage de machine virtuelle](#).
- Définissez les composants de stratégie de stockage adéquats. Reportez-vous à la section [Créer des composants de stratégie de stockage](#).
- Privilèges nécessaires : **Stratégies de stockage VM.Mettre à jour** et **Stratégies de stockage VM.Afficher**.

Procédure

- 1 Ouvrez l'assistant **Créer une stratégie de stockage VM**.
 - a Cliquez sur **Menu > Stratégies et profils**.
 - b Sous **Stratégies et profils**, cliquez sur **Stratégies de stockage VM**.
 - c Cliquez sur **Créer**.
- 2 Entrez le nom de la stratégie et sa description, puis cliquez sur **Suivant**.

Option	Action
vCenter Server	Sélectionnez l'instance de vCenter Server.
Nom	Entrez le nom de la stratégie de stockage, par exemple Stratégie de stockage Virtual Volumes.
Description	Entrez la description de la stratégie de stockage.

- 3 Sur la page **Structure de la stratégie** sous Règles spécifiques à la banque de données, activez des règles pour une entité de stockage cible, comme le stockage Virtual Volumes.

Vous pouvez activer des règles pour plusieurs banques de données. L'utilisation de plusieurs groupes de règles permet à une stratégie de définir d'autres paramètres de stockage, souvent à partir de plusieurs fournisseurs de stockage.

- 4** Sur la page des règles de *Virtual Volumes*, définir les règles de placement de stockage pour la banque de données Virtual Volumes cible.

a Cliquez sur l'onglet **Placement** et cliquez sur **Ajouter une règle**.

b Dans le menu déroulant Ajouter une règle, sélectionnez une capacité disponible et spécifiez sa valeur.

Par exemple, vous pouvez spécifier le nombre d'opérations de lecture par seconde pour les objets Virtual Volumes.

Vous pouvez inclure autant de règles que nécessaire pour l'entité de stockage sélectionnée. Assurez-vous que les valeurs que vous indiquez sont comprises dans la plage de valeurs annoncée par la banque de données Virtual Volumes.

c Pour ajuster votre demande de placement, cliquez sur l'onglet **Balises** et ajoutez une règle basée sur la balise.

Les règles basées sur une balise peuvent filtrer les banques de données par inclusion ou exclusion des critères de placement spécifiques. Par exemple, votre stratégie de stockage de VM peut inclure les banques de données Virtual Volumes situées au Texas et en Californie, mais exclure celles se trouvant au Nevada.

- 5** (Facultatif) Définissez des règles pour configurer des services spécifique à la banque de données.

Les services de données, telles que le chiffrement, la mise en cache ou la réPLICATION, sont proposés par le stockage. La stratégie de stockage de machine virtuelle qui fait référence à des services de données exige ces services pour la machine virtuelle lorsque la machine virtuelle est placée sur la banque de données Virtual Volumes.

a Cliquez sur l'onglet de la catégorie de service de données, par exemple **RéPLICATION**.

b Définissez des règles personnalisées pour la catégorie de service de données ou utilisez des composants prédéfinis.

Option	Description
Désactivé	Il s'agit d'un paramètre par défaut.
Utiliser le composant de stratégie de stockage	Sélectionnez un composant de stratégie de stockage dans le menu déroulant. Cette option est disponible uniquement si vous disposez dans votre base de données de composants prédéfinis.
Personnalisé	Définissez des règles personnalisées pour la catégorie de service de données en spécifiant un fournisseur approprié et des valeurs pour ces règles.

- 6** Sur la page **Compatibilité de stockage**, vérifiez la liste des banques de données qui correspondent à cette stratégie.

Si la stratégie inclut plusieurs ensembles de règles, la banque de données doit être conforme au minimum à un ensemble de règles et à toutes les règles de cet ensemble.

- 7 Sur la page **Vérifier et terminer**, vérifiez les paramètres de la stratégie de stockage, puis cliquez sur **Terminer**.

Pour modifier des paramètres, cliquez sur **Précédent** afin de revenir à la page concernée.

Résultats

La nouvelle stratégie de stockage de machine virtuelle compatible avec Virtual Volumes s'affiche dans la liste.

Étape suivante

Vous pouvez désormais associer cette stratégie à une machine virtuelle ou la définir comme stratégie par défaut.

Créer une stratégie de stockage de machines virtuelles pour le placement basé sur des balises

Les règles basées sur des balises réfèrent aux balises que vous attribuez aux banques de données et vous pouvez filtrer les banques de données à utiliser pour le placement des machines virtuelles. Pour définir le placement basé sur des balises dans vSphere Client, utilisez l'assistant **Créer une stratégie de stockage VM**.

Conditions préalables

- Vérifiez que l'interface des stratégies de stockage VM contient les informations relatives aux entités de stockage et aux services de données qui sont disponibles dans votre environnement de stockage. Reportez-vous à la section [Remplissage de l'interface des stratégies de stockage de machine virtuelle](#).
- Privilèges nécessaires : **Stratégies de stockage VM.Mettre à jour** et **Stratégies de stockage VM.Afficher**.

Procédure

- 1 Ouvrez l'assistant **Créer une stratégie de stockage VM**.
 - a Cliquez sur **Menu > Stratégies et profils**.
 - b Sous **Stratégies et profils**, cliquez sur **Stratégies de stockage VM**.
 - c Cliquez sur **Créer**.
- 2 Entrez le nom de la stratégie et sa description, puis cliquez sur **Suivant**.

Option	Action
vCenter Server	Sélectionnez l'instance de vCenter Server.
Nom	Entrez le nom de la stratégie de stockage.
Description	Entrez la description de la stratégie de stockage.

- 3 Sur la page **Structure de la stratégie** sous Règles spécifiques à une base de données, activez les règles de placement basé sur des balises.
- 4 Sur la page **Placement basé sur une balise**, créez les règles de balise.
 - a Cliquez sur **Ajouter une règle de balise** et définissez des critères de placement basés sur des balises. En voici un exemple :

Option	Exemple
Catégorie de balise	Niveau de service
Option d'utilisation	Utiliser le stockage marqué avec des balises
Balises	Gold

Toutes les banques de données avec la balise Gold deviennent compatibles en tant que cibles de placement de stockage.

- b (Facultatif) Ajoutez davantage de règles basées sur des balises.
- 5 Sur la page **Compatibilité de stockage**, vérifiez la liste des banques de données qui correspondent à cette stratégie.
- 6 Sur la page **Vérifier et terminer**, vérifiez les paramètres de la stratégie de stockage, puis cliquez sur **Terminer**.

Pour modifier des paramètres, cliquez sur **Précédent** afin de revenir à la page concernée.

Résultats

La nouvelle stratégie de stockage de machine virtuelle compatible avec les banques de données marquées s'affiche dans la liste.

Modifier ou cloner une stratégie de stockage de machine virtuelle

Si la configuration requise du stockage de machines virtuelles et de disques virtuels est modifiée, vous pouvez modifier la stratégie de stockage existante. Vous pouvez également créer une copie de la stratégie de stockage de machine virtuelle existante en la clonant. Pendant le clonage, vous pouvez choisir de personnaliser la stratégie de stockage d'origine.

Conditions préalables

Privilège requis : **StorageProfile.View**

Procédure

- 1 Dans vSphere Client, accédez à la stratégie de stockage.
 - a Cliquez sur **Menu > Stratégies et profils**.
 - b Sous **Stratégies et profils**, cliquez sur **Stratégies de stockage VM**.
- 2 Sélectionnez la stratégie de stockage, puis cliquez sur l'une des icônes suivantes :
 - **Modifier**

- Cloner

- 3 (Facultatif) Modifiez la règle et cliquez sur **OK**.
- 4 Si la modification concerne une stratégie de stockage qui est utilisée par une machine virtuelle, réappliquez la stratégie à la machine virtuelle.

Option	Description
Plus tard manuellement	Si vous choisissez cette option, l'état de conformité de l'ensemble des disques virtuels et des objets de base des machines virtuelles associés à la stratégie de stockage passe à Périmé. Pour mettre à jour la configuration et l'état de conformité, appliquez de nouveau manuellement la stratégie de stockage à toutes les entités associées. Reportez-vous à la section Réappliquer une stratégie de stockage de machine virtuelle .
Maintenant	Pour mettre à jour la machine virtuelle et l'état de conformité immédiatement après avoir modifié la stratégie de stockage.

À propos des composants de stratégie de stockage

Une stratégie de stockage de machine virtuelle peut inclure un ou plusieurs composants de base réutilisables et interchangeables, appelés composants de stratégie de stockage. Chaque composant décrit un service de données particulier à fournir pour la machine virtuelle. Vous pouvez définir les composants de stratégie d'avance et les associer à plusieurs stratégies de stockage de machine virtuelle.

Vous ne pouvez pas attribuer le composant prédéfini directement à une machine virtuelle ou à un disque virtuel. Vous devez plutôt ajouter le composant à la stratégie de stockage de machine virtuelle, puis attribuer la stratégie à la machine virtuelle.

Le composant décrit un type de service à partir d'un fournisseur de services. Les services peuvent varier selon le fournisseur que vous utilisez, mais ils appartiennent généralement à l'une des catégories suivantes.

- Compression
- Mise en cache
- Chiffrement
- RéPLICATION

Lorsque vous créez le composant de stratégie de stockage, vous définissez les règles pour un type et un niveau de service spécifiques.

L'exemple suivant montre que les machines virtuelles VM1 et VM2 ont des conditions requises de placement identiques, mais doivent avoir des niveaux différents de services de réPLICATION. Vous pouvez créer les composants d'une stratégie de stockage avec des paramètres de réPLICATION différents et ajouter ces composants aux stratégies de stockage associées.

Tableau 12-2. Composants de stratégie de stockage

Machine virtuelle	Règles de placement	Composant de stratégie de stockage
VM1 nécessite une réplication toutes les 2 heures	Banque de données Virtual Volumes	Réplication toutes les 2 heures
VM2 nécessite une réplication toutes les 4 heures	Banque de données Virtual Volumes	Réplication toutes les 4 heures

Le fournisseur du service peut être un système de stockage, un filtre d'E/S ou une autre entité. Si le composant fait référence à un filtre d'E/S, le composant est ajouté aux règles basées sur l'hôte de la stratégie de stockage. Les composants faisant référence à des entités autres que les filtres d'E/S (par exemple, un système de stockage) sont ajoutés aux groupes de règles spécifiques aux banques de données.

Lorsque vous utilisez les composants, suivez ces directives :

- Chaque composant ne peut inclure qu'un groupe de règles. Toutes les caractéristiques de ce groupe de règles appartiennent à un fournisseur unique des services de données.
- Si un composant est référencé dans la stratégie de stockage de machine virtuelle, vous ne pouvez pas le supprimer. Avant de supprimer le composant, vous devez le retirer de la stratégie de stockage ou supprimer la stratégie de stockage.
- Lorsque vous ajoutez des composants à la stratégie, vous ne pouvez utiliser qu'un seul composant de la même catégorie (par exemple, la mise en cache) par groupe de règles.

Créer des composants de stratégie de stockage

Un composant de stratégie de stockage décrit un service de données spécifique, tel que la réplication, qui doit être fourni pour la machine virtuelle. Vous pouvez définir le composant d'avance et l'associer à plusieurs stratégies de stockage de machine virtuelle. Les composants sont réutilisables et interchangeables.

Procédure

- 1 Dans vSphere Client, ouvrez la boîte de dialogue **Nouveau composant de stratégie de stockage**.
 - a Cliquez sur **Menu > Stratégies et profils**.
 - b Sous **Stratégies et profils**, cliquez sur **Composants de stratégie de stockage**.
- 2 Cliquez sur **Créer un composant de stratégie de stockage**.
- 3 Sélectionnez l'instance de vCenter Server.
- 4 Entrez un nom (par exemple, Réplication de 4 heures) et une description pour le composant de stratégie.

Assurez-vous que le nom n'est pas en conflit avec les noms d'autres composants ou de stratégies de stockage.
- 5 Sélectionnez la catégorie du service (par exemple, **Réplication**).

- 6 Sélectionnez le fournisseur de service.
- 7 Définissez des règles pour la catégorie sélectionnée.

Par exemple, si vous configurez une réPLICATION toutes les 4 heures, définissez la valeur Objectif de point de récupération (RPO) sur 4.

Pour un chiffrement basé sur des filtres d'E/S, définissez le paramètre **Autoriser les filtres d'E/S avant le chiffrement**. Le chiffrement fourni par le stockage ne nécessite pas ce paramètre.

Option	Description
Faux (par défaut)	N'autorise pas l'utilisation d'autres filtres d'E/S avant le filtre de chiffrement.
Vrai	Autorise l'utilisation d'autres filtres d'E/S avant le filtre de chiffrement. Les autres filtres, comme la réPLICATION, peuvent analyser les données de texte clair avant qu'elles soient chiffrées.

- 8 Cliquez sur **OK**.

Résultats

Le nouveau composant figure dans la liste de composants de stratégie de stockage.

Étape suivante

Vous pouvez ajouter le composant à la stratégie de stockage de machine virtuelle. Si le service de données auquel le composant fait référence est fourni par les filtres d'E/S, vous ajoutez le composant aux règles de la stratégie de stockage basé sur hôte. Les composants faisant référence à des entités autres que les filtres d'E/S (par exemple, un système de stockage) sont ajoutés aux groupes de règles spécifiques aux banques de données.

Modifier ou cloner les composants d'une stratégie de stockage

Vous pouvez modifier les composants d'une stratégie de stockage existante. Vous pouvez également créer une copie du composant existant en le clonant.

Procédure

- 1 Dans vSphere Client, accédez au composant de stratégie de stockage à modifier ou cloner.
 - a Cliquez sur **Menu > Stratégies et profils**.
 - b Sous **Stratégies et profils**, cliquez sur **Composants de stratégie de stockage**.

- 2** Sélectionnez le composant et cliquez sur l'une des icônes suivantes.

Option	Description
Modifier les paramètres	Lors de la modification, vous ne pouvez modifier ni la catégorie du service de données ni le fournisseur. Par exemple, si le composant d'origine fait référence à la réPLICATION fournie par des filtres d'E/S, ces paramètres doivent rester inchangés.
Cloner	Lors d'un clonage, vous pouvez personnaliser tous les paramètres du composant d'origine.

- 3** Modifiez les valeurs appropriées, puis cliquez sur **OK**.
- 4** Si une stratégie de stockage de machine virtuelle qui est attribuée à une machine virtuelle fait référence au composant de la stratégie que vous modifiez, réappliquez la stratégie de stockage à la machine virtuelle.

Élément de menu	Description
Plus tard manuellement	Si vous choisissez cette option, l'état de conformité de l'ensemble des disques virtuels et des objets de base des machines virtuelles associés à la stratégie de stockage passe à Périmé. Pour mettre à jour la configuration et l'état de conformité, appliquez de nouveau manuellement la stratégie de stockage à toutes les entités associées. Reportez-vous à la section Réappliquer une stratégie de stockage de machine virtuelle .
Maintenant	Pour mettre à jour la machine virtuelle et l'état de conformité immédiatement après avoir modifié la stratégie de stockage.

Stratégies de stockage et machines virtuelles

Après la définition d'une stratégie de stockage VM, vous pouvez l'appliquer à une machine virtuelle. Vous appliquez la stratégie de stockage lors du provisionnement de la machine virtuelle ou de la configuration de ses disques virtuels. Selon son type et sa configuration, la stratégie peut avoir diverses fins. La stratégie peut sélectionner la banque de données la plus appropriée pour la machine virtuelle et appliquer le niveau de service requis. Sinon, elle peut activer des services de données spécifiques pour la machine virtuelle et ses disques.

Si vous ne spécifiez pas la stratégie de stockage, le système utilise une stratégie de stockage par défaut associée à la banque de données. Si vos besoins en stockage pour les applications sur la machine virtuelle changent, vous pouvez modifier la stratégie de stockage qui était initialement appliquée à la machine virtuelle.

Attribuer des stratégies de stockage à des machines virtuelles

Vous pouvez attribuer une stratégie de stockage VM lors du déploiement initial d'une machine virtuelle ou alors que vous effectuez d'autres opérations de machine virtuelle telles qu'un clonage ou une migration.

Cette rubrique explique comment attribuer une stratégie de stockage VM lorsque vous créez une machine virtuelle. Pour plus d'informations sur les autres méthodes de déploiement, parmi lesquelles le clonage, le déploiement à partir d'un modèle, etc., reportez-vous à la documentation *Administration d'une machine virtuelle vSphere*.

Vous pouvez appliquer la même stratégie de stockage au fichier de configuration de la machine virtuelle et à tous ses disques virtuels. Si les besoins en stockage de vos disques virtuels et du fichier de configuration sont différents, vous pouvez associer différentes stratégies de stockage au fichier de configuration de machine virtuelle et aux disques virtuels sélectionnés.

Procédure

- 1 Démarrez le processus de provisionnement de la machine virtuelle et suivez la procédure appropriée.
- 2 Attribuez la même stratégie de stockage à tous les disques et les fichiers de machine virtuelle.

- a Sur la page **Sélectionner un stockage**, sélectionnez une stratégie de stockage dans le menu déroulant **Stratégie de stockage VM**.

Selon sa configuration, la stratégie de stockage sépare toutes les banques de données entre compatibles et incompatibles. Si la stratégie fait référence à des services de données proposés par une entité de stockage spécifique (par exemple, Virtual Volumes), la liste des ensembles compatibles inclut les banques de données représentant uniquement ce type de stockage.

- b Sélectionnez une banque de données appropriée dans la liste des banques de données compatibles.

Cette banque de données devient la ressource de stockage de destination pour le fichier de configuration de la machine virtuelle et pour tous les disques virtuels.

- c Si vous utilisez le service de réPLICATION avec Virtual Volumes, indiquez le groupe de réPLICATION.

Les groupes de réPLICATION indiquent quelles machines virtuelles et quels disques virtuels doivent être répliqués ensemble vers un site cible.

Option	Description
Groupe de réPLICATION préconfiguré	Groupes de réPLICATION qui sont configurés à l'avance du côté stockage. vCenter Server et ESXi découvrent les groupes de réPLICATION mais ne gèrent pas leur cycle de vie.
Groupe de réPLICATION automatique	Virtual Volumes crée un groupe de réPLICATION et attribue tous les objets de machine virtuelle à ce groupe.

3 Modifiez la stratégie de stockage VM du disque virtuel.

Utilisez cette option si les besoins en matière de placement de stockage sont différents pour les disques virtuels. Vous pouvez également utiliser cette option pour activer des services de filtre d'E/S (par exemple, la mise en mémoire cache et la réplication) pour vos disques virtuels.

- a Sur la page **Personnaliser le matériel**, développez le volet **Nouveau disque dur**.
- b Dans le menu déroulant **Stratégie de stockage VM**, sélectionnez la stratégie de stockage à attribuer au disque virtuel.
- c (Facultatif) Modifiez l'emplacement de stockage du disque virtuel.

Utilisez cette option pour stocker le disque virtuel dans une banque de données autre que celle dans laquelle réside le fichier de configuration de machine virtuelle.

4 Terminez le processus de provisionnement de la machine virtuelle.

Résultats

Une fois la machine virtuelle créée, les stratégies de stockage attribuées et leur état de conformité s'affichent dans l'onglet **Résumé**.

Étape suivante

En cas de changement des besoins en matière de placement de stockage pour le fichier de configuration ou les disques virtuels, vous pourrez modifier ultérieurement les attributions de stratégies virtuelles.

Modifier l'attribution d'une stratégie de stockage pour des fichiers et des disques de machine virtuelle

En cas de changement de vos besoins en stockage pour les applications installées sur la machine virtuelle, vous pouvez modifier la stratégie de stockage appliquée initialement à la machine virtuelle.

Vous pouvez modifier la stratégie de stockage appliquée à une machine virtuelle hors tension ou sous tension.

Lorsque vous modifiez la stratégie de stockage attribuée à une machine virtuelle, vous pouvez appliquer la même stratégie de stockage au fichier de configuration de la machine virtuelle et à tous ses disques virtuels. Vous pouvez également associer différentes stratégies de stockage au fichier de configuration de machine virtuelle et aux disques virtuels. Vous pouvez appliquer différentes stratégies lorsque, par exemple, les exigences de stockage pour vos disques virtuels et le fichier de configuration sont différentes.

Procédure

- 1 Dans vSphere Client, accédez à la machine virtuelle.
 - a Cliquez sur **Menu > Stratégies et profils**.
 - b Sous **Stratégies et profils**, cliquez sur **Stratégies de stockage VM**.
 - c Cliquez sur la stratégie de stockage que vous souhaitez modifier, puis cliquez sur **Conformité de la VM**.
Vous pouvez voir la liste des machines virtuelles qui utilisent cette stratégie de stockage.
 - d Cliquez sur la machine virtuelle dont vous souhaitez modifier la stratégie.
- 2 Cliquez sur l'onglet **Configurer**, puis sur **Stratégies**.
- 3 Cliquez sur **Modifier les stratégies de stockage VM**.
- 4 Spécifiez la stratégie de stockage à appliquer à la machine virtuelle.

Option	Actions
Appliquer la même stratégie de stockage à tous les objets de machine virtuelle	Sélectionnez la stratégie dans le menu déroulant Stratégie de stockage VM .
Appliquer différentes stratégies de stockage à l'objet de base de la machine virtuelle et à ses disques virtuels	<ol style="list-style-type: none"> a Activez l'option Configurer par disque. b Sélectionnez l'objet (par exemple, Accueil VM). c Dans la colonne Stratégie de stockage VM, sélectionnez la stratégie dans le menu déroulant.

- 5 Si vous utilisez une stratégie Virtual Volumes avec la réPLICATION, configuez le groupe de réPLICATION.
Les groupes de réPLICATION indiquent quelles machines virtuelles et quels disques virtuels doivent être réPLIQUÉS ensemble vers un site cible.
Tous les objETS de stockAGE d'une machine virtuelle doivent APPARTENIR au même groupe de réPLICATION. Vous ne pouvez pas ATTRIBUER DIFFÉRENTS groupES de réPLICATION à DIFFÉRENTS objETS de stockAGE d'une machine virtuelle.
- 6 Cliquez sur **OK** pour ENREGISTRER les modifications apportées à la stratégie de stockAGE de machine virtuelle.

Résultats

La stratégie de stockAGE est ATTRIBUÉE à la machine virtuelle et à ses disques.

Vérifier la conformité d'une stratégie de stockAGE de machine virtuelle

Vous pouvez vérIFIER si une machine virtuelle utilise une banQUE de données COMPATIBLE avec les besoins en stockAGE spéCIFIÉS dans la stratégie de stockAGE de machine virtuelle.

Conditions préalables

Vérifiez qu'une stratégie de stockage est associée à la machine virtuelle.

Procédure

- 1 Dans vSphere Client, accédez à la machine virtuelle.
- 2 Cliquez sur l'onglet **Configurer**, puis sur **Stratégies**.
- 3 Cliquez sur **Vérifier la conformité de la stratégie de stockage VM**.
Le système vérifie la conformité.
- 4 Affichez l'état de conformité.

État de conformité	Description
Conforme	La banque de données utilisée par la machine virtuelle ou le disque virtuel dispose de capacités de stockage compatibles avec les conditions requises par la stratégie.
Non conforme	La banque de données utilisée par la machine virtuelle ou le disque virtuel ne dispose pas de capacités de stockage compatibles avec les conditions requises par la stratégie. Vous pouvez migrer les fichiers de la machine virtuelle et ses disques virtuels vers des banques de données conformes.
Périmé	Cet état indique que la règle a été modifiée, mais que les nouvelles exigences n'ont pas été communiquées à la banque de données dans laquelle se trouvent les objets de la machine virtuelle. Pour communiquer les modifications, réappliquez- la règle aux objets dont l'état est Périmé.
Non applicable	Cette stratégie de stockage fait référence aux capacités de banque de données qui ne sont pas prises en charge par la banque de données dans laquelle se trouve la machine virtuelle.

Étape suivante

Lorsque vous ne pouvez pas rendre la banque de données compatible, migrez les fichiers ou les disques virtuels vers une banque de données compatible. Reportez-vous à la section [Rechercher des ressources de stockage compatibles pour une machine virtuelle non conforme](#).

Si l'état est Périmé, appliquez de nouveau la règle aux objets. Reportez-vous à la section [Réappliquer une stratégie de stockage de machine virtuelle](#).

Rechercher des ressources de stockage compatibles pour une machine virtuelle non conforme

Déterminez la banque de données compatible avec la stratégie de stockage associée à votre machine virtuelle.

Il peut arriver que l'état de la stratégie de stockage appliquée à une machine virtuelle soit non conforme. Cet état indique que la machine virtuelle ou ses disques utilisent des banques de données qui sont incompatibles avec la stratégie. Vous pouvez migrer les fichiers de la machine virtuelle et ses disques virtuels vers des banques de données compatibles.

Utilisez cette procédure pour déterminer les banques de données conformes à la stratégie.

Procédure

- 1 Vérifiez que la stratégie de stockage pour la machine virtuelle se trouve à l'état non conforme.
 - a Dans vSphere Client, accédez à la machine virtuelle.
 - b Cliquez sur l'onglet **Résumé**.
Le panneau Conformité de la stratégie de stockage VM, dans le volet Stratégies de stockage VM, affiche l'état Non conforme.
- 2 Accédez à la stratégie de stockage non conforme.
 - a Cliquez sur **Menu > Stratégies et profils**.
 - b Sous **Stratégies et profils**, cliquez sur **Stratégies de stockage VM**.
- 3 Affichez la liste des banques de données compatibles pour la stratégie de stockage non conforme.
 - a Cliquez sur la stratégie de stockage.
 - b Cliquez sur **Compatibilité de stockage**.
La liste des banques de données conformes à la stratégie s'affiche.

Étape suivante

Vous pouvez migrer la machine virtuelle ou ses disques vers l'une des banques de données de la liste.

Réappliquer une stratégie de stockage de machine virtuelle

Après avoir modifié une stratégie de stockage déjà associée à un objet de machine virtuelle, vous devez appliquer de nouveau la règle. En appliquant de nouveau la règle, vous communiquez les nouveaux besoins en stockage à la banque de données dans laquelle se trouve l'objet de machine virtuelle.

Conditions préalables

L'état de conformité d'une machine virtuelle est Périmé. L'état indique que la règle a été modifiée, mais que les nouvelles exigences n'ont pas été communiquées à la banque de données.

Procédure

- 1 Dans vSphere Client, accédez à la machine virtuelle.
- 2 Cliquez sur l'onglet **Configurer**, puis sur **Stratégies**.
- 3 Vérifiez que l'état de conformité est Périmé.
- 4 Cliquez sur **Réappliquer une stratégie de stockage de machine virtuelle**.

5 Vérifiez l'état de conformité.

État de conformité	Description
Conforme	La banque de données utilisée par la machine virtuelle ou le disque virtuel dispose des capacités de stockage requises par la stratégie de stockage.
Non conforme	<p>La banque de données prend en charge les conditions de stockage spécifiées, mais n'est actuellement pas conforme à la stratégie de stockage. Par exemple, l'état peut devenir Non conforme lorsque les ressources physiques de la banque de données sont indisponibles. Vous pouvez mettre la banque de données en conformité en effectuant des modifications dans la configuration physique de votre cluster hôte. Par exemple, en ajoutant des hôtes ou des disques au cluster. Si ces ressources supplémentaires répondent aux conditions de la stratégie de stockage, l'état devient Conforme.</p> <p>Lorsque vous ne pouvez pas rendre la banque de données compatible, migrez les fichiers ou les disques virtuels vers une banque de données compatible. Reportez-vous à la section Rechercher des ressources de stockage compatibles pour une machine virtuelle non conforme.</p>
Non applicable	La stratégie de stockage fait référence aux capacités de banque de données qui ne sont pas prises en charge par la banque de données.

Stratégies de stockage par défaut

Lorsque vous provisionnez une machine virtuelle sur une banque de données, vous devez attribuer à la machine virtuelle une stratégie de stockage de machine virtuelle compatible. Si vous ne configurez pas et n'attribuez pas explicitement la stratégie de stockage à la machine virtuelle, le système utilise une stratégie de stockage par défaut.

Stratégie de stockage par défaut fournie par VMware

La stratégie de stockage générique par défaut qu'ESXi fournit s'applique à toutes les banques de données et n'inclut pas de règles spécifiques à n'importe quel type de stockage.

En outre, ESXi offre les stratégies de stockage par défaut pour les banques de données orientées objet, vSAN ou Virtual Volumes. Ces stratégies garantissent le placement optimal des objets de machine virtuelle dans le stockage orienté objets.

Pour plus d'informations sur la stratégie de stockage par défaut pour Virtual Volumes, reportez-vous à la section [Virtual Volumes et stratégies de stockage de machine virtuelle](#).

Les banques de données VMFS et NFS n'ont pas de stratégies spécifiques par défaut et peuvent utiliser la stratégie générique par défaut ou une stratégie personnalisée que vous avez définie pour elles.

Stratégies de stockage par défaut définies par l'utilisateur

Vous pouvez créer une stratégie de stockage de machine virtuelle compatible avec vSAN ou Virtual Volumes. Vous pouvez ensuite désigner cette stratégie comme stratégie par défaut pour les banques de données vSAN et Virtual Volumes. La stratégie par défaut définie par l'utilisateur remplace la stratégie de stockage par défaut fournie par VMware.

Chaque banque de données vSAN et Virtual Volumes ne peut disposer que d'une stratégie par défaut à la fois. Cependant, vous pouvez créer une stratégie de stockage unique incluant plusieurs ensembles de règles de placement, de telle sorte qu'elle corresponde à plusieurs banques de données vSAN et Virtual Volumes. Vous pouvez désigner cette stratégie comme stratégie par défaut pour toutes les banques de données.

Lorsque la stratégie de stockage VM devient la stratégie par défaut d'une banque de données, vous ne pouvez pas supprimer cette stratégie sans la dissocier de la banque de données.

Modifier la stratégie de stockage par défaut d'une banque de données

Pour les banques de données Virtual Volumes ou vSAN, VMware fournit des stratégies de stockage utilisées par défaut lors du provisionnement des machines virtuelles. Vous pouvez modifier la stratégie de stockage par défaut pour une banque de données Virtual Volumes ou vSAN sélectionnée.

Note Ne désignez pas une stratégie de stockage avec des règles de réPLICATION comme une stratégie de stockage par défaut. Sinon, elle vous empêche de sélectionner des groupes de réPLICATION.

Conditions préalables

Créez une stratégie de stockage compatible avec Virtual Volumes ou vSAN. Vous pouvez créer une stratégie qui correspond aux deux types de stockage.

Procédure

- 1 Dans vSphere Client, accédez à la banque de données.
- 2 Cliquez sur l'onglet **Configurer**, puis sur **Général**.
- 3 Dans le volet Stratégie de stockage par défaut, cliquez sur **Modifier**.
- 4 Dans la liste des stratégies de stockage disponibles, sélectionnez la stratégie que vous souhaitez définir par défaut et cliquez sur **OK**.

Résultats

La stratégie de stockage sélectionnée devient la stratégie par défaut de la banque de données. Le système attribue cette stratégie à tous les objets de machine virtuelle que vous provisionnez sur la banque de données lorsqu'aucune autre stratégie n'est sélectionnée.

Utilisation de fournisseurs de stockage

13

Un fournisseur de stockage est un composant logiciel fourni par VMware ou développé par un tiers à l'aide de VASA (vSphere APIs for Storage Awareness). Le fournisseur de stockage est également appelé fournisseur VASA. Les fournisseurs de stockage s'intègrent à diverses entités de stockage comprenant des stockages physiques externes et des abstractions de stockage telles que vSAN et Virtual Volumes. Les fournisseurs de stockage peuvent également prendre en charge des solutions logicielles (par exemple, des filtres d'E/S).

Concepts du fournisseur de stockage

En général, vCenter Server et ESXi utilisent les fournisseurs de stockage pour obtenir des informations sur la configuration de stockage, sur son état, ainsi que sur les services de données de stockage proposés dans votre environnement. Ces informations s'affichent dans vSphere Client. Les informations vous aident à prendre des décisions appropriées sur le placement de la machine virtuelle, à définir les conditions requises du stockage et à surveiller votre environnement de stockage.

Fournisseurs de stockage de persistance

Les fournisseurs de stockage qui gèrent les baies et les abstractions de stockage sont appelés fournisseurs de stockage de persistance. Les fournisseurs qui prennent en charge Virtual Volumes ou vSAN appartiennent à cette catégorie. Outre le stockage, les fournisseurs de persistance peuvent fournir d'autres services de données tels que la réPLICATION.

Fournisseurs de services de données

Les fournisseurs de stockage de filtres d'E/S ou les fournisseurs de services de données constituent une autre catégorie de fournisseurs. Ces fournisseurs offrent des services de données incluant la mise en cache basée sur l'hôte, la compression et le chiffrement.

Les fournisseurs de stockage de persistance et les fournisseurs de services de données peuvent appartenir à l'une de ces catégories.

Fournisseurs de stockage intégrés

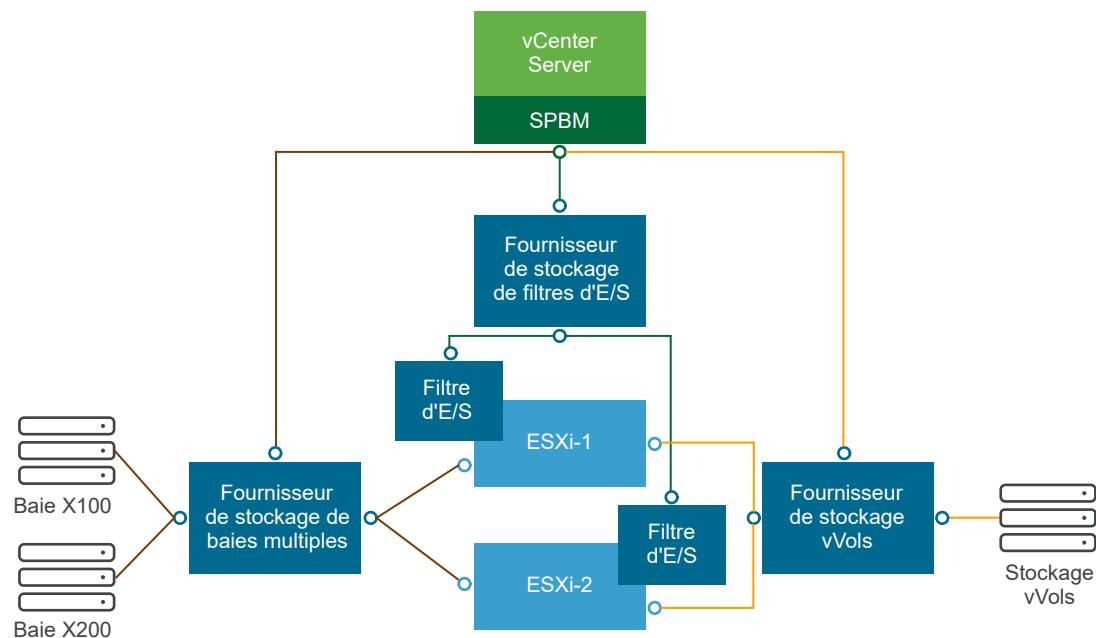
Les fournisseurs de stockage intégrés sont proposés par VMware. En général, ils ne nécessitent pas d'enregistrement. Par exemple, les fournisseurs de stockage qui prennent en charge vSAN ou les filtres d'E/S sont intégrés et sont automatiquement enregistrés.

Fournisseurs de stockage tiers

Lorsqu'un tiers propose un fournisseur de stockage, vous devez généralement enregistrer celui-ci. Le fournisseur Virtual Volumes est un exemple d'un tel fournisseur. Vous utilisez vSphere Client pour enregistrer et gérer chaque composant de fournisseur de stockage.

Pour plus d'informations, [Gérer les fournisseurs de stockage pour Virtual Volumes](#).

Le graphique suivant montre comment différents types de fournisseurs de stockage facilitent les communications entre vCenter Server et ESXi, et d'autres composants de votre environnement de stockage. Par exemple, les composants peuvent inclure des baies de stockage, le stockage Virtual Volumes et les filtres d'E/S.



Fournisseurs de stockage et représentation des données

Les informations fournies par le fournisseur de stockage peuvent être classées dans les catégories suivantes :

- Services de données de stockage et capacités. Ce type d'information est essentiel pour des fonctionnalités telles que vSAN, Virtual Volumes et les filtres d'E/S. Le fournisseur de stockage qui représente ces fonctionnalités s'intègre au mécanisme SPBM (Storage Policy Based Management). Le fournisseur de stockage collecte des informations sur les services de données qui sont proposés par des entités de stockage sous-jacentes ou les filtres d'E/S disponibles.

Vous faites référence à ces services de données lorsque vous définissez des besoins en stockage pour des machines virtuelles et des disques virtuels dans une stratégie de stockage. Selon votre environnement, le mécanisme SPBM garantit un placement de stockage approprié pour une machine virtuelle ou active des services de données spécifiques pour des disques virtuels. Pour des détails, veuillez vous reporter au [Création et gestion de stratégies de stockage de machine virtuelle](#).

- État du stockage. Cette catégorie inclut la génération de rapport sur l'état des diverses entités de stockage. Elle inclut également les alarmes et les événements de notification des modifications de configuration.

Ce type d'information peut vous permettre de dépanner des problèmes de connectivité et de performance de stockage. Par ailleurs, il peut vous aider à mettre en corrélation des alarmes et des événements générés par une baie aux changements correspondants de performance et de charge sur la baie.

- Informations Storage DRS pour la planification des ressources distribuées sur les périphériques de traitement par blocs ou les systèmes de fichiers. Ces informations aident à garantir que les décisions prises par Storage DRS sont compatibles avec les décisions de gestion de ressources internes pour les systèmes de stockage.

Exigences et considérations relatives au fournisseur de stockage

Lorsque vous utilisez un fournisseur de stockage tiers, les fournisseurs sont responsables de la fourniture de fournisseurs de stockage. Le programme VMware VASA définit une architecture qui intègre des fournisseurs de stockage tiers dans l'environnement vSphere afin que les hôtes vCenter Server et ESXi puissent communiquer avec les fournisseurs de stockage.

Pour utiliser des fournisseurs de stockage, respectez les exigences suivantes :

- Assurez-vous que tout fournisseur de stockage que vous utilisez est certifié par VMware et correctement déployé. Pour obtenir des informations sur le déploiement des fournisseurs de stockage, contactez votre distributeur de stockage.
- Assurez-vous que le fournisseur de stockage est compatible avec les versions de vCenter Server et de ESXi. Reportez-vous au *Guide de compatibilité VMware*.
- N'installez pas le fournisseur VASA sur le même système que vCenter Server.
- Si votre environnement contient des versions plus anciennes des fournisseurs de stockage, la fonctionnalité existante continue à fonctionner. Cependant, pour utiliser de nouvelles fonctionnalités, mettez à niveau votre fournisseur de stockage vers une nouvelle version.

Ce chapitre contient les rubriques suivantes :

- [Gestion des fournisseurs de stockage](#)

Gestion des fournisseurs de stockage

Vous devrez peut-être enregistrer certains types de fournisseurs de stockage pour établir leur connexion à vCenter Server. Vous pouvez ensuite vérifier et gérer les fournisseurs de stockage.

Enregistrement des fournisseurs de stockage

Utilisez vSphere Client pour enregistrer un fournisseur de stockage distinct pour chaque hôte d'un cluster.

Après l'inscription, vCenter Server peut détecter et utiliser la fonctionnalité de la dernière version de VASA.

Note Les fournisseurs de stockage intégrés ne nécessitent pas l'enregistrement. Par exemple, les fournisseurs de stockage qui prennent en charge vSAN ou les filtres d'E/S sont intégrés. Ils sont enregistrés et apparaissent automatiquement dans la liste des fournisseurs de stockage. Pour plus d'informations, consultez la documentation *Administration de VMware vSAN* et *Chapitre 15 Filtrage des E/S de machines virtuelles*.

Conditions préalables

Vérifiez que le composant de fournisseur de stockage est installé sur le côté stockage et obtenez ses informations d'identification auprès de votre administrateur de stockage.

Procédure

- 1 Accédez à vCenter Server.
- 2 Cliquez sur l'onglet **Configurer**, puis cliquez sur **Fournisseurs de stockage**.
- 3 Cliquez sur l'icône **Ajouter**.
- 4 Entrez les informations de connexion du fournisseur de stockage, notamment son nom, son URL et ses données d'identification.
- 5 Cliquez sur **OK**.

Résultats

vCenter Server enregistre le fournisseur de stockage et établit une connexion sécurisée avec lui.

Étape suivante

Pour résoudre les problèmes d'enregistrement de votre fournisseur de stockage, reportez-vous à l'article de la Base de connaissances VMware <https://kb.vmware.com/s/article/49798>.

Afficher des informations sur le fournisseur de stockage

Dès que vous enregistrez un composant d'un fournisseur de stockage dans vCenter Server, ce fournisseur figure dans la liste des fournisseurs de stockage. Certains fournisseurs de stockage sont automatiquement enregistrés et figurent automatiquement sur la liste après la configuration de l'entité qu'ils représentent (par exemple, vSAN ou filtres d'E/S).

Utilisez vSphere Client pour afficher les informations générales de fournisseur de stockage et les informations détaillées de chaque composant de stockage.

Procédure

- 1 Accédez à vCenter Server.
- 2 Cliquez sur l'onglet **Configurer**, puis cliquez sur **Fournisseurs de stockage**.
- 3 Dans la liste Fournisseurs de stockage, affichez les fournisseurs de stockage enregistrés dans vCenter Server.
La liste affiche des informations générales, notamment le nom du fournisseur de stockage, son URL et son état, ainsi que la version des API VASA.
- 4 Pour afficher des détails supplémentaires. Cliquez sur l'icône en regard du nom du fournisseur.

Note Un même fournisseur de stockage peut prendre en charge les systèmes de stockage de plusieurs distributeurs différents.

Vous pouvez afficher des informations sur les certificats du fournisseur et les entités de stockage qu'il représente.

Gérer les fournisseurs de stockage

Utilisez vSphere Client pour effectuer plusieurs opérations de gestion sur les fournisseurs de stockage enregistrés.

Procédure

- 1 Accédez à vCenter Server.
- 2 Cliquez sur l'onglet **Configurer**, puis cliquez sur **Fournisseurs de stockage**.
- 3 Cliquez sur l'icône pour effectuer l'une des actions globales suivantes pour tous les fournisseurs.

Icône	Description
Synchroniser les fournisseurs de stockage	Synchronisez tous les fournisseurs de stockage avec l'état actuel de l'environnement.
Nouvelle authentification des clients VASA de l'hôte	Authentifiez de nouveau tous les hôtes avec des banques de données Virtual Volumes auprès de leurs fournisseurs de stockage respectifs. Cette icône n'est disponible que pour les fournisseurs de données Virtual Volumes.

Note Cette opération prend du temps.

- 4 Pour gérer un fournisseur de stockage spécifique, accédez au fournisseur et cliquez sur l'icône **Action de ligne** (trois points) en regard du nom du fournisseur.

	Storage Provider	Status	URL	Last Rescan Time	VASA API Version	Certificate Expiry
⋮	vasa nvme	Offline	https://192.168.1.100:9080/vasa/	01/03/2023, 2:44:49 AM	5.0	350 days
⋮	Rescan	Online	https://192.168.1.100:9080/vasa/	01/03/2023, 2:56:03 AM	1.5	1810 days
⋮	Remove	Online	https://192.168.1.100:9080/vasa/	01/03/2023, 2:56:03 AM	1.5	1810 days
⋮	Refresh certificate	Online	https://192.168.1.100:9080/vasa/	01/13/2023, 1:11:14 AM	4.0 ⚠️	⚠️ 74 days
⋮	Upgrade Storage Provider	Online	https://192.168.1.100:9080/vasa/	01/03/2023, 2:56:57 AM	3.0	--
⋮	Re-authenticate vCenter Server	Online	https://192.168.1.100:9080/vasa/	01/03/2023, 2:56:57 AM	3.0	--

- 5 Sélectionnez l'un des éléments suivants dans le menu **Actions de ligne**.

La disponibilité des options de menu dépend du type de fournisseur de stockage utilisé.

Par exemple, vous ne pouvez pas annuler manuellement l'enregistrement ou mettre à niveau certains fournisseurs de stockage fournis par VMware, tels que les fournisseurs de stockage vSAN ou de filtres d'E/S.

Option	Description
Réanalyser	Mettez à jour les données de stockage pour le fournisseur. vCenter Server met périodiquement à jour les données de stockage dans sa banque de données. Les mises à jour sont partielles et reflètent uniquement les modifications que les fournisseurs de stockage communiquent à vCenter Server à ce moment. Lorsque cela est nécessaire, vous pouvez exécuter une synchronisation de base de données complète pour le fournisseur de stockage sélectionné.
Supprimer	Annulez l'enregistrement des fournisseurs de stockage que vous n'utilisez pas. Une fois cette opération effectuée, vCenter Server ferme la connexion et supprime le fournisseur de stockage de sa configuration.
Actualiser le certificat	vCenter Server vous avertit lorsqu'un certificat attribué à un fournisseur de stockage est sur le point d'expirer. Vous pouvez actualiser le certificat pour continuer à utiliser le fournisseur. Si vous ne parvenez pas à actualiser le certificat avant qu'il n'expire, vCenter Server cesse d'utiliser le fournisseur.

Option	Description
Mettre à niveau le fournisseur de stockage	<p>Lorsque vCenter Server vous informe d'une nouvelle version de VASA disponible, acceptez cette version pour l'activer dans votre environnement vSphere. vCenter Server active les nouvelles capacités exposées par le fournisseur de stockage et communique ces informations à tous les hôtes de l'inventaire.</p> <p>Lorsque vous effectuez cette action, vous devez entrer les informations d'identification du fournisseur de stockage.</p> <p>Vous ne pouvez pas sélectionner une version VASA spécifique pour une mise à niveau si plusieurs versions sont disponibles. vCenter Server effectue uniquement les mises à niveau vers la dernière version.</p> <p>Note Vous pouvez choisir d'effectuer les mises à niveau à votre propre rythme. Pour plus d'informations, consultez Virtual VolumesSécurité.</p>
Nouvelle authentification de vCenter Server	<p>Nouvelle authentification de vCenter Server auprès du fournisseur de stockage.</p> <p>Cette action autorise à nouveau vCenter Server auprès du fournisseur de stockage s'il a perdu l'authentification et a besoin d'informations d'identification.</p> <p>Vous devez entrer les informations d'identification du fournisseur de stockage.</p>

Utilisation de VMware vSphere Virtual Volumes

14

VMware vSphere Virtual Volumes, également connu sous le nom vVols, virtualise les périphériques de stockage en faisant abstraction des ressources matérielles physiques en pools de capacité logiques. La fonctionnalité Virtual Volumes modifie le paradigme de gestion du stockage de la gestion de l'espace au sein de banques de données à la gestion d'objets de stockage abstraits par des baies de stockage. Avec Virtual Volumes, une machine virtuelle individuelle, et non la banque de données, devient une unité de gestion de stockage, tandis que le matériel de stockage prend le contrôle complet du contenu, de la disposition et de la gestion du disque virtuel.

La fonctionnalité Virtual Volumes mappe les disques virtuels et leurs dérivés, clones, snapshots et répliques, directement à des objets, nommés volumes virtuels, sur un système de stockage. Ce mappage permet à vSphere de décharger les opérations de stockage intensives telles que les snapshots, le clonage et la réPLICATION sur le système de stockage.

Ce chapitre contient les rubriques suivantes :

- Concepts et architecture de Virtual Volumes
- Virtual VolumesSécurité
- Snapshots de volume virtuel
- Avant d'activer Virtual Volumes
- Configurer Virtual Volumes
- Provisionner des machines virtuelles sur des banques de données Virtual Volumes
- Gérer les fournisseurs de stockage pour Virtual Volumes
- NVMe et Virtual Volumes
- Virtual Volumes et réPLICATION
- Meilleures pratiques d'utilisation de Virtual Volumes
- Dépannage de Virtual Volumes

Concepts et architecture de Virtual Volumes

Découvrez les différents composants de la fonctionnalité Virtual Volumes.



(Virtual Volumes, première partie : Concepts)

Objets de volume virtuel

Les volumes virtuels sont des encapsulations de fichiers de machines virtuelles, de disque virtuel et de leurs dérivés.

Les volumes virtuels sont nativement stockés à l'intérieur d'un système de stockage connecté à vos hôtes ESXi par Ethernet ou SAN. Ils sont exportés en tant qu'objets par un système de stockage et sont gérés entièrement par matériel côté stockage. Un volume virtuel est généralement identifié par un GUID unique. Les volumes virtuels ne sont pas prévisionnés, mais plutôt créés automatiquement lorsque vous effectuez des opérations de gestion de machines virtuelles. Ces opérations incluent la création d'une machine virtuelle, le clonage et la prise de snapshots. ESXi et vCenter Server associent un ou plusieurs volumes virtuels à une machine virtuelle.

Types de Virtual Volumes

Le système crée les types suivants de volumes virtuels pour les principaux éléments constituant la machine virtuelle :

Data-vVol

Volume virtuel de données correspondant directement à chaque fichier de disque virtuel .vmdk. À l'instar des fichiers de disque virtuel sur les banques de données traditionnelles, les volumes virtuels sont présentés à des machines virtuelles en tant que disques SCSI ou NVMe. Les data-vVol peuvent être provisionnés de manière statique ou dynamique.

Config-vVol

Un volume virtuel de configuration, ou répertoire de base, constitue un petit répertoire contenant les fichiers de métadonnées d'une machine virtuelle. Les fichiers incluent un fichier .vmx, des fichiers descripteurs de disques virtuels, des fichiers journaux, etc. Le volume virtuel de configuration est formaté avec un système de fichiers. Lorsque ESXi utilise le protocole NVMe ou SCSI pour se connecter au stockage, les volumes virtuels de configuration sont formatés avec VMFS. Avec le protocole NFS, les volumes virtuels de configuration sont présentés comme un répertoire NFS. En général, il est provisionné de manière dynamique.

Note À partir de vSphere 7.0 Update 2, les partenaires peuvent augmenter la valeur de config-vVol à plus de 4 Go. Collaborez avec votre partenaire Virtual Volumes sur la mise en œuvre de cette option si elle est prise en charge par votre partenaire et applicable à votre environnement.

Swap-vVol

Créé lors de la première mise sous tension d'une machine virtuelle. Il s'agit d'un volume virtuel qui stocke des copies de pages de mémoire d'une machine virtuelle qui ne peuvent pas être conservées dans la mémoire. Sa taille dépend de celle de la mémoire de la machine virtuelle. Par défaut, il est provisionné de manière statique.

Snapshot-vVol

Volume de mémoire virtuelle permettant de stocker le contenu de la mémoire d'une machine virtuelle pour un snapshot. Provisionnement statique.

Autre

Volume virtuel pour des fonctionnalités spécifiques. Par exemple, un volume virtuel de synthèse est créé pour la fonction CBRC (Content-Based Read Cache).

En général, une machine virtuelle crée au moins trois volumes virtuels, data-vVol, config-vVol et swap-vVol. Le nombre maximal dépend du nombre de disques virtuels et de snapshots situés sur la machine virtuelle.

En utilisant différents volumes virtuels pour différents composants de machine virtuelle, vous pouvez appliquer et manipuler des stratégies de stockage au niveau de granularité le plus détaillé. Par exemple, un volume virtuel qui contient un disque virtuel peut disposer d'un ensemble de services plus riche que le volume virtuel du disque de démarrage d'une machine virtuelle.

Provisionnement du disque

La fonctionnalité Virtual Volumes prend en charge un concept de disques virtuels à provisionnement dynamique ou statique. Toutefois, du point de vue des E/S, la mise en œuvre et la gestion du provisionnement dynamique ou statique par les baies sont transparentes pour l'hôte ESXi. ESXi décharge vers les baies de stockage toutes les fonctions liées au provisionnement dynamique.

Vous sélectionnez le type dynamique ou statique pour votre disque virtuel au moment de la création de la machine virtuelle. Si votre disque est provisionné de manière dynamique et se trouve sur une banque de données Virtual Volumes, vous ne pouvez pas modifier son type ultérieurement en gonflant le disque.

Disques partagés

Vous pouvez placer un disque partagé sur un stockage Virtual Volumes qui prend en charge les réservations SCSI persistantes pour Virtual Volumes. Vous pouvez utiliser ce disque comme disque quorum et éliminer les RDM dans les clusters MSCS. Pour plus d'informations, consultez la documentation *Gestion des ressources vSphere*.

Fournisseurs de stockage Virtual Volumes

Un fournisseur de stockage Virtual Volumes, également appelé fournisseur VASA, est un composant logiciel qui agit en tant que service de reconnaissance du stockage pour vSphere.

Le fournisseur règle les communications hors bande entre vCenter Server et les hôtes ESXi d'un côté et un système de stockage de l'autre.

Mis en œuvre à l'aide de VASA (VMware APIs for Storage Awareness), le fournisseur de stockage permet de gérer tous les aspects du stockage Virtual Volumes.

Le fournisseur de stockage fournit des informations depuis le conteneur de stockage sous-jacent. Les capacités du conteneur de stockage s'affichent dans vCenter Server et vSphere Client. À son tour, le fournisseur de stockage communique les besoins en stockage des machines virtuelles (que vous pouvez définir sous la forme d'une stratégie de stockage) à la couche de stockage. Ce processus d'intégration assure que tout volume virtuel créé dans la couche de stockage répond aux conditions requises de la stratégie.

En général, les distributeurs doivent proposer des fournisseurs de stockage capables de s'intégrer à vSphere et de prendre en charge Virtual Volumes. Chaque fournisseur de stockage doit être certifié par VMware et déployé adéquatement. Pour plus d'informations sur le déploiement et la mise à niveau du fournisseur de stockage Virtual Volumes vers une version compatible avec la version d'ESXi actuelle, contactez votre fournisseur de stockage.

Après avoir déployé le fournisseur de stockage, vous devez l'enregistrer dans vCenter Server.

Conteneurs de stockage Virtual Volumes

Contrairement au stockage traditionnel basé sur des blocs ou des fichiers, la fonctionnalité Virtual Volumes ne requiert pas de stockage préconfiguré du côté stockage. Virtual Volumes utilise plutôt un conteneur de stockage. Il s'agit d'un pool de capacité de stockage brut ou d'une agrégation de capacités de stockage qu'un système de stockage peut fournir aux volumes virtuels.

Un conteneur de stockage fait partie de la structure de stockage logique. Il s'agit d'une unité logique du matériel sous-jacent. Le conteneur de stockage regroupe logiquement les volumes virtuels en fonction des besoins administratifs et de gestion. Par exemple, le conteneur de stockage peut contenir tous les volumes virtuels créés pour un locataire dans un déploiement à locataires multiples, ou pour un service dans un déploiement d'entreprise. Chaque conteneur de stockage fait office de magasin de volumes virtuels et les volumes virtuels sont alloués à partir de la capacité du conteneur de stockage.

En général, un administrateur de stockage côté stockage définit les conteneurs de stockage. Le nombre de conteneurs de stockage, leur capacité et leur taille dépendent d'une mise en œuvre spécifique au fournisseur. Au moins un conteneur est requis par système de stockage.

Note Un même conteneur de stockage ne peut pas s'étendre à plusieurs baies physiques.

Une fois que vous avez enregistré un fournisseur de stockage associé au système de stockage, vCenter Server détecte tous les conteneurs de stockage configurés ainsi que leurs profils de capacité de stockage, points de terminaison de protocole et autres attributs. Un même conteneur de stockage peut exporter plusieurs profils de capacité. C'est pourquoi des machines virtuelles aux besoins et aux paramètres de stratégie de stockage différents peuvent faire partie d'un même conteneur de stockage.

Initialement, les conteneurs de stockage détectés ne sont pas tous connectés à un hôte spécifique et vous ne pouvez pas les voir dans vSphere Client. Pour monter un conteneur de stockage, vous devez le mapper à une banque de données Virtual Volumes.

Points de terminaison de protocole

Les systèmes de stockage gèrent tous les aspects des volumes virtuels, mais les hôtes ESXi n'ont pas directement accès aux volumes virtuels côté stockage. Au lieu de cela, les hôtes ESXi utilisent un proxy d'E/S logiques appelé « point de terminaison de protocole » pour communiquer avec les volumes virtuels et avec les fichiers de disque virtuel encapsulés par les volumes virtuels. ESXi s'appuie sur les points de terminaison de protocole pour établir un chemin de données à la demande entre les machines virtuelles et leurs volumes virtuels respectifs.

Chaque volume virtuel est lié à un point de terminaison de protocole spécifique. Lorsqu'une machine virtuelle résidant sur l'hôte réalise une opération d'E/S, le point de terminaison de protocole dirige les E/S vers le volume virtuel approprié. En général, un système de stockage nécessite seulement quelques points de terminaison de protocole. Un point de terminaison de protocole peut connecter à lui seul des centaines ou des milliers de volumes virtuels.

Côté stockage, un administrateur de stockage configure les points de terminaison de protocole, un ou plusieurs par conteneur de stockage. Les points de terminaison de protocole font partie de l'infrastructure de stockage physique. Le système de stockage exporte les points de terminaison de protocole avec les conteneurs de stockage associés à l'aide du fournisseur de stockage. Une fois que vous avez mappé le conteneur de stockage à une banque de données Virtual Volumes, l'hôte ESXi détecte les points de terminaison de protocole qui deviennent visibles dans vSphere Client. Les points de terminaison de protocole peuvent également être détectés lors d'une réanalyse du stockage. Plusieurs hôtes peuvent détecter et monter les points de terminaison de protocole.

Dans vSphere Client, la liste des points de terminaison de protocole disponibles est similaire à la liste des périphériques de stockage d'hôte. Différents transports de stockage peuvent être utilisés pour exposer les points de terminaison de protocole à ESXi. En cas d'utilisation du transport SCSI, le point de terminaison de protocole représente un proxy LUN défini par un nom WWN de LUN T10. Avec le protocole NFS, le point de terminaison de protocole est un point de montage tel qu'une adresse IP et un nom de partage. Vous pouvez configurer des chemins multiples sur un point de terminaison de protocole SCSI, mais pas sur un point de terminaison de protocole NFS. Quel que soit le protocole utilisé, une baie de stockage peut fournir plusieurs points de terminaison de protocole pour maximiser la disponibilité.

Les points de terminaison de protocole sont gérés par baie. ESXi et vCenter Server supposent que tous les points de terminaison de protocole signalés pour une baie sont associés à tous les conteneurs de celle-ci. Par exemple, si une baie contient deux conteneurs et trois points de terminaison de protocole, ESXi suppose que les volumes virtuels sur les deux conteneurs peuvent être liés aux trois points de terminaison de protocole.

Pour obtenir des informations spécifiques sur les points de terminaison de protocole et NVMe avec Virtual Volumes, reportez-vous à la section [NVMe et Virtual Volumes](#).

Liaison et annulation de liaison de Virtual Volumes

Au moment de la création, un volume virtuel est une entité passive qui n'est pas immédiatement prête pour les E/S. Pour accéder au volume virtuel, ESXi ou vCenter Server envoie une demande de liaison.

Le système de stockage répond par un ID de point de terminaison de protocole qui devient un point d'accès au volume virtuel. Le point de terminaison de protocole accepte toutes les demandes d'E/S vers le volume virtuel. Cette liaison existe jusqu'à ce que ESXi envoie une demande d'annulation de liaison concernant le volume virtuel.

Lors de demandes de liaisons ultérieures sur le même volume virtuel, le système de stockage peut renvoyer des ID de points de terminaison de protocole différents.

Lorsque vous utilisez le protocole NVMe, la réponse du volume virtuel de liaison fournit le NQN de sous-système NVMe et l'ID de l'espace de noms (nsid) de l'objet de volume virtuel de l'espace de noms. L'hôte ESXi utilise ces informations et les résout pour le groupe ANA au sein du sous-système. Un point de terminaison de protocole virtuel (vPE) correspondant à ce groupe ANA est créé s'il n'existe pas. Il est utilisé pour diriger toutes les demandes d'E/S vers les Virtual Volumes.

Lors de la réception de demandes de liaison simultanées vers un volume virtuel de plusieurs hôtes ESXi, le système de stockage peut renvoyer des liaisons de point de terminaison identiques ou différentes à chaque hôte ESXi à l'origine de la demande. Autrement dit, le système de stockage peut lier différents hôtes simultanés au même volume virtuel à l'aide de points de terminaison différents.

L'opération d'annulation de liaison supprime le point d'accès d'E/S pour le volume virtuel. Le système de stockage peut annuler la liaison entre le volume virtuel et son point de terminaison de protocole immédiatement ou après un délai, ou exécuter d'autres action. Un volume virtuel lié ne peut pas être supprimé tant que sa liaison n'est pas annulée.

Banques de données Virtual Volumes

Une banque de données Virtual Volumes représente un conteneur de stockage dans vCenter Server et vSphere Client.

Après que vCenter Server a détecté les conteneurs de stockage exportés par des systèmes de stockage, vous devez les monter en tant que banques de données Virtual Volumes. Les banques de données Virtual Volumes ne sont pas formatées d'une manière traditionnelle comme, par exemple, les banques de données VMFS. Vous devez les créer malgré tout, car toutes les fonctionnalités vSphere, notamment FT, HA, DRS, etc. nécessitent la construction de banque de données pour fonctionner correctement.

L'assistant de création de banques de données de vSphere Client vous permet de mapper un conteneur de stockage à une banque de données Virtual Volumes. La banque de données Virtual Volumes que vous créez correspond directement au conteneur de stockage spécifique.

Du point de vue d'un administrateur vSphere, la banque de données Virtual Volumes est semblable à toute autre banque de données et sert à contenir des machines virtuelles. Comme les autres banques de données, la banque de données Virtual Volumes peut être parcourue et répertoriée les volumes virtuels par nom de machine virtuelle. Comme les banques de données classiques, les banques de données Virtual Volumes prennent en charge le démontage et le montage. Cependant, les opérations telles que la mise à niveau et le redimensionnement ne s'appliquent pas à une banque de données Virtual Volumes. La capacité de la banque de données Virtual Volumes est configurable par l'administrateur de stockage hors de vSphere.

Les banques de données Virtual Volumes peuvent s'utiliser avec des banques de données VMFS et NFS traditionnelles et vSAN.

Note La taille d'un volume virtuel doit être un multiple de 1 Mo, avec une taille minimale de 1 Mo. Par conséquent, l'ensemble des disques virtuels provisionnés sur une banque de données Virtual Volumes doit constituer un multiple pair de 1 Mo. Si le disque virtuel que vous migrez vers la banque de données Virtual Volumes n'est pas un multiple pair de 1 Mo, étendez le disque manuellement jusqu'au multiple pair le plus proche de 1 Mo.

Virtual Volumes et stratégies de stockage de machine virtuelle

Une machine virtuelle qui s'exécute sur une banque de données Virtual Volumes nécessite une stratégie de stockage de machine virtuelle.

Une stratégie de stockage de machine virtuelle est un ensemble de règles qui contient des conditions requises pour une machine virtuelle en matière de qualité de service et de placement. La stratégie applique le placement approprié de la machine virtuelle dans le stockage Virtual Volumes et garantit que le stockage peut répondre aux spécifications de la machine virtuelle.

Vous utilisez l'interface de stratégies de stockage de machine virtuelle pour créer une stratégie de stockage Virtual Volumes. Lorsque vous l'attribuez à la machine virtuelle, la nouvelle stratégie garantit que le stockage Virtual Volumes répond aux besoins.

Stratégie de stockage Virtual Volumes par défaut

Pour Virtual Volumes, VMware fournit une stratégie de stockage par défaut ne s'accompagnant d'aucune stratégie ou condition requise de stockage, appelée stratégie Sans exigence Virtual Volumes. Cette stratégie s'applique aux objets de machine virtuelle lorsque vous ne spécifiez pas d'autre stratégie pour la machine virtuelle placée sur la banque de données Virtual Volumes. La stratégie Sans exigence permet aux baies de stockage de déterminer le placement optimal des objet VM.

La stratégie sans exigence par défaut fournie par VMware présente les caractéristiques suivantes :

- Impossible de supprimer, modifier ou cloner cette stratégie.
- La stratégie est uniquement compatible avec les banques de données Virtual Volumes.
- Vous pouvez créer une stratégie de stockage VM pour Virtual Volumes et la définir comme stratégie par défaut.

Virtual Volumes et protocoles de stockage

Un système de stockage Virtual Volumes fournit des points de terminaison de protocole détectables sur l'infrastructure du stockage physique. Les hôtes ESXi utilisent les points de terminaison de protocole pour se connecter aux volumes virtuels sur le stockage. L'utilisation de points de terminaison de protocole dépend des protocoles de stockage qui exposent les points de terminaison aux hôtes ESXi.

Virtual Volumes prend en charge les protocoles NFS versions 3 et 4.1, iSCSI, Fibre Channel, FCoE, NVMe over Fibre Channel et NVMe over TCP.

Quel que soit le protocole utilisé, les points de terminaison de protocole fournissent un accès uniforme au stockage SAN et au stockage NAS. Un volume virtuel, comme un fichier sur une banque de données classique, est présenté à une machine virtuelle en tant que disque SCSI ou NVMe.

Note Un conteneur de stockage est dédié à SAN (SCSI ou NVMe) ou NAS et ne peut pas être partagé entre ces types de protocole. Une baie peut contenir un conteneur de stockage avec des points de terminaison de protocole SCSI et un conteneur différent avec des points de terminaison de protocole NFS. Le conteneur ne peut pas utiliser une combinaison de protocoles d'accès au stockage SCSI, NVMe et NFS.

Transports basés sur Virtual Volumes et SCSI

Sur les baies de disque, Virtual Volumes prend en charge les protocoles Fibre Channel, FCoE et iSCSI.

En cas d'utilisation du protocole SCSI, le point de terminaison de protocole représente un proxy LUN défini par un WWN de LUN T10.

Comme tous les LUN basés sur des blocs, les points de terminaison de protocole sont détectés à l'aide de commandes de détection LUN standard. L'hôte ESXi recherche régulièrement de nouveaux périphériques et détecte de manière asynchrone les points de terminaison de protocole basés sur des blocs. Le point de terminaison de protocole peut être accessible au moyen de plusieurs chemins d'accès. Sur ces chemins d'accès, le trafic respecte des stratégies de sélection de chemin d'accès connues, comme toujours pour les LUN.

Sur les baies de disque SCSI, au moment de la création d'une machine virtuelle, ESXi crée un volume virtuel et lui attribue le format VMFS. Ce petit volume virtuel stocke tous les fichiers de métadonnées de machines virtuelles et est appelé le config-vVol. Le config-vVol fonctionne comme un localisateur de stockage de machine virtuelle pour vSphere.

Sur les baies de disque, Virtual Volumes prend en charge les mêmes commandes SCSI que VMFS et utilise ATS comme mécanisme de verrouillage.

Prise en charge de CHAP pour les points de terminaison iSCSI

Virtual Volumes prend en charge le protocole CHAP (Challenge Handshake Access Protocol) avec les cibles iSCSI. Cette prise en charge permet aux hôtes ESXi de partager les informations d'identification de l'initiateur CHAP avec des fournisseurs de stockage Virtual Volumes, également appelés fournisseurs VASA et aux fournisseurs de stockage Virtual Volumes de générer des événements système avertis au vCenter Server de modifications apportées aux informations d'identification de la cible CHAP sur la baie de stockage.

Chaque hôte ESXi peut avoir plusieurs HBA et des propriétés peuvent être configurées sur chaque HBA. L'une de ces propriétés est la méthode d'authentification que le HBA doit utiliser. L'authentification est facultative, mais si elle est implémentée, elle doit être prise en charge à la fois par l'initiateur et la cible. CHAP est une méthode d'authentification qui peut être utilisée dans les deux sens entre l'initiateur et la cible.

Pour plus d'informations sur les différentes méthodes d'authentification CHAP, consultez [Sélection de la méthode d'authentification CHAP](#). Pour configurer CHAP sur votre hôte ESXi, consultez [Configuration des paramètres CHAP pour les adaptateurs de stockage iSCSI ou iSER](#).

Transports Virtual Volumes et NFS

Avec le stockage NAS, un point de terminaison de protocole est un partage NFS que l'hôte ESXi monte à l'aide d'une adresse IP ou d'un nom DNS et d'un nom de partage. Virtual Volumes prend en charge le protocole NFS versions 3 et 4.1 pour accéder au stockage NAS. Les formats IPv4 et IPv6 sont pris en charge.

Quel que soit la version utilisée, une baie de stockage peut fournir plusieurs points de terminaison de protocole pour maximiser la disponibilité.

En outre, NFS version 4.1 introduit des mécanismes de jonction qui activent l'équilibrage de charge et la gestion multivoie.

Virtual Volumes sur les périphériques NAS prend en charge les mêmes RPC (Remote Procedure Calls) NFS que les hôtes ESXi utilisent lors de la connexion aux points de montage NFS.

Sur les périphériques NAS, un config-vVol est une sous-arborescence de répertoire correspondant à un config-vVolID. Le config-vVol doit prendre en charge les répertoires et d'autres opérations nécessaires au protocole NFS.

Virtual Volumes et NVMe

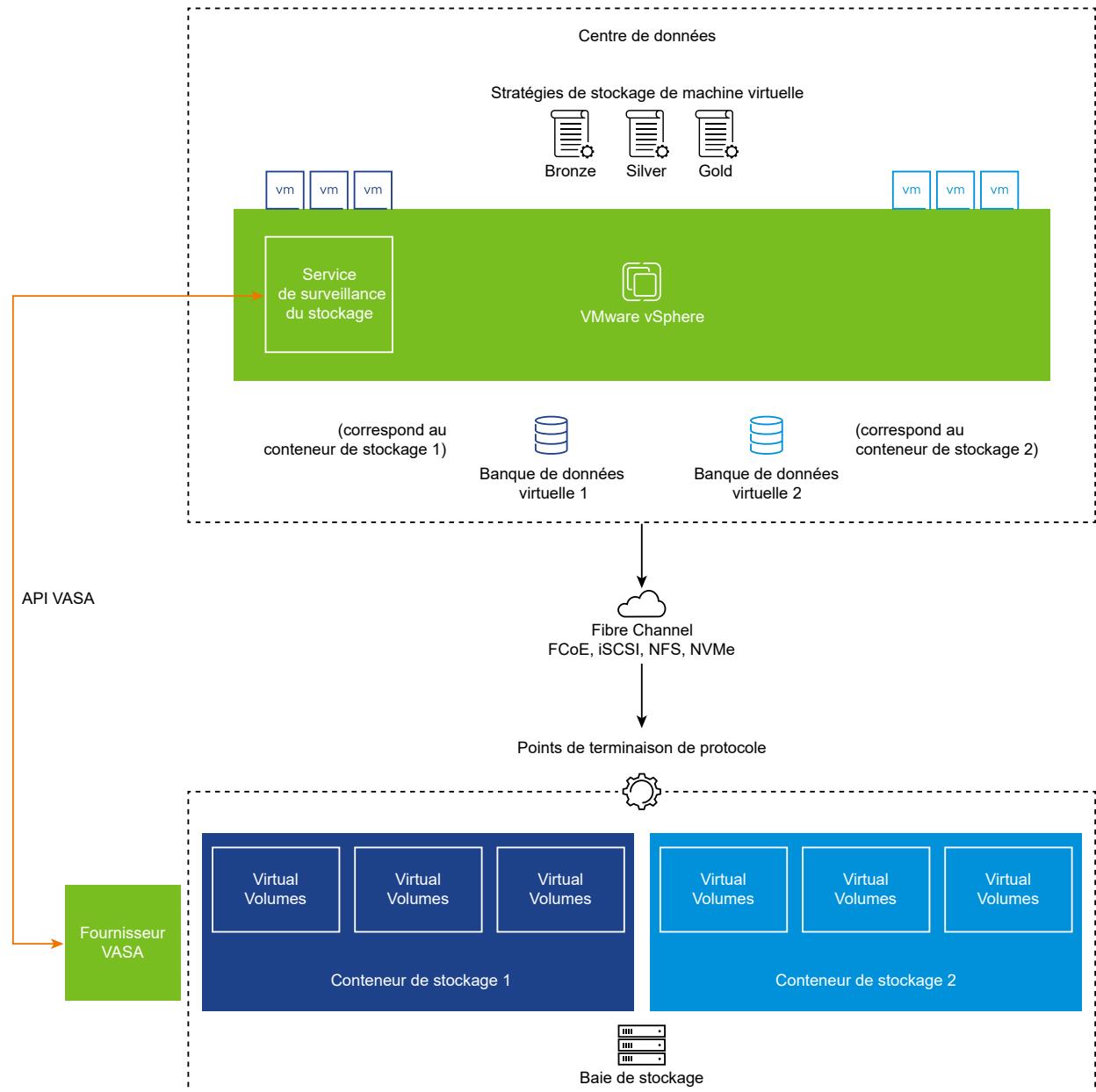
Virtual Volumes prend en charge les protocoles NVMe, notamment NVMe over Fibre Channel et NVMe over TCP. Un objet de volume virtuel est mappé à un espace de noms dans un sous-système NVMe. Les groupes ANA dans le sous-système NVMe sont affichés comme des points de terminaison de protocole virtuel sur l'hôte ESXi.

Les points de terminaison de protocole virtuel sont utilisés pour la gestion de l'état des chemins à mesure que l'état du groupe ANA change. L'hôte ESXi détecte les groupes ANA dynamiquement, selon les besoins. Cela signifie que le point de terminaison de protocole virtuel est créé uniquement lorsque l'hôte ESXi a besoin d'un accès E/S à un volume virtuel d'espace de noms dans le sous-système NVMe. Les vVols de configuration sur NVMe sont semblables aux SCSI formatés avec VMFS. Ils sont également utilisés pour stocker les fichiers de métadonnées de machine virtuelle.

Pour configurer des NVMe avec Virtual Volumes sur votre hôte ESXi, reportez-vous à la section [NVMe et Virtual Volumes](#).

Architecture de Virtual Volumes

Un diagramme architectural offre un aperçu de la façon dont les différents composants de la fonctionnalité Virtual Volumes interagissent les uns avec les autres.



Pour plus d'informations sur l'architecture Virtual Volumes, visionnez la vidéo.



([Virtual Volumes, deuxième partie : Architecture](#))

Virtual Volumes Sécurité

Certificats de sécurité avec vSphere 8.0 et versions antérieures

vSphere inclut VMware Certificate Authority (VMCA). Par défaut, la VMCA crée tous les certificats internes utilisés dans l'environnement vSphere. Elle génère des certificats pour les hôtes ESXi récemment ajoutés et les fournisseurs VASA de stockage qui gèrent les systèmes de stockage Virtual Volumes.

La communication avec le fournisseur VASA est protégée par des certificats SSL. Ces certificats peuvent être générés par le fournisseur VASA ou par la VMCA.

- Les certificats peuvent être fournis directement par le fournisseur VASA pour une utilisation à long terme. Ils peuvent être générés automatiquement et signés automatiquement ou bien dérivés d'une autorité de certification externe.
- Les certificats peuvent être générés par la VMCA en vue d'une utilisation par le fournisseur VASA.

Lorsqu'un hôte ou un fournisseur VASA est inscrit, la VMCA suit automatiquement ces étapes, sans passer par l'administrateur vSphere.

- 1 Lorsqu'un fournisseur VASA est ajouté au service de gestion du stockage vCenter Server, un certificat signé automatiquement est généré.
- 2 Une fois le certificat vérifié, le service de gestion du stockage requiert une demande de signature de certificat de la part du fournisseur VASA.
- 3 Une fois la demande de signature de certificat reçue et validée, le service de gestion du stockage la présente à la VMCA, de la part du fournisseur VASA, et réclame un certificat signé par l'autorité de certification.

La VMCA peut être configurée pour fonctionner en tant qu'autorité de certification autonome ou comme subordonnée d'une autorité de certification d'entreprise. Si vous configurez la VMCA comme subordonnée, celle-ci signe la demande de signature de certificat avec la chaîne complète.

- 4 Le certificat signé avec les certificats racines est transmis au fournisseur VASA. Le fournisseur VASA peut authentifier toutes les connexions sécurisées futures provenant du service de gestion du stockage sur vCenter Server et sur les hôtes ESXi.

Prise en charge de VASA 5 et sécurité avec vSphere 8.0 Update 1

Tous les fournisseurs de stockage avec VASA 5 et versions ultérieures utilisent un mécanisme d'authentification plus strict, qui nécessite l'authentification d'ESXi dans le contexte de vCenter Server. VASA 5 améliore la sécurité et offre un modèle de gestion considérablement modifié qui inclut les modifications majeures suivantes :

- Pour chaque système vCenter Server qui s'enregistre dans la baie à l'aide de VASA 5 ou version ultérieure, le fournisseur VASA crée une instance de serveur Web dédié ou un hôte virtuel, qui peut être soit une instance de serveur Web virtuel ou une instance complètement distincte. Le client VASA dans vCenter Server s'appuie sur l'authentification et l'autorisation basées sur les certificats pour accéder à son hôte virtuel dédié créé sur la baie. Tous les

certificats clients VASA, y compris les certificats vCenter Server et ESXi, sont enregistrés auprès de l'hôte virtuel. Cela crée une forte isolation entre les différents systèmes vCenter Server lorsque les systèmes sont authentifiés. En outre, les fournisseurs VASA peuvent offrir un accès distinct aux ressources et une meilleure isolation à différents systèmes vCenter Server.

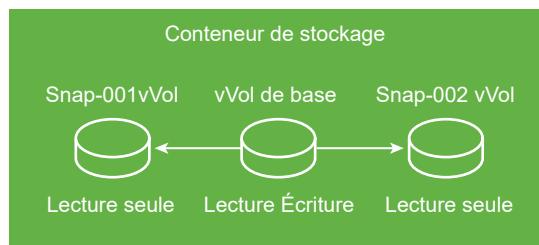
- Avec VASA 5, le client VASA utilise un certificat dédié pour les communications VASA. Chaque système vCenter Server provisionne un certificat pour le fournisseur VASA, qui est géré via un hôte virtuel dédié spécifique à vCenter Server. Tous les hôtes ESXi qui prennent en charge VASA 5 utilisent l'hôte virtuel dédié créé par leur système vCenter Server de gestion.
- vCenter Server provisionne le certificat client VASA pour chaque nouvel hôte ESXi 8.0 Update 1 et synchronise la clé publique du certificat avec le fournisseur VASA. Contrairement au précédent modèle de sécurité qui authentifie l'émetteur de l'autorité de certification pour le certificat client, le fournisseur VASA identifie et autorise désormais un client individuel à l'aide de la clé publique.
- Pour respecter les exigences de sécurité de VMware, vSphere n'approuve pas les certificats auto-signés pour les communications TLS. La seule exception se produit pendant une courte période lorsque le fournisseur VASA est enregistré et à des fins de compatibilité descendante. Un administrateur de baie peut utiliser un certificat d'autorité de certification personnalisé pour le fournisseur VASA afin de remplacer le certificat auto-signé au niveau de la baie à des fins de compatibilité descendante et de démarrage.
- Pour éviter de perdre l'accès au fournisseur VASA, suivez ces directives. Pour plus d'informations, consultez [Gérer les fournisseurs de stockage pour Virtual Volumes](#).
 - Vous ne devez pas annuler l'enregistrement de votre fournisseur VASA et l'enregistrer à nouveau pour effectuer la mise à niveau. Utilisez plutôt un mécanisme de mise à niveau approprié pour votre fournisseur VASA. Lorsque vCenter Server vous informe qu'une nouvelle version de VASA est disponible, assurez-vous d'accéder à cette version dans un délai raisonnable. Pour effectuer la mise à niveau à partir de vSphere Client, utilisez l'option **Mettre à niveau le fournisseur de stockage**.
 - Actualisez régulièrement le certificat du fournisseur VASA. Assurez-vous d'actualiser le certificat dans un délai raisonnable après avoir été averti par vCenter Server que le certificat attribué au fournisseur VASA est sur le point d'expirer. Utilisez l'option **Actualiser le certificat** de vSphere Client.
 - Lorsque vous renouvez le certificat racine VMCA ou le certificat client vCenter Server, SMS peut perdre la connexion avec le fournisseur VASA. Si le fournisseur est hors ligne, utilisez l'option **Nouvelle authentification de vCenter Server**.
 - Si un hôte perd l'authentification, vous pouvez corriger cet échec d'authentification à l'aide de l'option **Nouvelle authentification des clients VASA de l'hôte**.

Snapshots de volume virtuel

Un snapshot conserve l'état et les données d'une machine virtuelle au moment de sa création. Les snapshots sont utiles lorsque vous devez retourner à plusieurs reprises au même état mais que vous ne souhaitez pas créer plusieurs machines virtuelles. Les snapshots de volumes virtuels ont plusieurs fonctions. Vous pouvez les utiliser pour créer une copie en mode suspension à des fins de sauvegarde ou d'archivage, ou pour créer un environnement de test et de restauration pour les applications. Vous pouvez également les utiliser pour provisionner instantanément des images d'application.

Dans un environnement Virtual Volumes, les snapshots sont gérés par ESXi et vCenter Server, mais ils sont effectués par la baie de stockage.

Chaque snapshot crée un objet de volume virtuel supplémentaire, un volume virtuel de snapshot, qui stocke le contenu de la mémoire de la machine virtuelle. Les données de la machine virtuelle d'origine sont copiées vers cet objet et restent en lecture seule, afin d'empêcher le système d'exploitation invité d'écrire sur le snapshot. Vous ne pouvez pas redimensionner le volume virtuel de snapshot. En général, lors de la réPLICATION de la machine virtuelle, son volume virtuel de snapshot est également répliqué.



Ce volume virtuel de base reste actif ou ouvert en lecture et en écriture. Lorsqu'un autre snapshot est créé, il conserve le nouvel état et les données de la machine virtuelle au moment où vous effectuez le snapshot.

Lorsque vous supprimez des snapshots, seul le volume virtuel de base est conservé, tandis que les objets de volume virtuel de snapshot sont supprimés. Le volume virtuel de base représente l'état le plus récent de la machine virtuelle. Contrairement aux snapshots des banques de données traditionnelles, les volumes virtuels de snapshot n'ont pas besoin de valider leur contenu dans le volume virtuel de base.



Pour plus d'informations sur la création et la gestion de snapshots, reportez-vous à la documentation *Administration d'une machine virtuelle vSphere*.

Avant d'activer Virtual Volumes

Pour utiliser Virtual Volumes, assurez-vous que votre stockage et votre environnement vSphere sont correctement configurés.

Préparer le système de stockage pour Virtual Volumes

Pour préparer votre environnement de système de stockage pour Virtual Volumes, procédez comme suit. Pour plus d'informations, contactez votre fournisseur de stockage.

- Le système de stockage ou la baie de stockage que vous utilisez doit prendre en charge Virtual Volumes et s'intégrer aux composants vSphere via VASA (vSphere APIs for Storage Awareness). La baie de stockage doit prendre en charge le provisionnement léger et les snapshots.
- Le fournisseur de stockage Virtual Volumes doit être déployé.
- Les composants suivants doivent être configurés du côté stockage :
 - Points de terminaison de protocole. Sauf NVMe.
 - Conteneurs de stockage
 - Profils de stockage
 - Configurations de réPLICATION si vous prévoyez d'utiliser Virtual Volumes avec la réPLICATION. Reportez-vous à la section [Conditions requises en matière de réPLICATION avec Virtual Volumes](#).
- Si vous utilisez NVMe, créez des sous-systèmes NVM et associez les NQN d'hôte Virtual Volumes à des sous-systèmes NVM pertinents. Cette étape de configuration dépend de la conception NVMe spécifique au partenaire. Pour plus d'informations, contactez votre fournisseur de baie.

Préparer l'environnement vSphere

- Assurez-vous de suivre les directives de configuration correspondant au type de stockage que vous utilisez, NVMe over Fibre Channel, NVMe over TCP, Fibre Channel, FCoE, iSCSI ou NFS. Si nécessaire, installez et configurez des adaptateurs de stockage sur vos hôtes ESXi.
 - Si vous utilisez iSCSI, activez les adaptateurs iSCSI logiciels sur vos hôtes ESXi. Configurez la découverte dynamique et entrez l'adresse IP de votre système de stockage Virtual Volumes. Reportez-vous à la section [Configurer l'adaptateur iSCSI logiciel](#).
 - Si vous utilisez NVMe, suivez les conditions requises pour NVMe over Fibre Channel et NVMe over TCP. Reportez-vous à la section [Conditions requises et limitations du stockage VMware NVMe](#).
- Synchronisez tous les composants de la baie de stockage avec vCenter Server et tous les hôtes ESXi. Utilisez NTP (Network Time Protocol) pour effectuer cette synchronisation.

Pour plus d'informations, contactez votre fournisseur et reportez-vous au *Guide de compatibilité VMware*

Synchroniser l'environnement vSphere Storage avec un serveur de temps réseau

Si vous utilisez Virtual Volumes, configurez le protocole NTP (Network Time Protocol) pour vous assurer que tous les hôtes ESXi sur le réseau vSphere sont synchronisés.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Système**, sélectionnez **Configuration de temps**.
- 4 Cliquez sur **Modifier** et configurez le serveur NTP.
 - a Sélectionnez **Utiliser le protocole de temps du réseau (activer le client NTP)**.
 - b Définissez la stratégie de démarrage du service NTP.
 - c Entrez les adresses IP du serveur NTP avec lequel synchroniser.
 - d Cliquez sur **Démarrer** ou **Redémarrer** dans la section État du service NTP.
- 5 Cliquez sur **OK**.

L'hôte se synchronise avec le serveur NTP.

Configurer Virtual Volumes

Pour configurer Virtual Volumes dans l'environnement vSphere, suivez plusieurs étapes.

Conditions préalables

Suivez les instructions fournies dans la section [Avant d'activer Virtual Volumes](#).

Procédure

- 1 Enregistrer des fournisseurs de stockage pour Virtual Volumes.
- 2 Créer une banque de données Virtual Volumes.
- 3 Vérifier et gérer des points de terminaison de protocole.
- 4 (Facultatif) Modifier la stratégie de sélection de chemin d'accès pour un point de terminaison de protocole.

Enregistrer des fournisseurs de stockage pour Virtual Volumes

Votre environnement Virtual Volumes doit inclure des fournisseurs de stockage, également nommés fournisseurs VASA. En général, des intervenants tiers développent des fournisseurs de stockage au moyen d'API VASA (VMware APIs for Storage Awareness). Les fournisseurs de

stockage facilitent la communication entre vSphere et le côté stockage. Utilisez vSphere Client pour enregistrer les fournisseurs de stockage Virtual Volumes.

Après l'enregistrement, le fournisseur Virtual Volumes communique avec vCenter Server. Le fournisseur signale les caractéristiques du stockage sous-jacent et les services de données tels que la réPLICATION fournis par le système de stockage. Les caractéristiques s'affichent dans l'interface des stratégies de stockage de machine virtuelle et peuvent être utilisées pour créer une stratégie de stockage de machine virtuelle compatible avec la banque de données Virtual Volumes. Après l'application de cette stratégie de stockage à une machine virtuelle, la stratégie est poussée sur le stockage Virtual Volumes. La stratégie applique le placement optimal de la machine virtuelle dans le stockage Virtual Volumes et garantit que le stockage peut répondre aux spécifications de la machine virtuelle. Si votre stockage fournit des services supplémentaires, comme la mise en cache ou la réPLICATION, la stratégie autorise ces services pour la machine virtuelle.

Conditions préalables

Vérifiez qu'une version appropriée du fournisseur de stockage Virtual Volumes est installée côté stockage. Procurez-vous les informations d'identification du fournisseur de stockage.

Procédure

- 1 Accédez à vCenter Server.
- 2 Cliquez sur l'onglet **Configurer**, puis cliquez sur **Fournisseurs de stockage**.
- 3 Cliquez sur l'icône **Ajouter**.
- 4 Entrez les informations de connexion du fournisseur de stockage, notamment son nom, son URL et ses données d'identification.
- 5 Pour terminer l'enregistrement, cliquez sur **OK**.

vCenter Server découvre et enregistre le fournisseur de stockage Virtual Volumes.

- 6 Vérifiez les informations disponibles pour votre fournisseur.

Basculez entre **Fournisseurs de stockage** et **Baies de fournisseur** pour afficher des informations sur votre fournisseur et la baie qu'il représente.

Étape suivante

Pour gérer ou mettre à niveau les fournisseurs de stockage, reportez-vous à la section [Gérer les fournisseurs de stockage pour Virtual Volumes](#).

Créer une banque de données Virtual Volumes

Vous utilisez l'assistant **Nouvelle banque de données** pour créer une banque de données Virtual Volumes.

Procédure

- 1 Dans le navigateur d'objets vSphere Client, accédez à un hôte, à un cluster ou à un centre de données.
- 2 Dans le menu contextuel, sélectionnez **Stockage > Nouvelle banque de données**.
- 3 Sélectionnez **vVol** comme type de banque de données.
- 4 Entrez le nom de la banque de données et sélectionnez un conteneur de stockage de sauvegarde dans la liste des conteneurs de stockage.

Assurez-vous d'utiliser un nom qui ne correspond pas à celui d'une autre banque de données de l'environnement de votre centre de données.

Si vous montez la même banque de données Virtual Volumes sur plusieurs hôtes, le nom de la banque de données doit être le même sur tous les hôtes.

- 5 Sélectionnez les hôtes qui exigent un accès à la banque de données.
- 6 Passez en revue les options de configuration puis cliquez sur **Terminer**.

Étape suivante

Après avoir créé la banque de données Virtual Volumes, vous pouvez effectuer les tâches suivantes :

- Renommer la banque de données, parcourir les fichiers de la banque de données, démonter la banque de données, etc. Reportez-vous à la section [Opérations administratives de base pour les banques de données](#).

Note Vous ne pouvez pas ajouter la banque de données Virtual Volumes à un cluster de banques de données.

- Provisionnez des machines virtuelles sur la banque de données Virtual Volumes. Reportez-vous à la documentation [Provisionner des machines virtuelles sur des banques de données Virtual Volumes](#) et [Administration d'une machine virtuelle vSphere](#).

Vérifier et gérer des points de terminaison de protocole

Les hôtes ESXi utilisent un proxy d'E/S logiques appelé « point de terminaison de protocole » pour communiquer avec les volumes virtuels et avec les fichiers de disque virtuel encapsulés par les volumes virtuels. Le système de stockage utilise un fournisseur de stockage pour exporter les points de terminaison de protocole et les conteneurs de stockage associés.

Une fois que vous avez mappé un conteneur de stockage à une banque de données Virtual Volumes, les points de terminaison de protocole deviennent visibles dans vSphere Client. Vous pouvez vérifier les propriétés des points de terminaison de protocole et modifier des paramètres spécifiques.

Note Cela ne s'applique pas si vous créez des banques de données Virtual Volumes avec le stockage NVMe. Si une baie que vous utilisez prend uniquement en charge le stockage NVMe, les points de terminaison de protocole n'apparaissent pas dans la liste.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Points de terminaison de protocole**.
- 4 Pour afficher les détails d'un élément spécifique, sélectionnez-le dans la liste.
- 5 Utilisez les onglets dans Détails des points de terminaison de protocole pour accéder à des informations supplémentaires et modifier les propriétés du point de terminaison de protocole sélectionné.

Onglet	Description
Propriétés	Consultez les propriétés et caractéristiques de l'élément. Pour les éléments SCSI (bloc), consultez et modifiez les stratégies de chemins multiples.
Chemins (points de terminaison de protocole SCSI uniquement)	Consultez les chemins disponibles pour le point de terminaison de protocole. Désactivez ou activez un chemin sélectionné. Modifiez la stratégie de sélection de chemin.
Banques de données	Affichez une banque de données Virtual Volumes correspondante. Réalisez les opérations de gestion de banque de données.

Modifier la stratégie de sélection de chemin d'accès pour un point de terminaison de protocole

Si l'hôte ESXi utilise le transport SCSI pour communiquer avec les points de terminaison de protocole représentant une baie de stockage, vous pouvez modifier les stratégies de chemins multiples attribuées par défaut aux points de terminaison de protocole. Utilisez la boîte de dialogue **Modifier les règles de chemins multiples** pour modifier une stratégie de sélection de chemin.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Stockage**, cliquez sur **Points de terminaison de protocole**.

- 4 Sélectionnez le point de terminaison de protocole dont vous voulez modifier les chemins et cliquez sur l'onglet **Propriétés**.
- 5 Sous Règles de gestion multivoie, sélectionnez **Modifier la gestion multivoie** dans le menu **Actions**.
- 6 Sélectionnez une stratégie de chemin et configurez ses paramètres.
Pour plus d'informations sur les stratégies de chemin d'accès pour les périphériques SCSI, reportez-vous à [Path Selection Plug-Ins et règles](#).
- 7 Pour enregistrer vos paramètres et quitter la boîte de dialogue, cliquez sur **OK**.

Provisionner des machines virtuelles sur des banques de données Virtual Volumes

Vous pouvez provisionner des machines virtuelles sur une banque de données Virtual Volumes.

Note L'ensemble des disques virtuels provisionnés sur une banque de données Virtual Volumes doivent constituer un multiple égal de 1 Mo.

Une machine virtuelle qui s'exécute sur une banque de données Virtual Volumes nécessite une stratégie de stockage de machine virtuelle appropriée.

Une fois la machine virtuelle provisionnée, vous pouvez réaliser des tâches de gestion de machine virtuelle habituelles. Pour plus d'informations, reportez-vous à la documentation *Administration d'une machine virtuelle vSphere*.

Procédure

- 1 Définissez une stratégie de stockage de machine virtuelle pour Virtual Volumes.

VMware fournit une stratégie de stockage sans exigences par défaut pour Virtual Volumes. Le cas échéant, vous pouvez créer une stratégie de stockage personnalisée compatible avec Virtual Volumes.

Reportez-vous à la section [Créer une stratégie de stockage de machine virtuelle pour Virtual Volumes](#).

- 2 Attribuez la stratégie de stockage Virtual Volumes à des machines virtuelles.

Pour garantir que la banque de données Virtual Volumes satisfait les besoins spécifiques en stockage lorsque vous allouez une machine virtuelle, associez la stratégie de stockage Virtual Volumes à la machine virtuelle.

Reportez-vous à la section [Attribuer des stratégies de stockage à des machines virtuelles](#).

- 3 Modifiez la stratégie de stockage par défaut d'une banque de données Virtual Volumes.

Pour les machines virtuelles provisionnées sur des banques de données Virtual Volumes, VMware fournit une stratégie sans condition par défaut. Vous ne pouvez pas modifier cette stratégie, mais vous pouvez désigner une stratégie récemment créée à utiliser par défaut.

Reportez-vous à la section [Modifier la stratégie de stockage par défaut d'une banque de données](#).

Gérer les fournisseurs de stockage pour Virtual Volumes

Après avoir enregistré des fournisseurs de stockage pour Virtual Volumes, utilisez vSphere Client pour gérer les fournisseurs.

Conditions préalables

Enregistrez les fournisseurs de stockage. Reportez-vous à la section [Enregistrer des fournisseurs de stockage pour Virtual Volumes](#).

Procédure

- 1 Accédez à vCenter Server.
- 2 Cliquez sur l'onglet **Configurer**, puis cliquez sur **Fournisseurs de stockage**.
- 3 Cliquez sur l'icône pour effectuer l'une des actions globales suivantes pour tous les fournisseurs Virtual Volumes.

Icône	Description
Synchroniser les fournisseurs de stockage	Synchronisez tous les fournisseurs de stockage avec l'état actuel de l'environnement.
Nouvelle authentification des clients VASA de l'hôte	Authentifiez à nouveau tous les hôtes auprès de leurs fournisseurs de stockage respectifs. S'applique aux hôtes ESXi version 8.0 Update 1 ou ultérieure. Les hôtes doivent prendre en charge VASA 5.

Note Cette opération prend du temps.

- 4 Pour gérer un fournisseur de stockage spécifique, accédez au fournisseur et cliquez sur l'icône **Action de ligne** (trois points) en regard du nom du fournisseur.

Storage Provider	Status	URL	Last Rescan Time	VASA API Version	Certificate Expiry
vasa nvme	Offline	https://192.168.1.100:9080/vasa/	01/03/2023, 2:44:49 AM	5.0	350 days
Rescan	Online	https://192.168.1.100:9080/vasa/	01/03/2023, 2:56:03 AM	1.5	1810 days
Remove	Online	https://192.168.1.100:9080/vasa/	01/03/2023, 2:56:03 AM	1.5	1810 days
Refresh certificate	Online	https://192.168.1.100:9080/vasa/	01/13/2023, 1:11:14 AM	4.0 ⚠️	⚠️ 74 days
Upgrade Storage Provider	Online	https://192.168.1.100:9080/vasa/	01/03/2023, 2:56:57 AM	3.0	--
Re-authenticate vCenter Server	Online	https://192.168.1.100:9080/vasa/	01/03/2023, 2:56:57 AM	3.0	--

- 5 Sélectionnez l'un des éléments suivants dans le menu **Actions de ligne**.

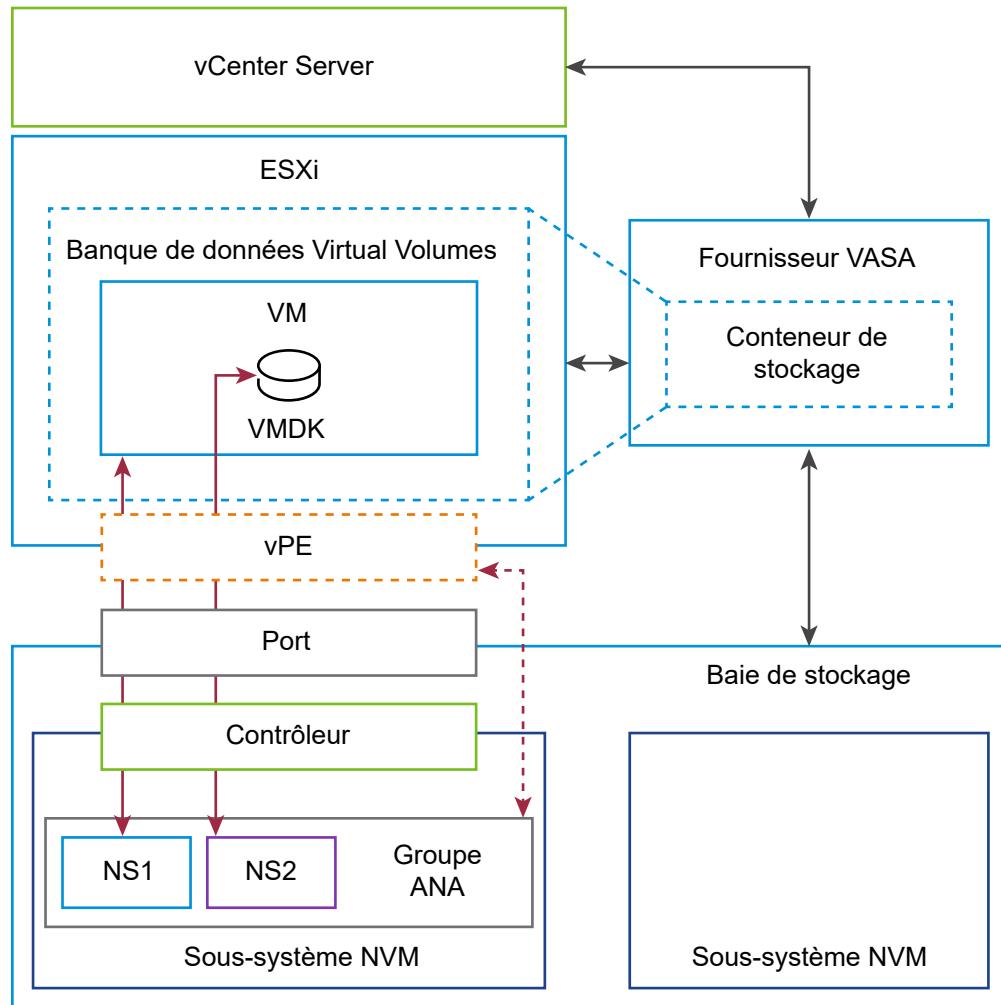
Option	Description
Réanalyser	Mettez à jour les données de stockage pour le fournisseur. vCenter Server met périodiquement à jour les données de stockage dans sa banque de données. Les mises à jour sont partielles et reflètent uniquement les modifications que les fournisseurs de stockage communiquent à vCenter Server à ce moment. Lorsque cela est nécessaire, vous pouvez exécuter une synchronisation de base de données complète pour le fournisseur de stockage sélectionné.
Supprimer	Annulez l'enregistrement des fournisseurs de stockage que vous n'utilisez pas. Une fois cette opération effectuée, vCenter Server ferme la connexion et supprime le fournisseur de stockage de sa configuration.
Actualiser le certificat	vCenter Server vous avertit lorsqu'un certificat attribué à un fournisseur de stockage est sur le point d'expirer. Vous pouvez actualiser le certificat pour continuer à utiliser le fournisseur. Si vous ne parvenez pas à actualiser le certificat avant qu'il n'expire, vCenter Server cesse d'utiliser le fournisseur.
Mettre à niveau le fournisseur de stockage	Lorsque vCenter Server vous informe d'une nouvelle version de VASA disponible, acceptez cette version pour l'activer dans votre environnement vSphere. vCenter Server active les nouvelles capacités exposées par le fournisseur de stockage et communique ces informations à tous les hôtes de l'inventaire. Lorsque vous effectuez cette action, vous devez entrer les informations d'identification du fournisseur de stockage. Vous ne pouvez pas sélectionner une version VASA spécifique pour une mise à niveau si plusieurs versions sont disponibles. vCenter Server effectue uniquement les mises à niveau vers la dernière version. Note Vous pouvez choisir d'effectuer les mises à niveau à votre propre rythme. Pour plus d'informations, consultez Virtual VolumesSécurité .
Nouvelle authentification de vCenter Server	Nouvelle authentification de vCenter Server auprès du fournisseur de stockage. Cette action autorise à nouveau vCenter Server auprès du fournisseur de stockage s'il a perdu l'authentification et a besoin d'informations d'identification. Vous devez entrer les informations d'identification du fournisseur de stockage.

NVMe et Virtual Volumes

Virtual Volumes prend en charge les protocoles NVMe over Fibre Channel et NVMe over TCP.

Lorsque vous utilisez ce protocole, après l'enregistrement du fournisseur de stockage (VASA), le système termine automatiquement la configuration sous-jacente. Vous créez uniquement la banque de données. Les points de terminaison de protocole virtuel (vPE) et les connexions sont gérés par le fournisseur de stockage.

Familiarisez-vous avec les concepts suivants spécifiques à la configuration de NVMe avec Virtual Volumes.



Espace de noms de volume virtuel

En général, un espace de noms peut être considéré comme l'équivalent NVMe d'un LUN. Chaque type de volume virtuel (de données, de configuration ou d'échange) crée un espace de noms avec un rapport 1:1 entre le volume virtuel et l'espace de noms. Les limites de l'espace de noms dépendent du fournisseur de la baie.

Groupe d'accès à l'espace de noms asymétrique (ANA)

Avec l'implémentation SCSI ou NFS de Virtual Volumes, le conteneur de stockage regroupe logiquement les objets de volume virtuel. Avec NVMe, le regroupement des volumes virtuels dépend de la baie. En général, au niveau de la baie, les espaces de noms des volumes virtuels sont regroupés dans un groupe ANA. La baie détermine le nombre de groupes ANA, chacun

ayant un ANAGRPID unique dans le sous-système NVM. Les espaces de noms de volume virtuel sont alloués et actifs uniquement sur la demande BIND au fournisseur VASA. La demande BIND ajoute également l'espace de noms au groupe ANA. Un espace de noms reste alloué et actif jusqu'à ce que le dernier hôte annule la liaison du volume virtuel.

Point de terminaison de protocole virtuel (vPE)

Avec les protocoles SCSI ou NFS, les points de terminaison de protocole représentent un LUN proxy ou un point de montage NFS. Dans vSphere Client, la liste des points de terminaison de protocole disponibles est similaire à la liste des périphériques de stockage d'hôte.

Dans NVMe avec Virtual Volumes, le point de terminaison de protocole virtuel est une représentation logique du groupe ANA dans lequel résident les volumes virtuels. Le vPE n'existe pas tant qu'aucune machine virtuelle n'est mise sous tension. Une fois la machine virtuelle sous tension, le vPE est créé afin que l'hôte puisse accéder aux volumes virtuels dans le groupe ANA.

Configurer NVMe avec Virtual Volumes

Suivez ces étapes pour configurer NVMe avec Virtual Volumes sur votre hôte ESXi.

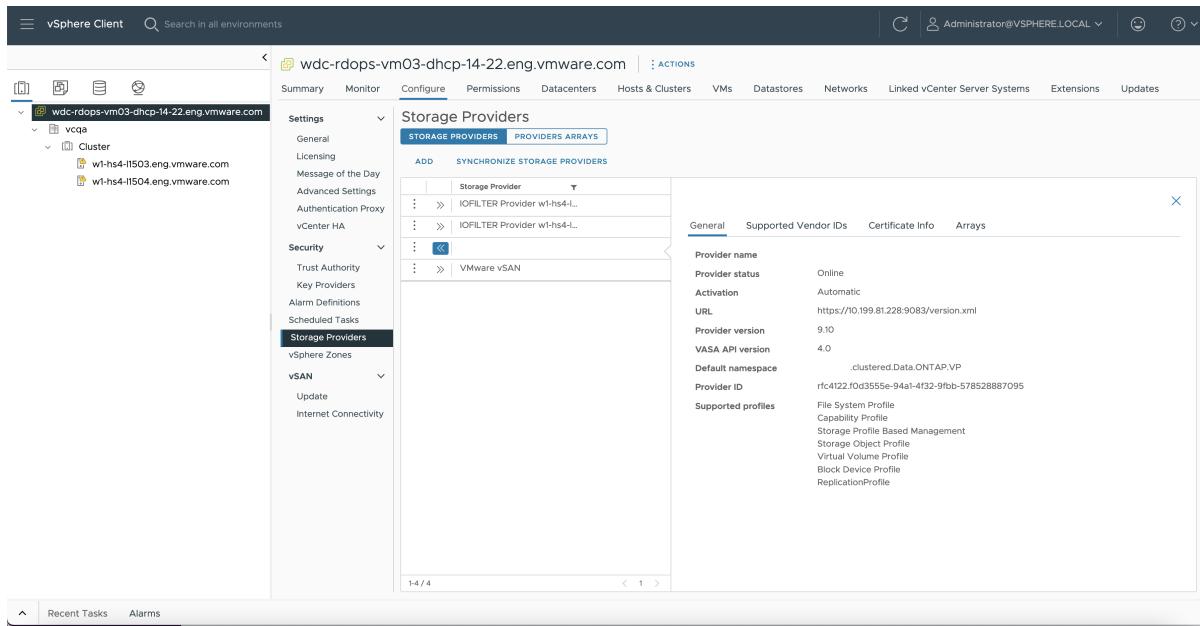
Conditions préalables

- Assurez-vous que votre fournisseur de stockage (VASA) prend en charge NVMe avec Virtual Volumes.
- Assurez-vous que votre baie de stockage prend en charge NVMe avec la capacité Virtual Volumes.
- Préparez votre environnement vSphere et un système de stockage. Pour plus d'informations, reportez-vous à [Avant d'activer Virtual Volumes](#) et [Conditions requises et limitations du stockage VMware NVMe](#).
- Si vous utilisez NVMe over TCP, configurez les adaptateurs pour le stockage NVMe over TCP. Reportez-vous à la section [Configuration des adaptateurs pour le stockage NVMe over TCP](#).

Procédure

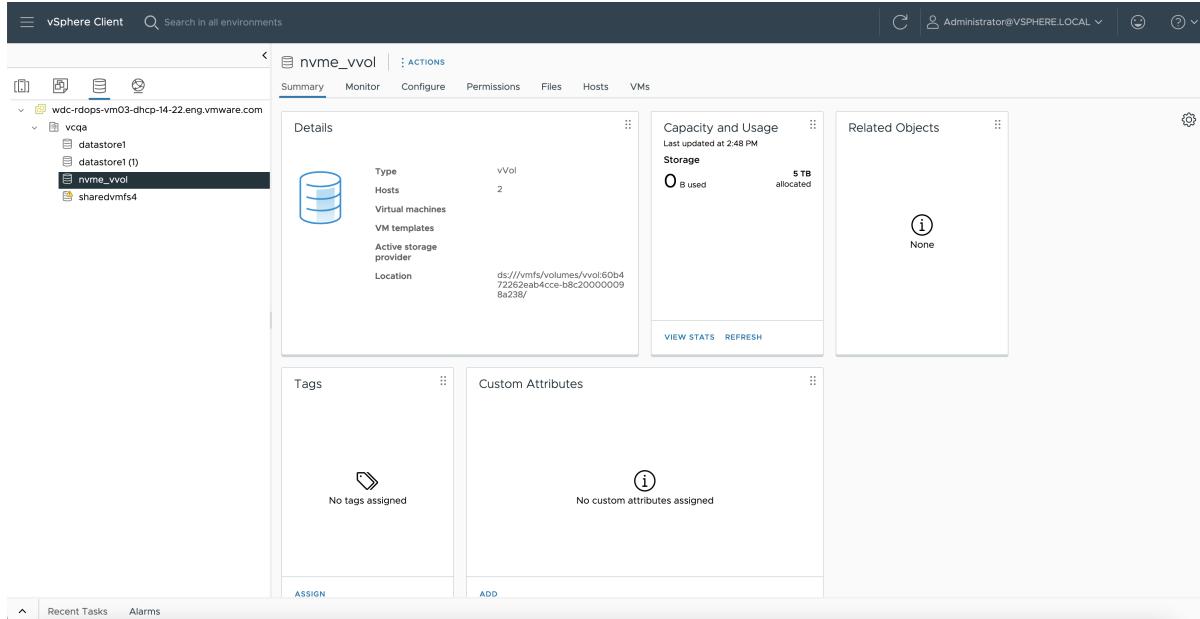
1 Enregistrez le fournisseur de stockage .

Pour plus d'informations, consultez [Enregistrer des fournisseurs de stockage pour Virtual Volumes](#).



2 Créez une banque de données Virtual Volumes.

Lors de la création de la banque de données, sélectionnez les conteneurs de stockage qui prennent en charge la capacité NVMe. Pour plus d'informations, consultez [Créer une banque de données Virtual Volumes](#).



3 Si vous utilisez NVMe over TCP, ajoutez un contrôleur.

Reportez-vous à la section [Ajouter des contrôleurs pour NVMe over Fabrics](#).

Note Vous n'est pas besoin de configurer le contrôleur pour NVMe over Fibre Channel. Une fois que vous avez créé la banque de données, le système détecte les contrôleurs.

Adapter	Model	Type	Status	Identifier	Targets	Devices
vmhba3	Dell BOSS-1 Adapter	Block SCSI	Unknown	--	2	2
vmhba0	Dell HBA330 Mini	SAS	Unknown	--	1	1
vmhba4	ISP2812-based 64/32G Fibre Channel to PCIe Controller	Fibre Chann..	Online	20:00:34:80:0d:77:70:b8 21...	1	5
vmhba5	ISP2812-based 64/32G Fibre Channel to PCIe Controller	Fibre Chann..	Online	20:00:34:80:0d:77:70:b9 21...	1	5
vmhba6	ISP2812-based 64/32G Fibre Channel to PCIe Controller	Fibre Chann..	Online	20:00:34:80:0d:77:70:b8 21...	0	0
vmhba65	ISP2812-based 64/32G Fibre Channel to PCIe Controller	Fibre Chann..	Online	20:00:34:80:0d:77:70:b9 21...	0	0
vmhba1	Lewisburg SATA AHCI Controller	Block SCSI	Unknown	--	0	0
vmhba2	Lewisburg SATA AHCI Controller	Block SCSI	Unknown	--	0	0

Name	Subsystem NQN	Transport Type
nqn.2014-08.org.nvmeexpress.discovery#vmhba65#203900a098b32f50	nqn.2014-08.org.nvmeexpress.discovery	fibreChannel
nqn.2014-08.org.nvmeexpress.discovery#vmhba65#203900a098b32f50:206700a098b32f50	nqn.2014-08.org.nvmeexpress.discovery	fibreChannel
nqn.2014-08.org.nvmeexpress.discovery#vol#vmhba65#203900a098b32f50:202300a098b32f...	nqn.2014-08.org.nvmeexpress.discovery	fibreChannel
nqn.2014-08.org.nvmeexpress.discovery#vol#vmhba65#203900a098b32f50:206700a098b32f...	nqn.2014-08.org.nvmeexpress.discovery	fibreChannel
nqn.1992-08.com...sn.celc4e9ac7e11feba08500a098b27291:subsystem.nvme_vvol_16608...	nqn.1992-08.com...sn.celc4e9ac7e11feba...	fibreChannel
nqn.1992-08.com...sn.celc4e9ac7e11feba08500a098b27291:subsystem.nvme_vvol_16608...	nqn.1992-08.com...sn.celc4e9ac7e11feba...	fibreChannel

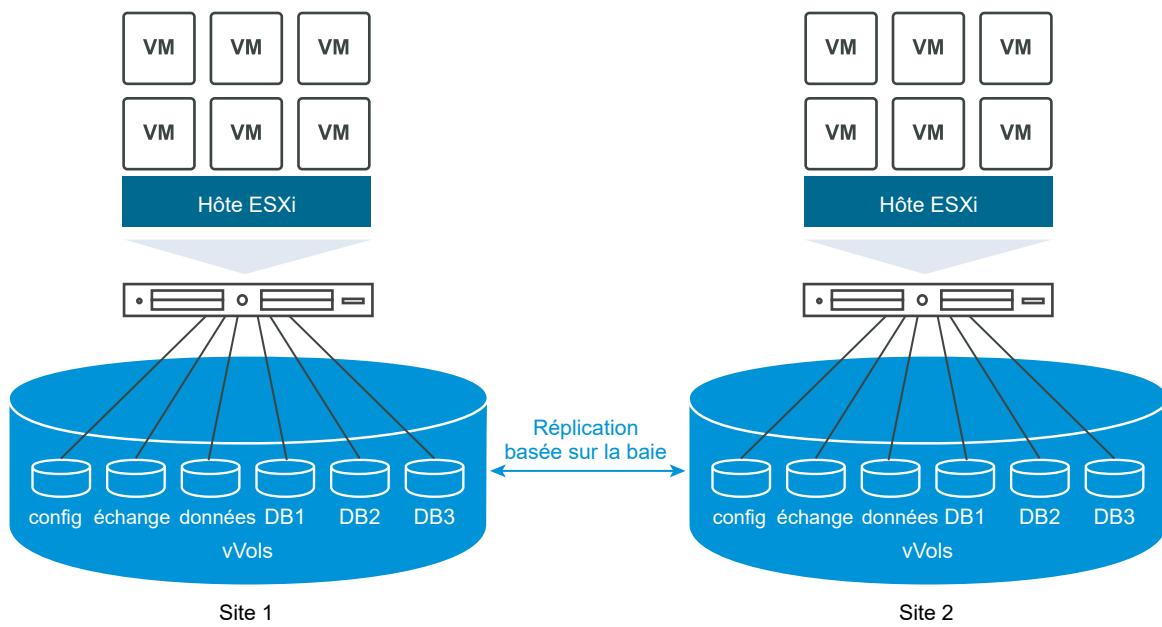
Virtual Volumes et réPLICATION

Virtual Volumes prend en charge la réPLICATION et la récupération d'urgence. La réPLICATION basée sur la baie vous permet de délester la réPLICATION des machines virtuelles sur votre baie de stockage et d'utiliser l'ensemble des fonctionnalités de réPLICATION de la baie. Vous pouvez réPLiquer un objet de machine virtuelle unique, comme un disque virtuel. Vous pouvez également regrouper plusieurs objets de machine virtuelle ou des machines virtuelles afin de les réPLiquer en une seule unité.

La réPLICATION basée sur la baie est régie par des stratégies. Une fois votre stockage Virtual Volumes configuré pour la réPLICATION, des informations sur les fonctionnalités de réPLICATION et les groupes de réPLICATION sont livrées à partir de la baie par le fournisseur de stockage. Ces informations sont affichées dans l'interface des stratégies de stockage de machine virtuelle de vCenter Server.

La stratégie de stockage de machine virtuelle vous permet de décrire les conditions requises de la réPLICATION pour vos machines virtuelles. Les paramètres que vous spécifiez dans la stratégie de stockage dépendent de la manière dont votre baie met en œuvre la réPLICATION. Par exemple, votre stratégie de stockage de machine virtuelle peut inclure des paramètres de planification de réPLICATION, de fréquence de réPLICATION ou de d'objectif de point de récupération (RPO). La stratégie peut également indiquer la cible de réPLICATION, un site secondaire sur lequel vos machines virtuelles sont réPLiquées, ou spécifier si les réPLICAS doivent être supprimés.

En attribuant la stratégie de réPLICATION au cours du provisionnement de la machine virtuelle, vous demandez des services de réPLICATION pour votre machine virtuelle. Ensuite, la baie prend en charge la gestion de tous les processus et planifications de réPLICATION.



Conditions requises en matière de réPLICATION avec Virtual Volumes

Lors de l'activation de Virtual Volumes avec la réPLICATION, en plus des spécifications générales relatives à Virtual Volumes, votre environnement doit respecter des conditions préalables particulières.

Pour en savoir plus sur les spécifications générales relatives à Virtual Volumes, reportez-vous à [Avant d'activer Virtual Volumes](#).

Conditions requises pour le stockage

La mise en œuvre de la réPLICATION de Virtual Volumes dépend de votre baie et peut être différente pour les fournisseurs de stockage. En général, les conditions requises suivantes s'appliquent à tous les fournisseurs.

- Les baies de stockage que vous utilisez pour mettre en œuvre la réPLICATION doivent être compatibles avec Virtual Volumes.
- Elles doivent également s'intégrer à la version du fournisseur de stockage (VASA) compatible avec la réPLICATION de Virtual Volumes.
- Les baies de stockage doivent prendre en charge la réPLICATION et être configurées de manière à utiliser les mécanismes de réPLICATION fournis par le fournisseur. Les configurations habituelles comprennent généralement une ou deux cibles de réPLICATION. Toutes les configurations requises, comme le couplage du site répliqué et du site cible, doivent également être appliquées du côté du stockage.
- Le cas échéant, les groupes de réPLICATION et les domaines de pannes de Virtual Volumes doivent être préconfigurés du côté du stockage.

Pour plus d'informations, contactez votre fournisseur et reportez-vous à *Guide de compatibilité VMware*.

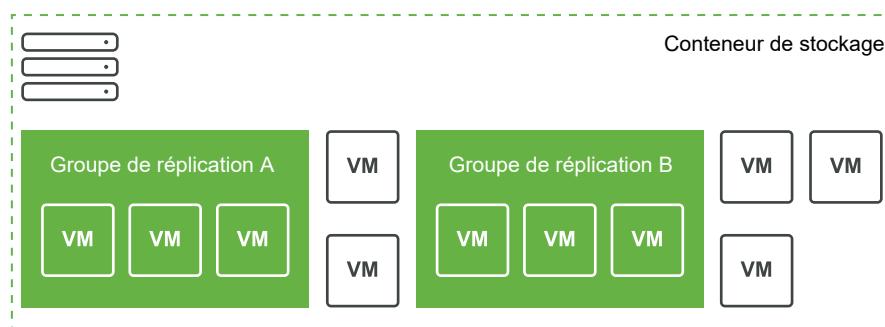
Conditions requises pour vSphere

- Utilisez des versions de vCenter Server et de ESXi qui prennent en charge la réPLICATION de stockage Virtual Volumes. Les hôtes vCenter Server et ESXi qui sont antérieurs à la version 6.5 ne prennent pas en charge le stockage Virtual Volumes de réPLICATION. Toute tentative de création d'une machine virtuelle répliquée sur un hôte incompatible échoue et renvoie une erreur. Pour plus d'informations, consultez *Guide de compatibilité VMware*.
- Si vous prévoyez de migrer une machine virtuelle, vérifiez que les ressources cibles, comme les hôtes ESXi et les banques de données Virtual Volumes, prennent en charge la réPLICATION de stockage.

Virtual Volumes et groupes de réPLICATION

Lorsque votre stockage offre des services de réPLICATION, en plus des conteneurs de stockage et des points de terminaison de protocole, votre administrateur de stockage peut configurer des groupes de réPLICATION du côté du stockage.

vCenter Server et ESXi peuvent détecter des groupes de réPLICATION, mais ne gèrent pas leur cycle de vie. Les groupes de réPLICATION, également appelés groupes de cohérence, indiquent quelles machines virtuelles et quels disques virtuels doivent être répliqués ensemble vers un site cible. Une machine virtuelle unique ne peut pas s'étendre sur plusieurs groupes de réPLICATION.



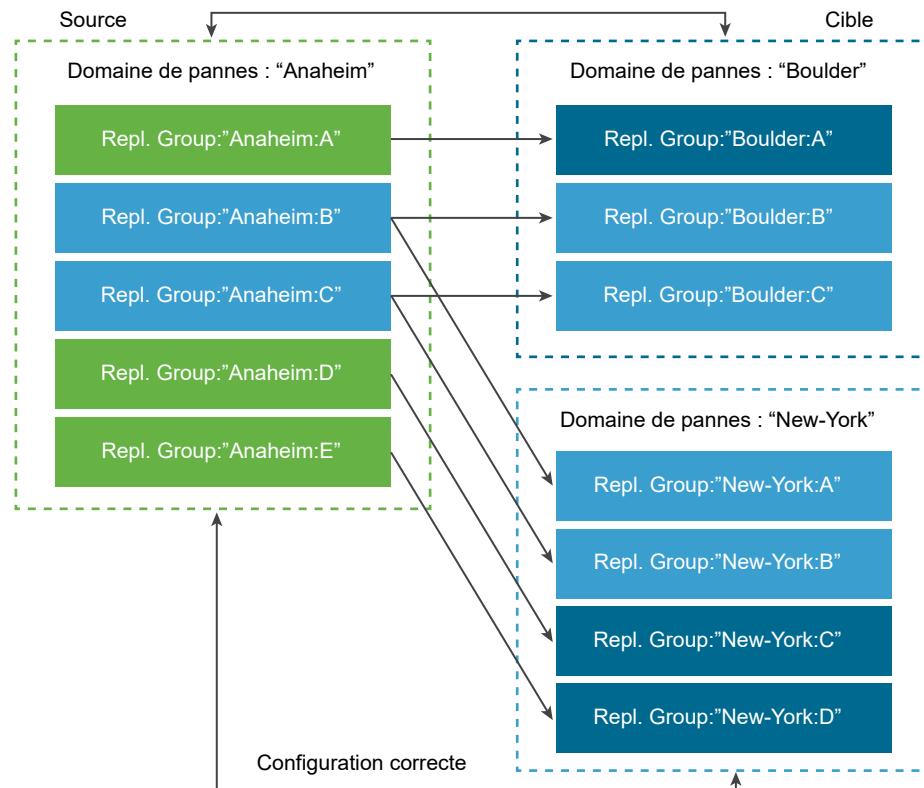
Si aucun groupe préconfiguré n'est disponible, Virtual Volumes peut utiliser une méthode automatique. Cette méthode permet à Virtual Volumes de créer un groupe de réPLICATION à la demande et d'associer ce groupe à un objet Virtual Volumes en cours de provisionnement. Si vous utilisez le groupe de réPLICATION automatique, tous les composants d'une machine virtuelle sont attribués au groupe. Vous ne pouvez pas combiner des groupes de réPLICATION préconfigurés et automatiques pour les composants de la même machine virtuelle.

Virtual Volumes et domaines de pannes

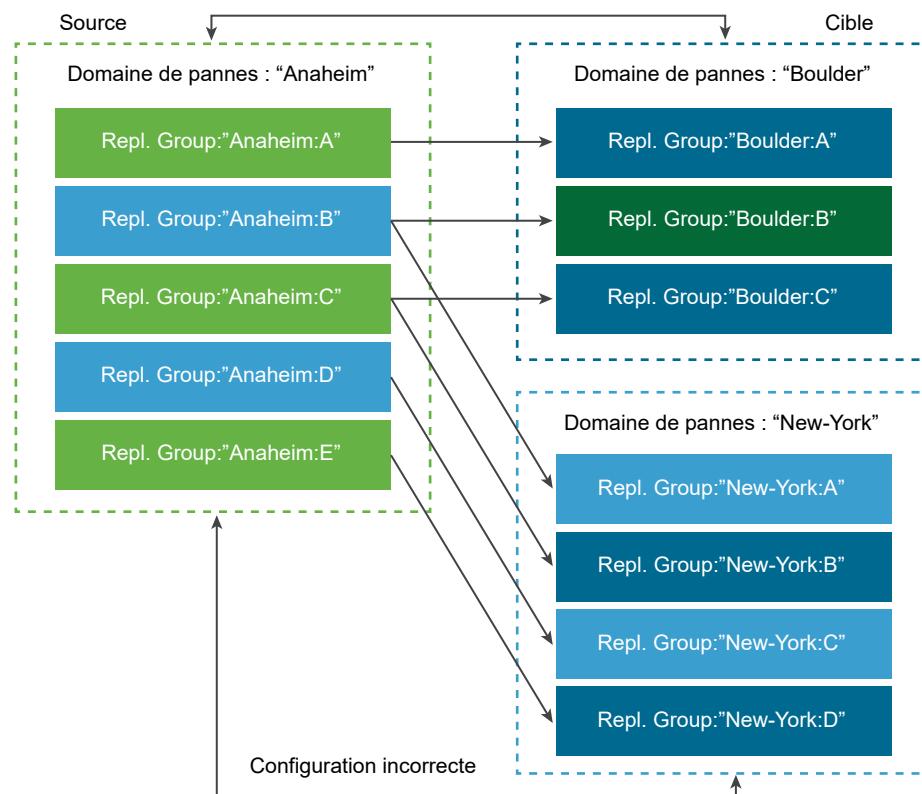
Dans l'environnement Virtual Volumes, les domaines de pannes définissent la manière dont des groupes de réPLICATION spécifiques doivent être combinés pendant leur réPLICATION entre un site source et un site cible.

Les domaines de pannes sont configurés et signalés par la baie de stockage et ne sont pas exposés dans vSphere Client. Le mécanisme SPBM (Storage Policy Based Management) détecte les domaines de pannes et les utilise à des fins de validation pendant la création d'une machine virtuelle.

Par exemple, provisionnez deux machines virtuelles, l'une associée au groupe de réPLICATION Anaheim:B, l'autre associée au groupe de réPLICATION Anaheim:C. SPBM valide le provisionnement, car chaque machine virtuelle se trouve dans son propre groupe de réPLICATION avec les domaines de pannes cibles correspondants.



Ensuite, provisionnez deux machines virtuelles, l'une associée au groupe de réPLICATION Anaheim:B, l'autre associée au groupe de réPLICATION Anaheim:D. Cette configuration n'est pas valide. Les deux groupes de réPLICATION se répliquent dans le domaine de pannes New-York, mais un seul se réplique dans le domaine de pannes Boulder.



Workflow de réPLICATION de Virtual Volumes

Si des informations relatives aux capacités de réPLICATION de la baie de stockage Virtual Volumes s'affichent dans vCenter Server, vous pouvez activer la réPLICATION de vos machines virtuelles.

Le workflow permettant d'activer la réPLICATION de vos machines virtuelles inclut une procédure courante de provisionnement de la machine virtuelle sur le stockage Virtual Volumes.

- 1 Définissez la stratégie de stockage de machine virtuelle compatible avec le stockage de réPLICATION. Les règles basées sur les banques de données de la stratégie doivent inclure le composant de réPLICATION. Reportez-vous à la section [Créer une stratégie de stockage de machine virtuelle pour Virtual Volumes](#).

Après avoir configuré la stratégie de stockage incluant la réPLICATION, vCenter Server détecte les groupes de réPLICATION disponibles.

- 2 Attribuez la stratégie de réPLICATION à votre machine virtuelle. Si celle-ci est configurée, sélectionnez un groupe de réPLICATION compatible ou utilisez l'attribution automatique. Reportez-vous à la section [Attribuer des stratégies de stockage à des machines virtuelles](#).

Directives et considérations relatives à la réPLICATION

Lorsque vous utilisez la réPLICATION avec Virtual Volumes, vous devez tenir compte de considérations spécifiques.

- Vous pouvez appliquer la stratégie de stockage de réPLICATION uniquement à un volume virtuel de configuration et à un volume virtuel de données. D'autres objets de machines virtuelles héritent de la stratégie de réPLICATION comme suit :
 - Le volume virtuel de mémoire hérite de la stratégie du volume virtuel de configuration.
 - Le volume virtuel de synthèse hérite de la stratégie du volume virtuel de données.
 - Le volume virtuel d'échange, qui existe quand une machine virtuelle est mise sous tension, est exclu de la réPLICATION.
- Si vous n'appliquez pas la stratégie de réPLICATION à un disque de machine virtuelle, le disque n'est pas répliqué.
- La stratégie de stockage de réPLICATION ne doit pas être utilisée comme stratégie de stockage par défaut pour une banque de données. Sinon, elle vous empêche de sélectionner des groupes de réPLICATION.
- La réPLICATION conserve l'historique des snapshots. Si un snapshot a été créé et répliqué, vous pouvez revenir au snapshot correspondant à l'application.
- Vous pouvez répliquer un clone lié. Si un clone lié est répliqué sans son parent, il devient un clone complet.
- Si un fichier descripteur appartient à un disque virtuel d'une machine virtuelle, mais réside dans l'Accueil VM d'une autre machine virtuelle, les deux machines virtuelles doivent se trouver dans le même groupe de réPLICATION. Si les machines virtuelles sont situées dans des groupes de réPLICATION distincts, ils doivent tous deux être basculés simultanément. Sinon, le descripteur peut devenir indisponible après le basculement. En conséquence, la machine virtuelle peut échouer à se mettre sous tension.
- Dans votre environnement Virtual Volumes avec réPLICATION, vous pouvez exécuter périodiquement un workflow de basculement de test pour vous assurer que les charges de travail récupérées sont opérationnelles après un basculement.

Les machines virtuelles de test résultantes créées pendant le test de basculement sont entièrement opérationnelles et adaptées à des opérations administratives générales. Cependant, certains éléments doivent être pris en compte :

- Toutes les machines virtuelles créées pendant le test de basculement doivent être supprimées avant l'arrêt du test de basculement. Cette suppression permet de garantir qu'aucun snapshot ou volume lié à un snapshot, qui fait partie de la machine virtuelle (par exemple, le volume virtuel de snapshot), n'interfère sur l'arrêt du test de basculement.
- Vous pouvez créer des clones complets des machines virtuelles de test.

- Vous pouvez créer des clones rapides uniquement si la stratégie appliquée à la nouvelle machine virtuelle contient le même ID de groupe de réPLICATION que la machine virtuelle clonée. Les tentatives de placement de la machine virtuelle enfant à l'extérieur du groupe de réPLICATION de la machine virtuelle parente échouent.

Meilleures pratiques d'utilisation de Virtual Volumes

Observez les recommandations suivantes lors de l'utilisation de Virtual Volumes avec ESXi et vCenter Server.

- [Directives et limitations lors de l'utilisation de Virtual Volumes](#)

Pour garantir une expérience optimale avec la fonctionnalité Virtual Volumes, vous devez observer des directives spécifiques.

- [Meilleures pratiques pour le provisionnement de conteneurs de stockage](#)

Suivez ces meilleures pratiques lorsque vous provisionnez des conteneurs de stockage côté baie Virtual Volumes.

- [Meilleures pratiques pour les performances de Virtual Volumes](#)

Pour garantir des performances optimales de Virtual Volumes, suivez ces recommandations.

Directives et limitations lors de l'utilisation de Virtual Volumes

Pour garantir une expérience optimale avec la fonctionnalité Virtual Volumes, vous devez observer des directives spécifiques.

Virtual Volumes prend en charge les capacités, fonctionnalités et produits VMware suivants :

- Avec Virtual Volumes, vous pouvez utiliser des services de stockage avancés, notamment la réPLICATION, le chiffrement, la déduplication et la compression sur des disques virtuels individuels. Contactez votre fournisseur de stockage pour connaître les services qu'il prend en charge avec Virtual Volumes.
- La fonctionnalité Virtual Volumes prend en charge un logiciel de sauvegarde qui utilise vSphere APIs - Data Protection. Les volumes virtuels sont modélisés sur des disques virtuels. Les produits de sauvegarde qui utilisent vSphere APIs - Data Protection sont tout autant pris en charge sur les volumes virtuels qu'ils le sont sur des fichiers VMDK d'un LUN. Les snapshots créés par un logiciel de sauvegarde à l'aide de vSphere APIs - Data Protection sont reconnus comme des snapshots non-vVols par vSphere et le logiciel de sauvegarde.

Note Les Virtual Volumes ne prennent pas en charge le mode de transport SAN. vSphere APIs - Data Protection sélectionne automatiquement une autre méthode de transfert des données.

Pour plus d'informations sur l'intégration à vSphere Storage APIs - Data Protection, consultez votre fournisseur de logiciel de sauvegarde.

- Les Virtual Volumes prennent en charge des fonctionnalités vSphere telles que vSphere vMotion, Storage vMotion, les snapshots, les clones liés et DRS.

- Vous pouvez utiliser des produits de mise en cluster, comme Oracle Real Application Clusters, avec Virtual Volumes. Pour utiliser ces produits, vous activez le paramètre d'écriture multiple d'un disque virtuel stocké sur la banque de données Virtual Volumes.

Pour plus d'informations, reportez-vous à l'article de la base de connaissances à l'adresse <http://kb.vmware.com/kb/2112039>. Pour obtenir une liste des fonctionnalités et des produits pris en charge par la fonction Virtual Volumes, reportez-vous aux *matrices d'interopérabilité des produits VMware*.

Limitations de Virtual Volumes

Améliorez votre expérience de Virtual Volumes en prenant connaissance des limitations suivantes :

- Comme l'environnement Virtual Volumes nécessite vCenter Server, vous ne pouvez pas utiliser Virtual Volumes avec un hôte autonome.
- La fonctionnalité Virtual Volumes ne prend pas en charge les RDM.
- Un conteneur de stockage Virtual Volumes ne peut pas couvrir plusieurs baies physiques. Certains fournisseurs présentent plusieurs baies physiques sous la forme d'une seule baie. Dans ce cas, techniquement, vous continuez d'utiliser une baie logique.
- Les profils d'hôte contenant des banques de données Virtual Volumes sont spécifiques à vCenter Server. Après l'extraction de ce type de profil d'hôte, vous ne pouvez l'attacher qu'à des hôtes et des clusters gérés par le même système vCenter Server que l'hôte de référence. Pour plus d'informations, reportez-vous au document *Configurations maximales*.

Limitations des Virtual Volumes avec NVMe

Les fonctionnalités suivantes ne sont pas prises en charge pour NVMe over Virtual Volumes spécifique à vSphere version 8.0 :

- Opérations de réPLICATION et Site Recovery Manager.
- RÉSERVATIONS NVMe.
- Opérations de désallocation et déMAPPAGE NVMe.
- Partage de disque entre les machines virtuelles.
- Migration NVMe intrabande.

Meilleures pratiques pour le provisionnement de conteneurs de stockage

Suivez ces meilleures pratiques lorsque vous provisionnez des conteneurs de stockage côté baie Virtual Volumes.

Création de conteneurs en fonction de vos limites

Sachant que les conteneurs de stockage appliquent des limites logiques lors du regroupement de volumes virtuels, le conteneur que vous créez doit respecter les limites que vous souhaitez appliquer.

Les exemples peuvent inclure un conteneur créé pour un locataire dans un déploiement à locataires multiples ou un conteneur pour un service dans un déploiement d'entreprise.

- des organismes ou des services, par exemple, un organisme financier ou un service des ressources humaines ;
- Des groupes ou des projets (par exemple, Équipe A et Équipe rouge) ;
- des clients.

Mise de toutes les capacités de stockage dans un conteneur unique

Les conteneurs de stockage sont des banques de données individuelles. Un conteneur de stockage peut exporter plusieurs profils de capacité de stockage. C'est pourquoi des machines virtuelles aux besoins et aux paramètres de stratégie de stockage différents peuvent faire partie d'un même conteneur de stockage.

La modification des profils de stockage doit être une opération côté baie, et non une migration de stockage vers un autre conteneur.

Évitez de sur-provisionner vos conteneurs de stockage

Lorsque vous provisionnez un conteneur de stockage, les limites spatiales que vous appliquez dans le cadre de la configuration du conteneur ne sont que des limites logiques. Ne prévoyez pas un conteneur plus grand que nécessaire pour l'utilisation prévue. Si vous augmentez ultérieurement la taille du conteneur, vous n'aurez besoin ni de le reformater ni de le repartitionner.

Utilisation de l'interface utilisateur de gestion spécifique au stockage pour provisionner des points de terminaison de protocole

Chaque conteneur de stockage a besoin de points de terminaison de protocole (PE) auxquels les hôtes ESXi ont accès.

Lorsque vous utilisez le stockage des blocs, le point de terminaison de protocole représente un LUN proxy défini par un nom WWN de LUN T10. Pour le stockage NFS, le point de terminaison de protocole est un point de montage, tel qu'une adresse IP ou un nom DNS, et un nom de partage. Pour le stockage NVMe, le PE est un groupe ANA et les espaces de noms de proxy sont virtuels.

Généralement, la configuration des points de terminaison de protocole est spécifique à la baie. Lorsque vous configurez des points de terminaison de protocole, vous devez les associer à des processeurs de stockage spécifiques ou à certains hôtes. Pour éviter les erreurs lors de la création de points de terminaison de protocole, ne les configurez pas manuellement. Lorsque cela est possible, utilisez plutôt des outils de gestion spécifiques au stockage.

N'attribuez aucun ID au-dessus de Disk.MaxLUN aux LUN de points de terminaison de protocole

Par défaut, un hôte ESXi peut accéder à des ID de LUN dans la plage comprise entre 0 et 1023. Si l'ID du LUN de point de terminaison de protocole que vous souhaitez configurer est 1024 ou plus, l'hôte peut ignorer le point de terminaison de protocole.

Si votre environnement utilise des ID de LUN supérieurs à 1023, modifiez le nombre de LUN analysés au moyen du paramètre `Disk.MaxLUN`. Reportez-vous à la section [Modifier le nombre de périphériques de stockage analysés](#).

Meilleures pratiques pour les performances de Virtual Volumes

Pour garantir des performances optimales de Virtual Volumes, suivez ces recommandations.

Utilisation de différentes stratégies de stockage de machine virtuelle pour des composants Virtual Volumes individuels

Par défaut, tous les composants d'une machine virtuelle dans l'environnement Virtual Volumes obtiennent une stratégie de stockage de machine virtuelle unique. Cependant, les caractéristiques de performance sont variables entre les différents composants (par exemple, un disque virtuel de base de données et un disque virtuel de journal correspondant). Selon les exigences de performance, vous pouvez attribuer différentes stratégies de stockage de machine virtuelle à des disques virtuels individuels et au fichier de base de machine virtuelle, ou config-vVol.

Lorsque vous utilisez vSphere Client, vous ne pouvez pas modifier l'attribution de stratégie de stockage de machine virtuelle pour swap-vVol, memory-vVol ou snapshot-vVol.

Reportez-vous à la section [Créer une stratégie de stockage de machine virtuelle pour Virtual Volumes](#).

Obtention d'un profil d'hôte avec Virtual Volumes

La meilleure manière d'obtenir un profil d'hôte avec Virtual Volumes consiste à configurer un hôte de référence et à extraire son profil. Si vous modifiez manuellement un profil d'hôte existant dans vSphere Client et que vous attachez le profil modifié à un nouvel hôte, vous risquez de déclencher des erreurs de conformité. D'autres problèmes imprévisibles peuvent également se produire. Pour plus d'informations, reportez-vous à l'article [2146394 de la base de connaissances VMware](#).

Surveillance de la charge d'E/S sur un point de terminaison de protocole individuel

- Toutes les E/S de volume virtuel transitent par des points de terminaison de protocole (PE). Les baies sélectionnent des points de terminaison de protocole à partir de plusieurs points de terminaison de protocole accessibles par un hôte ESXi. Les baies peuvent effectuer un équilibrage de charge et modifier le chemin de liaison qui connecte le volume virtuel au point de terminaison de protocole. Reportez-vous à la section [Liaison et annulation de liaison de Virtual Volumes](#).

- Pour le stockage des blocs, ESXi accorde une grande profondeur de file d'attente à l'E/S en raison d'un nombre potentiellement élevé de volumes virtuels. Le paramètre `Scsi.ScsiVVolPESNRO` contrôle le nombre d'E/S pouvant être mises en file d'attente pour des points de terminaison de protocole. Vous pouvez configurer le paramètre sur la page Paramètres système avancés de vSphere Client.

Surveillance des limites de baie

Une seule machine virtuelle peut occuper plusieurs volumes virtuels. Reportez-vous à la section [Objets de volume virtuel](#).

Supposons que votre machine virtuelle dispose de deux disques virtuels et que vous prenez deux snapshots avec la mémoire. Votre machine virtuelle peut occuper jusqu'à 10 objets Virtual Volumes : un objet config-vVol, un objet swap-vVol, deux objets data-vVol, quatre objets snapshot-vVol et deux objets snapshot-vVol de mémoire.

Garantir que le fournisseur de stockage est disponible

Pour accéder au stockage Virtual Volumes, votre hôte ESXi nécessite un fournisseur de stockage (fournisseur VASA). Il est intégré au microprogramme de la baie de stockage ou déployé en tant que dispositif sous la forme d'une machine virtuelle. Si votre fournisseur VASA est un dispositif basé sur une machine virtuelle, le fournisseur de stockage est toujours disponible. Pour garantir que le fournisseur de stockage est toujours disponible, procédez comme suit :

- Ne migrez pas une machine virtuelle de fournisseur de stockage vers un stockage Virtual Volumes.
- Sauvegardez votre machine virtuelle de fournisseur de stockage.
- Le cas échéant, utilisez vSphere HA ou Site Recovery Manager pour protéger la machine virtuelle du fournisseur de stockage.

Dépannage de Virtual Volumes

Les rubriques de dépannage fournissent des solutions aux problèmes que vous pouvez rencontrer lors de l'utilisation de Virtual Volumes.

- [Virtual Volumes et commandes esxcli](#)

Vous pouvez utiliser les commandes `esxcli storage vvol` pour dépanner votre environnement Virtual Volumes.

- [Collecte d'informations statistiques pour les Virtual Volumes](#)

Vous pouvez utiliser la commande `vvol stats` sur votre hôte ESXi pour suivre les statistiques de performances.

- [La banque de données Virtual Volumes est inaccessible](#)

Après que vous avez créé une banque de données Virtual Volumes, celle-ci reste inaccessible.

- Erreurs lors de la migration de machines virtuelles ou du déploiement d'environnements OVF de machine virtuelle vers des banques de données Virtual Volumes

Les tentatives de migration d'une machine virtuelle ou de déploiement d'un environnement OVF de machine virtuelle vers des banques de données Virtual Volumes ont échoué.

Virtual Volumes et commandes esxcli

Vous pouvez utiliser les commandes `esxcli storage vvol` pour dépanner votre environnement Virtual Volumes.

Les options de commande suivantes sont disponibles.

Tableau 14-1. Commandes esxcli storage vvol

Espace de noms	Option de commande	Description
<code>esxcli storage core device</code>	<code>list</code>	Identifiez les points de terminaison de protocole. L'entrée de sortie <code>Is_VVOL</code> PE: <code>true</code> indique que le périphérique de stockage est un point de terminaison de protocole.
<code>esxcli storage vvol daemon</code>	<code>unbindall</code>	Dissocie tous les volumes virtuels des fournisseurs VASA connus de l'hôte ESXi.
<code>esxcli storage vvol protocolendpoint</code>	<code>list</code>	Répertorie tous les points de terminaison de protocole auxquels votre hôte peut accéder.
<code>esxcli storage vvol storagecontainer</code>	<code>list</code> <code>abandonedvvol scan</code>	Établissez la liste de tous les conteneurs de stockage disponibles. Analysez le conteneur de stockage spécifié pour les volumes virtuels abandonnés.
<code>esxcli storage vvol vasacontext</code>	<code>get</code>	Affichez le contexte VASA (VC UUID) associé à l'hôte.
<code>esxcli storage vvol vasaprovider</code>	<code>list</code>	Établissez la liste de tous les fournisseurs de stockage (VASA) associés à l'hôte.

Collecte d'informations statistiques pour les Virtual Volumes

Vous pouvez utiliser la commande `vvol stats` sur votre hôte ESXi pour suivre les statistiques de performances.

Les options de commande suivantes sont disponibles.

Commande	Description	Options
<code>esxcli storage vvol stats get</code>	Obtenez des statistiques pour tous les fournisseurs VASA (par défaut) ou pour l'espace de noms ou l'entité spécifié(e) dans l'espace de noms donné.	<code>-e --entity= str</code> Entrer l'ID d'entité. <code>-n --namespace= str</code> Entrer l'expression d'espace de noms du noeud. <code>-r --raw</code> Utilisez la sortie au format brut.
<code>esxcli storage vvol stats list</code>	Lister tous les nodes de statistiques (par défaut) ou les nodes sous un espace de noms spécifié.	<code>-n --namespace= str</code> Entrer l'expression d'espace de noms du noeud.
<code>esxcli storage vvol stats enable</code>	Activez le suivi des statistiques pour l'espace de noms complet.	
<code>esxcli storage vvol stats disable</code>	Désactivez le suivi des statistiques pour l'espace de noms complet.	
<code>esxcli storage vvol stats add</code>	Activez le suivi des statistiques pour une entité spécifique sous un espace de noms spécifique.	<code>-e --entity= str</code> Entrer l'ID d'entité. <code>-n --namespace= str</code> Entrer l'expression d'espace de noms du noeud.
<code>esxcli storage vvol stats remove</code>	Supprime une entité spécifique pour le suivi des statistiques sous l'espace de noms spécifié.	<code>-e --entity= str</code> Entrer l'ID d'entité. <code>-n --namespace= str</code> Entrer l'expression d'espace de noms du noeud.
<code>esxcli storage vvol stats reset</code>	Réinitialisez le compteur de statistiques pour l'espace de noms ou l'entité de statistiques spécifiée.	<code>-e --entity= str</code> Entrer l'ID d'entité. <code>-n --namespace= str</code> Entrer l'expression d'espace de noms du noeud.

La banque de données Virtual Volumes est inaccessible

Après que vous avez créé une banque de données Virtual Volumes, celle-ci reste inaccessible.

Problème

vSphere Client affiche la banque de données comme étant inaccessible. Vous ne pouvez pas utiliser la banque de données pour alimenter la machine virtuelle.

Cause

Ce problème peut se produire lorsque vous ne parvenez pas à configurer des points de terminaison de protocole pour le conteneur de stockage SCSI ou les groupes NVMe ANA mappés à la banque de données virtuelle. Comme les LUN traditionnels, les points de terminaison de protocole SCSI doivent être configurés de façon à pouvoir être détectés par un hôte ESXi.

Solution

Avant de créer des banques de données virtuelles pour les conteneurs SCSI, configurez les points de terminaison de protocole côté stockage.

Erreurs lors de la migration de machines virtuelles ou du déploiement d'environnements OVF de machine virtuelle vers des banques de données Virtual Volumes

Les tentatives de migration d'une machine virtuelle ou de déploiement d'un environnement OVF de machine virtuelle vers des banques de données Virtual Volumes ont échoué.

Problème

Un modèle OVF ou une machine virtuelle en cours de migration depuis une banque de données non virtuelle peut inclure des fichiers volumineux supplémentaires, tels que des images disque ISO, des images DVD et des fichiers image. Si ces fichiers supplémentaires causent le dépassement de la limite de 4 Go du volume virtuel de configuration, la migration ou le déploiement vers une banque de données virtuelle échoue.

Cause

Le volume virtuel de configuration, ou config-vVol, contient plusieurs fichiers relatifs aux machines virtuelles. Dans les banques de données traditionnelles et non virtuelles, ces fichiers sont directement stockés dans le répertoire de base de la machine virtuelle. À l'instar du répertoire de base de la machine virtuelle, le config-vVol inclut généralement le fichier de configuration de la machine virtuelle, les fichiers descripteurs du disque virtuel et de snapshot, les fichiers de journaux, les fichiers de verrouillage, etc.

Dans les banques de données virtuelles, tous les autres fichiers volumineux, tels que les disques virtuels, les snapshots de mémoire, les fichiers d'échange et de prétraitement sont stockés sous forme de volumes virtuels séparés.

Les fichiers Config-vVols sont créés sous forme de volumes virtuels de 4 Go. Le contenu générique de config-vVol requiert habituellement uniquement une partie de cette allocation de 4 Go, c'est pourquoi ces fichiers sont généralement provisionnés de façon dynamique, permettant de conserver de l'espace de sauvegarde. Tout fichier volumineux supplémentaire, tel que image ISO, image DVD et fichier image, peut provoquer le dépassement de la limite de config-vVol fixée à 4 Go. Si de tels fichiers sont inclus dans un modèle OVF, le déploiement de l'OVF de machine virtuelle vers un stockage Virtual Volumes échoue. Si ces fichiers font partie d'une machine virtuelle, la migration de celle-ci depuis une banque de données traditionnelle vers un stockage Virtual Volumes échoue également.

Note À partir de vSphere 7.0 Update 2, les partenaires peuvent augmenter la valeur de config-vVol à plus de 4 Go. Collaborez avec votre partenaire Virtual Volumes sur la mise en œuvre de cette option si elle est prise en charge par votre partenaire et applicable à votre environnement.

Solution

- Pour la migration de machine virtuelle. Avant de migrer une machine virtuelle depuis une banque de données traditionnelle vers une banque de données virtuelle, supprimez le contenu superflu du répertoire de base de la machine virtuelle afin que la taille de config-vVol soit inférieure à la limite de 4 Go.

- Pour le déploiement OVF. Comme vous ne pouvez pas déployer de modèle OVF contenant trop de fichiers vers une banque de données virtuelle, déployez d'abord la machine virtuelle vers une banque de données non virtuelle. Supprimez tout contenu superflu du répertoire de base de la machine virtuelle, puis migrez la machine virtuelle résultante vers le stockage Virtual Volumes.

Filtrage des E/S de machines virtuelles

15

Les filtres d'E/S sont des composants logiciels pouvant être installés sur les hôtes ESXi et offrir des services de données supplémentaires aux machines virtuelles. Les filtres traitent les demandes d'E/S, qui transfèrent des données entre le système d'exploitation invité d'une machine virtuelle et les disques virtuels.

Les filtres d'E/S peuvent être proposés par VMware ou créés par des tiers via les API VAO (vSphere APIs for I/O Filtering).

Ce chapitre contient les rubriques suivantes :

- À propos des filtres d'E/S
- Utilisation de périphériques de stockage Flash avec des filtres d'E/S de cache
- Configuration système requise pour les filtres d'E/S
- Configurer des filtres d'E/S dans l'environnement vSphere
- Activer les services de données de filtre d'E/S sur des disques virtuels
- Gestion des filtres d'E/S
- Directives et meilleures pratiques applicables aux filtres d'E/S
- Gestion des incidents d'installation des filtres d'E/S

À propos des filtres d'E/S

Les filtres d'E/S peuvent obtenir un accès direct au chemin d'E/S de la machine virtuelle. Vous pouvez activer le filtre d'E/S au niveau d'un disque virtuel individuel. Les filtres d'E/S sont indépendants de la topologie de stockage.

VMware offre plusieurs catégories de filtres d'E/S. En outre, des fournisseurs tiers peuvent créer les filtres d'E/S. Ils sont généralement distribués en tant que modules qui fournissent un programme d'installation permettant de déployer les composants de filtre sur vCenter Server et des clusters d'hôtes ESXi.

Une fois les filtres d'E/S déployés, vCenter Server configure et enregistre un fournisseur de stockage de filtres d'E/S, également appelé fournisseur VASA, pour chaque hôte du cluster. Le fournisseur de stockage communique avec vCenter Server et rend les services de données offerts par le filtre d'E/S visible dans l'interface Stratégies de stockage VM. Vous pouvez référencer ces services de données lorsque vous définissez des règles communes pour une stratégie de VM. Après avoir associé des disques virtuels à cette stratégie, les filtres d'E/S sont activés sur les disques virtuels.

Prise en charge de banques de données

Les filtres d'E/S peuvent prendre en charge tous les types de banques de données, notamment les suivants :

- VMFS
- NFS 3
- NFS 4.1
- vVol
- vSAN

Types de filtres d'E/S

VMware fournit certaines catégories de filtres d'E/S installés sur vos hôtes ESXi. En outre, les partenaires de VMware peuvent créer les filtres d'E/S au moyen du programme de développeur VAIO (vSphere APIs for I/O Filtering). Les filtres d'E/S peuvent avoir diverses fins.

Les types de filtres pris en charge sont notamment :

- RéPLICATION. Réplique l'ensemble des opérations d'E/S d'écriture vers un emplacement cible externe, comme un hôte ou un cluster différent.
- CHIFFREMENT. Fourni par VMware. Fournit des mécanismes de chiffrement de machines virtuelles. Pour plus d'informations, consultez la documentation *Sécurité vSphere*.
- MISE EN CACHE. Implémente un cache pour les données d'un disque virtuel. Le filtre peut utiliser un périphérique de stockage flash local pour placer les données dans le cache et augmenter les taux d'IOPS et d'utilisation du matériel pour le disque virtuel. Si vous utilisez le filtre de mise en cache, vous pouvez avoir besoin de configurer une ressource Virtual Flash.
- CONTRÔLE D'E/S DE STOCKAGE. Fourni par VMware. Limite la charge d'E/S vers une banque de données et contrôle la quantité d'E/S de stockage allouée à des machines virtuelles pendant des périodes d'encombrement d'E/S. Pour plus d'informations, consultez la documentation *Gestion des ressources vSphere*.

Note Vous pouvez installer plusieurs filtres d'une même catégorie, par exemple la mise en cache, sur votre hôte ESXi. Cependant, vous ne pouvez avoir qu'un seul filtre d'une même catégorie par disque virtuel.

Composants de filtrage d'E/S

Plusieurs composants prennent part au processus de filtrage d'E/S.

Les composants de base de filtrage d'E/S sont les suivants :

VAIO Filter Framework

Une combinaison du monde utilisateur et de l'infrastructure VMkernel fournie par ESXi. Avec l'infrastructure, vous pouvez ajouter des plug-ins de filtre au chemin d'E/S vers et depuis des disques virtuels. L'infrastructure inclut un fournisseur de stockage de filtres d'E/S (fournisseur VASA). Le fournisseur s'intègre à SPBM (Storage Policy Based Management) et exporte les capacités de filtre vers vCenter Server.

Plug-in de filtre d'E/S

Composant logiciel fourni par VMware ou développé par des partenaires de VMware qui intercepte et filtre les données d'E/S en transit entre les disques virtuels et les systèmes d'exploitation invités. Si les partenaires de VMware développent le filtre d'E/S, le filtre peut inclure des composants facultatifs supplémentaires qui aident à sa configuration et à sa gestion.

La figure suivante illustre les composants de filtrage d'E/S et le flux d'E/S entre le système d'exploitation invité et le disque virtuel.



Chaque composant VMX (Virtual Machine Executable) d'une machine virtuelle contient une structure de filtre qui gère les plug-ins de filtre d'E/S attachés au disque virtuel. La structure de filtre appelle des filtres lorsque les demandes d'E/S se déplacent entre le système d'exploitation invité et le disque virtuel. En outre, le filtre intercepte tout accès d'E/S vers le disque virtuel qui se produit à l'extérieur d'une machine virtuelle en cours d'exécution.

Les filtres s'exécutent séquentiellement selon un ordre spécifique. Par exemple, un filtre de réplication s'exécute avant un filtre de cache. Plusieurs filtres peuvent fonctionner sur le disque virtuel, mais un seul par catégorie.

Une fois que la demande d'E/S a été vérifiée par tous les filtres, elle accède à sa destination, à savoir la machine virtuelle ou le disque virtuel.

Du fait que les filtres s'exécutent dans l'espace utilisateur, tout incident lié au filtre impacte la machine virtuelle, mais pas l'hôte ESXi.

Fournisseurs de stockage pour filtres d'E/S

Lorsque des filtres d'E/S sont installés sur des hôtes ESXi, l'infrastructure de filtre d'E/S configure et enregistre un fournisseur de stockage, aussi appelé fournisseur VASA, pour chaque hôte du cluster.

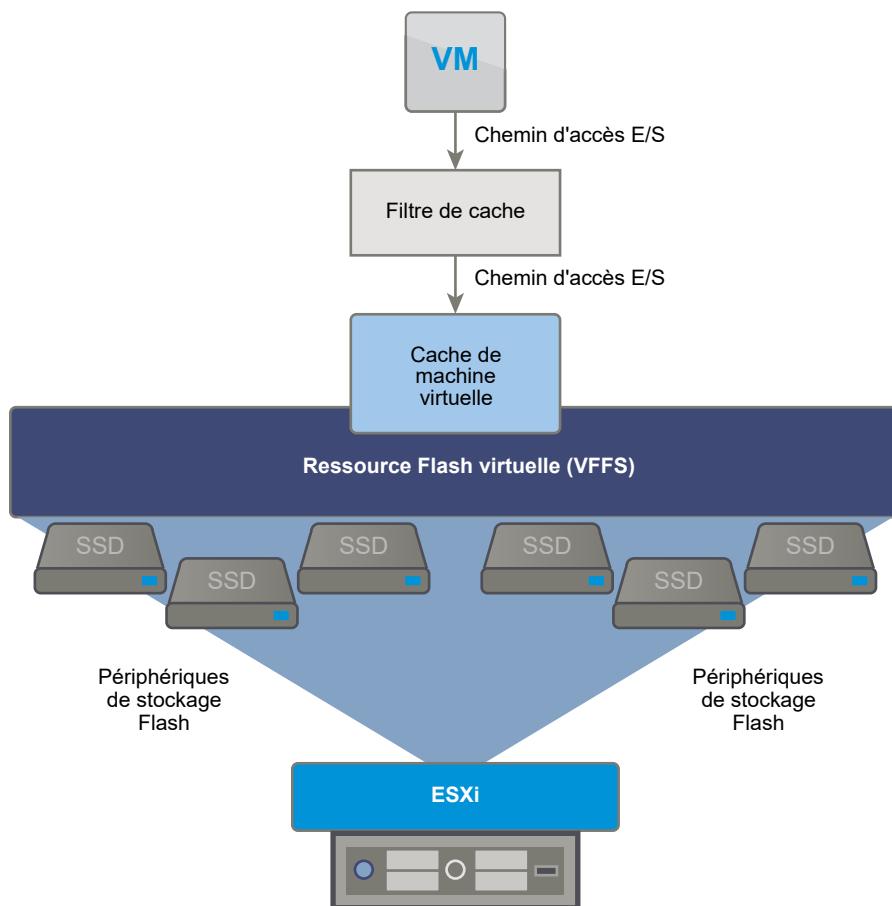
Les fournisseurs de stockage pour filtrage d'E/S sont des composants logiciel fournis par vSphere. Ils s'intègrent au vCenter Server avec les filtres d'E/S et aux capacités de service de données de rapport que les filtres d'E/S prennent en charge.

Les possibilités remplissent l'interface des stratégies de stockage de machine virtuelle et peuvent être référencées dans une stratégie de stockage de machine virtuelle. Vous appliquez ensuite cette stratégie à des disques virtuels afin que les filtres d'E/S puissent traiter les E/S des disques.

Utilisation de périphériques de stockage Flash avec des filtres d'E/S de cache

Un filtre d'E/S de mise en cache peut utiliser un périphérique Flash local pour mettre en cache des données de machine virtuelle.

Si votre filtre d'E/S de mise en cache utilise des périphériques Flash locaux, vous devez configurer une ressource Virtual Flash, également appelée volume VFFS. Vous configurez la ressource sur votre hôte ESXi avant d'activer le filtre. Lorsqu'il traite les E/S en lecture de la machine virtuelle, le filtre crée un cache de la machine virtuelle et le place sur le volume VFFS.



Pour configurer une ressource Virtual Flash, vous utilisez des périphériques Flash connectés à votre hôte. Pour augmenter la capacité de votre ressource Virtual Flash, vous pouvez ajouter des lecteurs Flash supplémentaires. Un lecteur Flash doit être alloué à la ressource Virtual Flash de manière exclusive. Il ne peut pas être partagé avec un autre service vSphere, par exemple vSAN ou VMFS. Reportez-vous à la section [Configurer une ressource Virtual Flash](#).

Configuration système requise pour les filtres d'E/S

Pour pouvoir utiliser des filtres d'E/S dans votre environnement, vous devez respecter des conditions requises spécifiques.

Les conditions requises suivantes s'appliquent.

- Utilisez la dernière version de ESXi et de vCenter Server compatible avec les filtres d'E/S. Les anciennes versions risquent de ne pas prendre en charge les filtres d'E/S ou de ne fournir qu'une prise en charge partielle.
- Vérifiez les conditions requises supplémentaires que des solutions de partenaires individuels peuvent imposer. Dans des cas spécifiques, votre environnement peut nécessiter des périphériques Flash, de la mémoire physique supplémentaire, ou une connectivité réseau et une bande passante. Pour plus d'informations, prenez contact avec votre fournisseur ou votre représentant VMware.
- Serveur Web utilisé pour héberger les modules de partenaires pour l'installation des filtres. Le serveur doit rester disponible après l'installation initiale. Lorsqu'un nouvel hôte joint le cluster, le serveur transmet à l'hôte en mode push les composants de filtre d'E/S.

Configurer des filtres d'E/S dans l'environnement vSphere

Pour configurer les services de données que les filtres d'E/S fournissent pour vos machines virtuelles, suivez plusieurs étapes.

Conditions préalables

- Créez un cluster qui inclut au moins un hôte ESXi.
- Pour plus d'informations sur les filtres d'E/S fournis par des tiers, contactez votre fournisseur ou votre représentant VMware.

Procédure

1 Installer des filtres d'E/S dans un cluster

Si vous utilisez des filtres d'E/S fournis par des tiers, installez les filtres d'E/S dans un cluster d'hôtes ESXi.

2 Afficher les filtres d'E/S et les fournisseurs de stockage

Utilisez vSphere Client pour vérifier les filtres d'E/S disponibles dans votre environnement et vous assurer que les fournisseurs de filtres d'E/S s'affichent comme prévu et sont actifs.

Installer des filtres d'E/S dans un cluster

Si vous utilisez des filtres d'E/S fournis par des tiers, installez les filtres d'E/S dans un cluster d'hôtes ESXi.

Les partenaires de VMware créent des filtres d'E/S au moyen du programme de développeur VAO (vSphere APIs for I/O Filtering).

Les modules de filtre sont distribués sous forme de modules ZIP de bundle de solutions qui peuvent inclure des démons de filtre d'E/S, des bibliothèques de filtres d'E/S, des fournisseurs CIM et d'autres composants associés.

Pour déployer les filtres, vous utilisez généralement des programmes d'installation proposés par des fournisseurs. L'installation est effectuée au niveau du cluster ESXi. Vous ne pouvez pas directement installer les filtres sur des hôtes sélectionnés.

Conditions préalables

- Privilège requis : **Host.Configuration.Query patch**.
- Vérifiez que la solution de filtre d'E/S est certifiée par VMware.

Procédure

- ◆ Exécutez le programme d'installation mis à disposition par le fournisseur.

Le programme d'installation déploie l'extension de filtre d'E/S approprié sur vCenter Server et les composants de filtrage sur tous les hôtes d'un cluster.

Un fournisseur de stockage, également appelé fournisseur VASA, est automatiquement enregistré pour chaque hôte ESXi du cluster. L'inscription automatique réussie du fournisseur de stockage de filtre d'E/S déclenche un événement au niveau de l'hôte. Si les fournisseurs de stockage ne parviennent pas à s'enregistrer automatiquement, le système déclenche des alertes sur les hôtes.

Afficher les filtres d'E/S et les fournisseurs de stockage

Utilisez vSphere Client pour vérifier les filtres d'E/S disponibles dans votre environnement et vous assurer que les fournisseurs de filtres d'E/S s'affichent comme prévu et sont actifs.

Après l'installation d'un filtre d'E/S de tiers, un fournisseur de stockage, également appelé fournisseur VASA, est automatiquement enregistré pour chaque hôte ESXi du cluster.

L'inscription automatique réussie du fournisseur de stockage de filtre d'E/S déclenche un événement au niveau de l'hôte. Si les fournisseurs de stockage ne parviennent pas à s'enregistrer automatiquement, le système déclenche des alertes sur les hôtes.

Procédure

- 1 Vérifiez que les fournisseurs de stockage de filtres d'E/S s'affichent comme prévu et sont actifs.
 - a Accédez à vCenter Server.
 - b Cliquez sur l'onglet **Configurer**, puis cliquez sur **Fournisseurs de stockage**.
 - c Contrôlez les fournisseurs de stockage pour les filtres d'E/S.

Lorsque les fournisseurs de filtres d'E/S sont correctement enregistrés, les possibilités et les services de données que les filtres proposent remplissent l'interface des stratégies de stockage de machine virtuelle.
- 2 Vérifiez que les composants de filtres d'E/S sont répertoriés sur votre cluster et les hôtes ESXi.

Option	Actions
Afficher les filtres d'E/S sur un cluster	a Accédez au cluster. b Cliquez sur l'onglet Configurer . c Sous Configuration , cliquez sur Filtres d'E/S pour vérifier les filtres installés dans le cluster.
Afficher les filtres d'E/S sur un hôte	a Accédez à l'hôte. b Cliquez sur l'onglet Configurer . c Sous Stockage , cliquez sur Filtres d'E/S pour vérifier les filtres installés sur l'hôte.

Activer les services de données de filtre d'E/S sur des disques virtuels

L'activation des services de données fournis par les filtres d'E/S est un processus en deux étapes. Vous créez une stratégie de machine virtuelle basée sur les services de données fournis par les filtres d'E/S et vous attachez ensuite cette stratégie à une machine virtuelle.

Conditions préalables

Pour les filtres d'E/S de mise en cache, configurez la ressource Virtual Flash sur votre hôte ESXi avant d'activer le filtre. Reportez-vous à la section [Configurer une ressource Virtual Flash](#).

Procédure

- 1 Définir une stratégie VM basée sur des services de filtres d'E/S

Assurez-vous que la stratégie de machine virtuelle répertorie les services de données fournis par les filtres d'E/S.

Reportez-vous à la section [Créer une stratégie de stockage de machine virtuelle pour les services de données basés sur l'hôte](#).

2 Attribuer la stratégie de filtre d'E/S à une machine virtuelle

Pour activer les services de données fournis par le filtre d'E/S, associez la stratégie de filtre d'E/S aux disques virtuels. Vous pouvez attribuer la stratégie lorsque vous provisionnez la machine virtuelle.

Reportez-vous à la section [Attribuer la stratégie de filtre d'E/S à des machines virtuelles](#).

Étape suivante

Si vous souhaitez plus tard désactiver le filtre d'E/S pour une machine virtuelle, vous pouvez supprimer les règles de filtrage de la stratégie de stockage de machine virtuelle et réappliquer la stratégie. Reportez-vous à la section [Modifier ou cloner une stratégie de stockage de machine virtuelle](#). Vous pouvez également modifier les paramètres de la machine virtuelle et sélectionner une autre stratégie de stockage qui n'inclut pas le filtre.

Attribuer la stratégie de filtre d'E/S à des machines virtuelles

Pour activer les services de données fournis par les filtres d'E/S, associez la stratégie de filtre d'E/S aux disques virtuels. Vous pouvez attribuer la stratégie lorsque vous créez ou modifiez une machine virtuelle.

Vous pouvez attribuer la stratégie de filtre d'E/S lors du déploiement initial d'une machine virtuelle. Cette rubrique explique comment attribuer la stratégie lors de la création d'une machine virtuelle. Pour plus d'informations sur les autres méthodes de déploiement, consultez la documentation *Administration d'une machine virtuelle vSphere*.

Note Vous ne pouvez pas modifier ni attribuer la stratégie de filtre d'E/S lorsque vous migrez ou clonez une machine virtuelle.

Conditions préalables

Vérifiez que le filtre d'E/S est installé sur l'hôte ESXi où s'exécute la machine virtuelle.

Procédure

- 1 Démarrez le processus de provisionnement de la machine virtuelle et suivez la procédure appropriée.
- 2 Attribuez la même stratégie de stockage à tous les disques et les fichiers de machine virtuelle.
 - a Sur la page **Sélectionner un stockage**, sélectionnez une stratégie de stockage dans le menu déroulant **Stratégie de stockage VM**.
 - b Sélectionnez la banque de données dans la liste des banques de données compatibles, puis cliquez sur **Suivant**.

Cette banque de données devient la ressource de stockage de destination pour le fichier de configuration de la machine virtuelle et pour tous les disques virtuels. La stratégie active également les services de filtre d'E/S pour les disques virtuels.

3 Modifiez la stratégie de stockage VM du disque virtuel.

Utilisez cette option pour activer les filtres d'E/S uniquement pour vos disques virtuels.

- a Sur la page **Personnaliser le matériel**, développez le volet **Nouveau disque dur**.
- b Dans le menu déroulant **Stratégie de stockage VM**, sélectionnez la stratégie de stockage à attribuer au disque virtuel.
- c (Facultatif) Modifiez l'emplacement de stockage du disque virtuel.

Utilisez cette option pour stocker le disque virtuel dans une banque de données autre que celle dans laquelle réside le fichier de configuration de machine virtuelle.

4 Terminez le processus de provisionnement de la machine virtuelle.

Résultats

Une fois la machine virtuelle créée, les stratégies de stockage attribuées et leur état de conformité s'affichent dans l'onglet **Résumé**.

Étape suivante

Vous pouvez modifier l'attribution de stratégie virtuelle ultérieurement. Reportez-vous à la section [Modifier l'attribution d'une stratégie de stockage pour des fichiers et des disques de machine virtuelle](#).

Gestion des filtres d'E/S

Vous pouvez exécuter le programme d'installation mis à disposition par votre fournisseur pour installer, désinstaller ou mettre à niveau les filtres d'E/S.

Lorsque vous travaillez avec les filtres d'E/S, les considérations suivantes s'appliquent :

- vCenter Server utilise ESX Agent Manager (EAM) pour installer et désinstaller les filtres d'E/S. En tant qu'administrateur, ne faites jamais directement appel aux API d'EAM pour les agences EAM créées ou utilisées par vCenter Server. Toutes les opérations liées aux filtres d'E/S doivent passer par les API VIM. Si vous modifiez sans le vouloir une agence EAM créée par vCenter Server, vous devez annuler les modifications. Si vous détruissez sans le vouloir une agence EAM utilisée par des filtres d'E/S, il vous faut faire appel à `Vim.IoFilterManager#uninstallIoFilter` pour désinstaller les filtres d'E/S affectés. Une fois la désinstallation effectuée, procédez à une nouvelle installation.
- Lorsqu'un nouvel hôte rejoint le cluster qui possède des filtres d'E/S, ceux-ci sont déployés sur l'hôte. vCenter Server inscrit le fournisseur de stockage de filtres d'E/S pour l'hôte. Toute modification du cluster est visible dans l'interface de stratégies de stockage de machine virtuelle du vSphere Client.
- Lorsque vous déplacez un hôte hors d'un cluster ou le supprimez de vCenter Server, les filtres d'E/S sont désinstallés de l'hôte. vCenter Server annule l'enregistrement du fournisseur de stockage de filtre d'E/S.

- Si vous utilisez un hôte ESXi sans état, celui-ci peut perdre ses VIB de filtre d'E/S lors d'un redémarrage. vCenter Server vérifie les bundles installés sur l'hôte après le redémarrage et envoie les VIB de filtre d'E/S vers l'hôte si nécessaire.

Désinstaller des filtres d'E/S d'un cluster

Vous pouvez désinstaller des filtres d'E/S déployés dans un cluster d'hôtes ESXi.

Conditions préalables

- Privilèges nécessaires :**Host.Config.Patch**.

Procédure

- 1 Désinstallez le filtre d'E/S en exécutant le programme d'installation mis à disposition par votre fournisseur.

Lors de la désinstallation, un programme d'installation de filtres d'E/S tiers place automatiquement les hôtes en mode de maintenance.

Si la désinstallation est réussie, le filtre et tous les composants qui s'y rapportent sont supprimés des hôtes.

- 2 Vérifiez que les composants de filtre d'E/S sont correctement désinstallés de vos hôtes ESXi. Sélectionnez l'une des méthodes suivantes :

- Exécutez la commande `esxcli software vib list`.
- Affichez les filtres d'E/S dans vSphere Client. Reportez-vous à la section [Afficher les filtres d'E/S et les fournisseurs de stockage](#).

Le filtre désinstallé ne figure plus dans la liste.

Mettre à niveau les filtres d'E/S d'un cluster

Après la mise à niveau de vos hôtes ESXi, utilisez les programmes d'installation proposés par les fournisseurs de filtres d'E/S pour mettre à niveau les filtres d'E/S déployés dans le cluster de l'hôte ESXi.

Une mise à niveau consiste dans la désinstallation des composants de l'ancien filtre et leur remplacement par les composants du nouveau filtre. Pour déterminer si une installation correspond à une mise à niveau, vCenter Server examine le nom et la version des filtres installés. Si le nom du filtre installé correspond au nom du nouveau filtre mais que les versions sont différentes, l'installation est considérée comme une mise à niveau.

Conditions préalables

- Privilèges nécessaires :**Host.Config.Patch**.
- Mettez à niveau vos hôtes vers ESXi 8.0. Si vous utilisez vSphere Lifecycle Manager pour la mise à niveau, reportez-vous à la documentation de *Gestion du cycle de vie des hôtes et des clusters*.

Procédure

- Pour mettre à niveau le filtre, exécutez le programme d'installation mis à disposition par le fournisseur.

Lors de la mise à niveau, un programme d'installation de filtres d'E/S tiers place automatiquement les hôtes en mode de maintenance.

Le programme d'installation identifie les composants de filtre installés et les supprime avant d'installer les nouveaux composants.

- Vérifiez que les composants de filtre d'E/S sont correctement mis à niveau sur vos hôtes ESXi : Sélectionnez l'une des méthodes suivantes :
 - Exécutez la commande `esxcli software vib list`.
 - Affichez les filtres d'E/S dans vSphere Client. Reportez-vous à la section [Afficher les filtres d'E/S et les fournisseurs de stockage](#).

Résultats

Après la mise à niveau, le système remet les hôtes en mode opérationnel.

Directives et meilleures pratiques applicables aux filtres d'E/S

Lorsque vous utilisez les filtres d'E/S dans votre environnement, suivez les directives et meilleures pratiques spécifiques.

- Comme les filtres d'E/S sont indépendants de la banque de données utilisée, tous les types de banques de données, notamment VMFS, NFS, Virtual Volumes et vSAN, sont compatibles avec les filtres d'E/S.
- Les filtres d'E/S prennent en charge les RDM en mode de compatibilité virtuelle. Aucune prise en charge n'est assurée pour les RDM en mode de compatibilité physique.
- Vous ne pouvez pas modifier ni attribuer la stratégie de filtre d'E/S lorsque vous migrez ou clonez une machine virtuelle. Vous pouvez modifier la stratégie après la migration ou le clonage.
- Lorsque vous clonez ou migrez une machine virtuelle avec une stratégie de filtre d'E/S d'un hôte vers un autre, assurez-vous qu'un filtre compatible est installé sur l'hôte de destination. Cette exigence s'applique aux migrations lancées par un administrateur ou par des fonctionnalités telles que HA ou DRS.
- Lorsque vous convertissez un modèle vers une machine virtuelle et que le modèle est configuré avec une stratégie de filtre d'E/S, un filtre d'E/S compatible doit être installé sur l'hôte de destination.

- Si vous utilisez vCenter Site Recovery Manager pour répliquer des disques virtuels, les disques résultants sur le site de récupération n'ont pas les stratégies de filtre d'E/S. Vous devez créer les stratégies de filtre d'E/S sur le site de récupération et les rattacher aux disques répliqués.
- Si une arborescence de snapshot est associée à votre machine virtuelle, vous ne pouvez pas ajouter, modifier ou supprimer la stratégie de filtre d'E/S pour la machine virtuelle.

Migration de machines virtuelles avec des filtres d'E/S

Lors de la migration d'une machine virtuelle avec des filtres d'E/S, des considérations spécifiques s'appliquent.

Si vous utilisez Storage vMotion pour migrer une machine virtuelle avec des filtres d'E/S, une banque de données de destination doit être connectée aux hôtes avec des filtres d'E/S installés.

Il est possible que vous deviez migrer une machine virtuelle avec des filtres d'E/S entre différents types de banques de données (par exemple, entre VMFS et Virtual Volumes). Dans ce cas, assurez-vous que la stratégie de stockage de machine virtuelle inclut des groupes de règles pour chaque type de banque de données que vous prévoyez d'utiliser. Par exemple, si vous migrez votre machine virtuelle entre les banques de données VMFS et Virtual Volumes, il vous faut créer une stratégie de stockage de machine virtuelle mixte incluant les règles suivantes :

- les règles communes pour les filtres d'E/S ;
- l'ensemble de règles 1 pour la banque de données VMFS ; Comme la gestion du stockage basée sur des stratégies n'offre pas de stratégie VMFS explicite, l'ensemble de règles doit contenir des règles basées sur des balises pour la banque de données VMFS.
- Ensemble de règles 2 pour la banque de données Virtual Volumes

Lorsque Storage vMotion migre la machine virtuelle, l'ensemble de règles approprié à la banque de données cible est sélectionné. Les règles relatives au filtre d'E/S ne sont pas modifiées.

Si vous ne spécifiez pas de règles pour des banques de données et définissez uniquement des règles communes pour les filtres d'E/S, le système applique des stratégies de stockage par défaut aux banques de données.

Gestion des incidents d'installation des filtres d'E/S

Normalement, tous les hôtes ESXi d'un cluster possèdent le même ensemble de filtres d'E/S. Parfois, des erreurs peuvent se produire lors de l'installation.

Si l'installation d'un filtre d'E/S échoue sur un hôte, le système génère un événement pour indiquer l'erreur. En outre, sur l'hôte, une alerte précise la cause de l'erreur. Exemples d'erreurs :

- L'URL de VIB n'est pas accessible depuis l'hôte.
- Le format du VIB n'est pas valide.
- Le VIB requiert que l'hôte soit en mode de maintenance lors d'une mise à niveau ou d'une désinstallation.

- Le VIB requiert que l'hôte redémarre après l'installation ou la désinstallation.
- Les tentatives visant à faire passer l'hôte en mode de maintenance ont échoué car la machine virtuelle ne peut pas être évacuée de l'hôte.
- Le VIB requiert une installation ou une désinstallation manuelle.

vCenter Server peut résoudre certains problèmes. Pour d'autres, il se peut que vous deviez intervenir. Par exemple, il est possible que vous deviez modifier l'URL de VIB, évacuer ou mettre hors tension manuellement des machines virtuelles ou encore installer ou désinstaller manuellement des VIB.

Installer les filtres d'E/S sur un hôte ESXi unique

À des fins de dépannage, vous pouvez télécharger un composant ESXi du filtre d'E/S, modularisé dans un fichier VIB, et l'installer sur l'hôte ESXi. Utilisez la commande `esxcli` pour installer le fichier VIB.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- 1 Installez les fichiers VIB en exécutant la commande suivante :

```
esxcli software vib install --depot path_to_VMware_vib_ZIP_file
```

Les options de la commande `install` vous permettent d'effectuer un essai, de spécifier un VIB en particulier, d'outrepasser la vérification de niveau d'acceptation, etc. N'outrepassez pas la vérification sur les systèmes de production. Consultez la documentation de *Référence d'ESXCLI*.

- 2 Pour vérifier que les VIB sont installés sur votre hôte ESXi.

```
esxcli software vib list
```

Accélération matérielle du stockage

16

La fonctionnalité d'accélération matérielle permet à l'hôte ESXi de s'intégrer à des systèmes de stockage conformes. L'hôte peut décharger certaines opérations de gestion de stockage et de machine virtuelle sur les systèmes de stockage. Avec l'assistance matérielle du stockage, votre hôte effectue les opérations plus rapidement et consomme moins de CPU, de mémoire et de bande passante de stockage.

Les périphériques de stockage des blocs ainsi que les périphériques NAS, iSCSI et Fibre Channel prennent en charge l'accélération matérielle.

Pour de plus amples détails, consultez l'article de la base de connaissances VMware à l'adresse <http://kb.vmware.com/kb/1021976>.

Ce chapitre contient les rubriques suivantes :

- [Avantages de l'accélération matérielle](#)
- [Conditions requises pour l'accélération matérielle](#)
- [État de la prise en charge de l'accélération matérielle](#)
- [Accélération pour les périphériques de stockage de blocs](#)
- [Accélération matérielle sur les périphériques NAS](#)
- [Considérations sur l'accélération matérielle](#)

Avantages de l'accélération matérielle

Lorsque la fonctionnalité de l'accélération matérielle est prise en charge, l'hôte peut obtenir une assistance matérielle et effectuer les tâches plus rapidement et plus efficacement.

L'hôte obtient une assistance pour les activités suivante

- Migration des machines virtuelles avec Storage vMotion
- Déploiement des machines virtuelles depuis les modèles
- Clonage des machines virtuelles ou des modèles
- Verrouillage en cluster VMFS et opérations de métadonnées pour les fichiers des machines virtuelles
- Provisionnement statique de disques virtuels

- Création des machines virtuelles tolérant les pannes
- Création et clonage des disques dynamiques sur les banques de données NFS

Conditions requises pour l'accélération matérielle

La fonctionnalité d'accélération matérielle fonctionne uniquement si vous utilisez une association hôte/baie de stockage appropriée.

Tableau 16-1. Conditions requises de stockage pour l'accélération matérielle

ESXi	Pérophériques de stockage des blocs	Pérophériques NAS
ESXi	Prend en charge la norme T10 SCSI ou les plug-ins de stockage des blocs pour l'intégration de la baie (VAAI)	Prend en charge les plug-ins NAS pour l'intégration de la baie

Note Si votre structure de stockage SAN ou NAS utilise un dispositif intermédiaire devant un système de stockage qui prend en charge l'accélération matérielle, le dispositif intermédiaire doit également prendre en charge l'accélération matérielle et être certifié correctement. Le dispositif intermédiaire pourrait être un dispositif de virtualisation du stockage, un dispositif d'accélération E/S, un dispositif de chiffrement, etc.

État de la prise en charge de l'accélération matérielle

Pour chaque périphérique de stockage et banque de données, vSphere Client affiche le statut de prise en charge de l'accélération matérielle.

Les valeurs d'état sont Inconnu, Pris en charge et Non pris en charge. La valeur initiale est Inconnu.

Pour les périphériques de traitement par blocs, le statut passe à Pris en charge après l'opération de déchargement réussie par l'hôte. Si l'opération de déchargement échoue, l'état passe à Non pris en charge. Le statut reste Inconnu si le périphérique assure une prise en charge partielle de l'accélération.

Avec NAS, le statut devient Pris en charge lorsque le stockage peut effectuer au moins une opération de déchargement matériel.

Lorsque les périphériques de stockage ne prennent pas en charge ou assurent une prise en charge partielle des opérations de l'hôte, votre hôte reprend ses méthodes natives pour effectuer des opérations non prises en charge.

Accélération pour les périphériques de stockage de blocs

Avec l'accélération matérielle, votre hôte peut s'intégrer aux périphériques de stockage des blocs, Fibre Channel ou iSCSI, et utiliser des opérations de baie de stockage.

L'accélération matérielle ESXi prend en charge les opérations de baie suivantes :

- Copie intégrale, appelée également blocs de clone ou déchargements de copie. Les baies de stockage peuvent effectuer des copies intégrales de données à l'intérieur de la baie sans que l'hôte ne lise et n'écrive les données. Cette opération permet de réduire le temps et la charge de réseau lors du clonage de machines virtuelles, assurant ainsi le provisionnement depuis un modèle, ou la migration avec vMotion.
- Mise à zéro des blocs (Block zeroing), également appelée commande write same. Les baies de stockage peuvent mettre à zéro un grand nombre de blocs de façon à fournir un nouveau stockage alloué, exempt de données écrites antérieurement. Cette opération permet de réduire le temps et la charge du réseau lors de la création de machines virtuelles et du formatage des disques virtuels.
- Verrouillage assisté par le matériel, également appelé ATS (atomic test and set). Prend en charge le verrouillage de la machine virtuelle discrète sans utiliser les réservations SCSI. Cette opération permet le verrouillage de disque par secteur, au lieu de tout le LUN comme pour les réservations SCSI.

Consultez votre fournisseur concernant la prise en charge de l'accélération matérielle. Certaines baies de stockage exigent que vous activiez la prise en charge du côté stockage.

Sur votre hôte, l'accélération matérielle est disponible par défaut. Si votre stockage ne prend pas en charge l'accélération matérielle. Vous pouvez la désactiver.

Outre la prise en charge de l'accélération matérielle, ESXi inclut la prise en charge du provisionnement dynamique de baie. Pour plus d'informations, consultez [ESXi et provisionnement dynamique de la baie](#).

Désactiver l'accélération matérielle des périphériques de stockage des blocs

Sur votre hôte, l'accélération matérielle des périphériques de stockage des blocs est activée par défaut. Vous pouvez utiliser les paramètres avancés de vSphere Client pour désactiver les opérations d'accélération matérielle.

Comme pour tous les paramètres avancés, avant de désactiver l'accélération matérielle, contactez l'équipe du support VMware.

Procédure

- 1 Dans vSphere Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Configurer**.
- 3 Sous **Système**, cliquez sur **Paramètres système avancés**.
- 4 Pour désactiver l'accélération matérielle, remplacez la valeur de ces options par 0 :
 - VMFS3.HardwareAcceleratedLocking
 - DataMover.HardwareAcceleratedMove

- DataMover.HardwareAcceleratedInit

Gestion de l'accélération matérielle sur les périphériques de stockage des blocs

Pour intégrer les baies de stockage des blocs, vSphere utilise les extensions ESXi appelées Storage APIs - Array Integration (VAAI). Avec cette intégration, vSphere peut utiliser des opérations matérielles de baies.

Dans vSphere 5.x et versions ultérieures, ces extensions sont mises en œuvre par les commandes basées sur la norme SCSI T10. Ainsi, avec les périphériques qui prennent en charge la norme SCSI T10, votre hôte ESXi peut communiquer directement et ne nécessite pas de plug-ins VAAI.

Si le périphérique ne prend pas en charge la norme SCSI T10 ou fournit une prise en charge partielle, ESXi recommence à utiliser les plug-ins VAAI installés sur votre hôte. L'hôte peut également utiliser une combinaison de plug-ins et commandes SCSI T10. Les plug-ins VAAI sont spécifiques au fournisseur et peuvent être développés par VMware ou un partenaire. Pour gérer le périphérique VAAI, votre hôte connecte le filtre VAAI et le plug-in VAAI spécifique au fournisseur au périphérique.

Pour plus d'informations sur la manière de déterminer si votre stockage nécessite les plug-ins VAAI ou prend en charge l'accélération matérielle via les commandes SCSI T10, consultez le *Guide de compatibilité VMware* ou contactez votre fournisseur de stockage.

Vous pouvez utiliser plusieurs commandes `esxcli` pour interroger des périphériques de stockage pour obtenir davantage d'informations sur la prise en charge de l'accélération matérielle. Pour les périphériques qui nécessitent les plug-ins VAAI, les commandes de règle de réclamation sont également disponibles. Pour plus d'informations sur les commandes `esxcli`, reportez-vous à *Démarrage avec ESXCLI*.

Afficher les plug-ins d'accélération matérielle et le filtre

Pour communiquer avec les périphériques qui ne prennent pas en charge la norme SCSI T10, votre hôte utilise un filtre VAAI unique et un plug-in VAAI propre au fournisseur. Utilisez la commande `esxcli` pour afficher le filtre d'accélération matérielle et les plug-ins actuellement chargés sur votre système.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Exécutez la commande `esxcli storage core plugin list --plugin-class=value`.

Pour `value`, entrez l'un des paramètres suivants :

- Tapez `VAAI` pour afficher les plug-ins.

Le résultat de cette commande est semblable à ce qui suit :

```
#esxcli storage core plugin list --plugin-class=VAAI
Plugin name      Plugin class
VMW_VAAIP_EQL   VAAI
VMW_VAAIP_NETAPP VAAI
VMW_VAAIP_CX    VAAI
```

- Tapez `Filter` pour afficher le filtre.

Le résultat de cette commande est semblable à ce qui suit :

```
esxcli storage core plugin list --plugin-class=Filter
Plugin name  Plugin class
VAAI_FILTER  Filter
```

Vérification de l'état de prise en charge de l'accélération matérielle

Utilisez la commande `esxcli` pour vérifier le statut de prise en charge de l'accélération matérielle d'un périphérique de stockage particulier.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Exécutez la commande `esxcli storage core device list -d=device_ID`.

La sortie indique le statut de l'accélération matérielle, ou VAAI, lequel peut être inconnu, pris en charge ou non pris en charge.

```
# esxcli storage core device list -d naa.XXXXXXXXXXXXXX4c
naa.XXXXXXXXXXXXXX4c
Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXXXXX4c)
Size: 20480
Device Type: Direct-Access
Multipath Plugin: NMP
XXXXXXXXXXXXXXXXXX
Attached Filters: VAAI_FILTER
VAAI Status: supported
XXXXXXXXXXXXXXXXXX
```

Vérification des détails de prise en charge de l'accélération matérielle

Utilisez la commande `esxcli` pour demander si le périphérique de stockage des blocs fournit la prise en charge de l'accélération matérielle.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Exécutez la commande **esxcli storage core device vaai status get -d=device_ID**.

Si un plug-in VAAI gère le périphérique, le résultat indique le nom du plug-in attaché au périphérique. Le résultat indique également le statut de prise en charge pour chaque primitive basée sur la norme SCSI T10, si disponible. Le résultat apparaît dans l'exemple suivant :

```
# esxcli storage core device vaai status get -d naaXXXXXXXXXXXX4c
naa.XXXXXXXXXXXXX4c
  VAAI Plugin Name: VMW_VAAIP_SYMM
  ATS Status: supported
  Clone Status: supported
  Zero Status: supported
  Delete Status: unsupported
```

Liste de règles de réclamation d'accélération matérielle

Chaque périphérique de stockage des blocs géré par un plug-in VAAI nécessite deux règles de réclamation. Une règle de réclamation spécifie le filtre d'accélération matérielle tandis que l'autre l'accélération matérielle du plug-in pour le périphérique. Vous pouvez utiliser les commandes **esxcli** pour répertorier le filtre d'accélération matérielle et les règles de réclamation du plug-in.

Procédure

- 1 Pour répertorier les règles de réclamation du filtre, exécutez la commande **esxcli storage core claimrule list --claimrule-class=Filter**.

Dans cet exemple, les règles de réclamation du filtre spécifient les périphériques que le filtre VAAI_FILTER réclame.

```
# esxcli storage core claimrule list --claimrule-class=Filter
  Rule Class   Rule   Class      Type    Plugin      Matches          XCOPY Use Array
  Reported Values  XCOPY Use Multiple Segments  XCOPY Max Transfer Size KiB
  Filter        65430  runtime vendor VAAI_FILTER
  vendor=EMC model=SYMMETRIX                         False
  False                      0
  Filter        65430  file     vendor VAAI_FILTER
  vendor=EMC model=SYMMETRIX                         False
  False                      0
  Filter        65431  runtime vendor VAAI_FILTER
  vendor=DGC model=*                                False
  False                      0
  Filter        65431  file     vendor VAAI_FILTER
  vendor=DGC model=*                                False
  False                      0
```

- 2 Pour répertorier les règles de réclamation du plug-in VAAI, exécutez la commande **esxcli storage core claimrule list --claimrule-class=VAAI**.

Dans cet exemple, les règles de réclamation VAAI spécifient les périphériques que le plug-in VAAI réclame.

```
esxcli storage core claimrule list --claimrule-class=VAAI
Rule Class    Rule Class   Type     Plugin      Matches          XCOPY Use
Array Reported Values  XCOPY Use Multiple Segments  XCOPY Max Transfer Size Kib
VAAI          65430    runtime vendor  VMW_VAAIP_SYMM
vendor=EMC model=SYMMETRIX                         False
False                      0
VAAI          65430    file     vendor  VMW_VAAIP_SYMM
vendor=EMC model=SYMMETRIX                         False
False                      0
VAAI          65431    runtime vendor  VMW_VAAIP_CX
vendor=DGC model=*                                False
False                      0
VAAI          65431    file     vendor  VMW_VAAIP_CX
vendor=DGC model=*                                False
False                      0
```

Ajout de règles de réclamation d'accélération matérielle

Pour configurer l'accélération matérielle pour une nouvelle baie, ajoutez deux règles de réclamation, une pour le filtre VAAI et une autre pour le plug-in VAAI. Pour activer les nouvelles règles de réclamation, définissez d'abord les règles, puis chargez-les sur votre système.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes esxcli dans ESXi Shell.

Procédure

- Définissez une nouvelle règle de réclamation pour le filtre VAAI en exécutant la commande **esxcli storage core claimrule add --claimrule-class=Filter --plugin=VAAI_FILTER**.
- Définissez une nouvelle règle de réclamation pour le plug-in VAAI en exécutant la commande **esxcli storage core claimrule add --claimrule-class=VAAI**.
- Chargez les deux règles de réclamation en exécutant les commandes suivantes :


```
esxcli storage core claimrule load --claimrule-class=Filter
esxcli storage core claimrule load --claimrule-class=VAAI
```

- 4 Exécutez la règle de réclamation du filtre VAAI à l'aide de la commande `esxcli storage core claimrule run --claimrule-class=Filter`.

Note Seules les règles de classe de filtre doivent être exécutées. Lorsque le filtre VAAI réclame un périphérique, il trouve automatiquement le bon plug-in VAAI auquel se relier.

Exemple : Définition des règles de réclamation d'accélération matérielle

Cet exemple montre comment configurer l'accélération matérielle pour les baies IBM à l'aide du plug-in VMW_VAAIP_T10. Utilisez la séquence de commandes suivante. Pour plus d'informations sur les options utilisées par cette commande, consultez [Ajout de règles de réclamation de gestion multivoie](#).

```
# esxcli storage core claimrule add --claimrule-class=Filter --
plugin=VAAI_FILTER --type=vendor --vendor=IBM --autoassign
# esxcli storage core claimrule add --claimrule-class=VAAI --
plugin=VMW_VAAIP_T10 --type=vendor --vendor=IBM --autoassign
# esxcli storage core claimrule load --claimrule-class=Filter
# esxcli storage core claimrule load --claimrule-class=VAAI
# esxcli storage core claimrule run --claimrule-class=Filter
```

Configurer les paramètres XCOPY

XCOPY est une des primitives de VAAI qui est utilisée pour le déchargement des tâches dans la baie de stockage. Par exemple, vous pouvez utiliser XCOPY pour décharger des opérations telles que la migration ou le clonage de machines virtuelles vers la baie plutôt que de consommer des ressources vSphere pour effectuer ces tâches.

Vous pouvez utiliser le mécanisme XCOPY avec toutes les baies de stockage qui prennent en charge le plug-in VMW_VAAIP_T10 basé sur SCSI T10 développé par VMware. Pour activer le mécanisme XCOPY, créez une règle de réclamation de la classe VAAI.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Utilisez la commande suivante et entrez les options XCOPY :

```
esxcli storage core claimrule add --claimrule-class=VAAI
```

Pour plus d'informations sur les options utilisées par cette commande, consultez [Ajout de règles de réclamation de gestion multivoie](#).

Option	Description
-al --xcopy-use-array-values	Utilisez les valeurs indiquées par la baie pour les commandes XCOPY.
-s --xcopy-use-multi-segs	Utilisez plusieurs segments pour les commandes XCOPY. Valide uniquement si <code>--xcopy-use-array-values</code> est spécifié.
-m --xcopy-max-transfer-size	Taille maximale de transfert en Mo pour les commandes XCOPY lorsque vous utilisez une taille de transfert différente de celle indiquée par la baie. Valide uniquement si <code>--xcopy-use-array-values</code> est spécifié.
-k --xcopy-max-transfer-size-kib	Taille maximale en Kio de transfert pour les commandes XCOPY lorsque vous utilisez une taille de transfert différente de celle indiquée par la baie. Valide uniquement si <code>--xcopy-use-array-values</code> est spécifié.
-e --extended-xcopy-support	Utilisez la commande XCOPY étendue pour optimiser la copie des données entre des banques de données qui se trouvent dans différentes baies de stockage.

Exemple : Configuration de XCOPY

- ```
esxcli storage core claimrule add -r 914 -t vendor -V XtremIO -M XtremApp -P VMW_VAAIP_T10 -c VAAI -a -s -k 64
```
- ```
# esxcli storage core claimrule add -r 65430 -t vendor -V EMC -M SYMMETRIX -P VMW_VAAIP_SYMM -c VAAI -a -s -m 200
```

Optimiser la copie des données avec le paramètre XCOPY étendu

Le paramètre XCOPY étendu optimise la copie des données entre les banques de données de deux baies différentes. Il vous permet de migrer et de cloner des charges de travail pour décharger XCOPY entre deux baies différentes.

Caractéristiques XCOPY étendues :

- Utilisez une nouvelle option XCOPY étendue dans une règle de réclamation.

```
esxcli storage core claimrule add -t vendor -V fournisseur -M nom de modèle -P
VMW_VAAIP_T10 -c VAAI --autoassign -e
```

Exemple :

```
esxcli storage core claimrule add -t vendor -V DellEMC -M PowerStore -P
VMW_VAAIP_T10 -c VAAI --autoassign -e
```

- L'option XCOPY étendue est prise en charge uniquement sur le plug-in T10.

Procédure

- 1 Utilisez la commande suivante pour vérifier l'état XCOPY étendu.

```
esxcli storage core device vaai status get -d device
```

Exemple :

```
[root@tpp-h127:~] esxcli storage core device vaai status get -d
naa.68ccf098007f554c61148eb1786e6749
naa.68ccf098007f554c61148eb1786e6749
  VAAI Plugin Name: VMW_VAAIP_T10
  ATS Status: supported
  Clone Status: supported
  Zero Status: supported
  Delete Status: supported
  Ex Clone Status: supported"
```

- 2 Activez l'option XCOPY étendue pour la baie de stockage prise en charge.
 - a Vérifiez si le périphérique de plug-in VAAI_FILTER est ajouté.
 esxcli storage core claimrule list -c Filter
 - b Si le terminal n'est pas ajouté pour le plug-in VAAI_FILTER, utilisez la commande suivante.
 esxcli storage core claimrule add -t vendor -V fournisseur -M nom de modèle -P VAAI_FILTER -c Filter --autoassign
 - c Chargez la règle de réclamation VAAI_FILTER.
 esxcli storage core claimrule load -c Filter
 - d Ajoutez la règle de réclamation XCOPY étendue avec le plug-in T10.
 esxcli storage core claimrule add -t vendor -V fournisseur -M nom de modèle -P VMW_VAAIP_T10 -c VAAI --autoassign -e

Note

- La règle de réclamation de l'étape D utilise la taille de transfert ESXi par défaut et un segment unique pour les commandes XCOPY. Pour utiliser des valeurs indiquées par la baie de taille de transfert différente et de plusieurs segments, utilisez les paramètres facultatifs *-a*, *-s*, *-m/-k* avec la commande ci-dessus.
- La configuration XCOPY étendue fonctionne sur différentes baies.
- Ajoutez une règle de réclamation avec des paramètres facultatifs tels que *-a*, *-s* ou *-m/-k* pour les périphériques source et de destination. Dans ce cas, la taille de transfert minimale des baies source et de destination sera prise en compte pour le transfert de données.

Périphérique source :

```
esxcli storage core claimrule add -t vendor -V fournisseur -M nom de modèle
-P VMW_VAAIP_T10 -c VAAI --autoassign -a -s
```

Périphérique de destination :

```
esxcli storage core claimrule add -t vendor -V fournisseur -M nom de modèle
-P VMW_VAAIP_T10 -c VAAI --autoassign -a -s -e
```

- e Chargez le plug-in VAAI_T10.

```
esxcli storage core claimrule load -c VAAI
```

- f Exécutez les options de règle de réclamation récemment ajoutées.

```
esxcli storage core claimrule run --claimrule-class=Filter
```

Suppression de règles de réclamation d'accélération matérielle

Utilisez la commande `esxcli` pour supprimer les règles de réclamation d'accélération matérielle existantes.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Exécutez les commandes suivantes :

```
esxcli storage core claimrule remove -r claimrule_ID --claimrule-
class=Filter

esxcli storage core claimrule remove -r claimrule_ID --claimrule-
class=VAAI
```

Accélération matérielle sur les périphériques NAS

L'accélération matérielle permet aux hôtes ESXi de s'intégrer aux périphériques NAS et d'utiliser plusieurs opérations matérielles fournies par le stockage NAS. L'accélération matérielle utilise des API VAAI (vSphere APIs for Array Integration) pour faciliter la communication entre les hôtes et les périphériques de stockage.

L'infrastructure VAAI NAS prend en charge les deux versions du stockage NFS, à savoir NFS 3 et NFS 4.1.

Le VAAI NAS utilise un ensemble de primitives de stockage pour décharger les opérations de stockage de l'hôte à la baie. La liste suivante indique les opérations NAS prises en charge :

Clone de fichier complet

Prend en charge une capacité du périphérique NAS à cloner des fichiers de disque virtuel. Cette opération est similaire au clonage de blocs VMFS, excepté que les périphériques NAS克隆ent des fichiers entiers au lieu de segments de fichiers. Les tâches qui tirent parti de l'opération de clonage complet de fichiers incluent le clonage de machine virtuelle, Storage vMotion et le déploiement de machines virtuelles à partir de modèles.

Lorsque l'hôte ESXi copie des données avec NAS VAAI, il n'a pas besoin de lire les données du NAS et d'écrire les données sur le NAS. L'hôte envoie simplement la commande copy pour la décharger vers le NAS. Le processus de copie est effectué dans le NAS, ce qui réduit la charge sur l'hôte.

Clone de fichier rapide

Cette opération, également appelée snapshots basés sur la baie ou natifs, décharge la création de snapshots de machines virtuelles et de clones liés sur la baie.

Espace de réserve

Prend en charge une capacité des baies de stockage à allouer de l'espace pour un fichier de disque virtuel au format statique.

En général, lorsque vous créez un disque virtuel sur une banque de données NFS, le serveur NAS détermine la politique d'allocation. La politique d'allocation par défaut sur la plupart des serveurs NAS est dynamique et ne garantit pas le stockage de sauvegarde du fichier. Toutefois, l'opération de réserve d'espace peut demander au périphérique NAS d'utiliser les mécanismes spécifiques au fournisseur pour réserver un espace pour un disque virtuel. Par conséquent, vous pouvez créer des disques virtuels lourds sur la banque de données NFS si le serveur NAS de sauvegarde prend en charge l'opération d'espace de réserve.

Statistiques étendues

Prend en charge la visibilité sur l'utilisation de l'espace pour les périphériques NAS. Cette opération vous permet d'interroger les détails d'utilisation de l'espace pour les disques virtuels sur les banques de données NFS. Les détails incluent la taille d'un disque virtuel et la consommation d'espace du disque virtuel. Cette fonctionnalité est utile pour le provisionnement dynamique.

Avec les périphériques de stockage NAS, l'intégration de l'accélération matérielle est mise en œuvre par le biais de plug-ins NAS spécifiques au fournisseur. Ces plug-ins sont généralement créés par les fournisseurs et sont distribués en tant que modules fournisseur. Aucune règle de réclamation n'est requise pour le fonctionnement des plug-ins.

Plusieurs outils sont disponibles pour l'installation et la mise à jour des compléments NAS. Ils incluent les commandes `esxcli` et vSphere Lifecycle Manager. Pour plus d'informations, reportez-vous à *Mise à niveau de VMware ESXi* et à la documentation *Gestion du cycle de vie des hôtes et des clusters*. Pour les recommandations d'installation et de mise à jour, consultez l'article de la base de connaissances.

Note Les fournisseurs de stockage NAS peuvent fournir des paramètres supplémentaires qui peuvent affecter les performances et le fonctionnement de VAAI. Suivez les recommandations du fournisseur et configurez les paramètres appropriés sur la baie de stockage NAS et ESXi. Pour plus d'informations, reportez-vous à la documentation du fournisseur de stockage.

Activer les snapshots natifs NAS sur des machines virtuelles

Si votre déploiement inclut des baies NAS qui prennent en charge les API vSphere pour l'intégration de baie (VAAI), vous pouvez utiliser la technologie de clonage rapide de fichiers, également appelée snapshots NFS natifs, pour effectuer des snapshots de machine virtuelle. Avec cette technologie, le périphérique NFS copie la machine virtuelle sans que l'hôte ESXi lise ni écrive de données. Cette opération peut réduire le temps et la charge réseau lors de la création de snapshots de VM.

Par défaut, toutes les VM nouvellement créées prennent en charge la technologie de snapshot ESXi traditionnelle. Pour utiliser la technologie de snapshot native NFS, activez-la pour la VM.

Conditions préalables

- Vérifiez que la baie NAS prend en charge l'opération de clonage rapide de fichiers avec le programme VAAI NAS.
- Sur votre hôte ESXi, installez le plug-in NAS spécifique au fournisseur qui prend en charge le clonage rapide de fichiers avec VAAI.
- Suivez les recommandations de votre fournisseur de stockage NAS pour configurer tous les paramètres requis sur la baie NAS et ESXi. Pour plus d'informations, reportez-vous à la documentation du fournisseur de stockage.

Procédure

- 1 Dans vSphere Client, cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
- 2 Cliquez sur l'onglet **Options VM** et développez le menu **Avancé**.
- 3 Cliquez sur **Modifier la configuration** en regard de Paramètres de configuration.
- 4 Configurez le paramètre **`snapshot.alwaysAllowNative`**.

Si le paramètre existe, assurez-vous que sa valeur est définie sur True. Si le paramètre n'est pas présent, ajoutez-le et définissez sa valeur sur True.

Nom	Valeur
<code>snapshot.alwaysAllowNative</code>	True

Note Les machines virtuelles stockées sur des banques de données NFS et configurées avec **`snapshot.alwaysAllowNative`** peuvent rencontrer l'erreur Invalid Disk Chain. Pour plus d'informations, consultez l'article [89923 de la base de connaissances VMware](#).

Considérations sur l'accélération matérielle

Lorsque vous utilisez la fonctionnalité d'accélération matérielle avec ESXi, certaines considérations s'appliquent.

Plusieurs raisons pourraient provoquer l'échec d'une opération accélérée par le matériel.

Pour toute primitive que la baie ne met pas en œuvre, la baie renvoie une erreur. L'erreur déclenche l'hôte ESXi pour tenter de réaliser l'opération en utilisant ses méthodes natives.

Le système de déplacement des données VMFS n'exploite pas les déchargements matériels et utilise plutôt un déplacement de données logicielles dans l'un des cas suivants :

- Les banques de données VMFS source et destination ont différentes tailles de bloc.
- Le type de fichier source est RDM et le type de fichier de destination est non RDM (fichier ordinaire).
- Le type de VMDK source est eagerzeroedthick et le type de VMDK destination est dynamique.
- Le VMDK source ou destination est dans le format fragmenté ou hébergé.
- La machine virtuelle source a un snapshot.
- L'adresse logique et la longueur de transfert dans l'opération demandée ne sont pas alignées selon l'alignement minimum requis par le périphérique de stockage. Toutes les banques de données créées avec vSphere Client sont alignées automatiquement.
- Le VMFS a de multiples LUN ou extensions, et ces derniers sont sur différentes baies.

Le clonage matériel entre les baies, même dans la même banque de données VMFS, ne fonctionne pas.

Provisionnement de stockage et récupération d'espace

17

vSphere prend en charge deux modèles de provisionnement de stockage : le provisionnement statique et le provisionnement dynamique.

Provisionnement statique

C'est un modèle traditionnel du provisionnement de stockage. Avec le provisionnement statique, une quantité importante d'espace de stockage est fournie d'avance en prévision des futurs besoins de stockage. Toutefois, l'espace pourrait rester inutilisé et entraîner une sous-utilisation de la capacité de stockage.

Provisionnement dynamique

À la différence du provisionnement statique, cette méthode se base sur une allocation flexible à la demande de l'espace de stockage, ce qui élimine les problèmes de sous-utilisation du stockage . Avec ESXi, vous pouvez utiliser deux modèles de provisionnement dynamique, au niveau de la baie et au niveau du disque virtuel.

Le provisionnement dynamique vous permet de signaler un espace de stockage virtuel plus important que la capacité physique réelle. Cet écart peut entraîner un sur-abonnement de stockage, également appelé surprovisionnement. Lorsque vous utilisez le provisionnement dynamique, surveillez l'utilisation réelle du stockage pour éviter des incidents en cas d'insuffisance d'espace de stockage physique.

Ce chapitre contient les rubriques suivantes :

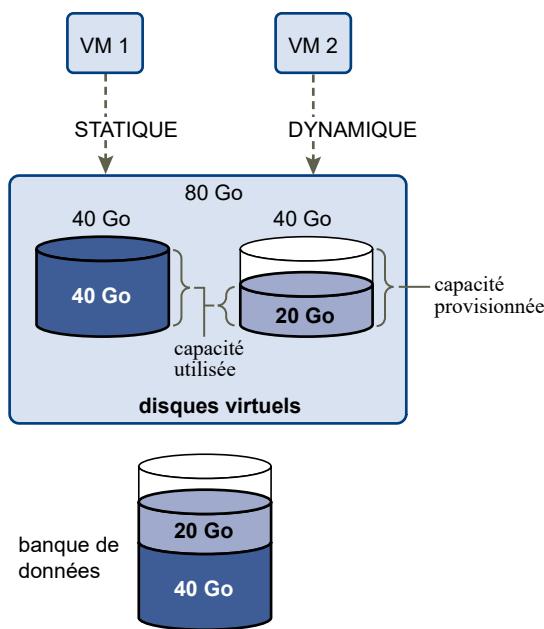
- [Provisionnement dynamique du disque virtuel](#)
- [ESXi et provisionnement dynamique de la baie](#)
- [Récupération d'espace de stockage](#)

Provisionnement dynamique du disque virtuel

Lorsque vous créez une machine virtuelle, une certaine quantité d'espace de stockage sur une banque de données est allouée aux fichiers du disque virtuel.

Par défaut, ESXi offre une méthode de provisionnement classique d'espace de stockage pour les machines virtuelles. Cette méthode vous permet d'estimer la quantité de stockage dont la machine virtuelle aura besoin pour tout son cycle de vie. Ensuite, vous provisionnez une quantité fixe d'espace de stockage au disque virtuel de machine virtuelle à l'avance, par exemple, 40 Go. Tout l'espace provisionné est alloué au disque virtuel. Un disque virtuel qui occupe immédiatement tout l'espace alloué est appelé un disque statique.

ESXi prend en charge le provisionnement dynamique pour les disques virtuels. La fonctionnalité de provisionnement dynamique au niveau du disque vous permet de créer des disques virtuels dans un format dynamique. Pour un disque virtuel dynamique, ESXi alloue tout l'espace requis pour les activités actuelles et futures du disque, par exemple 40 Go. Toutefois, le disque dynamique utilise uniquement l'espace de stockage nécessaire aux opérations initiales du disque. Dans cet exemple, le disque à provisionnement dynamique occupe uniquement 20 Go de stockage. Si le disque a besoin de plus d'espace, il peut s'étendre et occuper son espace alloué de 40 Go.



À propos des règles de provisionnement des disques virtuels

Lorsque vous effectuez certaines opérations de gestion de machines virtuelles, vous pouvez spécifier une stratégie de provisionnement pour le fichier de disque virtuel. Ces opérations sont notamment la création d'un disque virtuel, le clonage d'une machine virtuelle vers un modèle ou la migration d'une machine virtuelle.

Les banques de données NFS avec l'accélération matérielle et les banques de données VMFS prennent en charge les règles de provisionnement de disque suivantes. Dans les banques de données NFS qui ne prennent pas en charge l'accélération matérielle, seul le format dynamique est disponible.

Vous pouvez utiliser Storage vMotion ou Storage vMotion entre hôtes pour convertir les disques virtuels d'un format dans un autre.

Provisionnement statique mis à zéro en différé

Crée un disque virtuel au format épais par défaut. L'espace nécessaire pour le disque virtuel est alloué lors de la création du disque. Les données qui demeurent sur le périphérique physique ne sont pas effacées pendant la création. Elles seront mises à zéro plus tard sur demande, à la première écriture de la machine virtuelle. Les machines virtuelles ne lisent pas les données périmées du disque physique.

Provisionnement statique immédiatement mis à zéro

Un type de disque virtuel statique qui prend en charge des fonctions telles que Fault Tolerance. L'espace nécessaire au disque virtuel est alloué lors de la création. Contrairement au format de provisionnement statique mis à zéro en différé, les données restantes sur le périphérique physique seront remises à zéro lorsque le disque virtuel sera créé. La création de disques virtuels dans ce format peut être plus longue que pour d'autres types de disques. L'augmentation de la taille d'un disque virtuel immédiatement mis à zéro génère un temps de latence important pour la machine virtuelle.

Provisionnement dynamique

Employez ce format pour économiser de l'espace de stockage. Pour le disque dynamique, vous fournissez la quantité d'espace de banque de données dont le disque a besoin, en fonction de la valeur que vous avez indiquée pour la taille de disque virtuel. Toutefois, le disque dynamique démarre avec un petit espace et il utilise au début uniquement l'espace de banque de données dont il a besoin pour ses opérations initiales. Si le disque à approvisionnement en allégé nécessite plus d'espace par la suite, il peut grandir jusqu'à sa capacité maximale et occuper l'intégralité de l'espace de banque de données qui lui a été affecté.

Le provisionnement dynamique est la méthode la plus rapide pour créer un disque virtuel, car il crée un disque qui comprend uniquement les informations d'en-tête. Il n'alloue pas ou ne met pas à zéro les blocs de stockage. Les blocs de stockage sont alloués et mis à zéro au premier accès.

Note Si un disque virtuel est compatible avec des solutions de mise en cluster, telles que Fault Tolérance, ne créez pas un disque fin.

Création de disques virtuels alloués dynamiquement

Pour économiser de l'espace de stockage, vous pouvez créer un disque virtuel dans un format alloué dynamiquement. Ce disque virtuel alloué dynamiquement démarre avec une petite taille et se développe au fur et à mesure que de l'espace disque est nécessaire. Vous pouvez créer des disques alloués dynamiquement uniquement sur les banques de données qui prennent en charge le provisionnement dynamique au niveau du disque.

Cette procédure suppose que vous créez une nouvelle machine virtuelle. Pour plus d'informations, reportez-vous à la documentation *Administration d'une machine virtuelle vSphere*.

Procédure

- 1 Créez une machine virtuelle.
 - a Cliquez avec le bouton droit sur n'importe quel objet de l'inventaire valide comme objet parent d'une machine virtuelle (un centre de données, un dossier, un cluster, un pool de ressources ou un hôte, par exemple) et sélectionnez **Nouvelle machine virtuelle**.
 - b Sélectionnez **Créer une nouvelle machine virtuelle** et cliquez sur **Suivant**.
 - c Suivez les étapes requises pour créer une machine virtuelle.
- 2 Configurez le disque virtuel dynamique.
 - a Sur la page Personnaliser le matériel, cliquez sous l'onglet **Matériel virtuel**.
 - b Cliquez sur le triangle **Nouveau disque dur** pour développer les options du disque dur.
 - c (Facultatif) Ajustez la taille du disque par défaut.

Avec un disque virtuel à provisionnement léger, la valeur de la taille du disque indique l'espace provisionné et garanti sur le disque. Dans un premier temps, le disque virtuel peut ne pas utiliser tout l'espace alloué. La valeur d'utilisation du stockage réelle peut être inférieure à la taille du disque virtuel.
 - d Sélectionnez **Provisionnement dynamique** pour provisionner le disque.
- 3 Terminez la création de la machine virtuelle.

Résultats

Vous avez créé une machine virtuelle avec un disque au format alloué dynamiquement.

Étape suivante

Si vous avez créé un disque virtuel au format alloué dynamiquement, vous pouvez l'agrandir à sa taille totale ultérieurement.

Affichage des ressources de stockage des machines virtuelles

Vous pouvez consulter comment l'espace de stockage est alloué pour vos machines virtuelles.

Procédure

- 1 Accédez à la machine virtuelle.
- 2 Double-cliquez sur la machine virtuelle et cliquez sur l'onglet **Résumé**.
- 3 Vérifiez les informations d'utilisation de stockage dans la zone supérieure droite de l'onglet **Résumé**.

Résultats

L'**utilisation du stockage** affiche l'espace de banque de données réellement occupé par les fichiers de la machine virtuelle, y compris les fichiers de configuration et journaux, les snapshots, les disques virtuels, etc. Lorsque la machine virtuelle est en fonctionnement, l'espace de stockage utilisé comprend également les fichiers d'échange.

Pour les machines virtuelles avec des disques alloués dynamiquement, la valeur réelle d'utilisation du stockage peut être inférieure à la taille du disque virtuel.

Déterminer le format de disque d'une machine virtuelle

Vous pouvez déterminer si votre disque virtuel est au format dynamique ou épais.

Procédure

- 1 Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
- 2 Cliquez sur l'onglet **Matériel Virtuel**.
- 3 Cliquez sur le triangle **Disque dur** pour développer les options du disque dur.
La zone de texte **Type** affiche le format de votre disque virtuel.

Étape suivante

Si votre disque virtuel est au format dynamique, vous pouvez le gonfler à la taille normale.

Gonfler les disques virtuels dynamiques

Vous pouvez transformer un disque virtuel que vous avez créé au format dynamique en disque virtuel statique.

Pour gonfler le disque virtuel dynamique, vous devez utiliser le navigateur de banque de données.

Conditions préalables

- Assurez-vous que la banque de données sur laquelle réside la machine virtuelle offre suffisamment d'espace.
- Assurez-vous que le disque virtuel est dynamique.
- Supprimez les snapshots.
- Mettez la machine virtuelle hors tension.

Procédure

- 1 Dans vSphere Client, accédez au dossier du disque virtuel que vous souhaitez gonfler.
 - a Accédez à la machine virtuelle.
 - b Cliquez sur l'onglet **Banques de données**.
La banque de données sélectionnée stockant les fichiers de machine virtuelle est répertoriée.
 - c Cliquez avec le bouton droit sur la banque de données et sélectionnez **Parcourir les fichiers**.
Le navigateur de banque de données affiche le contenu de la banque de données.
- 2 Développez le dossier de la machine virtuelle et accédez au fichier de disque virtuel que vous voulez convertir.
Le fichier possède l'extension `.vmdk` et est marqué de l'icône de disque virtuel ().
- 3 Sélectionnez le fichier de disque virtuel et cliquez sur **Gonfler**.

Note L'option n'est peut-être pas disponible si le disque virtuel est dynamique ou lorsque la machine virtuelle est en cours d'exécution.

Résultats

Le disque virtuel gonflé occupe la totalité de l'espace de banque de données qui lui a été affecté à l'origine.

Traitement du sur-abonnement de banque de données

Comme l'espace alloué pour les disques légers peut être supérieur à l'espace validé, un sur-abonnement de la banque de données peut survenir, ce qui fait que l'espace total alloué pour les disques de la machine virtuelle sur la banque de données est supérieur à la capacité réelle.

Le sur-abonnement peut être possible, car toutes les machines virtuelles à disques légers n'ont généralement pas besoin de tout l'espace de banque de données alloué en même temps.

Cependant, si vous souhaitez éviter le sur-abonnement à la banque de données, vous pouvez configurer une alarme qui vous avertit lorsque l'espace alloué atteint un certain seuil.

Pour plus d'informations sur le réglage des alarmes, consultez la documentation *Gestion de vCenter Server et des hôtes*.

Si vos machines virtuelles nécessitent plus d'espace, l'espace de la banque de données est alloué sur la base du premier arrivé, premier servi. Lorsque la banque de données manque d'espace, vous pouvez ajouter plus de stockage physique et augmenter la banque de données.

Reportez-vous à la section [Augmenter la capacité d'une banque de données VMFS](#).

ESXi et provisionnement dynamique de la baie

Vous pouvez utiliser des baies de stockage à provisionnement dynamique avec ESXi.

L'hôte ESXi s'intègre au stockage basé sur des blocs et effectue ces tâches :

- L'hôte peut reconnaître des LUN à provisionnement dynamique sous-jacents et surveiller leur utilisation de l'espace pour éviter de manquer d'espace physique. L'espace LUN peut changer si, par exemple, votre banque de données VMFS se développe ou si vous utilisez Storage vMotion pour migrer des machines virtuelles vers le LUN à provisionnement dynamique. L'hôte vous avertit des failles dans l'espace LUN physique et des conditions de manque d'espace.
- L'hôte peut exécuter la commande T10 unmap automatique depuis les systèmes d'exploitation invités de VMFS6 et de la machine virtuelle pour récupérer de l'espace inutilisé de la baie. VMFS5 prend en charge une méthode manuelle de récupération d'espace.

Note ESXi ne prend pas en charge l'activation ou la désactivation du provisionnement fin d'un périphérique de stockage.

Configuration requise

Pour utiliser les fonctionnalités de rapport de provisionnement dynamique et de récupération d'espace, respectez ces conditions requises :

- Utilisez une version appropriée d'ESXi.

Tableau 17-1. Versions d'ESXi et prise en charge du provisionnement dynamique

Composants de provisionnement dynamique pris en charge	ESXi 6.0 et versions antérieures	ESXi 6.5 et versions ultérieures
Provisionnement dynamique	Oui	Oui
Commande unmap provenant de VMFS	Manuelle pour VMFS5. Utilisez esxcli storage vmfs unmap.	Automatique pour VMFS6
Commande unmap provenant du système d'exploitation invité	Oui. Prise en charge limitée.	Oui (VMFS6)

- Utilisez les systèmes de stockage qui prennent en charge VAAI (vSphere Storage APIs - Array Integration) basé sur T10, notamment le provisionnement dynamique et la récupération d'espace. Pour plus d'informations, contactez votre fournisseur de stockage et consultez la documentation *Guide de compatibilité VMware*.

Surveillance de l'utilisation de l'espace

La fonctionnalité de l'intégration de provisionnement dynamique vous permet de surveiller l'utilisation de l'espace sur les LUN à provisionnement dynamique et d'éviter de manquer d'espace.

L'exemple de flux suivant démontre l'interaction de l'hôte ESXi et de la baie de stockage qui interagissent pour générer des avertissements de rupture d'espace et de manque d'espace pour un LUN à provisionnement dynamique. Le même mécanisme s'applique lorsque vous utilisez Storage vMotion pour migrer des machines virtuelles au LUN sous-jacent à provisionnement dynamique.

- 1 Grâce aux outils spécifiques de stockage, votre administrateur de stockage assure le provisionnement d'un LUN dynamique et définit un seuil logiciel qui, lorsqu'il est atteint, déclenche une alerte. Cette étape est spécifique au fournisseur.
- 2 À l'aide de vSphere Client, vous créez une banque de données VMFS sur le LUN à provisionnement dynamique. La banque de données s'étend sur toute la taille logique signalée par le LUN.
- 3 Étant donné que l'espace utilisé par la banque de données augmente et atteint le seuil logiciel défini, les actions suivantes ont lieu :
 - a La baie de stockage signale la rupture à votre hôte.
 - b Votre hôte déclenche une alarme d'avertissement pour la banque de données.

Vous pouvez contacter l'administrateur de stockage pour demander plusieurs espaces physiques. Sinon, vous pouvez utiliser Storage vMotion pour évacuer vos machines virtuelles avant que le LUN manque de capacité.
- 4 S'il ne reste plus d'espace pour l'allocation au LUN à provisionnement dynamique, les actions suivantes ont lieu :
 - a La baie de stockage signale un état de manque d'espace à votre hôte.
 - b L'hôte interrompt les machines virtuelles et génère une alarme de manque d'espace.

Vous pouvez résoudre l'état de manque d'espace permanent en demandant plus d'espace physique à l'administrateur de stockage.

Identifier les périphériques de stockage à provisionnement dynamique

Utilisez la commande `esxcli` pour vérifier si un périphérique de stockage particulier est à provisionnement dynamique.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes `esxcli` dans ESXi Shell.

Procédure

- ◆ Exécutez la commande `esxcli storage core device list -d=device_ID`.

Résultats

Le statut de provisionnement dynamique suivant indique que le périphérique est à provisionnement dynamique.

```
# esxcli storage core device list -d naa.XXXXXXXXXXXXXX4c
naa.XXXXXXXXXXXXXX4c
Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXXXXX4c)
Size: 20480
Device Type: Direct-Access
Multipath Plugin: NMP
-----
Thin Provisioning Status: yes
-----
```

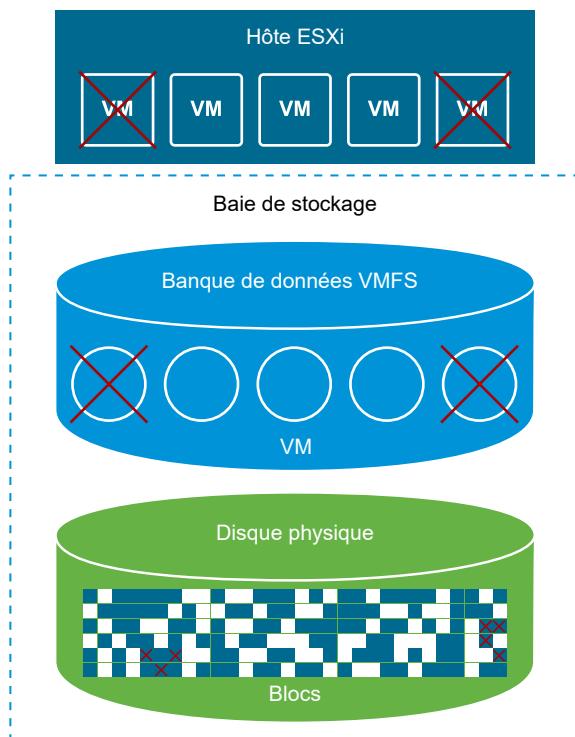
Un statut inconnu indique qu'un périphérique de stockage est statique.

Note Certains systèmes de stockage présentent tous les périphériques comme étant à provisionnement dynamique que les périphériques soient dynamiques ou statiques. Leur statut de provisionnement dynamique est toujours **oui**. Pour plus d'informations, consultez votre fournisseur de stockage.

Récupération d'espace de stockage

ESXi prend en charge la commande de récupération d'espace, également appelée commande unmap SCSI ou commande de désallocation de gestion du jeu de données NVMe, qui est soumise depuis une banque de données VMFS ou un système d'exploitation invité de machine virtuelle. La commande aide les baies de stockage à provisionnement dynamique à récupérer de l'espace inutilisé de la banque de données VMFS et des disques virtuels dynamiques sur la banque de données. La banque de données VMFS6 peut envoyer la commande de récupération d'espace automatiquement. Dans la banque de données VMFS5, vous pouvez récupérer manuellement de l'espace de stockage.

Vous libérez de l'espace de stockage dans la banque de données VMFS lorsque vous supprimez ou migrez la machine virtuelle, consolidez un snapshot, etc. Dans la machine virtuelle, de l'espace de stockage est libéré lorsque vous supprimez des fichiers sur le disque virtuel dynamique. Ces opérations laissent des blocs d'espace inutilisés sur la baie de stockage. Cependant, lorsque la baie ne sait pas que les données ont été supprimées à partir des blocs, ces derniers restent alloués par la baie jusqu'à ce que la banque de données les libère. VMFS utilise la commande SCSI unmap pour indiquer à la baie que les blocs de stockage contiennent des données supprimées, de telle sorte que la baie peut annuler l'allocation de ces blocs.



La commande peut également être soumise directement à partir du système d'exploitation invité. Les banques de données VMFS5 et VMFS6 assurent la prise en charge de la commande unmap soumise depuis le système d'exploitation invité. Cependant, le niveau de prise en charge est limité sur VMFS5.

Selon le type de votre banque de données VMFS, vous utilisez différentes méthodes pour configurer la récupération d'espace pour la banque de données et vos machines virtuelles.

Regardez la vidéo suivante pour en savoir plus sur le fonctionnement de la récupération d'espace.



(Récupération d'espace avec VMFS)

- **Récupération d'espace sur les banques de données VMFS**

La suppression ou le retrait de fichiers d'une banque de données VMFS 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. ESXi prend en charge la récupération d'espace libre, qui est également appelée opération unmap.

- **Demandes de récupération d'espace provenant de systèmes d'exploitation invités**

ESXi prend en charge les commandes unmap soumises directement depuis un système d'exploitation invité pour récupérer de l'espace de stockage. Le niveau de prise en charge et les conditions requises varient selon le type de banque de données où réside votre machine virtuelle.

Récupération d'espace sur les banques de données VMFS

La suppression ou le retrait de fichiers d'une banque de données VMFS 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. ESXi prend en charge la récupération d'espace libre, qui est également appelée opération unmap.

L'opération permet à la baie de stockage de récupérer l'espace libre inutilisé. L'espace non mappé peut ensuite être utilisé pour d'autres demandes d'allocation de stockage et à d'autres besoins.

Récupération automatique d'espace libre sur la banque de données VMFS6

Sur les banques de données VMFS6, ESXi prend en charge la récupération asynchrone automatique d'espace libre. VMFS6 peut exécuter la commande unmap pour libérer de l'espace de stockage libre en arrière-plan sur des baies de stockage à provisionnement dynamique prenant en charge les opérations unmap.

Le traitement automatique de l'opération unmap offre plusieurs avantages :

- Les demandes unmap sont envoyées à un rythme constant, ce qui contribue à éviter une charge instantanée sur la baie de sauvegarde.
- Les régions libérées sont traitée par lots et démappées ensemble.
- Les performances d'E/S des autres charges de travail ne sont pas affectées par la commande unmap.

Dans les banques de données VMFS6, vous pouvez configurer les paramètres de récupération d'espace suivants.

Granularité de récupération d'espace

La granularité définit la taille minimale du secteur de l'espace libéré que le stockage sous-jacent peut récupérer. Le stockage ne peut pas récupérer les secteurs d'une taille inférieure à la granularité spécifiée.

Pour VMFS6, la granularité de la récupération correspond à la taille de bloc. Lorsque vous spécifiez une taille de bloc de 1 Mo, la granularité est également 1 Mo. Les secteurs de stockage d'une taille inférieure à 1 Mo ne sont pas récupérés.

Note Certaines baies de stockage recommandent une granularité de démapping optimale. ESXi prend en charge le traitement unmap automatique sur les baies avec la granularité unmap de 1 Mo ou supérieure, par exemple 16 Mo. Sur les baies disposant d'une granularité optimale de 1 Mo et d'une taille inférieure, l'opération unmap est prise en charge si la granularité présente un facteur de 1 Mo. Par exemple, 1 Mo est divisible par 512 octets, 4 kilo-octets, ou 64 kilo-octets, etc.

Méthode de récupération d'espace

La méthode peut être fixe ou par priorité. Lorsque la priorité est la méthode que vous utilisez, vous configurez le taux de priorité. Pour la méthode fixe, vous devez indiquer le taux de récupération en Mo par seconde.

Vous pouvez utiliser vSphere Client pour définir la méthode de priorité lorsque vous créez la banque de données VMFS6. Pour activer la méthode fixe, vous pouvez modifier ultérieurement les paramètres de récupération d'espace pour la banque de données existante.

Vous pouvez également utiliser la commande `esxcli storage vmfs reclaim config set` pour définir des paramètres de récupération d'espace.

Taux de priorité de récupération d'espace

Ce paramètre définit le rythme auquel l'opération de récupération d'espace est effectuée lorsque vous utilisez la méthode de récupération par priorité. Généralement, VMFS6 peut envoyer les commandes unmap en rafales ou sporadiquement selon la charge de travail et la configuration. Pour VMFS6, vous pouvez spécifier l'une des options suivantes.

Priorité de récupération d'espace	Description	Configuration
Aucun	Désactive les opérations unmap pour la banque de données.	vSphere Client Commande <code>esxcli</code>
Basse (par défaut)	Envoie la commande unmap à un taux moins fréquent (25 à 50 Mo par seconde).	vSphere Client Commande <code>esxcli</code>
Moyen	Envoie la commande à un rythme deux fois plus rapide que le taux faible (50 à 100 Mo par seconde).	Commande <code>esxcli</code>
Haut	Envoie une commande à un rythme trois fois plus rapide que le taux faible (plus de 100 Mo par seconde).	Commande <code>esxcli</code>

Après l'activation de la récupération d'espace, la banque de données VMFS6 peut commencer à libérer les blocs d'espace inutilisé uniquement lorsqu'elle comprend au moins un fichier ouvert. Cette condition peut être remplie lorsque, par exemple, vous mettez sous tension l'une des machines virtuelles sur la banque de données.

Configurer la récupération prioritaire lors de la création d'une banque de données VMFS6

Les paramètres de récupération d'espace contrôlent de quelle manière les blocs supprimés ou non mappés sont récupérés sur les périphériques qui sauvegardent la banque de données. Lorsque vous créez une banque de données VMFS6 dans vSphere Client, la seule méthode de récupération d'espace que vous pouvez spécifier est la méthode de priorité. Vous pouvez également désactiver la récupération d'espace lors de la création de la banque de données.

Procédure

- 1 Dans le navigateur d'objets vSphere Client, accédez à un hôte, à un cluster ou à un centre de données.

- 2 Dans le menu contextuel, sélectionnez **Stockage > Nouvelle banque de données**.
- 3 Suivez les étapes requises pour créer une banque de données VMFS6.
- 4 Sur la page **Configuration de la partition**, spécifiez les paramètres de récupération d'espace.

Ces paramètres permettent de définir la granularité et la priorité avec lesquelles les opérations de récupération d'espace sont effectuées. Vous pouvez également utiliser cette page pour désactiver la récupération d'espace pour la banque de données.

Option	Description
Taille du bloc	Pour une banque de données VMFS, la taille de bloc permet de définir la taille de fichier maximale et la quantité d'espace qu'occupe le fichier. VMFS6 prend en charge la taille de bloc de 1 Mo.
Granularité de récupération d'espace	Spécifiez la granularité de l'opération unmap. La granularité de l'opération unmap équivaut à la taille de bloc, qui est 1 Mo. Les secteurs de stockage d'une taille inférieure à 1 Mo ne sont pas récupérés.
Priorité de récupération d'espace	Sélectionnez l'une des options suivantes. <ul style="list-style-type: none"> ■ Faible (par défaut) Utilisez la méthode de priorité pour la récupération d'espace. L'opération unmap est effectuée avec une faible priorité. ■ Aucune. Sélectionnez cette option si vous ne souhaitez pas utiliser les opérations de récupération d'espace pour la banque de données.

Note Dans vSphere Client, les seuls paramètres disponibles pour la priorité de récupération d'espace sont Basse et Aucune. Pour modifier les paramètres sur Moyenne ou Haute, utilisez la commande esxcli.

- 5 Terminez le processus de création de la banque de données.

Résultats

Après l'activation de la récupération d'espace, la banque de données VMFS6 peut commencer à libérer les blocs d'espace inutilisés uniquement lorsqu'elle comprend au moins un fichier ouvert. Cette condition peut être remplie lorsque, par exemple, vous mettez sous tension l'une des machines virtuelles sur la banque de données.

Configurer la récupération fixe pour la banque de données VMFS6 existante

Pour activer la méthode de récupération fixe, modifiez les paramètres de récupération d'espace de la banque de données.

Procédure

- 1 Dans vSphere Client, accédez à la banque de données.
- 2 Sélectionnez **Modifier la récupération d'espace** dans le menu contextuel.

3 Spécifiez le paramètre de récupération d'espace.

Option	Description
Activer la récupération d'espace automatique au taux fixe	Utilisez la méthode fixe pour la récupération d'espace. Spécifiez le taux de récupération en Mo par seconde. La valeur minimale disponible est de 10 Mo par seconde.
Désactiver la récupération d'espace	Les blocs supprimés ou non mappés ne sont pas récupérés. Sélectionnez cette option si vous souhaitez désactiver les opérations de récupération d'espace pour la banque de données.

- 4 Cliquez sur OK pour enregistrer les nouveaux paramètres.**
- 5 Démontez et remontez la banque de données pour que les modifications prennent effet.**
- Démontage des banques de données.**
 - Monter des banques de données.**
- 6 Répétez cette procédure pour tous les hôtes ESXi qui accèdent à la banque de données.**

Résultats

La valeur modifiée de la priorité de récupération d'espace figure sur la page **Général** pour la banque de données.

Utiliser la commande ESXCLI pour modifier la récupération d'espace sur VMFS6

Vous pouvez modifier la priorité, la granularité et d'autres paramètres par défaut pour la récupération d'espace.

Procédure

- 1 Sur l'hôte ESXi, utilisez la commande suivante pour définir les paramètres de récupération d'espace.**

```
esxcli storage vmfs reclaim config set
```

La commande accepte les options suivantes :

Option	Description
-b --reclaim-bandwidth	Bande passante fixée pour la récupération d'espace en Mo par seconde.
-g --reclaim-granularity	Granularité minimale de la récupération d'espace automatique en octets.
-m --reclaim-method	Méthode de récupération d'espace automatique. Options prises en charge : <ul style="list-style-type: none"> ■ priorité ■ corrigé
-p --reclaim-priority	Priorité de la récupération d'espace automatique. Options prises en charge : <ul style="list-style-type: none"> ■ aucune ■ faible ■ moyenne ■ haute

Option	Description
<code>-l --volume-label</code>	Étiquette du volume VMFS cible.
<code>-u --volume-uuid</code>	UUID du volume VMFS cible.

Vous pouvez utiliser les exemples suivants.

- Définissez la méthode de récupération sur Fixe et le taux sur 100 Mo par seconde.

```
esxcli storage vmfs reclaim config set --volume-label datastore_name --reclaim-method fixed -b 100
```

- Désactivez la récupération automatique d'espace VMFS.

```
esxcli storage vmfs reclaim config set --volume-label datastore_name --reclaim-priority none
```

2 Démontez la banque de données VMFS6 de tous les autres hôtes ESXi sur lesquels elle est montée, puis remontez-la.

- Démontage des banques de données.
- Monter des banques de données.

Cette étape garantit que tous les hôtes ESXi sur lesquels la banque de données VMFS6 a été montée mettent à jour les paramètres de récupération de celle-ci.

Vérifier les paramètres de récupération d'espace automatique sur VMFS6

Après la configuration ou la modification des paramètres de récupération d'espace pour une banque de données VMFS6, vous pouvez vérifier vos paramètres.

Procédure

- Dans vSphere Client, accédez à la banque de données.
- Cliquez sur l'onglet **Configurer**.
- Cliquez sur **Général**.
- Sous **Récupération d'espace**, vérifiez le paramètre pour la priorité de récupération d'espace.

Si vous avez configuré des valeurs via la commande esxcli, une priorité moyenne ou haute pour la récupération d'espace, par exemple, ces valeurs s'affichent également dans vSphere Client.

Résultats

Properties	
Name	Datastore
File system	VMFS 6.82
Drive type	HDD
Capacity	
Total Capacity	15.75 GB
Provisioned Space	1.66 GB
Free Space	14.09 GB
Datastore Capabilities	
Thin Provisioning	Supported
Storage I/O Control	Disabled
Space Reclamation	
Space reclamation	Enabled at fixed rate
Reclamation rate	100 MB/s

Exemple : Obtention des paramètres de récupération d'espace VMFS6

Vous pouvez également utiliser la commande **esxcli storage vmfs reclaim config get -l=VMFS_label | -u=VMFS_uuid** pour obtenir des informations pour la configuration de récupération d'espace.

```
# esxcli storage vmfs reclaim config get -l my_datastore
Reclaim Granularity: 1048576 Bytes
Reclaim Priority: low
```

Récupérer manuellement l'espace de stockage accumulé sur VMFS5

Sur les banques de données VMFS qui ne prennent pas en charge la récupération d'espace automatique, telles que VMFS5, vous pouvez utiliser la commande esxcli pour récupérer manuellement de l'espace de stockage inutilisé.

Lorsque vous utilisez la commande, gardez à l'esprit qu'elle peut envoyer plusieurs demandes unmap à la fois. Cette action peut bloquer une partie des ressources pendant l'opération.

Lorsque vous utilisez la commande, gardez à l'esprit qu'elle peut envoyer plusieurs demandes unmap à la fois. Cette action peut bloquer une partie des ressources pendant l'opération.

Conditions préalables

Installez ESXCLI. Voir *Démarrage avec ESXCLI*. Pour le dépannage, exécutez des commandes esxcli dans ESXi Shell.

Procédure

- Pour récupérer des blocs de stockage inutilisés sur le périphérique à provisionnement dynamique, exécutez la commande suivante :

```
esxcli storage vmfs unmap
```

La commande accepte les options suivantes :

Option	Description
<code>-l --volume-label=volume_label</code>	L'étiquette du volume VMFS à démappeler. Cet argument est obligatoire. Si vous précisez une valeur pour cet argument, n'utilisez pas <code>-u --volume-uuid=volume_uuid</code> .
<code>-u --volume-uuid=volume_uuid</code>	L'UUID du volume VMFS à démappeler. Cet argument est obligatoire. Si vous précisez une valeur pour cet argument, n'utilisez pas <code>-l --volume-label=volume_label</code> .
<code>-n --reclaim-unit=number</code>	Nombre de blocs VMFS à démappeler par itération. Cet argument est facultatif. Si vous ne précisez rien pour cet argument, la commande utilise la valeur par défaut 200.

- 2 Pour vérifier si le processus unmap est terminé, recherchez unmap dans le fichier `vmkernel.log`.

Demandes de récupération d'espace provenant de systèmes d'exploitation invités

ESXi prend en charge les commandes unmap soumises directement depuis un système d'exploitation invité pour récupérer de l'espace de stockage. Le niveau de prise en charge et les conditions requises varient selon le type de banque de données où réside votre machine virtuelle.

Dans la machine virtuelle, de l'espace de stockage est libéré notamment lorsque vous supprimez des fichiers sur le disque virtuel dynamique. Le système d'exploitation invité notifie à VMFS la libération de l'espace en envoyant la commande unmap. La commande unmap envoyée depuis le système d'exploitation invité libère de l'espace dans la banque de données VMFS. La commande poursuit ensuite son action sur la baie de telle sorte que cette dernière puisse récupérer les blocs d'espace libérés.

Récupération d'espace pour les machines virtuelles VMFS6

VMFS6 prend généralement en charge les demandes de récupération d'espace automatique qui sont générées depuis le système d'exploitation invité, puis transmet ces demandes à la baie. De nombreux systèmes d'exploitation invités peuvent envoyer la commande unmap et ne nécessitent pas de configuration supplémentaire. Les systèmes d'exploitation invités qui ne prennent pas en charge les opérations unmap automatiques peuvent nécessiter l'intervention de l'utilisateur. Pour plus d'informations sur les systèmes d'exploitation invités qui prennent en charge la récupération d'espace automatique sur VMFS6, contactez votre fournisseur.

Généralement, les systèmes d'exploitation invités envoient les commandes unmap en fonction de la granularité de l'opération unmap qu'ils annoncent. Pour obtenir des informations détaillées, reportez-vous à la documentation fournie avec votre système d'exploitation invité.

Les éléments à prendre en compte suivants s'appliquent lorsque vous utilisez la récupération d'espace avec VMFS6 :

- VMFS6 traite la demande unmap provenant du système d'exploitation invité uniquement lorsque l'espace à récupérer est égal à 1 Mo ou à un multiple de 1 Mo. Si l'espace est inférieur à 1 MB ou n'est pas un multiple de 1 Mo, les demandes unmap ne sont pas traitées.
- Pour les machines virtuelles avec des snapshots au format SEspars par défaut, VMFS6 prend en charge la récupération d'espace automatique uniquement sur les hôtes ESXi 6.7 ou version ultérieure.

La récupération d'espace affecte uniquement le snapshot supérieur et fonctionne lorsque la machine virtuelle est sous tension.

Récupération d'espace pour les machines virtuelles VMFS5

Généralement, la commande unmap générée depuis le système d'exploitation invité sur VMFS5 ne peut pas être transmise directement à la baie. Vous devez exécuter la commande `esxcli storage vmfs unmap` pour déclencher des opérations unmap pour la baie.

Cependant, pour un nombre limité de systèmes d'exploitation invités, VMFS5 prend en charge les demandes de récupération d'espace automatique.

Pour envoyer les demandes unmap du système d'exploitation invité à la baie, la machine virtuelle doit répondre aux conditions requises suivantes :

- Le disque virtuel doit être dynamiquement provisionné.
- Le matériel de la machine virtuelle doit être de version 11 (ESXi 6.0) ou version ultérieure.
- Le paramètre avancé `EnableBlockDelete` doit être défini sur 1.
- Le système d'exploitation invité doit pouvoir identifier le disque virtuel comme étant dynamique.

Démarrage avec Stockage cloud natif

18

Stockage cloud natif est une solution qui fournit une gestion complète des données pour les applications avec état. Lorsque vous utilisez Stockage cloud natif, vous pouvez créer des applications avec état en conteneur capables de résister à des redémarrages et à des pannes. Les conteneurs avec état exploitent le stockage exposé par vSphere en utilisant des primitives comme le volume standard, le volume permanent et le provisionnement dynamique.

Avec Stockage cloud natif, vous pouvez créer des volumes de conteneur permanents indépendants du cycle de vie de la machine virtuelle et du conteneur. Le stockage vSphere sauvegarde les volumes et vous pouvez définir une stratégie de stockage directement sur les volumes. Après avoir créé les volumes, vous pouvez les examiner ainsi que leurs objets de stockage de sauvegarde dans vSphere Client et surveiller la conformité de leur stratégie de stockage.

vSphere Stockage cloud natif prend en charge les volumes persistants dans les distributions Kubernetes suivantes :

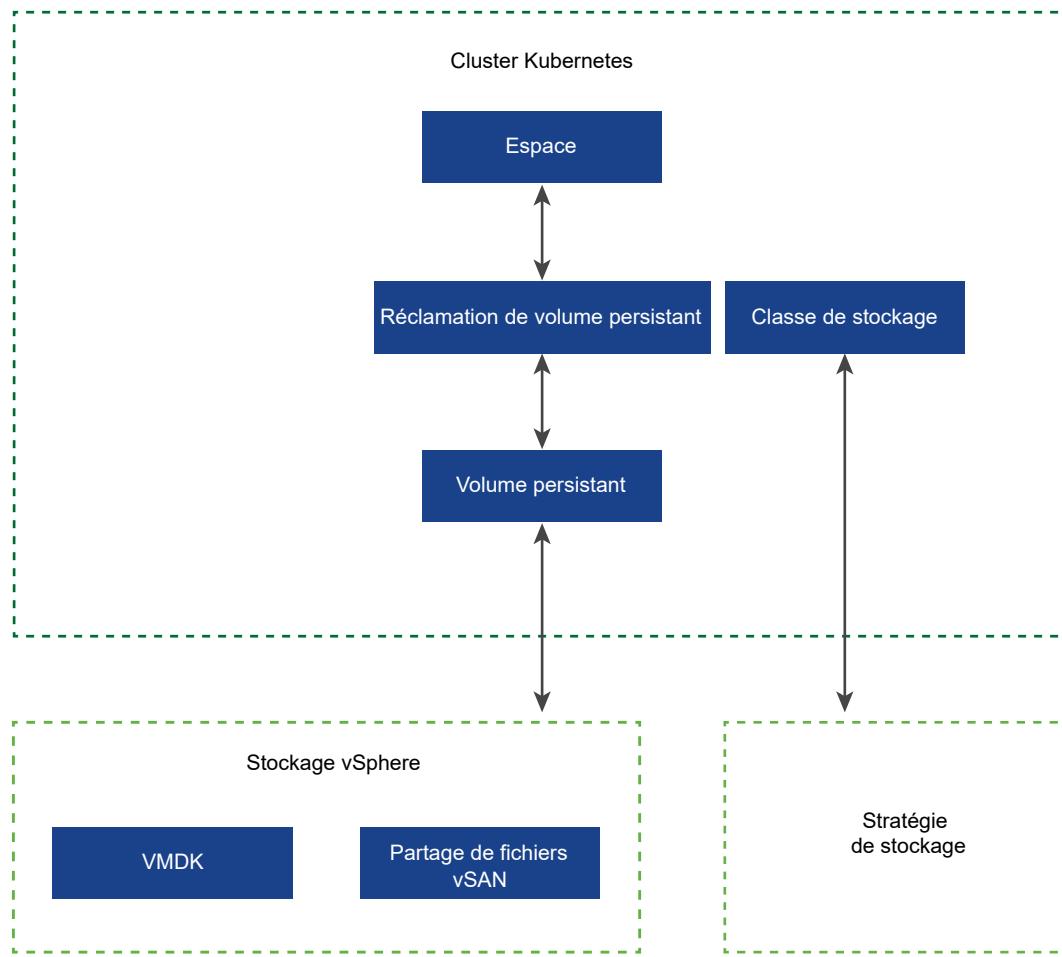
- Kubernetes générique, également appelé version standard, que vous installez à partir des référentiels officiels. La documentation *Stockage vSphere* couvre uniquement les versions Kubernetes génériques.
- vSphere with Tanzu. Pour plus d'informations, consultez la documentation *Concepts et planification de vSphere with Tanzu*.

Ce chapitre contient les rubriques suivantes :

- [Concepts et terminologie du Stockage cloud natif](#)
- [Stockage natif sur le cloud pour les administrateurs vSphere](#)

Concepts et terminologie du Stockage cloud natif

Familiarisez-vous avec plusieurs concepts essentiels à l'environnement vSphere Stockage cloud natif.



Cluster Kubernetes

Dans l'environnement Stockage cloud natif, vous pouvez déployer un cluster Kubernetes générique au sein d'un cluster de machines virtuelles. Au-dessus du cluster Kubernetes, vous déployez vos applications contenant des conteneurs. Les applications peuvent être avec état et sans état.

Note Pour plus d'informations sur un cluster Superviseur et Tanzu Kubernetes Grid que vous pouvez exécuter dans l'environnement vSphere with Tanzu, reportez-vous à la documentation de *Concepts et planification de vSphere with Tanzu*.

Espace

Un espace est un groupe d'un ou de plusieurs applications en conteneur qui partagent des ressources telles que le stockage et le réseau. Les conteneurs à l'intérieur d'un espace sont démarrés, arrêtés et répliqués en tant que groupe.

Orchestrator de conteneur

Plates-formes open source, telles que Kubernetes, pour le déploiement, la mise à l'échelle et la gestion d'applications en conteneur sur des clusters d'hôtes. Les plates-formes fournissent une infrastructure centrée sur les conteneurs.

Application avec état

Puisque les applications en conteneur évoluent de sans état à avec état, elles nécessitent un stockage permanent. Contrairement aux applications sans état qui n'enregistrent pas les données entre les sessions, les applications avec état enregistrent les données dans un stockage permanent. Les données conservées sont appelées l'état de l'application. Vous pouvez ensuite récupérer les données et les utiliser lors de la prochaine session. La plupart des applications sont avec état. Une base de données est un exemple d'application avec état.

PersistentVolume

Les applications avec état utilisent PersistentVolumes pour stocker leurs données. Un PersistentVolume est un volume Kubernetes capable de conserver son état et ses données. Il est indépendant d'un espace et peut continuer à exister même lorsque l'espace est supprimé ou reconfiguré. Dans l'environnement vSphere, les objets PersistentVolume utilisent les disques virtuels vSphere de type FCD (First Class Disk, disque de première classe) ou les partages de fichiers vSAN en tant qu'espace de stockage de sauvegarde. Les disques de première classe sont également appelés disques virtuels améliorés (IVD) ou disques virtuels gérés.

- Les disques virtuels prennent en charge les volumes qui sont montés en tant que ReadWriteOnce. Ces volumes ne peuvent être utilisés que par un seul espace dans Kubernetes.

Vous pouvez utiliser la technologie de chiffrement vSphere pour protéger les disques virtuels FCD qui sauvegardent les volumes persistants. Pour plus d'informations, consultez [Utilisation du chiffrement avec le stockage cloud natif](#).

- Les partages de fichiers vSAN prennent en charge les volumes ReadWriteMany qui sont montés par plusieurs nœuds. Ces volumes peuvent être partagés entre plusieurs espaces ou applications s'exécutant sur des nœuds Kubernetes ou sur des clusters Kubernetes. Pour plus d'informations sur les configurations possibles avec des partages de fichiers, reportez-vous à [Utilisation du service de fichiers vSAN pour provisionner des volumes de fichiers](#).

StorageClass

Kubernetes utilise StorageClass pour définir différents niveaux de stockage et pour décrire différents types d'exigences pour le stockage effectuant la sauvegarde de PersistentVolume. Dans l'environnement vSphere, une classe de stockage peut être liée à une stratégie de stockage. En tant qu'administrateur vSphere, vous créez des stratégies de stockage qui décrivent les différentes exigences de stockage. Les stratégies de stockage de machine virtuelle peuvent être utilisées dans le cadre de la définition de StorageClass pour le provisionnement dynamique de volumes.

L'exemple suivant de fichier YAML référence la stratégie de stockage **Gold** que vous avez créée précédemment à l'aide de vSphere Client. Le VMDK de volume permanent qui en résulte est placé sur une banque de données compatible qui répond aux conditions requises de la stratégie de stockage **Gold**.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: gold-sc
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
  provisioner: csi.vsphere.vmware.com
  parameters:
    storagepolicyname: "Gold"
```

PersistentVolumeClaim

En général, les applications ou les espaces peuvent demander un stockage permanent via un PersistentVolumeClaim. La PersistentVolumeClaim spécifie le type et la classe du stockage, le mode d'accès, ReadWriteOnce ou ReadWriteMany et d'autres paramètres pour le PersistentVolume. La demande peut ensuite provisionner dynamiquement l'objet PersistentVolume correspondant et le disque virtuel sous-jacent ou le partage de fichiers vSAN dans l'environnement vSphere.

Une fois la réclamation créée, le PersistentVolume est automatiquement lié à la réclamation. Les espaces utilisent la réclamation pour monter le PersistentVolume et accéder au stockage.

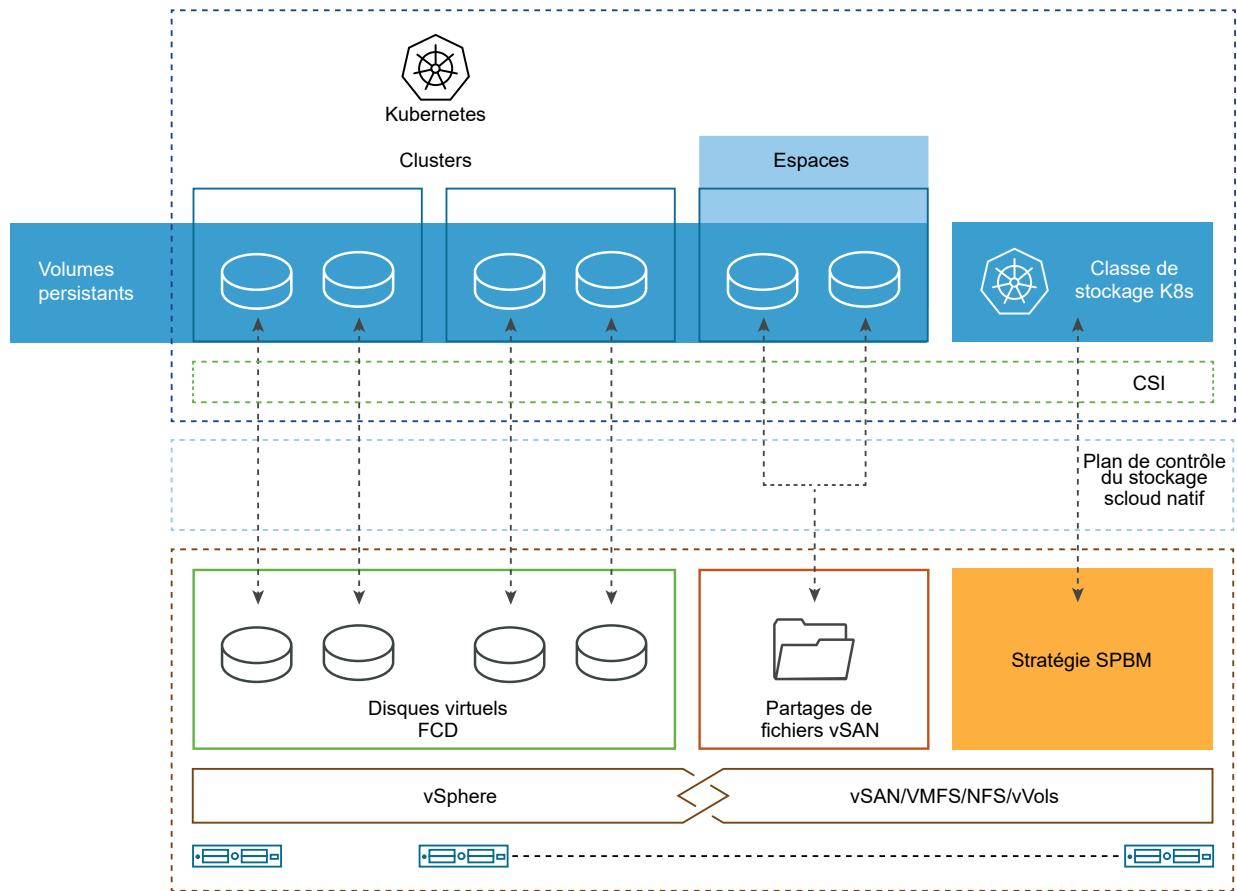
Lorsque vous supprimez cette réclamation, l'objet PersistentVolume correspondant et le stockage sous-jacent sont supprimés.

```
kind: PersistentVolumeClaim
metadata:
  name: persistent-VMDK
spec:
  accessModes:
  - ReadWriteOnce
  resources:
  requests:
    storage: 5Gi
  storageClassName: gold-sc
```

Composants Stockage cloud natif

Le Stockage cloud natif utilise plusieurs composants pour s'intégrer au stockage vSphere.

L'illustration suivante montre comment ces composants interagissent.



Cluster Kubernetes

Dans l'environnement Stockage cloud natif, un cluster Kubernetes générique est déployé sur un cluster de machines virtuelles déployées ou de noeuds qui s'exécutent dans vSphere. Un utilisateur Kubernetes interagit directement avec le cluster lors du déploiement d'applications avec état au-dessus de celui-ci.

Note Pour plus d'informations sur un cluster Superviseur et Tanzu Kubernetes Grid que vous pouvez exécuter dans l'environnement vSphere with Tanzu, reportez-vous à la documentation de *Concepts et planification de vSphere with Tanzu*.

Interface de stockage de conteneur (CSI) pour vSphere

Pour consommer les ressources de l'infrastructure sous-jacente, le cluster requiert un pilote CSI.

vSphere CSI est un plug-in hors arborescence qui expose le stockage vSphere aux charges de travail en conteneur sur les orchestrateurs de conteneurs, tels que Kubernetes. Ce plug-in active vSAN et d'autres types de stockage vSphere.

vSphere CSI communique directement avec le plan de contrôle CNS sur vCenter Server pour toutes les opérations de provisionnement du stockage. vSphere CSI prend en charge les fonctionnalités suivantes :

- Provisionnement dynamique de volumes de conteneur.
- Fonctionnalité de disque de première classe vSphere.
- Zones Kubernetes.
- Montages conventionnels et bruts.
- vCenter Server unique et centres de données et clusters multiples.
- Provisionnement à partir de plusieurs banques de données ou clusters de banques de données.
- Service de fichiers vSAN

Sur Kubernetes, le pilote CSI est utilisé avec l'interface CPI (vSphere Cloud Provider Interface) hors arborescence. Le pilote CSI est fourni en tant qu'image de conteneur et doit être déployé par l'administrateur du cluster. Pour plus d'informations, reportez-vous à la section [Déploiement de pilotes](#) de la documentation du [Pilote Kubernetes vSphere CSI](#).

Pour plus d'informations sur les variantes de CSI utilisées dans un Superviseur et les clusters Tanzu Kubernetes Grid, reportez-vous à la documentation de *Concepts et planification de vSphere with Tanzu*.

Composant serveur du Stockage cloud natif

Le composant du serveur CNS, ou le plan de contrôle CNS, réside dans vCenter Server. Il s'agit d'une extension de la gestion de vCenter Server qui met en œuvre le provisionnement et les opérations de cycle de vie pour les volumes de conteneur.

Lors du provisionnement de volumes de conteneurs, il interagit avec vCenter Server pour créer des objets de stockage dont dépendent les volumes. La fonctionnalité de gestion basée sur une stratégie de stockage garantit un niveau de service requis pour les volumes.

Le stockage cloud natif exécute également des opérations de requête qui vous permettent de gérer et de surveiller les volumes de conteneur et leurs objets de stockage de sauvegarde via l'instance de vCenter Server.

Disque de première classe (FCD)

Également appelé disque virtuel amélioré (IVD) ou disque virtuel géré. Il s'agit d'un disque virtuel nommé qui n'est pas associé à une machine virtuelle. Ces disques résident sur une banque de données vSAN VMFS, NFS ou vVols et sauvegardent des volumes de conteneurs ReadWriteOnce.

La technologie FCD permet d'effectuer des opérations de cycle de vie liées à des volumes persistants en dehors du cycle de vie de la machine virtuelle ou de l'espace. Si la machine virtuelle est un nœud Kubernetes qui exécute plusieurs applications basées sur des conteneurs et utilise des volumes et des disques virtuels persistants pour plusieurs applications, le stockage cloud natif facilite les opérations de cycle de vie à la granularité du conteneur et du volume persistant.

Service de fichiers vSAN

Il s'agit d'une couche de vSAN qui fournit des partages de fichiers. Il prend actuellement en charge les partages de fichiers NFSv3 et NFSv4.1. Stockage cloud natif utilise des partages de fichiers vSAN pour les volumes persistants de type ReadWriteMany. Un seul volume ReadWriteMany peut être monté par plusieurs nœuds. Le volume peut être partagé entre plusieurs espaces ou applications s'exécutant sur des nœuds Kubernetes ou sur des clusters Kubernetes.

Gestion basée sur des stratégies de stockage (SPBM, Storage Policy Based Management)

La gestion basée sur des stratégies de stockage est un service vCenter Server qui prend en charge le provisionnement de volumes permanents selon les conditions requises de stockage spécifiées. Après le provisionnement, le service surveille la conformité du volume avec les caractéristiques de stratégie requises.

Utilisation du service de fichiers vSAN pour provisionner des volumes de fichiers

Le service de fichiers vSAN met en œuvre des partages de fichiers vSAN consommés par des volumes persistants de type ReadWriteMany (RWM). Un seul volume RWM peut être monté par plusieurs nœuds. Le volume peut être partagé entre plusieurs espaces ou applications s'exécutant sur des nœuds Kubernetes ou sur des clusters Kubernetes.

Lorsqu'un espace Kubernetes demande un volume RWM, Stockage cloud natif communique avec le service de fichiers vSAN pour créer un partage de fichiers basé sur NFS de la taille et de la classe de stockage demandées. Stockage cloud natif monte ensuite le volume RWM dans le nœud worker Kubernetes sur lequel l'espace s'exécute. Si plusieurs nœuds demandent l'accès au volume RWM, Stockage cloud natif détermine que le volume RWM existe déjà pour ce déploiement particulier et monte le volume existant dans les nœuds.

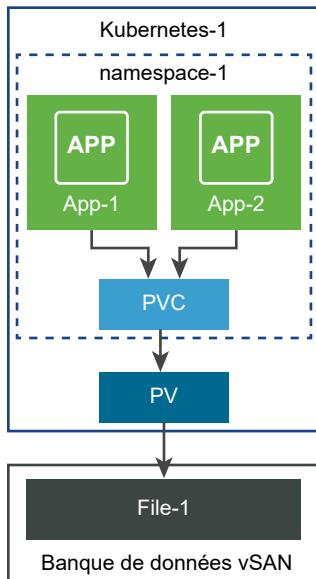
Pour pouvoir prendre en charge les volumes RWM, votre environnement doit inclure les éléments suivants.

- vSphere 7.0 et version ultérieure avec vSAN
- Services de fichiers vSAN activé. Pour plus d'informations, reportez-vous à la section [Service de fichiers vSAN](#) dans la documentation *Administration de VMware vSAN*.
- Kubernetes version 1.14 et version ultérieure.
- Version compatible de CSI. Pour plus d'informations, reportez-vous à la documentation [Plug-in de stockage de conteneur VMware vSphere](#).

Vous pouvez utiliser différentes configurations pour les volumes de fichiers.

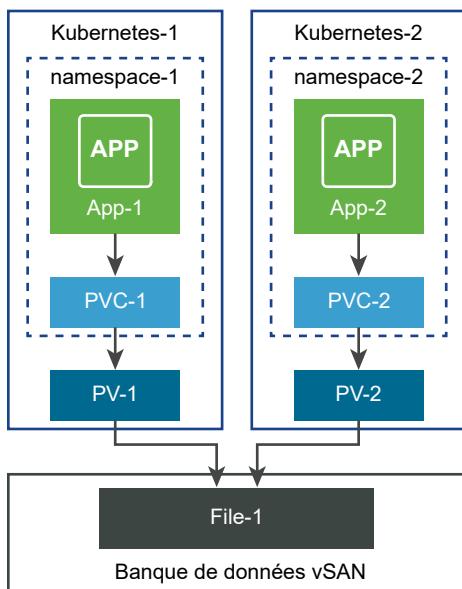
Volume de fichiers unique partagé entre des applications dans le même espace de noms

Dans cet exemple, un volume de fichiers unique est utilisé comme stockage partagé entre différentes applications dans le même espace de noms. Vous utilisez une réclamation de volume persistant unique pour provisionner le volume de fichiers.



Volume de fichiers unique partagé entre des applications et des espaces de noms

Cet exemple utilise un seul volume de fichiers comme stockage partagé entre différentes applications et différents espaces de noms. Pour chaque espace de noms, vous créez une réclamation de volume persistant distincte pour provisionner le même volume de fichiers.



Utilisateurs de Stockage cloud natif

Les types d'utilisateurs impliqués dans le processus de création et de surveillance de volumes Kubernetes dans l'environnement du Stockage cloud natif vSphere sont généralement répartis en deux catégories : les utilisateurs Kubernetes et les administrateurs vSphere. Les deux types d'utilisateurs ont accès à différents outils et effectuent différentes tâches.

Utilisateur Kubernetes CNS

L'utilisateur Kubernetes peut être un développeur Kubernetes et un propriétaire d'application, un administrateur Kubernetes ou combiner des fonctions des deux catégories. Les tâches que l'utilisateur Kubernetes effectue dans l'environnement du Stockage cloud natif sont les suivantes :

- Déployez et gérez vSphere CSI. Pour plus d'informations , reportez-vous à la section [Déploiement du plug-in vSphere Container Storage](#) de la documentation [Démarrage avec le plug-in VMware vSphere Container Storage](#).
- Provisionnez les volumes persistants. Pour plus d'informations sur les volumes de blocs, reportez-vous à la page du [Pilote vSphere CSI - Volume de blocs](#). Pour plus d'informations sur les volumes de fichiers, reportez-vous à la page du [Pilote vSphere CSI - Volume de fichiers](#).
- Exécuter des opérations de cycle de vie pour les volumes permanents.
- Exécuter des opérations de cycle de vie pour les classes de stockage.

Utilisateur vSphere CNS

Un utilisateur vSphere du stockage cloud natif ou un administrateur vSphere a accès à vSphere Client pour effectuer les tâches suivantes :

- Exécuter des opérations de cycle de vie pour les stratégies de stockage de machine virtuelle. Par exemple, créer une stratégie de stockage de machine virtuelle à utiliser pour une classe de stockage Kubernetes et communiquer son nom à l'utilisateur Kubernetes. Reportez-vous à la section [Créer une stratégie de stockage pour Kubernetes](#).
- Utiliser la section Stockage cloud natif de vSphere Client pour surveiller la santé et la conformité de la stratégie de stockage des volumes de conteneur dans les clusters Kubernetes. Reportez-vous à la section [Surveiller les volumes de conteneur entre les clusters Kubernetes](#).

Stockage natif sur le cloud pour les administrateurs vSphere

Un administrateur de vSphere fournit des ressources de stockage à l'équipe Kubernetes et crée des stratégies de stockage de machine virtuelle qui décrivent différentes exigences de stockage et classes de services. Une fois que les charges de travail Kubernetes avec stockage persistant sont provisionnées, l'administrateur vSphere peut surveiller le cycle de vie des ressources de stockage de sauvegarde et leur conformité aux exigences.

Configuration requise de Stockage cloud natif

Votre environnement de Stockage cloud natif et les machines virtuelles qui participent au cluster Kubernetes doivent répondre à plusieurs conditions requises.

Configuration requise d'Stockage cloud natif

- Version compatible de vSphere.
- Une version compatible de Kubernetes.
- Cluster Kubernetes déployé sur les machines virtuelles. Pour plus d'informations sur le déploiement du plug-in vSphere CSI et l'exécution du cluster Kubernetes sur vSphere, reportez-vous à la documentation de [Plug-in VMware vSphere Container Storage](#).

Conditions requises pour les machines virtuelles de cluster Kubernetes

- Machines virtuelles avec la version matérielle 15 ou ultérieure. Installez VMware Tools sur chaque machine virtuelle de nœud.
- Recommandations matérielles pour les machines virtuelles :
 - Définissez la CPU et la mémoire de manière appropriée en fonction des exigences de charge de travail.
 - Utilisez le contrôleur VMware paravirtual SCSI pour le disque principal sur la machine virtuelle du nœud.

- Toutes les machines virtuelles doivent avoir accès à une banque de données partagée, telle que vSAN.
- Définissez le paramètre `disk.EnableUUID` sur chaque machine virtuelle de nœud. Reportez-vous à la section [Configurer des machines virtuelles de cluster Kubernetes](#).
- Pour éviter des erreurs et un comportement imprévisible, ne prenez pas de snapshots des machines virtuelles de nœuds CNS.

Configuration requise pour le volume de fichiers CNS

- Utilisez vSphere version 7.0 ou versions ultérieures avec une version Kubernetes compatible.
- Utilisez une version compatible de CSI. Pour plus d'informations, reportez-vous à la documentation de [VMware vSphere Container Storage Plug-in](#).
- Activez et configuez le service de fichiers vSAN. Vous devez configurer les domaines de service de fichiers, les pools d'adresses IP, le réseau, etc. nécessaires. Pour plus d'informations, reportez-vous à la documentation *Administration de VMware vSAN*.
- Suivez les directives spécifiques pour configurer l'accès réseau depuis un système d'exploitation invité du nœud Kubernetes vers un partage de fichiers vSAN. Reportez-vous à la section [Configuration de l'accès réseau à un partage de fichiers vSAN](#).

Configuration de l'accès réseau à un partage de fichiers vSAN

Pour pouvoir provisionner des volumes persistants `ReadWriteMany` dans votre environnement Kubernetes vSphere générique, configurez les réseaux, les commutateurs et les routeurs nécessaires à partir des nœuds Kubernetes vers le réseau du service de fichiers vSAN.

Configuration du réseau

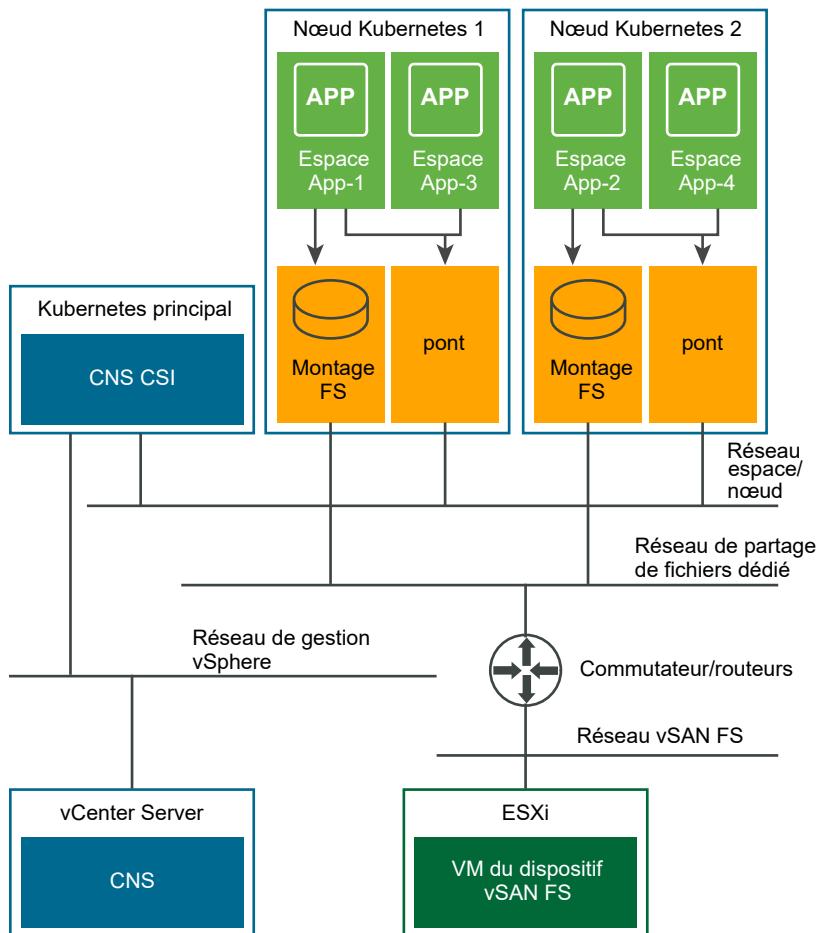
Lors de la configuration des réseaux, respectez les conditions requises suivantes :

- Sur chaque nœud Kubernetes, vous pouvez utiliser une carte réseau virtuelle dédiée au trafic de partage de fichiers vSAN. Cette option est requise uniquement si vous souhaitez utiliser un chemin de trafic de données sécurisé pour vos volumes de fichiers.
- Si vous utilisez une carte réseau virtuelle dédiée, assurez-vous que le trafic via la carte réseau virtuelle dédiée peut être acheminé vers un ou plusieurs réseaux de services de fichiers vSAN.
- Assurez-vous que seul le système d'exploitation invité sur chaque nœud Kubernetes peut accéder directement au partage de fichiers vSAN via l'adresse IP de partage de fichiers. Les espaces du nœud ne peuvent pas effectuer un test ping ou accéder au partage de fichiers vSAN par son adresse IP.

Le pilote du dispositif CNS CSI garantit que seuls les espaces configurés pour utiliser le volume de fichiers CNS peuvent accéder au partage de fichiers vSAN en créant un point de montage dans le système d'exploitation invité.

- Évitez de créer un conflit d'adresses IP entre les machines virtuelles de nœuds et les partages de fichiers vSAN.

L'illustration suivante est un exemple de la configuration du réseau CNS avec le service de partage de fichiers vSAN.



Dans l'illustration, l'exemple de configuration de mise en réseau est conforme à ces directives.

- La configuration utilise des réseaux distincts pour différents éléments dans l'environnement CNS.

Réseau	Description
Réseau de gestion vSphere	Généralement, dans un cluster Kubernetes générique, chaque nœud a accès à ce réseau.
Réseau d'espace ou de nœud	Kubernetes utilise ce réseau pour la communication entre les nœuds ou les espaces.
Réseau de partage de fichiers dédié	Le trafic de données du volume de fichiers CNS utilise ce réseau.
Réseau de partage de fichiers vSAN	Réseau sur lequel le partage de fichiers vSAN est activé et où des partages de fichiers sont disponibles.

- Chaque nœud Kubernetes dispose d'une carte réseau virtuelle dédiée au trafic de fichiers. Cette carte réseau virtuelle est distincte de celle utilisée pour le nœud à des fins de communication entre les espaces et entre les nœuds. Cette configuration est utilisée uniquement à titre d'exemple, mais n'est pas obligatoire.
- Seules les applications configurées pour utiliser le partage de fichiers CNS ont accès aux partages de fichiers vSAN via le point de montage dans le système d'exploitation invité du nœud. Par exemple, dans l'illustration, les actions suivantes sont réalisées :
 - Les espaces App-1 et App-2 sont configurés pour utiliser un volume de fichiers et ont accès au partage de fichiers via le point de montage créé par le pilote CSI.
 - Les espaces App-3 et App-4 ne sont pas configurés avec un volume de fichiers et ne peuvent pas accéder aux partages de fichiers.
- Les partages de fichiers vSAN sont déployés en tant que conteneurs dans une machine virtuelle du dispositif de partage de fichiers vSAN sur l'hôte ESXi. Un système de déploiement Kubernetes, c'est-à-dire un logiciel ou un service pouvant configurer, déployer et gérer des clusters Kubernetes, configure les routeurs et les commutateurs nécessaires de sorte que le système d'exploitation invité dans le nœud Kubernetes puisse accéder aux partages de fichiers vSAN.

Limitations de sécurité

Bien que les cartes réseau virtuelles dédiées empêchent un espace non autorisé d'accéder directement aux partages de fichiers, il existe certaines limitations de sécurité :

- La fonctionnalité du fichier CNS part du principe qu'un utilisateur disposant de l'ID de volume de fichiers CNS est un utilisateur autorisé du volume. Tout utilisateur disposant de l'ID de volume de fichiers CNS peut accéder aux données stockées dans le volume.
- Le volume de fichiers CNS prend uniquement en charge l'authentification AUTH_SYS, qui est une authentification basée sur l'ID d'utilisateur. Pour protéger l'accès aux données du volume de fichiers CNS, vous devez utiliser les ID d'utilisateur appropriés pour les conteneurs accédant au volume de fichiers CNS.
- Un volume persistant ReadWriteMany non lié faisant référence à un volume de fichiers CNS peut être lié par une réclamation de volume persistant créée par n'importe quel utilisateur Kubernetes sous n'importe quel espace de noms. Assurez-vous que seuls les utilisateurs autorisés ont accès à Kubernetes pour éviter les problèmes de sécurité.

Configuration du pilote CSI pour accéder aux clusters de services de fichiers vSAN

En fonction de la configuration, le pilote CSI peut provisionner des volumes de fichiers sur un ou plusieurs clusters vSAN sur lesquels le service de fichiers est activé.

Vous pouvez limiter l'accès à des clusters vSAN spécifiques sur lesquels le service de fichiers est activé. Lors du déploiement du cluster Kubernetes, configurez le pilote CSI avec l'accès à des clusters vSAN de services de fichiers spécifiques. Par conséquent, le pilote CSI peut provisionner les volumes de fichiers uniquement sur ces clusters vSAN.

Dans la configuration par défaut, le pilote CSI utilise tous les clusters vSAN de services de fichiers disponible dans vCenter Server pour le provisionnement du volume de fichiers. Le pilote CSI ne vérifie pas quel cluster vSAN de service de fichiers est accessible lors du provisionnement du volume de fichiers.

Rôles et privilèges de Stockage cloud natif

L'utilisateur vSphere CNS doit disposer de privilèges spécifiques pour effectuer des opérations liées à Stockage cloud natif.

Vous pouvez créer plusieurs rôles afin d'attribuer des ensembles d'autorisations sur les objets qui font partie de l'environnement Stockage cloud natif.

Note Ces rôles doivent être créés uniquement pour les clusters Kubernetes génériques. Si vous travaillez dans l'environnement vSphere with Tanzu, utilisez le rôle Gestionnaire de stockage de charge de travail pour les opérations de stockage.

Pour plus d'informations sur les rôles et les autorisations dans vSphere et sur la création d'un rôle, reportez-vous à la documentation de *Sécurité vSphere*.

Nom du rôle	Nom de privilège	Description	Requis sur
Stockage cloud natif - Banque de données	Banque de données > Opérations de fichier de niveau inférieur	Permet l'exécution d'opérations de lecture, d'écriture, de suppression et de changement de nom dans le navigateur de la banque de données.	Banque de données partagée sur laquelle résident des volumes persistants.
CNS-HOST-CONFIG-STORAGE	Hôte > Configuration > Configuration de partition de stockage	Permet la gestion de la banque de données vSAN.	Requis sur un cluster vSAN avec service de fichiers vSAN. Requis pour le volume de fichiers uniquement.
Stockage cloud natif - Machine virtuelle	Machine virtuelle > Modifier la configuration > Ajouter un disque existant	Permet l'ajout d'un disque virtuel existant à une machine virtuelle.	Toutes les machines virtuelles de nœud du cluster.
	Machine virtuelle > Modifier la configuration > Ajouter ou supprimer un périphérique	Permet l'ajout ou la suppression de n'importe quel périphérique non-disque.	
CNS-SEARCH-AND-SPBM	Stockage cloud natif > Possibilité de recherche	Permet à l'administrateur de stockage d'afficher l'interface utilisateur du stockage cloud natif.	Instance racine de vCenter Server.

Nom du rôle	Nom de privilège	Description	Requis sur
	Stockage à base de profils > Vue du stockage à base de profils	Permet d'afficher les stratégies de stockage définies.	
Lecture seule	Rôle par défaut	<p>Les utilisateurs qui ont le rôle Lecture seule pour un objet sont autorisés à afficher l'état et les détails de l'objet. Par exemple, les utilisateurs disposant de ce rôle peuvent trouver la banque de données partagée accessible à toutes les machines virtuelles de nœud.</p> <p>Pour les environnements sensibles à la zone et à la topologie, tous les ancêtres de machines virtuelles de nœuds, tels qu'un hôte, un cluster et un centre de données, doivent avoir le rôle en lecture seule défini pour l'utilisateur vSphere configuré pour utiliser le pilote CSI et CCM. Cela est nécessaire pour permettre la lecture des balises et des catégories afin de préparer la topologie des nœuds.</p>	Tous les hôtes sur lesquels résident les machines virtuelles des nœuds Centre de données

Créer une stratégie de stockage pour Kubernetes

L'objet de stockage vSphere qui va sauvegarder une application en conteneur Kubernetes doit répondre à des exigences de stockage spécifiques. En tant qu'utilisateur vSphere, vous créez une stratégie de stockage de machine virtuelle basée sur les conditions requises fournies par l'utilisateur Kubernetes.

La stratégie de stockage sera associée au disque virtuel ou au partage de fichiers vSAN qui sauvegarde le conteneur Kubernetes.

Si vous disposez de plusieurs instances de vCenter Server dans votre environnement, créez la stratégie de stockage de machine virtuelle sur chaque instance. Utilisez le même nom de stratégie sur toutes les instances.

Conditions préalables

- L'utilisateur Kubernetes identifie le cluster Kubernetes dans lequel l'application en conteneur avec état sera déployée.

- L'utilisateur Kubernetes collecte les conditions requises de stockage de l'application en conteneur et les communique à l'utilisateur vSphere.
- Privilèges nécessaires : **Stratégies de stockage VM. Mettre à jour** et **Stratégies de stockage VM. Afficher**.

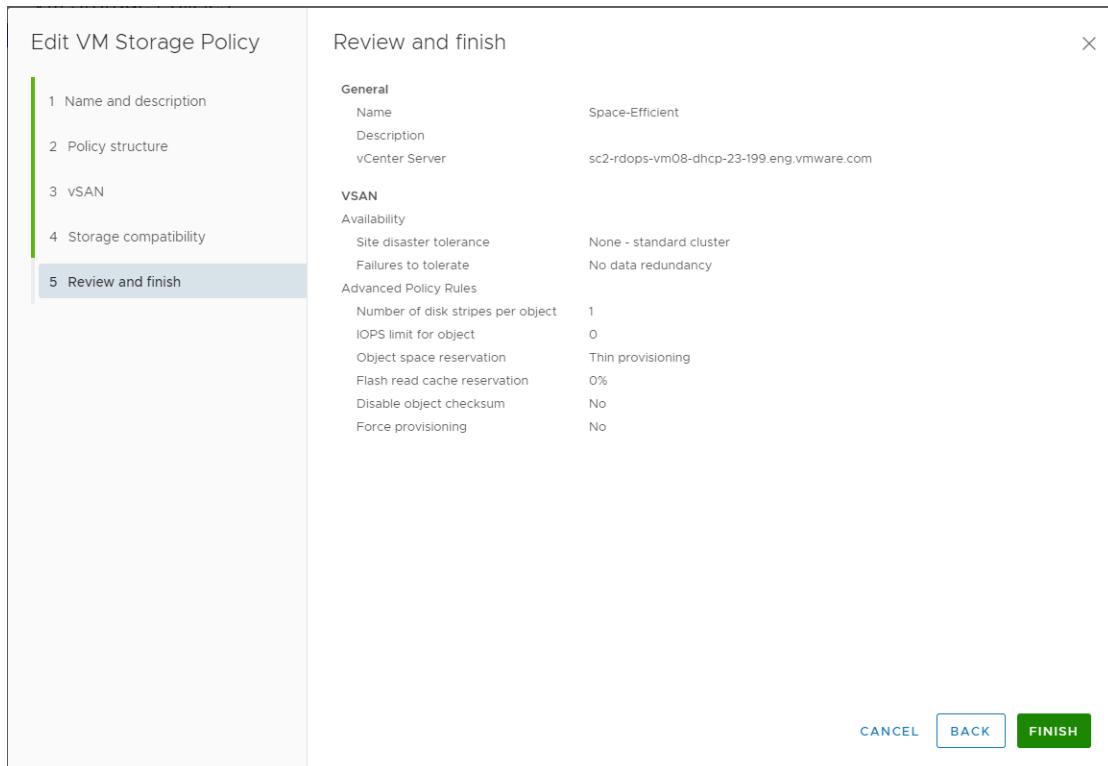
Procédure

- 1 Dans vSphere Client, ouvrez l'assistant **Créer une stratégie de stockage de machine virtuelle**.
 - a Cliquez sur **Menu > Stratégies et profils**.
 - b Sous **Stratégies et profils**, cliquez sur **Stratégies de stockage VM**.
 - c Cliquez sur **Créer**.
- 2 Entrez le nom de la stratégie et sa description, puis cliquez sur **Suivant**.

Option	Action
vCenter Server	Sélectionnez l'instance de vCenter Server.
Nom	Entrez le nom de la stratégie de stockage, par exemple Espace optimisé .
Description	Entrez la description de la stratégie de stockage.

- 3 Sur la page **Structure de la stratégie**, sous Règles spécifiques à une banque de données, sélectionnez **Activer les règles de stockage vSAN**, puis cliquez sur **Suivant**.
- 4 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**.
 - b Dans l'onglet **Règles de stratégie avancées**, définissez des règles de stratégie avancées, telles que le nombre de bandes de disque par objet la réservation du cache de lecture Flash.
- 5 Sur la page **Compatibilité de stockage**, vérifiez la liste des banques de données vSAN qui correspondent à cette stratégie, puis cliquez sur **Suivant**.

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



Étape suivante

Vous pouvez désormais informer l'utilisateur Kubernetes du nom de la stratégie de stockage. La stratégie de stockage de machine virtuelle que vous avez créée sera utilisée dans le cadre de la définition de classe de stockage pour le provisionnement dynamique de volumes.

Configurer des machines virtuelles de cluster Kubernetes

Sur chaque machine virtuelle de nœud, activez le paramètre `disk.EnableUUID` afin que les machines virtuelles puissent monter les disques virtuels.

Effectuez ces étapes pour chacun des nœuds de machine virtuelle qui font partie du cluster.

Conditions préalables

- Créez plusieurs machines virtuelles pour votre cluster Kubernetes. Pour plus d'informations sur les conditions requises des machines virtuelles, reportez-vous à [Configuration requise de Stockage cloud natif](#).
- Privilège nécessaire : **Machine virtuelle. Configuration. Paramètres**.

Note Pour éviter des erreurs et un comportement imprévisible, ne prenez pas de snapshots des machines virtuelles de nœuds CNS.

Procédure

- 1 Dans vSphere Client, cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
- 2 Cliquez sur l'onglet **Options VM** et développez le menu **Avancé**.
- 3 Cliquez sur **Modifier la configuration** en regard de Paramètres de configuration.
- 4 Configurez le paramètre **disk.EnableUUID**.

Si le paramètre existe, assurez-vous que sa valeur est définie sur True. Si le paramètre n'est pas présent, ajoutez-le et définissez sa valeur sur True.

Nom	Valeur
disk.EnableUUID	True

Surveiller les volumes de conteneur entre les clusters Kubernetes

Une fois qu'une application avec état est déployée dans Kubernetes, les volumes et leurs objets de stockage vSphere de stockage deviennent visibles dans vSphere Client. Vous pouvez afficher et surveiller les volumes et résoudre les éventuels problèmes de stockage.

Note Si vous rencontrez des défaillances sur le serveur CNS Kubernetes, les objets CNS dans vSphere Client risquent de ne pas s'afficher correctement tant que la synchronisation complète n'a pas lieu.

Procédure

- 1 Accédez à l'instance de vCenter Server, à un centre de données ou à une banque de données.
- 2 Cliquez sur l'onglet **Surveiller** et cliquez sur **Volumes de conteneur** sous **Stockage cloud natif**.
- 3 Observez les volumes de conteneurs disponibles dans votre environnement et surveillez l'état de conformité de la stratégie de stockage.

Volume Name	Label	Datastore	Compliance Status	Volume ID	Accessibility	Capacity Quota
pvc-64afe5ef-28d...	SEE ALL	vsanDatastore	Compliant	a710734-51ef-4372-a7...	Accessible	5.00 GB

- 4 Cliquez sur le lien **TOUT AFFICHER** dans la colonne Étiquette pour afficher des détails supplémentaires.

Les détails incluent le nom de PersistentVolumeClaim, StorageClass, etc. et vous permettent de mapper le volume aux objets Kubernetes qui lui sont associés.

- 5 Cliquez sur le lien dans la colonne **Nom de volume** pour vérifier les détails du placement, de la conformité et de la stratégie de stockage.

Note L'écran **Objets virtuels** est disponible uniquement lorsque la banque de données sous-jacente est vSAN.

Name	Placement and Availability	Storage Policy
VM home	Healthy	--
Virtual machine swap object	Healthy	vSAN Default Storage Policy
k8s-node3	Healthy	vSAN Default Storage Policy
Hard disk 1	Healthy	vSAN Default Storage Policy
Hard disk 2	Healthy	Space-Efficient
VM home	Healthy	--
VM home	Healthy	vSAN Default Storage Policy
Virtual machine swap object	Healthy	vSAN Default Storage Policy
k8s-node4	Healthy	

Utilisation du chiffrement avec le stockage cloud natif

Vous pouvez utiliser la technologie de chiffrement vSphere pour protéger les disques virtuels FCD qui sauvegardent les volumes persistants.

L'utilisation du chiffrement dans votre environnement vSphere nécessite de la préparation et inclut la configuration d'une connexion approuvée entre vCenter Server et un fournisseur de clés. vCenter Server peut ensuite récupérer des clés du fournisseur de clés si nécessaire. Pour plus d'informations sur les composants qui participent au processus de chiffrement vSphere, consultez [Composants de chiffrement de machine virtuelle vSphere](#) dans la documentation de *Sécurité vSphere*.

Procédure

- 1 Configurez le fournisseur de clés dans votre environnement vSphere.

Pour plus d'informations, consultez [Configurer le cluster du serveur de gestion des clés](#).

2 Chiffrez toutes les machines virtuelles de nœuds sur le cluster Kubernetes.

Utilisez vSphere Client pour effectuer cette étape.

a Accédez à une machine virtuelle de nœud.

b Cliquez avec le bouton droit et, dans le menu contextuel, sélectionnez **Stratégies de VM > Modifier les stratégies de stockage des VM**.

c Dans le menu déroulant **Stratégie de stockage des VM**, sélectionnez **Stratégie de chiffrement des VM** et cliquez sur **OK**.

Pour accélérer le processus de chiffrement des machines virtuelles du nœud, vous ne pouvez chiffrer que la page d'accueil de la machine virtuelle.

3 Créez des volumes persistants chiffrés dans le cluster Kubernetes à l'aide de la configuration de vSphere CSI.

a Créez un StorageClass qui fait référence à la stratégie de stockage de chiffrement de la machine virtuelle.

Utilisez le fichier YAML suivant comme exemple.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: encryption
provisioner: csi.vsphere.vmware.com
parameters:
  storagePolicyName: "VM Encryption Policy"
  datastore: vsanDatastore
```

b Utilisez PersistentVolumeClaim pour provisionner le volume persistant.

PersistentVolumeClaim doit inclure le nom de la classe de stockage de chiffrement dans le champ `storageClassName`.

Utilisation de vmkfstools

19

`vmkfstools` est l'une des commandes ESXi Shell de gestion des volumes VMFS, des périphériques de stockage et des disques virtuels. Vous pouvez effectuer de nombreuses opérations de stockage en utilisant la commande `vmkfstools`. Par exemple, vous pouvez créer et gérer les banques de données VMFS sur une partition physique ou manipuler des fichiers de disque virtuel, stockés sur des banques de données VMFS ou NFS.

Note Après une modification avec `vmkfstools`, vSphere Client risque de ne pas être mis à jour immédiatement. Utilisez une opération d'actualisation ou de réanalyse depuis le client.

Pour plus d'informations sur ESXi Shell, consultez *Démarrage avec ESXCLI*.

Ce chapitre contient les rubriques suivantes :

- [Syntaxe des commandes vmkfstools](#)
- [Options de la commande vmkfstools](#)

Syntaxe des commandes vmkfstools

En règle générale, vous n'avez pas besoin de vous connecter en tant qu'utilisateur racine pour pouvoir exécuter les commandes `vmkfstools`. Toutefois, certaines commandes (telles que les commandes de système de fichiers) peuvent nécessiter une connexion d'utilisateur racine.

La commande `vmkfstools` prend en charge la syntaxe de la commande suivante :

`vmkfstools options target`.

La cible spécifie une partition, un dispositif ou un chemin pour y appliquer l'option de commande.

Tableau 19-1. Arguments de commande `vmkfstools`

Argument	Description
options	<p>Une ou plusieurs des options de ligne de commande et les arguments associés vous permettant de spécifier l'activité que <code>vmkfstools</code> doit effectuer. Par exemple, la sélection du format de disque lors de la création d'un disque virtuel.</p> <p>Après avoir entré cette option, vous devez spécifier une cible sur laquelle l'opération sera effectuée. La cible peut indiquer une partition, un périphérique ou un chemin.</p>
partition	Spécifie les partitions de disque. Cet argument utilise un format <i>disk_ID:P</i> , où <i>disk_ID</i> correspond à l'ID de périphérique renvoyé par la baie de stockage et <i>P</i> correspond à un nombre entier représentant le numéro de partition. Le numéro de partition doit être supérieur à zéro (0) et correspondre à une partition VMFS valide.
périphérique	<p>Spécifie les périphériques ou les volumes logiques. Cet argument utilise un nom de chemin du système de fichiers du périphérique ESXi. Il commence par <code>/vmfs/devices</code>, ce qui correspond au point de montage du système de fichier du périphérique.</p> <p>Lorsque vous spécifiez différents types de périphériques, utilisez les formats suivants :</p> <ul style="list-style-type: none"> ■ <code>/vmfs/devices/disks</code> pour les disques locaux ou SAN. ■ <code>/vmfs/devices/lvm</code> pour les volumes logiques ESXi. ■ <code>/vmfs/devices/generic</code> pour les périphériques SCSI génériques.
chemin	<p>Spécifie un fichier ou un système de fichiers VMFS. Cet argument est un chemin absolu ou relatif désignant un lien symbolique d'accès à un répertoire, à un mappage de périphérique brut ou à un fichier situé sous <code>/vmfs</code>.</p> <ul style="list-style-type: none"> ■ Pour spécifier un système de fichiers VMFS, utilisez le format suivant : <pre style="background-color: #f0f0f0; padding: 5px;"><code>/vmfs/volumes/file_system_UUID</code></pre> <p>ou</p> <pre style="background-color: #f0f0f0; padding: 5px;"><code>/vmfs/volumes/file_system_label</code></pre> <ul style="list-style-type: none"> ■ Pour spécifier un fichier sur une banque de données VMFS, utilisez ce format : <pre style="background-color: #f0f0f0; padding: 5px;"><code>/vmfs/volumes/file_system_label file_system_UUID/[dir] / myDisk.vmdk</code></pre> <p>Si le répertoire de travail actuel est le répertoire parent de <code>myDisk.vmdk</code>, n'entre pas le chemin d'accès complet.</p>

Options de la commande `vmkfstools`

La commande `vmkfstools` se compose de différentes options. Certaines d'entre elles s'adressent uniquement aux utilisateurs avancés.

Vous pouvez spécifier le format long ou le format à lettre unique, au choix. Par exemple, les commandes suivantes sont identiques :

```
vmkfstools --createfs vmfs6 --blocksize 1m disk_ID:P
vmkfstools -C vmfs6 -b 1m disk_ID:P
```

Sous-option -v

La sous-option `-v` indique le niveau de verbosité du résultat de la commande.

Le format de cette sous-option est le suivant :

```
-v --verbose number
```

Pour spécifier la valeur *number*, utilisez un nombre entier compris entre 1 et 10.

Vous pouvez spécifier la valeur de la sous-option `-v` via l'option `vmkfstools` de votre choix. Si le résultat de l'option n'est pas utilisable avec la sous-option `-v`, `vmkfstools` ignore `-v`.

Note Puisque vous pouvez inclure la sous-option `-v` dans toute ligne de commande `vmkfstools`, `-v` n'est pas mentionnée dans les descriptions d'options.

Options de système de fichiers

Les options de système de fichiers vous permettent de créer et gérer les banques de données VMFS. Ces options ne s'appliquent pas à NFS. Vous pouvez exécuter un grand nombre de ces tâches via vSphere Client.

Liste d'attributs d'une banque de données VMFS

Pour répertorier les attributs d'une banque de données VMFS, utilisez la commande `vmkfstools`.

```
-P | --queryfs
-h | --humanreadable
```

Lorsque vous utilisez cette option pour un fichier ou un répertoire qui réside sur une banque de données VMFS, l'option répertorie les attributs de la banque de données spécifiée. Les attributs répertoriés incluent généralement l'étiquette du système de fichiers, le nombre d'extensions de la banque de données, l'UUID et la liste des périphériques sur lesquels réside chaque extension.

Note Si l'un des périphériques hébergeant le système de fichiers VMFS est mis hors tension, le nombre d'extension et l'espace disponible sont modifiés en conséquence.

Vous pouvez spécifier la valeur de la sous-option `-h | --humanreadable` via l'option `-P`. Dans ce cas, `vmkfstools` répertorie la capacité du volume sous une forme plus lisible.

Exemple : Exemple de liste d'attributs VMFS

```
~ vmkfstools -P -h /vmfs/volumes/my_vmf
VMFS-5.81 (Raw Major Version: 14) file system spanning 1 partitions.
File system label (if any): my_vmf
Mode: public
Capacity 99.8 GB, 97.5 GB available, file block size 1 MB, max supported file size 62.9 TB
UUID: 571fe2fb-ec4b8d6c-d375-XXXXXXXXXXXX
Partitions spanned (on "lvm"):
    eui.3863316131XXXXXX:1
Is Native Snapshot Capable: YES
```

Création d'une banque de données VMFS ou d'une partition scratch

Utilisez la commande `vmkfstools` pour créer une banque de données VMFS ou une partition scratch.

```
-C|--createfs [vmfs5|vmfs6|vfat]
```

Cette option crée la banque de données VMFS sur la partition SCSI ou NVMe spécifiée (par exemple, *disk_ID:P*). La partition devient la partition principale de la banque de données. Pour VMFS5 et VMFS6, la seule taille de bloc disponible est 1 Mo.

Vous pouvez spécifier les sous-options suivantes avec l'option `-C`.

- `-S|--setfsname` - Définissez l'étiquette de volume de la banque de données VMFS que vous êtes en train de créer. Utilisez cette sous-option uniquement avec l'option `-C`. L'étiquette spécifiée peut comporter au maximum 128 caractères ; elle ne doit pas contenir d'espaces au début ou à la fin.

Note vCenter Server prend en charge la limite de 80 caractères pour toutes ses entités. Si le nom d'une banque de données excède cette limite, le nom est raccourci lorsque vous ajoutez cette banque de données à vCenter Server.

Une fois que vous avez défini une étiquette de volume, vous pouvez l'utiliser lorsque vous spécifiez la banque de données VMFS pour la commande `vmkfstools`. L'étiquette de volume apparaît dans les listes générées pour la commande `ls -l` et sous forme de lien symbolique d'accès au volume VMFS dans l'inventaire `/vmfs/volumes`.

Pour modifier l'étiquette de volume VMFS, utilisez la commande `ln -sf`. En voici un exemple :

```
ln -sf /vmfs/volumes/UUID /vmfs/volumes/datastore
```

datastore correspond à la nouvelle étiquette de volume à utiliser pour le VMFS *UUID*.

Note Si l'hôte est enregistré dans vCenter Server, tous les changements apportés à l'étiquette de volume VMFS sont écrasés par vCenter Server. Cette opération garantit que l'étiquette VMFS est cohérente pour tous les hôtes vCenter Server.

- `-Y|--unmapGranularity # [bBsSkMgGtT]` - Cette sous-option s'applique uniquement à VMFS6. Définissez la granularité de l'opération unmap. La granularité par défaut est 1 Mo. Comme pour la taille de bloc, entrez le type d'unité.
- `-O|--unmapPriority <none|low|medium|high>` - Cette sous-option s'applique uniquement à VMFS6. Définissez la priorité de l'opération unmap.

Exemple : Exemple de création d'un système de fichiers VMFS

Cet exemple illustre la création d'une banque de données VMFS6 appelée `my_vmfss` sur la partition `naa.ID:1`.

```
~ vmkfstools -C vmfs6 -S my_vmfss /vmfs/devices/disks/naa.ID:1
```

Ajout d'une extension à une banque de données VMFS

Utilisez la commande `vmkfstools` pour ajouter une extension à une banque de données VMFS.

Lorsque vous ajoutez une extension, vous étendez la banque de données VMFS de la partition principale à la partition spécifiée par `span_partition`.

```
-Z|--spanfs span_partition head_partition
```

Vous devez spécifier le nom de chemin complet pour les partitions principales et les partitions d'extension, par exemple `/vmfs/devices/disks/disk_ID:1`. Chaque fois que vous utilisez cette option, vous pouvez ajouter une extension à la banque de données VMFS, afin que la banque de données s'étende sur plusieurs partitions.

Attention Lorsque vous utilisez cette option, vous perdez toutes les données présentes sur le périphérique SCSI ou NVMe spécifié dans `span_partition`.

Exemple : Exemple d'extension d'une banque de données VMFS

Dans cet exemple, vous étendez la partition principale existante de la banque de données VMFS sur une nouvelle partition.

```
~ vmkfstools -Z /vmfs/devices/disks/naa.disk_ID_2:1 /vmfs/devices/disks/naa.disk_ID_1:1
```

La banque de données étendue est répartie sur deux partitions : `naa.disk_ID_1:1` et `naa.disk_ID_2:1`. Dans cet exemple, `naa.disk_ID_1:1` est le nom de la partition principale.

Développement d'une banque de données VMFS

Au lieu d'ajouter une extension à une banque de données VMFS, vous pouvez augmenter la taille d'une banque de données existante. Utilisez la commande `vmkfstools -G`.

Vous pouvez augmenter la taille de la banque de données après l'augmentation de la capacité du stockage sous-jacent.

La commande utilise l'option suivante :

```
-G|--growfs device
```

Cette option étend la banque de données VMFS ou son extension spécifique. Par exemple,

```
vmkfstools --growfs /vmfs/devices/disks/disk_ID:1 /vmfs/devices/disks/disk_ID:1
```

Options de disque virtuel

Les options de disque virtuel vous permettent de configurer, migrer et gérer les disques virtuels stockés sur vos banques de données. Vous pouvez également exécuter un grand nombre de ces tâches via vSphere Client.

Formats de disque pris en charge

Lorsque vous créez ou clonez un disque virtuel, vous pouvez utiliser la sous-option `-d|--diskformat` pour spécifier le format du disque.

Vous avez le choix entre les formats suivants :

- `zeroedthick` (valeur par défaut) - L'espace requis pour le disque virtuel est alloué au cours de la création. Les données qui demeurent sur le périphérique physique ne sont pas effacées pendant la création, mais sont mises à zéro sur demande à la première écriture sur la machine virtuelle. La machine virtuelle ne lit pas les données caduques du disque.
- `eagerzeroedthick` - L'espace requis pour le disque virtuel est alloué pendant la création. Contrairement au format `zeroedthick`, les données qui demeurent sur le périphérique physique sont mises à zéro pendant la création. La création de disques à ce format peut être plus longue que pour d'autres types de disques.
- `thin` - Disque virtuel léger. Contrairement au format `thick`, l'espace requis pour le disque virtuel n'est pas alloué pendant la création, mais il est fourni, mis à zéro, sur demande.
- `rdm:device` - Mappage du disque brut en mode compatibilité virtuelle.
- `rdmp:device` - Mappage du disque brut en mode compatibilité physique (émulation).
- `2gbsparsse` - Disque clairsemé doté de la taille d'extension maximale de 2 Go. Vous pouvez utiliser des disques dans ce format avec des produits VMware hébergés, tels que VMware Fusion. Cependant, vous ne pouvez pas mettre sous tension le disque clairsemé sur un hôte ESXi, sauf si vous avez préalablement réimporté le disque à l'aide de `vmkfstools` en utilisant un format compatible tel que `thick` ou `thin`.

Formats de disque sur les banques de données NFS

Les seuls formats de disque pouvant être utilisés pour NFS sont les suivants : `thin`, `thick`, `zeroedthick` et `2gbsparsse`.

Les formats `Thick`, `zeroedthick` et `thin` se comportent généralement de la même manière parce que le serveur NFS et non pas l'hôte ESXi détermine la stratégie d'allocation. Sur la plupart des serveurs NFS, la règle d'allocation par défaut est `thin`. Toutefois, sur les serveurs NFS qui prennent en charge les API de stockage - Intégration de baie, vous pouvez créer des disques virtuels dans le format `zeroedthick`. L'opération d'espace de réserve permet aux serveurs NFS d'allouer et de garantir de l'espace.

Pour plus d'informations sur les API d'intégration de baie, consultez [Chapitre 16 Accélération matérielle du stockage](#).

Création d'un disque virtuel

Pour créer un disque virtuel, utilisez la commande `vmkfstools`.

```
-c|--createvirtualdisk size[bB|sS|kK|mM|gG]
-d|--diskformat [thin|zeroedthick|eagerzeroedthick]
-W|--objecttype [file|vsan|vvol]
--policyFile fileName
```

Cette option permet de créer un disque virtuel à l'emplacement spécifié d'une banque de données. Spécifiez la taille du disque virtuel. Lorsque vous entrez la valeur du paramètre `size`, vous pouvez indiquer le type d'unité via l'ajout d'un suffixe `k` (kilo-octets), `m` (méga-octets) ou `g` (giga-octets). Le type d'unité n'est pas sensible à la casse. `vmkfstools` interprète indifféremment `k` ou `K` comme kilo-octets. Si vous ne spécifiez pas de type d'unité, `vmkfstools` utilise les octets par défaut.

Vous pouvez spécifier les sous-options suivantes avec l'option `-c`.

- `-d|--diskformat` permet de spécifier les formats de disque.
- `-W|--objecttype` spécifie si le disque virtuel est un fichier d'une banque de données VMFS ou NFS, un objet sur vSAN ou une banque de données Virtual Volumes.
- `--policyFile fileName` spécifie la stratégie de stockage de machine virtuelle pour le disque.

Exemple : Exemple de création de disque virtuel

Cet exemple illustre comment créer un fichier de disque virtuel de 2 giga-octets appelé `disk.vmdk`. Vous créez le disque sur la banque de données VMFS appelée `myVMFS`. Ce fichier de disque représente un disque virtuel vide auquel les machines virtuelles peuvent accéder.

```
vmkfstools -c 2048m /vmfs/volumes/myVMFS/disk.vmdk
```

Initialisation d'un disque virtuel

Pour initialiser un disque virtuel, utilisez la commande `vmkfstools`.

```
-w|--writezeros
```

Cette option permet de nettoyer le disque virtuel en inscrivant des zéros sur toutes les données qu'il contient. En fonction de la taille de votre disque virtuel et de la bande passante d'E/S utilisée pour le périphérique hébergeant le disque virtuel, l'exécution de cette commande peut être plus ou moins longue.

Attention Lorsque vous utilisez cette commande, vous perdez les données présentes sur le disque virtuel.

Gonflage d'un disque virtuel léger

Pour gonfler un disque virtuel léger, utilisez la commande `vmkfstools`.

```
-j | --inflatedisk
```

Cette option permet de convertir un disque virtuel léger (`thin`) en disque `eagerzeroedthick`, tout en préservant la totalité des données existantes. Cette option permet d'allouer les blocs qui ne l'ont pas encore été et de les mettre à zéro.

Conversion d'un disque virtuel Zeroedthick en disque Eagerzeroedthick

Pour convertir un disque virtuel `zeroedthick` en disque `eagerzeroedthick`, utilisez la commande `vmkfstools`.

```
-k | --eagerzero
```

Outre la conversion, cette option permet de préserver les données présentes sur le disque virtuel.

Suivez cet exemple :

```
vmkfstools --eagerzero /vmfs/volumes/myVMFS/VMName/disk.vmdk
```

Suppression de blocs mis à zéro

Utilisez la commande `vmkfstools` pour supprimer les blocs mis à zéro.

```
-K | --punchzero
```

Cette option permet de supprimer l'allocation de tous les blocs mis à zéro, en conservant uniquement ceux qui ont été alloués précédemment et qui contiennent des données. Le format du disque virtuel ainsi obtenu est le format de disque léger.

Suppression d'un disque virtuel

Utilisez la commande `vmkfstools` pour supprimer un fichier de disque virtuel dans le chemin spécifié sur le volume VMFS.

Utilisez l'option suivante :

```
-U | --deletevirtualdisk
```

Affectation d'un nouveau nom à un disque virtuel

Utilisez la commande `vmkfstools` pour renommer un fichier de disque virtuel dans le chemin spécifié sur le volume VMFS.

Vous devez spécifier le nom de fichier ou le chemin d'origine (*oldName*) et le nouveau nom de fichier ou le nouveau chemin (*newName*).

```
-E|--renamevirtualdisk oldNamenewName
```

Clonage ou conversion d'un disque virtuel ou d'un RDM

Utilisez la commande `vmkfstools` pour créer une copie d'un disque virtuel ou d'un disque brut donné.

Un utilisateur non-racine ne peut pas cloner un disque virtuel ou un RDM. Vous devez spécifier le nom de fichier ou le chemin d'origine (*oldName*) et le nouveau nom de fichier ou le nouveau chemin (*newName*).

```
-i|--clonevirtualdisk oldName newName
    -d|--diskformat [thin|zeroedthick|eagerzeroedthick|rdm:device|rdmp:device|2gbpsparse]
    -W|--objecttype [file|vsan|vvol]
    --policyFile fileName
    -N|--avoidnativeclone
```

Utilisez les sous-options suivantes pour modifier les paramètres correspondants pour la copie que vous créez.

- `-d|--diskformat` permet de spécifier les formats de disque.
- `-W|--objecttype` spécifie si le disque virtuel est un fichier d'une banque de données VMFS ou NFS, un objet sur vSAN ou une banque de données Virtual Volumes.
- `--policyFile fileName` spécifie la stratégie de stockage de machine virtuelle pour le disque.

Par défaut, ESXi utilise ses méthodes natives pour effectuer les opérations de clonage. Si votre baie prend en charge les technologies de clonage, vous pouvez décharger les opérations vers la baie. Pour éviter le clonage natif ESXi, spécifiez l'option `-N|--avoidnativeclone`.

Exemple : Exemple de clonage ou de conversion d'un disque virtuel

Cet exemple illustre le clonage du contenu d'un disque virtuel maître du référentiel `templates` vers un fichier de disque virtuel nommé `myOS.vmdk`, situé sur le système de fichiers `myVMFS`.

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold-master.vmdk /vmfs/volumes/myVMFS/myOS.vmdk
```

Vous pouvez configurer une machine virtuelle en vue de l'utilisation de ce disque : pour cela, ajoutez les lignes correspondantes au fichier de configuration de la machine virtuelle, comme indiqué dans l'exemple suivant :

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

Si vous souhaitez convertir le format du disque, utilisez la sous-option `-d|--diskformat`.

Cette sous-option est utile lorsque vous importez des disques virtuels dans un format incompatible avec ESXi, par exemple le format `2gbsparse`. Après la conversion du disque, vous pouvez attacher ce disque à une nouvelle machine virtuelle que vous créez dans ESXi.

Par exemple :

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold-master.vmdk /vmfs/volumes/myVMFS/myOS.vmdk
-d thin
```

Extension d'un disque virtuel

Après la création d'une machine virtuelle, vous pouvez utiliser la commande `vmkfstools` pour augmenter la taille d'un disque alloué à la machine virtuelle.

```
-X|--extendvirtualdisk newSize[bBsSkMmGgTt]
```

Spécifiez le paramètre `newSize` en ajoutant un suffixe d'unité approprié. Le type d'unité n'est pas sensible à la casse. `vmkfstools` interprète indifféremment `k` ou `K` comme kilo-octets. Si vous ne spécifiez pas de type d'unité, `vmkfstools` utilise les kilo-octets par défaut.

Le paramètre `newSize` définit la nouvelle taille totale (et pas uniquement l'incrément ajouté au disque).

Par exemple, pour augmenter la capacité d'un disque virtuel de 4-g de 1g, entrez : `vmkfstools -X 5g disk name`.

Vous pouvez étendre le disque virtuel au format `eagerzeroedthick` en utilisant l'option `-d eagerzeroedthick`.

Lorsque vous utilisez l'option `-x`, les éléments suivants s'appliquent :

- N'étendez pas le disque de base d'une machine virtuelle associée à des snapshots. En effet, cela vous empêcherait de valider les snapshots ou de restaurer la taille d'origine du disque de base.
- Après l'extension du disque, vous devrez éventuellement mettre à jour son système de fichiers. Le système d'exploitation invité reconnaît alors la nouvelle taille du disque et peut l'utiliser.

Mise à niveau de disques virtuels

Cette option convertit le fichier de disque virtuel spécifié des formats ESX Server 2 au format ESXi.

Utilisez cette option pour convertir les disques virtuels de type `LEGACYSPARSE`, `LEGACYPLAIN`, `LEGACYVMFS`, `LEGACYVMFS_SPARSE` et `LEGACYVMFS_RDM`.

```
-M|--migratevirtualdisk
```

Création d'un mappage de périphérique brut en mode de compatibilité virtuelle

Utilisez la commande `vmkfstools` pour créer un fichier RDM (Raw Device Mapping) sur un volume VMFS et pour mapper un LUN brut à ce fichier. Une fois ce mappage établi, vous pouvez accéder au LUN comme vous le feriez pour un disque virtuel VMFS classique. La longueur du fichier objet du mappage est équivalente à la taille du LUN brut désigné.

```
-r|--createrdm device
```

Lorsque vous spécifiez la valeur du paramètre *device*, respectez le format suivant :

```
/vmfs/devices/disks/disk_ID:P
```

Exemple : Exemple de création d'un fichier RDM en mode de compatibilité virtuelle

Dans cet exemple, vous créez un fichier RDM nommé *my_rdm.vmdk* et vous mappez le disque brut *disk_ID* sur ce fichier.

```
vmkfstools -r /vmfs/devices/disks/disk_ID my_rdm.vmdk
```

Vous pouvez configurer une machine virtuelle en vue de l'utilisation du fichier de mappage *my_rdm.vmdk* ; pour cela, ajoutez les lignes suivantes au fichier de configuration de la machine virtuelle :

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/my_rdm.vmdk
```

Création d'un mappage de périphérique brut en mode de compatibilité physique

Utilisez la commande `vmkfstools` pour mapper un périphérique de relais brut à un fichier sur un volume VMFS. Ce mappage permet à une machine virtuelle de contourner le filtrage de commandes SCSI ESXi lors de l'accès à son disque virtuel. Ce type de mappage est utile lorsque la machine virtuelle doit envoyer des commandes SCSI propriétaires (par exemple, lorsqu'un logiciel compatible SAN s'exécute sur la machine virtuelle).

```
-z|--createdmpassthru périphériqueexample.vmdk
```

Une fois ce type de mappage établi, vous pouvez l'utiliser pour l'accès au disque brut, comme vous le feriez pour les autres disques virtuels VMFS.

Lorsque vous spécifiez la valeur du chemin *device*, respectez le format suivant :

```
/vmfs/devices/disks/device_ID
```

Pour le nom *.vmdk*, utilisez ce format. Assurez-vous de créer la banque de données avant d'utiliser la commande.

```
/vmfs/volumes/datastore_name/example.vmdk
```

Par exemple,

```
vmkfstools -z /vmfs/devices/disks/naa.600a000000000000... /vmfs/volumes/datastore1/
mydisk.vmdk
```

Liste des attributs d'un RDM

Utilisez la commande vmkfstools pour répertorier les attributs d'un mappage de disque brut. Les attributs vous aident à identifier le périphérique de stockage auquel vos fichiers RDM correspondent.

```
-q|--queryrdm my_rdm.vmdk
```

Cette option imprime le nom du RDM du disque brut. Elle imprime également d'autres informations d'identification (ID de disque du disque brut, par exemple).

Exemple : Exemple de liste d'attributs RDM

```
# vmkfstools -q /vmfs/volumes/VMFS/my_vm/my_rdm.vmdk

Disk /vmfs/volumes/VMFS/my_vm/my_rdm.vmdk is a Passthrough Raw Device Mapping

Maps to: vml.0200000006005076801900207700000000000005323134352020
```

Affichage de la géométrie de disque virtuel

Utilisez la commande vmkfstools pour obtenir des informations sur la géométrie d'un disque virtuel.

```
-g|--geometry
```

Le résultat se présente comme suit : Geometry information C/H/S, où C représente le nombre de cylindres, H représente le nombre de têtes et S représente le nombre de secteurs.

Note Lorsque vous importez des disques virtuels depuis les produits VMware hébergés vers l'hôte ESXi, un message d'erreur de divergence de géométrie pourrait apparaître. Une divergence de géométrie de disque peut également déclencher des problèmes lorsque vous chargez un système d'exploitation invité ou exécutez une machine virtuelle récemment créée.

Vérification et réparation des disques virtuels

Utilisez la commande vmkfstools pour vérifier ou réparer un disque virtuel s'il est endommagé.

```
-x|--fix [check|repair]
```

Par exemple,

```
vmkfstools -x check /vmfs/volumes/my_datastore/my_disk.vmdk
```

Vérification de la cohérence de la chaîne de disques

Utilisez la commande `vmkfstools` pour vérifier l'intégralité de la chaîne de snapshots. Vous pouvez déterminer si l'un des maillons de la chaîne est corrompu ou si une relation parent-enfant non valide existe.

```
-e|--chainConsistent
```

Options de périphérique de stockage

Vous pouvez utiliser les options de périphérique de la commande `vmkfstools` pour effectuer des tâches d'administration des périphériques de stockage physique.

Gestion des réservations SCSI de LUN

Utilisez la commande `vmkfstools` pour réserver un LUN SCSI en vue d'un usage exclusif par l'hôte ESXi. Vous pouvez également libérer une réservation afin que d'autres hôtes puissent accéder au LUN et réinitialiser une réservation, forçant ainsi la libération de toutes les réservations sur la cible.

```
-L|--lock [reserve|release|lunreset|targetreset|busreset|readkeys|readresv] device
```

Attention L'utilisation de l'option `-L` peut interrompre les opérations des autres serveurs d'un SAN. Veillez à utiliser l'option `-L` uniquement pour le dépannage de configurations de clusters.

Sauf recommandation contraire de VMware, n'utilisez jamais cette option sur un LUN hébergeant un volume VMFS.

Vous pouvez spécifier l'option `-L` de différentes façons :

- `-L reserve` - Permet de réserver le LUN spécifié. Une fois la réservation effectuée, seul le serveur ayant réservé ce LUN peut y accéder. Si d'autres serveurs tentent d'accéder à ce LUN, un message d'erreur de réservation s'affiche.
- `-L release` - Permet de libérer la réservation du LUN spécifié. Dans ce cas, les autres serveurs peuvent de nouveau y accéder.
- `-L lunreset` - Permet de restaurer le LUN spécifié via la suppression des réservations associées ; le LUN redevient disponible pour tous les autres serveurs. Cette restauration n'affecte pas les autres LUN du périphérique. Si l'un d'entre eux est réservé, il le reste.
- `-L targetreset` - Permet de restaurer la cible complète. Cette opération supprime les réservations de tous les LUN associés à cette cible ; ces LUN redeviennent disponibles pour tous les serveurs.
- `-L busreset` - Permet de restaurer toutes les cibles accessibles sur le bus. Cette opération supprime les réservations de tous les LUN accessibles via le bus, et les rend de nouveau disponibles pour tous les serveurs.

- **-L readkeys** – Lit les clés de réservation enregistrées avec un LUN. S'applique à la fonctionnalité de réservation de groupe SCSI-III persistant.
- **-L readresv** – Lit l'état de réservation sur un LUN. S'applique à la fonctionnalité de réservation de groupe SCSI-III persistant.

Lorsque vous entrez la valeur du paramètre *device*, respectez le format suivant :

```
/vmfs/devices/disks/disk_ID:P
```

Rupture des verrous d'un périphérique

Utilisez la commande vmkfstools pour déverrouiller le périphérique sur une partition particulière.

```
-B|--breaklock device
```

Lorsque vous entrez la valeur du paramètre *device*, respectez le format suivant :

```
/vmfs/devices/disks/disk_ID:P
```

Vous pouvez utiliser cette commande en cas d'échec d'un hôte au milieu d'une opération de banque de données, telle que le développement de la banque de données, l'ajout d'une extension ou la resignature. Lorsque vous exécutez cette commande, vérifiez qu'aucun autre hôte ne détient le verrou.