VMware vSphere: installation, configuration, gestion

Manuel relatif au cours magistral
VMwareESXi6.7 et vCenterServer6.7

VMware® Education Services
VMware, Inc.
www.vmware.com/education

VMware vSphere:
installation, configuration, gestion
VMwareESXi6.7 et vCenterServer6.7
Référence EDU-FR-VSICM67-LECT (8/2018)
Manuel relatif au cours magistral

Copyright © 2018 VMware, Inc. Tous droits réservés. Le présent manuel et les supports de formation qui l'accompagnent sont protégés par les lois américaines et internationales sur le copyright et la propriété intellectuelle. Les produits VMware sont couverts par un ou plusieurs brevets, répertoriés à l'adresse http://www.vmware.com/fr/patents. VMware est une marque déposée ou une marque commerciale de VMware, Inc. ou de ses filiales, aux États-Unis et/ou dans d'autres juridictions. Toutes les autres marques et appellations commerciales mentionnées sont des marques déposées par leurs propriétaires respectifs.

Les supports de formation sont fournis « en l'état », et VMware, Inc. rejette expressément toutes les garanties ou prétentions à garanties expresses ou tacites, y compris les garanties de qualité marchande, d'adéquation à un usage ou but particulier ou de non-violation des droits de propriété intellectuelle, même si VMware, Inc. a été avisé de la possibilité de telles garanties ou prétentions à garanties. Ces supports de formation sont conçus pour être utilisés dans le cadre d'un cours avec instructeur ainsi qu'à des fins de référence en relation avec un tel cours. Ces supports ne sauraient être considérés comme un outil de formation autonome. L'utilisation des supports de formation dans le cadre d'une autoformation sans participation aux cours n'est pas recommandée.

Ces documents et les programmes informatiques auxquels ils se réfèrent sont la propriété de VMware, Inc. et sont le reflet des secrets commerciaux et informations confidentielles appartenant à VMware Inc. Toute reproduction, copie, diffusion, adaptation, modification ou cession sans autorisation expresse et écrite de VMware, Inc. est interdite.

www.vmware.com/education

Sommaire

Module 1 Présentation du cours 1

1-2 Importance 2
1-3 Objectifs de la formation (1) 3
1-4 Objectifs de la formation (2) 4
1-5 Vous êtes ici 5
1-6 Conventions typographiques 6
1-7 Références 7
1-8 Ressources en ligne VMware 8
1-9 Alignement sur la certification VCP-Foundations 9
1-10 Présentation des services de formation VMware 10
1-11 Présentation des certifications VMware 11

Module 2 Présentation de vSphere et du Software-Defined Data Center 13

2-2 Vous êtes ici 14
2-3 Importance 15
2-4 Leçons du module 16
2-5 Leçon 1 : Présentation de vSphere et des machines virtuelles 17
2-6 Objectifs de la formation 18
2-7 À propos des machines virtuelles 19
2-8 Avantages liés à l'utilisation de machines virtuelles 20
2-9 Les différents types de virtualisation 22
2-10 À propos du Software-Defined Data Center 23
2-11 vSphere et le Cloud Computing 25
2-12 Machine virtuelle : client et consommateur des ressources de l'hôte VMware ESXi 27
2-13 Architecture physique et architecture virtuelle 28
2-14 Partage des ressources physiques 29
2-15 Virtualisation des CPU 30
2-16 Utilisation de la mémoire hôte physique et virtualisée 31
2-17 Réseau physique et réseau virtuel 32
2-18 Comparaison des systèmes de fichiers physiques et des banques de données 34
2-19 Encapsulation des machines virtuelles 36
2-20 À propos des clients vSphere Client 37
2-21 À propos de vSphere Web Client 38
2-22 À propos de vSphere Client 40
2-23 À propos de VMware Host Client 41
2-24 À propos des fichiers de machine virtuelle 42
2-25 À propos du matériel virtuel de la machine virtuelle 44
2-26 Versions du matériel virtuel 46
2-27 À propos des ressources CPU et de mémoire 47
2-28 À propos du stockage virtuel 49
2-29 À propos des disques virtuels à provisionnement définitif 50
2-30 À propos des disques virtuels à provisionnement fin 51

2-31 À propos des réseaux virtuels 53
2-32 À propos des cartes réseau virtuelles (1) 55
2-33 À propos des cartes réseau virtuelles (2) 57
2-34 À propos des périphériques divers 59
2-35 À propos de la console de la machine virtuelle 60
2-36 Rappel des objectifs de la formation 61
2-37 Leçon 2 : Ressources partagées : présentation de VMware ESXi 62
2-38 Objectifs de la formation 63
2-39 À propos de VMware ESXi 64
2-40 Architecture virtuelle 66
2-41 Configuration d'un hôte VMware ESXi 67
2-42 Configuration d'un hôte VMware ESXi : accès root 68
2-43 Configuration d'un hôte VMware ESXi : réseau de gestion 69
2-44 Configuration d'un hôte VMware ESXi : autres paramètres 70
2-45 Paramètres d'accès distant : profil de sécurité 71
2-46 Gestion des comptes utilisateur : meilleures pratiques 72
2-47 Hôte VMware ESXi configuré en tant que client NTP 73
2-48 Démarrage rapide de VMware ESXi 74
2-49 Démonstration : Installation et configuration des hôtes VMware ESXi 75
2-50 Rappel des objectifs de la formation 76
2-51 Points clés 77

Module 3 Création de machines virtuelles 79

3-2 Vous êtes ici 80
3-3 Importance 81
3-4 Objectifs de la formation 82
3-5 À propos du provisionnement des machines virtuelles 83
3-6 Création de machines virtuelles avec l'assistant « New virtual machine » (1) 85
3-7 Création de machines virtuelles avec l'assistant « New virtual machine » (2) 86
3-8 Paramètres de l'assistant « New virtual machine » 87
3-9 Installation du système d'exploitation client 88
3-10 Déploiement de modèles OVF 89
3-11 À propos de VMware Tools 90
3-12 Gestion de VMware Tools 92
3-13 VMware Tools : images ISO prises en charge 93
3-14 Résolution des problèmes d'installation d'un système d'exploitation sur les machines virtuelles 94
3-15 Résolution des problèmes d'installation de VMware Tools sur un système d'exploitation client 95
3-16 Laboratoire 1 : Déploiement et configuration de machines virtuelles 96
3-17 Rappel des objectifs de la formation 97
3-18 Points clés 98

Module 4 vCenter Server 99
4-2 Vous êtes ici 100
4-3 Importance 101
4-4 Leçons du module 102
4-5 Leçon 1 : Gestion centralisée : Présentation de vCenter Server 103
4-6 Objectifs de la formation 104
4-7 À propos de la plate-forme de gestion vCenter Server 105
4-8 Architecture de vCenter Server 106
4-9 Services vCenter Server 108
4-10 Surveillance de l'intégrité et de l'état des services et des nœuds dans les systèmes vCenter Server 109
4-11 Communication entre VMware ESXi et vCenter Server 110
4-12 Rappel des objectifs de la formation 111
4-13 Leçon 2 : vCenter Server Appliance 112
4-14 Objectifs de la formation 113
4-15 Présentation de vCenter Server Appliance (1) 114
4-16 Présentation de vCenter Server Appliance (2) 115
4-17 Évolutivité de vCenter Server Appliance 116
4-18 À propos de Platform Services Controller 117
4-19 À propos de vCenter Single Sign-On 118
4-20 Domaines et sites multiples vCenter Single Sign-On 119
4-21 À propos d'Enhanced Linked Mode 120
4-22 Options de déploiement de vCenter Server 121
4-23 Platform Services Controller intégré 122
4-24 Système vCenter Server externe avec une instance intégrée du système vCenter Server 123
4-25 Platform Services Controller avec l'équilibreur de charge 124
4-26 API vCenter Server 125
4-27 Haute disponibilité pour vCenter Server Appliance 126
4-28 Rappel des objectifs de la formation 127
4-29 Leçon 3 : Déploiement de vCenter Server Appliance 128
4-30 Objectifs de la formation 129
4-31 Préparation du déploiement de vCenter Server Appliance 130
4-32 Programme d'installation de l'interface utilisateur native de vCenter Server Appliance 131
4-33 Installation, mise à niveau, migration et restauration de vCenter Server 132
4-34 Déploiement de vCenter Server Appliance 133
4-35 Déploiement de vCenter Server Appliance en deux phases 134
4-36 Assistant de déploiement de vCenter Server 135
4-37 Configuration de ports personnalisés pour un déploiement de vCenter Server Appliance 136
4-38 Se lancer avec vCenter Server 137
4-39 Ajout de clés de licence à vCenter Server 138
4-40 Configuration des paramètres de vCenter Server 139
4-41 Démonstration : Utilisation de vCenter Server Appliance 140
4-42 Rappel des objectifs de la formation 141

4-43 Leçon 4 : Gestion de l'inventaire vCenter Server 142
4-44 Objectifs de la formation 143
4-45 Accès aux clients vSphere. 144
4-46 Page d'accueil de vSphere Client 145
4-47 Utilisation du volet de navigation de vSphere Client 146
4-48 Vues de vCenter Server : « Hosts and Clusters » et « VMs and Templates » 147
4-49 Vues de vCenter Server : « Storage » et « Networks ». 148
4-50 Affichage des informations relatives aux objets. 149
4-51 Utilisation des filtres rapides dans vSphere Client. 150
4-52 Glissement d'objets dans vSphere Client 151
4-53 Utilisation de la fonctionnalité Épingler/Désépingler dans vSphere Web Client 152
4-54 À propos des objets du Data Center 153
4-55 Organisation des objets de l'inventaire dans des dossiers 154
4-56 Ajout d'un Data Center et d'objets organisationnels à vCenter Server 156
4-57 Ajout d'hôtes VMware ESXi à vCenter Server. 157
4-58 Configuration du mode verrouillage. 158
4-59 Mode de verrouillage strict. 159
4-60 Création de balises personnalisées pour les objets de l'inventaire 160
4-61 Laboratoire 2 : Utilisation de vCenter Server Appliance 161
4-62 Rappel des objectifs de la formation 162
4-63 Leçon 5 : Rôles et autorisations de vCenter Server 163
4-64 Objectifs de la formation 164
4-65 À propos des autorisations vCenter Server. 165
4-66 Ajout d'autorisations à l'inventaire vCenter Server 166
4-67 À propos des rôles. 168
4-68 À propos des objets. 169
4-69 À propos des autorisations globales 170
4-70 Affichage des rôles et des affectations 171
4-71 Application des autorisations : Scénario 1. 172
4-72 Application des autorisations : Scénario 2. 173
4-73 Application des autorisations : Scénario 3. 174
4-74 Application des autorisations : Scénario 4. 175
4-75 Création d'un rôle 176
4-76 Laboratoire 3 : Utilisateurs, groupes et autorisations 177
4-77 Rappel des objectifs de la formation 178
4-78 Leçon 6 : Sauvegarde et restauration de vCenter Server Appliance. 179
4-79 Objectifs de la formation 180
4-80 Connexion à l'interface de gestion de vCenter Server Appliance 181
4-81 Fonctions de l'interface de gestion de vCenter Server Appliance Management 182
4-82 À propos des fonctions natives de sauvegarde et de restauration de vCenter Server 183
4-83 Méthodes de sauvegarde et de restauration de vCenter Server Appliance 184
4-84 Sauvegarde de vCenter Server Appliance en mode fichier. 185
4-85 Restauration de vCenter Server Appliance en mode fichier 186

4-86 Planification des sauvegardes . . . 187
4-87 Création d'un planning de sauvegarde . . . 188
4-88 Affichage du planning de sauvegarde . . . 189
4-89 Rappel des objectifs de la formation . . . 190
4-90 Leçon 7 : Surveillance de vCenter Server Appliance . . . 191
4-91 Objectifs de la formation . . . 192
4-92 Événements de vCenter Server . . . 193
4-93 Journaux du système vCenter Server . . . 194
4-94 À propos des niveaux de journalisation . . . 195
4-95 Définition des niveaux de journalisation . . . 196
4-96 Transmission de fichiers journaux vCenter Server Appliance vers une autre machine hôte . . . 197
4-97 Intégrité de la base de données vCenter Server . . . 198
4-98 Gestion des services de vCenter Server . . . 199
4-99 Surveillance de vCenter Server Appliance . . . 200
4-100 Surveillance des services vCenter Server Appliance . . . 201
4-101 Alarmes vSphere pour la détection d'épuisement des ressources et de défaillances de services . . . 202
4-102 Mises à jour correctives mensuelles pour vCenter Server Appliance . . . 203
4-103 Rappel des objectifs de la formation . . . 204
4-104 Points clés . . . 205

Module 5 Configuration et gestion des réseaux virtuels . . . 207

5-2 Vous êtes ici . . . 208
5-3 Importance . . . 209
5-4 Leçons du module . . . 210
5-5 Leçon 1 : Présentation des commutateurs vSphere Standard . . . 211
5-6 Objectifs de la formation . . . 212
5-7 Types de connexion de commutateurs virtuels . . . 213
5-8 Ajout de la mise en réseau VMware ESXi . . . 214
5-9 Exemples de connexions de commutateurs virtuels . . . 215
5-10 À propos des commutateurs standard . . . 216
5-11 Affichage de la configuration des commutateurs standard . . . 217
5-12 À propos des VLAN . . . 218
5-13 Propriétés des adaptateurs réseau . . . 219
5-14 Types de commutateur virtuel . . . 220
5-15 Architecture de commutateur distribué . . . 221
5-16 Comparatif entre les commutateurs standard et les commutateurs distribués . . . 222
5-17 Rappel des objectifs de la formation . . . 223
5-18 Leçon 2 : Configuration des règles de commutateur standard . . . 224
5-19 Objectifs de la formation . . . 225
5-20 Règles relatives aux commutateurs et aux ports réseau . . . 226
5-21 Configuration de règles de sécurité . . . 227
5-22 Règles de paramétrage du trafic . . . 229

5-23 Configuration du paramétrage du trafic 230
5-24 Règle d'association de cartes d'interface réseau et de basculement 232
5-25 Méthode d'équilibrage de charge : ID du port virtuel d'origine 234
5-26 Méthode d'équilibrage de charge : Le hachage MAC source 236
5-27 Méthode d'équilibrage de charge : Le hachage IP source et de destination 238
5-28 Détection et gestion des défaillances réseau 240
5-29 Considérations relatives au réseau physique 242
5-30 Laboratoire 4 : Utilisation de commutateurs standard 243
5-31 Rappel des objectifs de la formation 244
5-32 Points clés 245

Module 6 Configuration et gestion du stockage virtuel 247

6-2 Vous êtes ici 248
6-3 Importance 249
6-4 Leçons du module 250
6-5 Leçon 1 : Concepts liés au stockage 251
6-6 Objectifs de la formation 252
6-7 À propos des banques de données 253
6-8 Généralités sur le stockage 254
6-9 Présentation des protocoles de stockage 256
6-10 À propos de VMFS 258
6-11 À propos de NFS 260
6-12 Présentation de vSAN 261
6-13 À propos de vSphere Virtual Volumes 262
6-14 À propos du mappage de périphériques bruts (RDM) 263
6-15 Considérations relatives au stockage physique 264
6-16 Rappel des objectifs de la formation 265
6-17 Leçon 2 : Stockage Fibre Channel 266
6-18 Objectifs de la formation 267
6-19 À propos de Fibre Channel 268
6-20 Composants d'un SAN Fibre Channel 269
6-21 Adressage et contrôle d'accès Fibre Channel 270
6-22 Multipathing avec Fibre Channel 272
6-23 Adaptateurs FCoE 274
6-24 Configuration d'un FCoE logiciel : La création de ports VMkernel 275
6-25 Configuration d'un FCoE logiciel : l'activation d'adaptateurs FCoE logiciels 276
6-26 Multipathing avec FCoE logiciel 277
6-27 Rappel des objectifs de la formation 278
6-28 Leçon 3 : Stockage iSCSI 279
6-29 Objectifs de la formation 280
6-30 Composants iSCSI 281
6-31 Adressage iSCSI 282
6-32 Conventions de nommage des périphériques de stockage 283

6-33 Adaptateurs iSCSI 284
6-34 Configuration des adaptateurs iSCSI 285
6-35 Configuration réseau de VMware ESXi pour le stockage IP 286
6-36 Activation de l'adaptateur iSCSI logiciel 287
6-37 Détection des cibles iSCSI 288
6-38 Sécurité iSCSI : l'authentification CHAP 289
6-39 Stockage iSCSI et multipathing 291
6-40 Laboratoire 5 : Accès au stockage iSCSI 293
6-41 Rappel des objectifs de la formation 294
6-42 Leçon 4 : Banques de données VMFS 295
6-43 Objectifs de la formation 296
6-44 Utiliser des banques de données avec des hôtes VMware ESXi 297
6-45 Création et affichage des banques de données VMFS 299
6-46 Exploration du contenu des banques de données. 300
6-47 Gestion des banques de données surprovisionnées. 301
6-48 Augmentation de la taille des banques de données VMFS 302
6-49 Suppression ou démontage de banques de données VMFS 303
6-50 Algorithmes de multipathing 305
6-51 Configuration de l'équilibrage de la charge de stockage 306
6-52 Laboratoire 6 : Gestion des banques de données VMFS 307
6-53 Rappel des objectifs de la formation 308
6-54 Leçon 5 : Banques de données NFS. 309
6-55 Objectifs de la formation 310
6-56 Composants NFS 311
6-57 Configuration des banques de données NFS 312
6-58 NFS v3 et NFS v4.1. 313
6-59 Compatibilité des versions de NFS avec les autres technologies vSphere. 314
6-60 Nom et configuration d'une banque de données NFS. 316
6-61 Configuration de l'authentification et des informations d'authentification NFS Kerberos des hôtes VMware ESXi. 317
6-62 Configuration des banques de données pour l'utilisation de Kerberos 318
6-63 Affichage d'informations relatives au stockage IP 319
6-64 Démontage des banques de données NFS. 320
6-65 Multipathing et stockage NFS 321
6-66 Activer la jonction de sessions NFS 4.1 323
6-67 Laboratoire 7 : Accès au stockage NFS 324
6-68 Rappel des objectifs de la formation 325
6-69 Leçon 6 : Banques de données vSAN. 326
6-70 Objectifs de la formation 327
6-71 À propos de vSAN 328
6-72 Exigences liées à vSAN. 330
6-73 Configuration de vSAN 332
6-74 Groupes de disques. 333

6-75 Affichage de l'onglet « vSAN Cluster Summary » 334
6-76 Utilisation de vSAN 335
6-77 Objets présents dans les banques de données vSAN 336
6-78 Stratégies de stockage pour machine virtuelle 337
6-79 Configuration des stratégies de stockage pour machine virtuelle 338
6-80 Affichage des banques de données vSAN des machines virtuelles 339
6-81 Rappel des objectifs de la formation 340
6-82 Points clés 341

Module 7 Gestion des machines virtuelles 343

7-2 Vous êtes ici 344
7-3 Importance 345
7-4 Leçons du module 346
7-5 Leçon 1 : Création de modèles et de clones 347
7-6 Objectifs de la formation 348
7-7 Utilisation de modèles 349
7-8 Création de modèles 350
7-9 Déploiement des machines virtuelles à partir d'un modèle 351
7-10 Mise à jour des modèles 352
7-11 Clonage des machines virtuelles 353
7-12 Personnalisation du système d'exploitation client 354
7-13 À propos des clones instantanés 356
7-14 Suppression d'une machine virtuelle 357
7-15 Rappel des objectifs de la formation 358
7-16 Leçon 2 : Utilisation des bibliothèques de contenu 359
7-17 Objectifs de la formation 360
7-18 À propos des bibliothèques de contenu 361
7-19 Ajout de modèles à une bibliothèque de contenu 362
7-20 Déploiement de machines virtuelles à partir de modèles stockés dans une bibliothèque de contenu 363
7-21 Avantages liés aux bibliothèques de contenu 364
7-22 Types de bibliothèque de contenu 366
7-23 Laboratoires 367
7-24 Laboratoire 8 : Utilisation des modèles et des clones 368
7-25 Laboratoire 9 : Utilisation des bibliothèques de contenu 369
7-26 Rappel des objectifs de la formation 370
7-27 Leçon 3 : Modification de machines virtuelles 371
7-28 Objectifs de la formation 372
7-29 Modification des paramètres d'une machine virtuelle 373
7-30 Périphériques installables à chaud 374
7-31 Création de fichiers de mappage de périphériques bruts (RDM) 376
7-32 Redimensionnement dynamique d'un disque virtuel 378
7-33 Gonflage de disques à provisionnement fin 379

7-34 Options de machine virtuelle 380
7-35 Options de VMware Tools 381
7-36 Options de démarrage 382
7-37 Laboratoire 10 : Modification de machines virtuelles 383
7-38 Rappel des objectifs de la formation 384
7-39 Leçon 4 : Migration de machines virtuelles 385
7-40 Objectifs de la formation 386
7-41 Migration de machines virtuelles 387
7-42 Comparaison des types de migration 388
7-43 Migration via vSphere vMotion 389
7-44 Workflow de la migration via vSphere vMotion 391
7-45 Contraintes liées à la migration via vSphere vMotion 393
7-46 Configuration hôte requise pour la migration via vSphere vMotion 395
7-47 Contraintes de CPU pour la migration via vSphere vMotion 396
7-48 Autres paramètres de cluster : EVC pour la migration via vSphere vMotion 397
7-49 CPU de référence pour un cluster EVC 398
7-50 Conditions requises pour un cluster EVC 399
7-51 EVC par VM 400
7-52 Modifier les paramètres de masque d'identification de CPU 401
7-53 Vérification des erreurs notifiées par vSphere vMotion 402
7-54 Migration via vSphere Storage vMotion 403
7-55 Fonctionnement de vSphere Storage vMotion 404
7-56 Consignes et contraintes relatives à vSphere Storage vMotion 405
7-57 Migration vSphere vMotion « Shared-Nothing » 406
7-58 Migrations entre instances de vCenter 408
7-59 Couche réseau et pile TCP/IP de VMkernel 409
7-60 Pile TCP/IP de vSphere vMotion 411
7-61 Migration vSphere vMotion longue distance 412
7-62 Configuration réseau requise pour la migration vSphere vMotion longue distance 413
7-63 Vérifications de compatibilité réseau pour les migrations entre instances de vCenter Server 414
7-64 vSphere vMotion chiffré 415
7-65 Laboratoire 11 : Migration de machines virtuelles 416
7-66 Rappel des objectifs de la formation 417
7-67 Leçon 5 : Création de snapshots de machine virtuelle 418
7-68 Objectifs de la formation 419
7-69 Snapshots de machine virtuelle 420
7-70 Prise de snapshots 421
7-71 Types de snapshot 422
7-72 Fichiers de snapshot de machine virtuelle (1) 423
7-73 Fichiers de snapshot de machine virtuelle (2) 425
7-74 Gestion des snapshots 426
7-75 Suppression de snapshots de machine virtuelle (1) 427
7-76 Suppression de snapshots de machine virtuelle (2) 428

7-77 Suppression de snapshots de machine virtuelle (3) 429
7-78 Suppression de tous les snapshots d'une machine virtuelle 430
7-79 À propos de la consolidation des snapshots 431
7-80 Détermination du moment où une consolidation des snapshots est nécessaire 432
7-81 Détermination du moment où une consolidation des snapshots est nécessaire 433
7-82 Exécution de la consolidation des snapshots 434
7-83 Configuration du nombre maximal de snapshots autorisé pour une machine virtuelle 435
7-84 Laboratoire 12 : Gestion des machines virtuelles 436
7-85 Rappel des objectifs de la formation 437
7-86 Points clés 438

Module 8 Gestion et surveillance des ressources 439

8-2 Vous êtes ici 440
8-3 Importance 441
8-4 Leçons du module 442
8-5 Leçon 1 : Concepts relatifs aux CPU et à la mémoire virtuels 443
8-6 Objectifs de la formation 444
8-7 Principes de base sur la virtualisation de la mémoire 445
8-8 Surdimensionnement de la mémoire des machines virtuelles 446
8-9 Techniques de récupération de la mémoire 448
8-10 Configuration de CPU virtuels multicœurs 450
8-11 À propos de l'hyperthreading 451
8-12 Équilibrage de charge CPU 452
8-13 Rappel des objectifs de la formation 453
8-14 Leçon 2 : Contrôles des ressources et pools de ressources 454
8-15 Objectifs de la formation 455
8-16 Parts, limites et réservations 456
8-17 Définition des paramètres de ressources pour des VM ponctuelles 457
8-18 Partage des ressources par les VMs 459
8-19 À propos des pools de ressources 460
8-20 Attributs des pools de ressources 461
8-21 Quelques raisons justifiant l'utilisation des pools de ressources 462
8-22 Exemple de pool de ressources 463
8-23 Exemple de pool de ressources : Parts de CPU 464
8-24 Exemple de pool de ressources : Contention CPU 465
8-25 À propos des réservations extensibles 466
8-26 Exemple de réservation extensible (1) 467
8-27 Exemple de réservation extensible (2) 468
8-28 Contrôle d'admission pour les réservations de CPU et de mémoire 469
8-29 Onglet « Resource Pool Summary Tab » 470
8-30 Onglet « Resource Reservation » 471
8-31 Planification des modifications apportées aux paramètres de ressources 472
8-32 Gestion de machines virtuelles à l'aide de vApps 473

8-33 Caractéristiques d'une vApp 474
8-34 Exportation et déploiement de vApps 475
8-35 Laboratoire 13 : Gestion des pools de ressources 476
8-36 Rappel des objectifs de la formation 477
8-37 Leçon 3 : Surveillance du taux d'utilisation des ressources 478
8-38 Objectifs de la formation 479
8-39 Méthodologie de réglage des performances 480
8-40 Outils de surveillance des ressources 481
8-41 Outils de surveillance du système d'exploitation client 482
8-42 Utilisation de l'outil Perfmon pour surveiller les ressources des VMs 483
8-43 Utilisation de l'outil esxtop pour surveiller les ressources des VMs. 484
8-44 Surveillance des objets d'inventaire via les diagrammes de performances 485
8-45 Utilisation des diagrammes de performances généraux 487
8-46 Utilisation des diagrammes de performances avancés 488
8-47 Options des diagrammes : Données en temps réel et historiques 489
8-48 À propos des types de diagramme 491
8-49 Enregistrement des diagrammes. 492
8-50 À propos des objets et des compteurs 493
8-51 À propos des types de statistiques 494
8-52 À propos des cumuls 495
8-53 Interprétation des données produites par les outils 497
8-54 Machines virtuelles limitées en ressources CPU. 498
8-55 VM limitées en ressources mémoire 500
8-56 Hôtes limités en ressources mémoire 501
8-57 Surveillance de la mémoire active des VMs 502
8-58 Machines virtuelles limitées en ressources disque 503
8-59 Surveillance de la latence de disque 504
8-60 Machines virtuelles limitées en ressources réseau 505
8-61 Laboratoire 14 : Surveillance des performances des machines virtuelles. 506
8-62 Rappel des objectifs de la formation 507
8-63 Leçon 4 : Utilisation des alarmes. 508
8-64 Objectifs de la formation 509
8-65 À propos des alarmes 510
8-66 Paramètres des alarmes 511
8-67 Déclencheurs d'alarmes 512
8-68 Configuration de déclencheurs de condition ou d'état. 513
8-69 Configuration des déclencheurs d'événement. 514
8-70 Configuration des actions 515
8-71 Configuration des notifications de vCenter Server 517
8-72 Affichage et accusé de réception des alarmes déclenchées. 518
8-73 Laboratoire 15 : Utilisation des alarmes 519
8-74 Rappel des objectifs de la formation 520
8-75 Points clés 521

Module 9 vSphere HA, vSphere Fault Tolerance et protection des données . 523
9-2 Vous êtes ici . . . 524
9-3 Importance . . . 525
9-4 Leçons du module . . . 526
9-5 Leçon 1 : Présentation de vSphere HA . . . 527
9-6 Objectifs de la formation . . . 528
9-7 Protection à tous les niveaux . . . 529
9-8 Disponibilité de vCenter Server : Recommandations . . . 531
9-9 À propos de vSphere HA . . . 532
9-10 Scénario d'utilisation de vSphere HA : Panne d'un hôte VMware ESXi . . . 533
9-11 Scénario d'utilisation de vSphere HA : Panne du système d'exploitation client . . . 534
9-12 Scénario d'utilisation de vSphere HA : Échec d'application . . . 535
9-13 Scénario d'utilisation de vSphere HA : Perte d'accès aux banques de données . . . 536
9-14 Scénario d'utilisation de vSphere HA : Protection des machines virtuelles contre l'isolation réseau . . . 537
9-15 Importance des réseaux de signal de pulsation redondants . . . 538
9-16 Redondance via l'association de cartes d'interface réseau . . . 539
9-17 Redondance via des réseaux supplémentaires . . . 540
9-18 Rappel des objectifs de la formation . . . 541
9-19 Leçon 2 : Architecture de vSphere HA . . . 542
9-20 Objectifs de la formation . . . 543
9-21 Architecture vSphere HA : Communication avec les agents . . . 544
9-22 Architecture vSphere HA : Signaux de pulsation réseau . . . 546
9-23 Architecture vSphere HA : Signaux de pulsation de banque de données . . . 547
9-24 Scénarios de panne vSphere HA . . . 548
9-25 Hôtes esclaves défaillants . . . 549
9-26 Hôtes maîtres défaillants . . . 550
9-27 Hôtes isolés . . . 551
9-28 Considérations de conception . . . 552
9-29 Pannes du stockage des machines virtuelles . . . 553
9-30 À propos de VMCP . . . 554
9-31 Rappel des objectifs de la formation . . . 555
9-32 Leçon 3 : Configuration de vSphere HA . . . 556
9-33 Objectifs de la formation . . . 557
9-34 À propos des clusters . . . 558
9-35 Conditions requises pour vSphere HA . . . 559
9-36 Configuration des paramètres de vSphere HA . . . 560
9-37 Paramètres de vSphere HA : « Failures and Responses » . . . 561
9-38 Paramètres de vSphere HA : « VM Monitoring » . . . 562
9-39 Paramètres de vSphere HA : « Heartbeat Datastores » . . . 563
9-40 Paramètres de vSphere HA : « Admission Control » . . . 564
9-41 Exemple : Contrôle d'admission basé sur un pourcentage des ressources du cluster . . . 565
9-42 Exemple : Contrôle d'admission basé sur des slots . . . 566

9-43 Paramètres de vSphere HA : « Performance Degradation VMs Tolerate » 567
9-44 Paramètres de vSphere HA : « Advanced Options » 568
9-45 À propos du redémarrage orchestré de vSphere HA 569
9-46 Configuration du redémarrage orchestré par vSphere HA 570
9-47 Dépendances des machines virtuelles lors du redémarrage orchestré 571
9-48 Configuration et maintenance du réseau 572
9-49 Réservation de ressources de cluster 573
9-50 Surveillance de l'état du cluster 574
9-51 Laboratoire 16 : Utilisation de vSphere HA 575
9-52 Rappel des objectifs de la formation 576
9-53 Leçon 4 : Présentation de vSphere Fault Tolerance 577
9-54 Objectifs de la formation 578
9-55 À propos de vSphere Fault Tolerance 579
9-56 Fonctionnalités de vSphere Fault Tolerance 581
9-57 vSphere Fault Tolerance avec vSphere HA et vSphere DRS 582
9-58 Fichiers VMDK redondants 583
9-59 Point de contrôle de vSphere Fault Tolerance 584
9-60 vSphere Fault Tolerance : Copie préalable 585
9-61 Point de contrôle rapide de vSphere Fault Tolerance 586
9-62 Fichiers partagés vSphere Fault Tolerance 587
9-63 À propos du fichier shared.vmft 588
9-64 Activation de vSphere Fault Tolerance sur une machine virtuelle 589
9-65 Rappel des objectifs de la formation 590
9-66 Leçon 5 : vSphere Replication 591
9-67 Objectifs de la formation 592
9-68 À propos de vSphere Replication 593
9-69 À propos de l'appliance vSphere Replication 594
9-70 Fonctions de réplication 595
9-71 Déploiement de l'appliance virtuelle vSphere Replication 596
9-72 Configuration de vSphere Replication pour une seule machine virtuelle 597
9-73 Configuration de plusieurs instantanés et de l'objectif de point de reprise 599
9-74 Récupération de machines virtuelles 601
9-75 vSphere Storage APIs - Data Protection 602
9-76 Délestage du traitement des sauvegardes 603
9-77 À propos du suivi des blocs modifiés 605
9-78 Rappel des objectifs de la formation 606
9-79 Points clés 607

Module 10 vSphere DRS 609

10-2 Vous êtes ici 610
10-3 Importance 611
10-4 Objectifs de la formation 612
10-5 À propos de vSphere DRS 613

10-6 Conditions requises pour le cluster vSphere DRS . . . 614
10-7 Paramètres du cluster vSphere DRS : Niveau d'automatisation . . . 615
10-8 Paramètres du cluster vSphere DRS : « Predictive DRS » . . . 617
10-9 Autres paramètres de cluster : Emplacement du fichier d'échange . . . 618
10-10 Paramètres du cluster vSphere DRS : affinité entre les machines virtuelles . . . 619
10-11 Paramètres du cluster vSphere DRS : groupes DRS . . . 620
10-12 Paramètres du cluster vSphere DRS : règles d'affinité VM/hôte . . . 621
10-13 Règle d'affinité VM/hôte : préférentielle . . . 622
10-14 Règle d'affinité VM/hôte : obligatoire . . . 623
10-15 Paramètres du cluster vSphere DRS : automatisation à l'échelle d'une VM . . . 624
10-16 Ajout d'un hôte à un cluster . . . 625
10-17 Affichage des informations relatives au cluster vSphere DRS . . . 626
10-18 Affichage des recommandations relatives à vSphere DRS . . . 628
10-19 Surveillance de l'état du cluster . . . 629
10-20 Mode maintenance et mode veille . . . 630
10-21 Suppression d'un hôte du cluster vSphere DRS . . . 631
10-22 Désactivation de vSphere DRS et restauration d'une arborescence de pools de ressources . . . 633
10-23 Méthodes d'amélioration des performances des machines virtuelles . . . 634
10-24 Utilisation de VMware vSphere HA avec vSphere DRS . . . 636
10-25 Laboratoire 17 : Mise en œuvre des clusters vSphere DRS . . . 637
10-26 Rappel des objectifs de la formation . . . 638
10-27 Points clés . . . 639

Module 11 vSphere Update Manager . . . 641

11-2 Vous êtes ici . . . 642
11-3 Importance . . . 643
11-4 Objectifs de la formation . . . 644
11-5 À propos de vSphere Update Manager . . . 645
11-6 Fonctionnalités de vSphere Update Manager . . . 647
11-7 Composants de vSphere Update Manager . . . 648
11-8 Configuration de vSphere Update Manager . . . 649
11-9 Références et groupes de références . . . 651
11-10 Création et modification de références d'extension ou de correctif . . . 653
11-11 Association de références . . . 654
11-12 Analyse de mises à jour . . . 655
11-13 Vérification de la conformité des objets vSphere . . . 656
11-14 Mise en conformité des objets . . . 657
11-15 Notification de rappel de correctif . . . 659
11-16 Intégration d'EAM avec vSphere Update Manager . . . 660
11-17 Intégration de vSAN avec vSphere Update Manager . . . 661
11-18 À propos des références système . . . 662
11-19 Intégration de vSphere Update Manager avec vSphere DRS . . . 663
11-20 Laboratoire 18 : Utilisation de vSphere Update Manager . . . 664

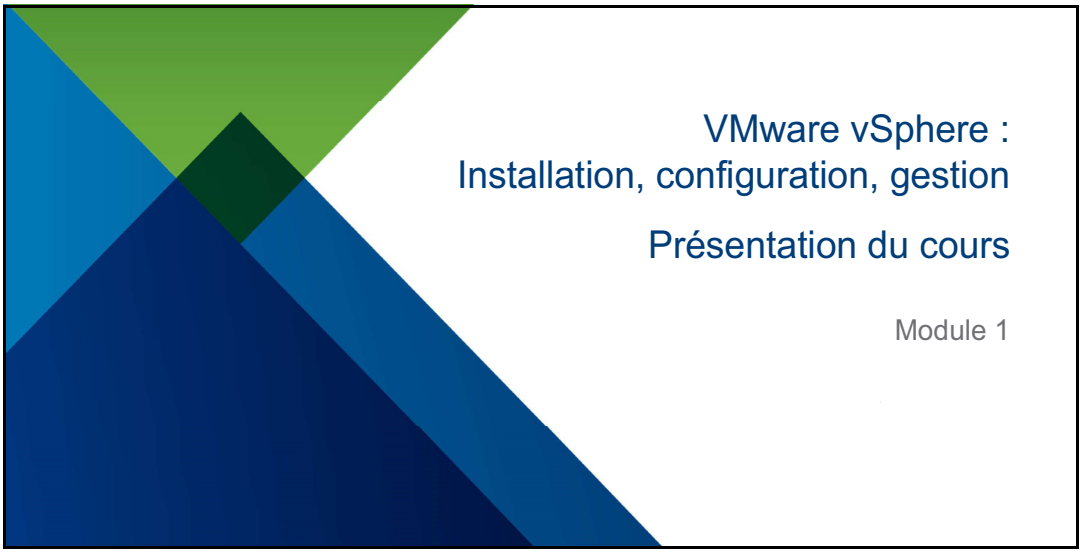
11-21 Rappel des objectifs de la formation 665
11-22 Points clés 666

Module 12 Résolution des problèmes vSphere 667

12-2 Vous êtes ici 668
12-3 Importance 669
12-4 Leçons du module 670
12-5 Leçon 1 : Outils de résolution des problèmes 671
12-6 Objectifs de la formation 672
12-7 À propos de la Base de connaissances VMware 673
12-8 À propos de la Communauté VMware 674
12-9 À propos de VMware Host Client 675
12-10 Surveillance de l'environnement virtuel à l'aide des diagrammes de performances 676
12-11 Visualisation et interprétation des informations de diagnostic 677
12-12 Emplacement des journaux vCenter Server 678
12-13 Journaux communs 679
12-14 Journaux de nœud de gestion 680
12-15 Journaux Platform Services Controller 681
12-16 Journal vCenter Server important pour la résolution des problèmes 682
12-17 Emplacement des journaux d'hôte VMware ESXi 683
12-18 Journaux d'hôte VMware ESXi utiles pour la résolution des problèmes 684
12-19 Visualisation des fichiers journaux vCenter Server dans vSphere Web Client 685
12-20 Visualisation des fichiers journaux dans DCUI 686
12-21 À propos de vSphere Syslog Collector 687
12-22 Rappel des objectifs de la formation 688
12-23 Leçon 2 : Présentation de la résolution des problèmes 689
12-24 Objectifs de la formation 690
12-25 Processus de résolution des problèmes 691
12-26 Définition d'un problème système 692
12-27 Collecte des symptômes d'un problème 693
12-28 Collecte d'informations supplémentaires 694
12-29 Identification des causes possibles et choix de l'approche appropriée 695
12-30 Détermination de la cause profonde 696
12-31 Résolution du problème 697
12-32 Exemple de scénario : définition du problème 698
12-33 Exemple : collecte d'informations 699
12-34 Exemple : identification des causes possibles 700
12-35 Exemple : résolution du problème 701
12-36 Définition des niveaux de gravité et des temps de réponse cibles VMware 702
12-37 Rappel des objectifs de la formation 703
12-38 Points clés 704

MODULE 1

Présentation du cours



1-2 Importance

Les administrateurs doivent posséder les connaissances, compétences et capacités requises pour créer et exécuter un environnement VMware vSphere®.

Ils doivent savoir installer et configurer des hôtes VMware ESXi™ ainsi que le logiciel VMware vCenter Server®. Ils doivent également connaître les procédures de gestion des hôtes VMware ESXi et des machines virtuelles avec vCenter Server.

1-3 Objectifs de la formation (1)

À la fin de ce cours, vous devriez être en mesure d'atteindre les objectifs suivants :

- installer et configurer les hôtes VMware ESXi ;
- déployer et configurer VMware vCenter® Server Appliance™ ;
- créer un planning de sauvegarde pour l'instance vCenter Server Appliance ;
- utiliser VMware vSphere® Client™ pour gérer l'inventaire et la configuration vCenter Server ;
- configurer des réseaux virtuels avec des commutateurs standard vSphere ;
- décrire les technologies de stockage prises en charge par vSphere ;
- configurer le stockage virtuel à l'aide du stockage iSCSI et NFS ;
- créer et gérer des banques de données VMware vSphere® VMFS ;
- utiliser vSphere Client pour créer des machines virtuelles, des modèles, des clones et des snapshots ;
- créer une bibliothèque de contenu pour déployer des machines virtuelles ;
- gérer l'utilisation des ressources de machine virtuelle et les pools de ressources.

1-4 Objectifs de la formation (2)

À la fin de ce cours, vous devriez être en mesure d'atteindre les objectifs suivants :

- migrer les machines virtuelles avec VMware vSphere® vMotion® et VMware vSphere® Storage vMotion® ;
- expliquer comment utiliser une méthodologie de résolution des problèmes pour diagnostiquer et corriger les problèmes dans un environnement vSphere ;
- accéder au shell vCenter Server Appliance pour diagnostiquer les problèmes et surveiller l'intégrité de la base de données vCenter Server ;
- utiliser la ligne de commande et VMware vRealize® Log Insight™ pour afficher les fichiers journaux ;
- créer et gérer un cluster vSphere configuré avec VMware vSphere® High Availability et VMware vSphere® Distributed Resource Scheduler™ ;
- décrire les méthodes de protection et de récupération des données de machine virtuelle ;
- utiliser VMware vSphere® Update Manager™ pour appliquer des correctifs et des mises à niveau aux hôtes VMware ESXi et aux machines virtuelles ;
- expliquer comment utiliser une méthodologie de résolution des problèmes pour diagnostiquer et corriger les problèmes dans vSphere.

1-5 Vous êtes ici

1. **Présentation du cours**
2. Présentation de vSphere et du Software-Defined Data Center
3. Création de machines virtuelles
4. vCenter Server
5. Configuration et gestion des réseaux virtuels
6. Configuration et gestion du stockage virtuel
7. Gestion des machines virtuelles
8. Gestion et surveillance des ressources
9. vSphere HA, vSphere Fault Tolerance et protection des données
10. vSphere DRS
11. vSphere Update Manager
12. Résolution des problèmes vSphere

1-6 Conventions typographiques

Ce cours fait appel aux conventions ci-après.

`Police de caractères à espacement fixe`	Noms de fichier, de dossier, de chemin et de commande. Accédez au dossier `VMS`.
`Police de caractères à espacement fixe en gras`	Saisie de l'utilisateur. Exemple : Saisissez la commande **`ipconfig /release`**.
Police de caractères gras	Commandes de l'interface utilisateur. Exemple : Cliquez sur l'onglet **Configuration**.
Italique	Titres de manuel et variables de substitution : • *Guide d'administration d'une machine virtuelle vSphere* • *Nom_hôte_VMware_ESXi*

1-7 Références

Titre	Emplacement
Guide d'installation et de configuration vSphere	https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-vcenter-server-67-installation-guide.pdf
Guide de gestion d'hôtes vCenter Server	https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-vcenter-server-67-host-management-guide.pdf
Guide d'administration d'une machine virtuelle vSphere	https://docs.vmware.com/en/VMware-vSphere/6.0/vsphere-esxi-vcenter-server-601-virtual-machine-admin-guide.pdf
Guide de réseau vSphere	https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-vcenter-server-67-networking-guide.pdf
Sécurité de vSphere	https://docs.vmware.com/en/VMware-vSphere/index.html
Guide de gestion des ressources de vSphere	https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-vcenter-server-67-resource-management-guide.pdf
Guide de disponibilité vSphere	https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-vcenter-server-67-availability-guide.pdf
Surveillance et performances vSphere	https://docs.vmware.com/en/VMware-vSphere/index.html

1-8 Ressources en ligne VMware

Documentation vSphere : https://docs.vmware.com/en/VMware-vSphere/index.html

Configurations maximales de VMware : https://configmax.vmware.com/home

Blog VMware vSphere : http://blogs.vmware.com/vsphere/

Communautés de VMware : http://communities.vmware.com

Support VMware : http://www.vmware.com/fr/support

Formations VMware : http://www.vmware.com/education

Certification VMware : https://www.vmware.com/fr/education-services/certification.html

Blog VMware sur les formations et certifications : http://blogs.vmware.com/education/

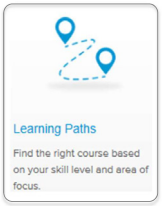
1-9 Alignement sur la certification VCP-Foundations

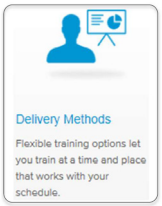
VMware vSphere : Le cours « Installation, configuration et gestion » s'aligne sur la certification VCP-Foundations :

- Le descriptif de l'examen VCP-Foundations a fourni la trame pour la conception du présent cours.
- Il est recommandé de se référer au descriptif de l'examen VCP-Foundations pour se préparer au test.
- Ce cours ne doit pas être l'unique ressource utilisée pour la préparation de l'examen.
- Pour plus de détails sur les certifications VMware, consultez la page suivante : https://mylearn.vmware.com/mgrReg/plan.cfm?plan=64178&ui=www_cert

1-10 Présentation des services de formation VMware

VMware Education propose des programmes de formation et de certification conçus pour développer vos compétences en matière de technologie VMware.





Les parcours de formation vous aident à identifier le cours dont vous avez besoin en fonction du produit, de votre rôle et de votre niveau d'expérience.

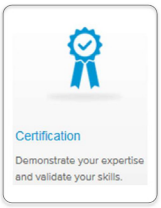
Par exemple, le présent cours s'inscrit dans le parcours de formation en infrastructure de virtualisation de Data Center.

Exemples de formats de formation :

- À la demande :
  - Solution d'autoformation associant modules de cours théoriques et laboratoires d'essai pratique. Ce format offre une alternative à la formation traditionnelle en salle de classe.
- Lab Connect :
  - Environnement de laboratoire technique en autoformation conçu pour vous aider à parfaire vos apprentissages.
  - Ces laboratoires à la demande basés sur le Cloud vous permettent de mettre en pratique les compétences acquises dans le cadre des cours avec instructeur et de vous entraîner avant de les appliquer en situation réelle.

1-11 Présentation des certifications VMware

La certification VMware établit un référentiel pour les professionnels de l'informatique et valide les compétences essentielles en matière de technologie VMware.



Le présent cours permet de remplir les conditions de formation nécessaires à l'obtention de la certification VMware Certified Professional 6 – Data Center Virtualization (VCP6-DCV).

VMware Learning Zone met à disposition sur le Cloud une bibliothèque de vidéos conçues pour vous aider à préparer efficacement l'examen de certification afin de l'aborder en toute confiance.

MODULE 2

Présentation de vSphere et du Software-Defined Data Center

2-2 Vous êtes ici

1. Présentation du cours
2. **Présentation de vSphere et du Software-Defined Data Center**
3. Création de machines virtuelles
4. vCenter Server
5. Configuration et gestion des réseaux virtuels
6. Configuration et gestion du stockage virtuel
9. Gestion des machines virtuelles
10. Gestion et surveillance des ressources
11. vSphere HA, vSphere Fault Tolerance et protection des données
12. vSphere DRS
13. vSphere Update Manager
14. Résolution des problèmes vSphere

2-3 Importance

En tant qu'administrateur vSphere, vous devez être familiarisé avec les nombreux composants de cette plate-forme. Vous devez également maîtriser les concepts et bonnes pratiques ci-après :

- Virtualisation, rôle de l'hyperviseur VMware ESXi dans la virtualisation, et machines virtuelles
- Composants essentiels de vSphere, et utilisation de vSphere dans le cadre du Software-Defined Data Center
- Mise en œuvre des clients vSphere à des fins d'administration et de gestion des environnements vSphere

2-4 Leçons du module

Leçon 1 :	Présentation de vSphere et des machines virtuelles
Leçon 2 :	Ressources partagées : présentation de VMware ESXi

2-5 Leçon 1 : Présentation de vSphere et des machines virtuelles

2-6 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Montrer comment vSphere s'inscrit dans le Software-Defined Data Center et dans l'infrastructure Cloud
- Expliquer comment vSphere interagit avec les CPU, la mémoire, les réseaux et les systèmes de stockage
- Naviguer dans vSphere Client et examiner les paramètres des VMs
- Identifier les fichiers qui constituent une machine virtuelle
- Identifier les méthodes d'accès à la console d'une machine virtuelle
- Identifier les cartes réseau virtuelles et les avantages de l'adaptateur VMXNET3
- Comparer les types de provisionnement de disque virtuel

2-7 À propos des machines virtuelles

Une machine virtuelle constitue une représentation logicielle d'un ordinateur physique et de ses composants.

Le logiciel de virtualisation convertit la machine physique et ses composants en fichiers.

Machine virtuelle

Composants des machines virtuelles

- Système d'exploitation
- VMware Tools™
- Ressources virtuelles, telles que :
  - CPU et mémoire
  - Cartes réseau
  - Disques et contrôleurs
  - Ports parallèles et série

La machine virtuelle comprend un ensemble de fichiers de spécification et de configuration, et repose sur les ressources physiques d'un hôte. Chaque machine virtuelle comprend des périphériques virtuels qui offrent les mêmes fonctionnalités que le matériel physique tout en garantissant des niveaux supérieurs de portabilité, de sécurité et de gérabilité.

Une machine virtuelle comprend généralement un système d'exploitation, des applications, VMware Tools™, ainsi que des ressources et des composants matériels virtuels, que vous gérez pratiquement de la même manière qu'un ordinateur physique.

VMware Tools est une suite d'utilitaires que vous installez sur le système d'exploitation d'une machine virtuelle, et qui permet d'optimiser les performances et la gestion de cette machine virtuelle.

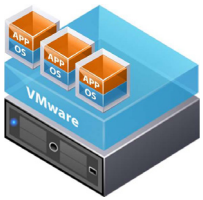
2-8 Avantages liés à l'utilisation de machines virtuelles

Machines physiques

- Difficiles à déplacer ou à copier
- Liées à un ensemble déterminé de composants matériels
- Cycle de vie généralement court
- Requièrent une intervention physique pour la mise à niveau du matériel

Machines virtuelles

- Faciles à déplacer ou à copier :
  - Encapsulées dans des fichiers
  - Indépendantes du matériel physique
- Simples à gérer :
  - Isolées des autres machines virtuelles exécutées sur le même matériel physique
  - Insensibles aux changements affectant le matériel physique



Dans le cas d'une machine physique, le système d'exploitation (par exemple, Windows, UNIX ou Linux) s'installe directement sur le matériel. Ce système d'exploitation requiert un pilote de périphérique spécifique pour chaque composant matériel pris en charge. À chaque mise à niveau d'un composant matériel de l'ordinateur, un nouveau pilote de périphérique doit être installé.

Lorsque les applications sont directement interfacées avec les pilotes matériels, toute mise à niveau du matériel et/ou des pilotes peut s'avérer lourde de conséquences en cas d'incompatibilité. Ces répercussions potentielles obligent le personnel chargé du support technique à tester les mises à niveau des composants matériels avec un vaste éventail de suites d'applications et de systèmes d'exploitation.

La virtualisation de ces systèmes permet de réaliser des économies sur ce poste, dans la mesure où les machines virtuelles sont 100 % logicielles.

De plus, les machines virtuelles sont isolées les unes des autres. Un serveur de base de données peut par conséquent coexister avec un serveur de messagerie sur un même ordinateur physique. Cette séparation entre les machines virtuelles prévient les problèmes résultant de conflits de dépendances logicielles. Aucun utilisateur, même s'il dispose de privilèges d'administrateur système sur le système d'exploitation client d'une machine virtuelle, n'est habilité à traverser cette couche d'isolation pour accéder à une autre machine virtuelle, à moins que l'administrateur système VMware ESXi™ lui ait expressément accordé l'autorisation d'accès requise. Du fait de l'isolation des machines virtuelles, une défaillance du système d'exploitation client exécuté sur une machine virtuelle n'affecte ni l'état, ni le fonctionnement des autres machines virtuelles s'exécutant sur le même hôte.

Une défaillance du système d'exploitation client n'a aucune incidence sur :

- l'accès des utilisateurs aux autres machines virtuelles ;
- l'accès des machines virtuelles opérationnelles aux ressources dont elles ont besoin ;
- les performances des autres machines virtuelles.

Les machines virtuelles vous permettent de consolider vos serveurs physiques et d'utiliser plus efficacement votre matériel. Dans la mesure où elle est constituée d'un ensemble de fichiers, une machine virtuelle vous offre des fonctionnalités qui ne sont pas disponibles ou qui sont moins efficaces dans les architectures physiques. Par exemple,

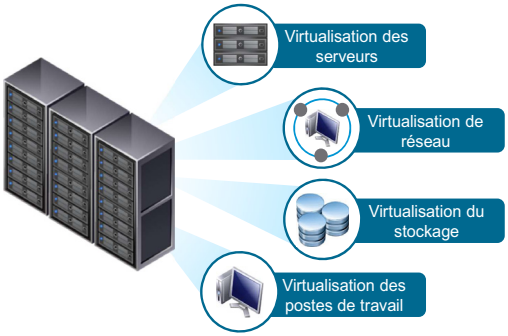
- vous pouvez provisionner des machines virtuelles de façon rapide et cohérente.
- Les machines virtuelles se prêtent à des scénarios de migration à chaud, de tolérance aux pannes, de haute disponibilité et de reprise d'activité améliorée, qui permettent de maximiser la disponibilité et réduire le temps de reprise en cas de défaillance.
- La mutualisation vous permet de combiner des machines virtuelles pour créer des configurations spécialisées, telles qu'une zone DMZ.

Les machines virtuelles permettent de prendre en charge les applications et systèmes d'exploitation legacy sur du nouveau matériel lorsque le contrat de maintenance du matériel existant arrive à expiration.

2-9 Les différents types de virtualisation

La virtualisation est le processus qui consiste à créer une version logicielle d'une entité physique, comme un serveur, un réseau de postes de travail ou un périphérique de stockage.

La virtualisation est la manière la plus efficace de réduire les dépenses informatiques tout en stimulant l'efficacité et la flexibilité des entreprises de toute taille.



La virtualisation des serveurs résout ces problèmes d'efficacité en permettant d'exécuter plusieurs systèmes d'exploitation sur un même serveur physique, sous la forme de machines virtuelles. Chacune d'elles peut accéder aux ressources de calcul du serveur sous-jacent.

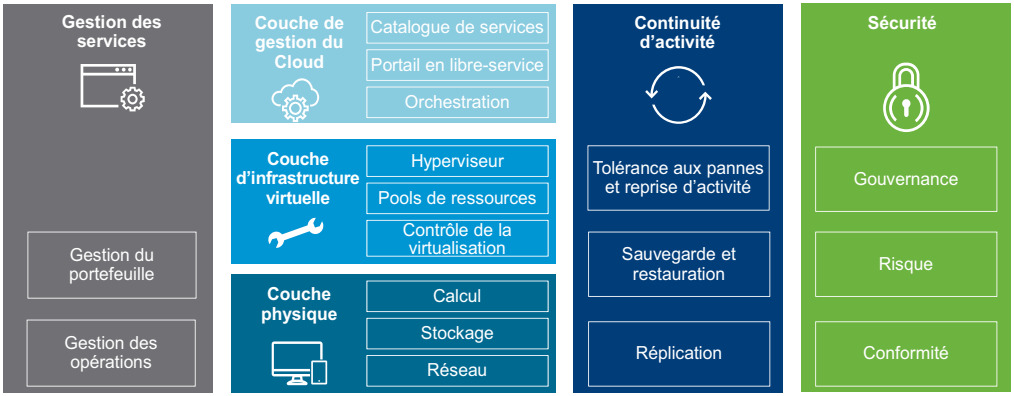
La virtualisation de réseau est la reproduction logicielle complète d'un réseau physique. Les applications du réseau virtuel s'exécutent de la même manière que si elles se trouvaient sur un réseau physique.

La virtualisation du stockage est le processus qui consiste à créer une version logicielle des périphériques de stockage réseau dans une unité paraissant unique.

Le déploiement de postes de travail sous la forme d'un service géré vous permet de réagir plus rapidement à l'évolution des besoins et des opportunités.

2-10 À propos du Software-Defined Data Center

Dans un Software-Defined Data Center, l'infrastructure est virtualisée à 100 % et le contrôle est entièrement automatisé par logiciel. vSphere est la pierre angulaire du Software-Defined Data Center.



Un Software-Defined Data Center est doté de ressources de calcul, de stockage, de réseau et de sécurité isolées, et son déploiement est plus rapide que celui d'un Data Center classique basé sur le matériel. Toutes les ressources (CPU, mémoire, disque et réseau) d'un software-defined virtual Data Center sont abstraites et intégrées dans des fichiers, offrant ainsi tous les avantages de la virtualisation à tous les niveaux de l'infrastructure, et ce, indépendamment de l'infrastructure physique sous-jacente.

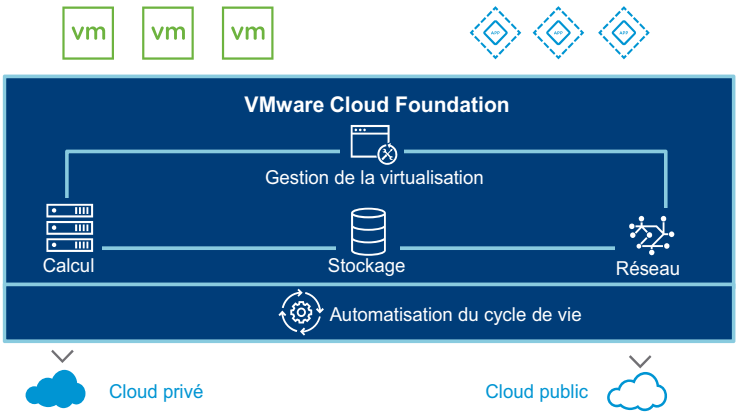
Le Software-Defined Data Center peut inclure les composants suivants :

- Gestion des services : utilisez la gestion des services pour suivre et analyser les opérations de plusieurs sources de données dans le SDDC multirégion. Déployez vRealize Operations Manager et vRealize Log Insight sur plusieurs nœuds pour obtenir une disponibilité continue et de meilleurs taux d'ingestion des journaux.
- Couche de gestion du Cloud : la couche de gestion du Cloud comprend le catalogue de services avec les installations à déployer, l'orchestration qui fournit les workflows pour le déploiement des éléments du catalogue, et le portail en libre-service qui permet aux utilisateurs d'utiliser le SDDC.
- Couche d'infrastructure virtuelle : cette couche établit un environnement virtualisé robuste dans lequel toutes les autres solutions s'intègrent. Cette couche comprend la plate-forme de virtualisation pour l'hyperviseur, les pools de ressources et le contrôle de la virtualisation. Il existe des processus et technologies supplémentaires dans l'infrastructure permettant l'activation des modèles Infrastructure sous forme de service (IaaS) et Plate-forme sous forme de service (PaaS).

- Couche physique : la couche la plus basse de la solution comprend les composants de calcul, de stockage et de réseau.
- Business Continuity : Utilisez la continuité d'activité pour créer des tâches de sauvegarde dans vSphere Data Protection pour vRealize Operations Manager, vRealize Log Insight, VMware NSX et vRealize Automation. En cas de dysfonctionnement matériel, vous pouvez restaurer les composants de ces produits grâce aux sauvegardes.
- La sécurité : les clients utilisent cette couche de la plate-forme pour répondre aux exigences de conformité liées aux charges de travail virtualisées et pour gérer les risques liés à l'activité.

2-11 vSphere et le Cloud Computing

Le Cloud Computing est fondé sur le regroupement efficace des ressources dans le cadre d'une infrastructure virtuelle autogérée à la demande.



Selon la définition établie par le NIST (National Institute of Standards and Technology), le Cloud Computing est un modèle permettant d'offrir à la demande un accès réseau omniprésent et pratique à un pool partagé de ressources informatiques configurables. Par exemple, les réseaux, serveurs, ressources de stockage, applications et services peuvent être provisionnés et lancés rapidement, avec un minimum de gestion ou d'interaction avec le fournisseur de services. vSphere est le socle technologique qui fournit les pools de ressources partagés et configurables. vSphere isole les ressources physiques du Data Center afin de séparer la charge de travail et le matériel physique. Une interface utilisateur logicielle peut fournir un cadre de gestion et de maintenance pour les processus d'abstraction et d'attribution.

VMware Cloud Foundation™ inclut une infrastructure Cloud intégrée (calcul, stockage, réseau et sécurité) et des services de gestion du Cloud qui permettent d'exécuter des applications d'entreprise dans des environnements privés et publics. Cloud Foundation étend l'hyperviseur principal vSphere avec des fonctionnalités intégrées de software-defined storage, de software-defined networking and security qui peuvent être consommées de manière flexible on premise ou en tant que service dans le Cloud public (VMware Cloud™ on AWS ou fournisseurs de Cloud VMware).

Cas d'utilisation :

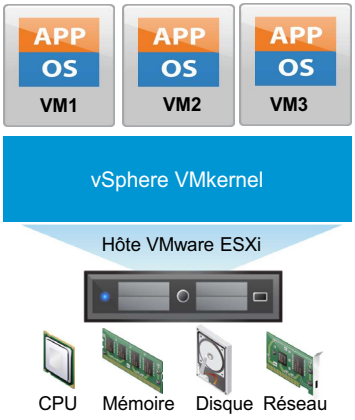
- Infrastructure Cloud : exploitez les hauts niveaux de performances, de disponibilité et d'évolutivité offerts par la plate-forme Software-Defined Data Center (SDDC) de VMware lors de l'exécution de vos applications stratégiques, telles que bases de données, applications Web et infrastructure de postes de travail virtuels (VDI).
- Automatisation de l'informatique : automatisation de la fourniture de l'infrastructure et des applications avec des fonctionnalités en libre-service.

- VDI : Solution complète de déploiement VDI à grande échelle. Elle simplifie la planification et la conception grâce à des solutions standardisées et testées, pleinement optimisées pour les charges de travail VDI.
- Cloud hybride : Créez un véritable Cloud hybride avec une infrastructure commune et un modèle opérationnel cohérent, et connectez votre Data Center on premise et off premise qui est compatible, étendu et distribué.

Pour en savoir plus sur les solutions de Cloud Computing de VMware, consultez le site http://www.vmware.com/fr/cloud-computing/overview.html.

2-12 Machine virtuelle : client et consommateur des ressources de l'hôte VMware ESXi

Toute application, quel que soit son système d'exploitation, peut être exécutée sur une machine virtuelle (cliente) et consommer les ressources CPU, mémoire, disque et réseau disponibles sur l'hôte.

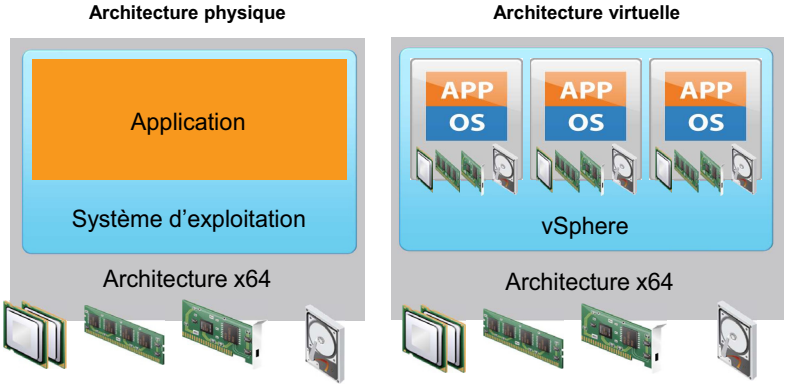


Une machine virtuelle est une abstraction logicielle d'une machine physique convertissant les composants en fichiers qui se comportent comme des composants physiques.

Pour connaître la liste complète des systèmes d'exploitation pris en charge, consultez la page https://www.vmware.com/resources/compatibility/search.php.

2-13 Architecture physique et architecture virtuelle

La virtualisation est une technologie qui permet d'abstraire les composants physiques sous la forme de composants logiciels, résolvant ainsi de nombreuses problématiques auxquelles les départements informatiques sont confrontés.

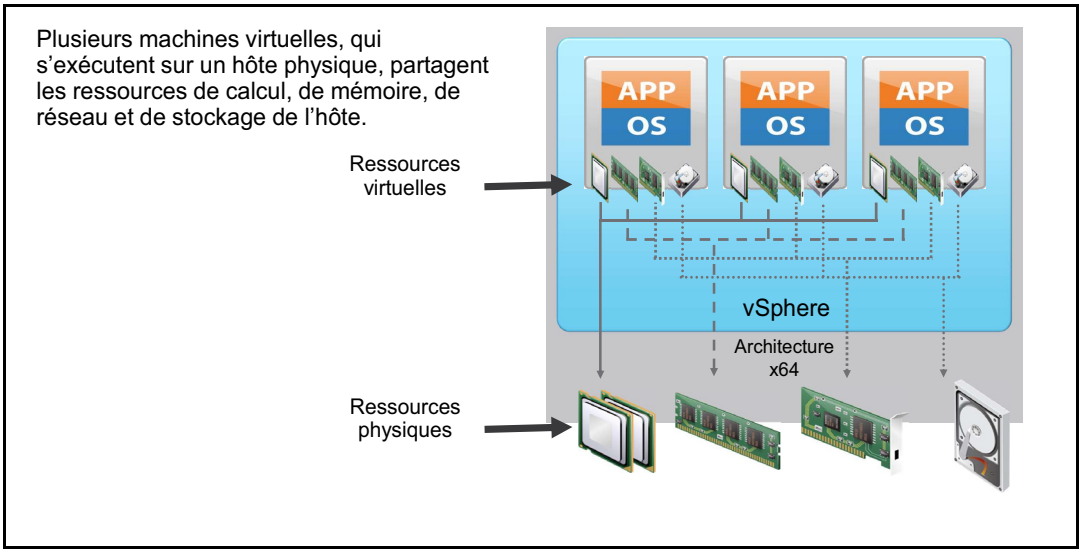


La virtualisation vous permet de consolider et d'exécuter différentes charges de travail sous forme de machines virtuelles sur un unique ordinateur. Une machine virtuelle est un ordinateur constitué de logiciels qui, à l'instar d'un ordinateur physique, exécute un système d'exploitation et des applications.

La diapositive montre les différences entre un hôte virtualisé et un hôte non virtualisé. Dans les architectures classiques, le système d'exploitation interagit directement avec le matériel installé. Le système d'exploitation planifie l'exécution des processus, alloue de la mémoire aux applications, envoie et reçoit des données sur les interfaces réseau, et effectue des opérations de lecture et d'écriture sur les périphériques de stockage connectés. En revanche, un hôte virtualisé interagit avec le matériel installé par le biais d'une fine couche logicielle appelée couche de virtualisation ou hyperviseur.

Ce dernier fournit de façon dynamique aux machines virtuelles les ressources matérielles physiques requises pour assurer leur fonctionnement. L'hyperviseur permet aux machines virtuelles de fonctionner de façon relativement indépendante par rapport à la couche matérielle physique sous-jacente. Par exemple, une machine virtuelle peut être transférée d'un hôte physique à un autre. De plus, ses disques virtuels peuvent être déplacés d'un type de stockage vers un autre sans altérer son fonctionnement.

2-14 Partage des ressources physiques



Grâce à la virtualisation, vous pouvez exécuter plusieurs machines virtuelles sur un même hôte physique, chacune d'elles ayant alors la possibilité de partager les ressources de cet ordinateur physique dans différents environnements. Les machines virtuelles partagent l'accès aux CPU, et leur exécution est planifiée par l'hyperviseur. De plus, chaque machine virtuelle se voit affecter sa propre région de mémoire, et partage l'accès aux cartes réseau et aux contrôleurs de disque physiques avec les autres machines virtuelles. Différentes machines virtuelles peuvent exécuter conjointement plusieurs systèmes d'exploitation et applications sur le même ordinateur physique.

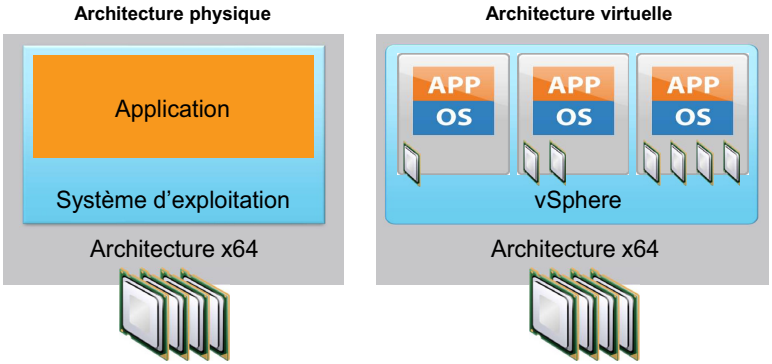
Lorsque plusieurs machines virtuelles s'exécutent sur un hôte VMware ESXi, une portion des ressources physiques est attribuée à chaque machine virtuelle. L'hyperviseur définit l'exécution des machines virtuelles de manière similaire à la gestion de l'allocation de mémoire et la planification de l'exécution des applications par un système d'exploitation classique. Ces machines virtuelles s'exécutent sur différents CPU.

Comme les applications, les machines virtuelles consomment de la bande passante réseau et de disque. La gestion des machines virtuelles fait cependant intervenir des mécanismes de contrôle élaborés pour déterminer la quantité de ressources accessible à chaque machine virtuelle. Avec les paramètres d'allocation de ressources par défaut, toutes les machines virtuelles associées à un même hôte VMware ESXi reçoivent une part égale des ressources disponibles.

2-15 Virtualisation des CPU

Dans un environnement physique, le système d'exploitation s'attribue toutes les CPU physiques du système.

La virtualisation des CPU donne la priorité aux performances et s'exécute directement sur les CPU disponibles.



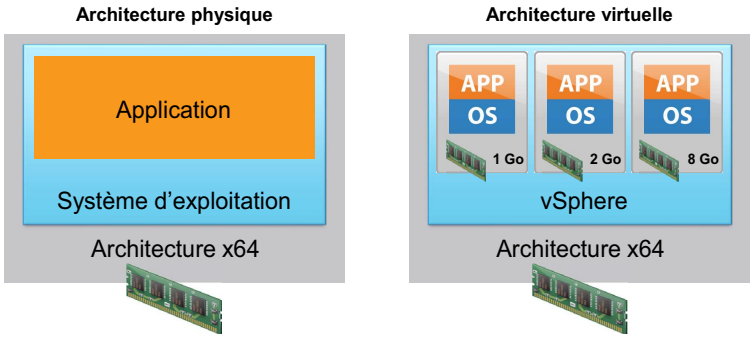
La couche de virtualisation exécute uniquement les instructions requises pour faire fonctionner les machines virtuelles comme si elles s'exécutaient directement sur une machine physique. La virtualisation des CPU se distingue de l'émulation. Grâce à un émulateur logiciel, certains programmes peuvent fonctionner sur un système informatique autre que celui pour lequel ils ont été conçus à l'origine. L'émulation permet d'assurer la portabilité, mais peut avoir un impact négatif sur les performances. La virtualisation des CPU se distingue de l'émulation dans la mesure où les systèmes d'exploitation clients pris en charge sont conçus pour des processeurs x64. L'hyperviseur permet aux systèmes d'exploitation de s'exécuter de manière native sur les processeurs x64 physiques de l'hôte.

Lorsqu'un grand nombre de machines virtuelles sont exécutées sur un hôte VMware ESXi, il arrive qu'elles entrent en concurrence pour l'accès aux ressources CPU. En cas de conflit portant sur les ressources CPU, l'hôte VMware ESXi a recours à l'allocation des processeurs physiques par tranche de temps à l'échelle de l'ensemble des machines virtuelles, ce qui permet à chacune d'elles de se comporter comme si elle disposait d'un nombre déterminé de processeurs virtuels.

2-16 Utilisation de la mémoire hôte physique et virtualisée

Dans un environnement physique, le système d'exploitation s'attribue toute la mémoire physique du système.

La virtualisation des CPU donne la priorité aux performances et s'exécute directement sur la RAM disponible.

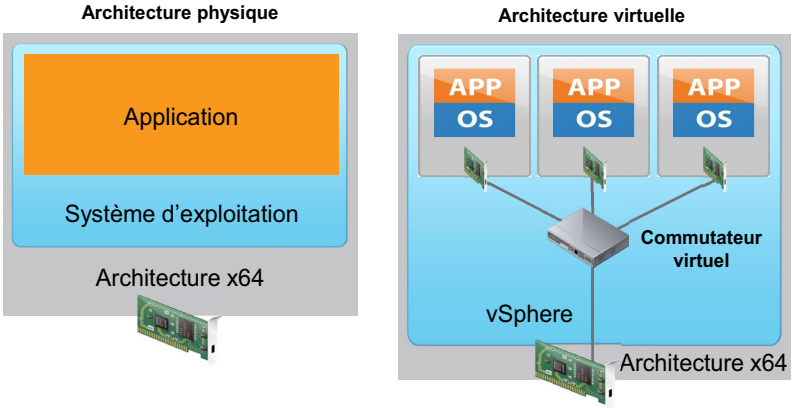


Chaque application lancée utilise les interfaces fournies par le système d'exploitation pour allouer ou libérer des pages de mémoire virtuelle au cours de son exécution. Technologie utilisée depuis plusieurs décennies par la plupart des systèmes d'exploitation généralistes, la mémoire virtuelle permet aux systèmes d'exploitation de présenter aux applications une capacité de mémoire supérieure à la mémoire physique accessible. Presque tous les processeurs modernes intègrent des composants matériels permettant sa prise en charge.

La mémoire virtuelle définit un espace d'adressage virtuel uniforme à l'usage des applications, tout en permettant au système d'exploitation et au matériel de gérer la traduction des adresses entre cet espace et l'espace d'adressage physique. Cette technique permet d'adapter l'environnement d'exécution en vue de la prise en charge d'espaces d'adressage étendus ainsi que de fonctionnalités de protection des processus, de mappage de fichiers et d'échange dans les systèmes informatiques modernes. Dans un environnement virtualisé, la couche de virtualisation VMware fournit à la machine virtuelle un espace mémoire adressable en continu créé lors de son démarrage. L'espace mémoire alloué est configuré lors de la création de la machine virtuelle et présente les mêmes propriétés que l'espace d'adressage virtuel. Cette configuration permet à l'hyperviseur d'exécuter simultanément plusieurs machines virtuelles tout en empêchant chacune d'elles d'accéder à la mémoire des autres.

2-17 Réseau physique et réseau virtuel

Les adaptateurs Ethernet virtuels et les commutateurs virtuels sont des composants essentiels du réseau virtuel.



Une machine virtuelle peut être configurée avec un ou plusieurs adaptateurs Ethernet virtuels. Un commutateur virtuel permet aux machines virtuelles hébergées sur un même hôte VMware ESXi de communiquer entre elles en utilisant les mêmes protocoles que sur un commutateur physique, et sans nécessiter l'ajout de matériel supplémentaire. Un commutateur virtuel prend également en charge les réseaux locaux virtuels compatibles avec les implémentations de VLAN standard des autres fournisseurs d'équipement réseau. Le réseau virtuel VMware vous permet de relier des machines virtuelles locales entre elles et de les connecter au réseau externe via un commutateur virtuel.

À l'instar d'un commutateur Ethernet physique, un commutateur virtuel assure le transfert de trames au niveau de la couche de liaison de données. Un hôte VMware ESXi peut héberger plusieurs commutateurs virtuels. La connexion d'un commutateur virtuel au réseau externe s'effectue au moyen d'adaptateurs Ethernet sortants appelés vmnic. Le commutateur virtuel est capable de relier plusieurs vmnic d'une manière analogue à l'association de cartes réseau sur un serveur classique, de façon à maximiser la disponibilité et la bande passante offertes aux machines virtuelles utilisant ce commutateur virtuel.

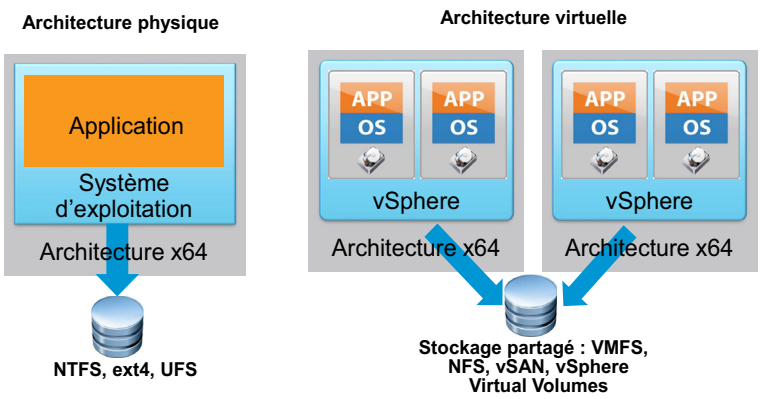
Les commutateurs virtuels présentent de nombreuses similitudes avec les commutateurs Ethernet physiques modernes. Tout comme un commutateur physique, chaque commutateur virtuel possède sa propre table de transfert. Ainsi, toutes les destinations recherchées par le commutateur correspondent uniquement aux ports du commutateur virtuel d'origine de la trame. Cette fonctionnalité améliore la sécurité dans la mesure où les pirates informatiques auront plus de mal à trouver une faille dans l'isolation d'un commutateur virtuel.

Les commutateurs virtuels prennent également en charge la segmentation du VLAN au niveau du port, qui permet de configurer chaque port comme un port d'accès ou de jonction donnant accès à un ou plusieurs VLAN.

Toutefois, contrairement aux commutateurs physiques, les commutateurs virtuels n'ont pas besoin du protocole STP (Spanning Tree Protocol), dans la mesure où la topologie de réseau mise en œuvre est à un seul niveau. Il n'est pas possible d'interconnecter plusieurs commutateurs virtuels, et le trafic réseau ne peut pas être directement transmis d'un commutateur virtuel à un autre commutateur virtuel situé sur le même hôte. Un commutateur virtuel fournit tous les ports dont vous pouvez avoir besoin au sein d'un commutateur. Il est inutile de configurer des commutateurs virtuels en cascade, puisqu'ils ne partagent pas d'adaptateurs Ethernet physiques et qu'aucune fuite ne peut se produire entre eux.

2-18 Comparaison des systèmes de fichiers physiques et des banques de données

vSphere VMFS permet de déployer une architecture de stockage distribuée, où différents hôtes VMware ESXi peuvent accéder concurremment en lecture ou en écriture au stockage partagé.



Pour stocker les disques virtuels, VMware ESXi utilise les banques de données. Celles-ci sont des conteneurs logiques qui masquent les caractéristiques du stockage physique des machines virtuelles et fournissent un modèle uniforme pour stocker les fichiers des machines virtuelles. Les banques de données que vous déployez sur des périphériques de stockage par blocs utilisent le format VMware vSphere® VMFS, un système de fichiers hautes performances spécialement optimisé pour le stockage de machines virtuelles.

VMFS a été conçu, construit et optimisé pour les environnements virtualisés. Il s'agit d'un système de fichiers en cluster hautement performant élaboré pour les machines virtuelles, qui utilise la journalisation répartie de ses métadonnées de système de fichiers pour assurer une reprise rapide et résiliente en cas de défaillance matérielle. VMFS améliore l'utilisation des ressources en permettant à plusieurs machines virtuelles de partager l'accès à un pool consolidé de stockage en cluster. Il constitue également la base des services d'infrastructure distribués, tels que la migration à chaud de machines virtuelles et de leurs fichiers, l'équilibrage dynamique des charges de travail entre les ressources de calcul disponibles, le redémarrage automatique des machines virtuelles et la tolérance aux pannes.

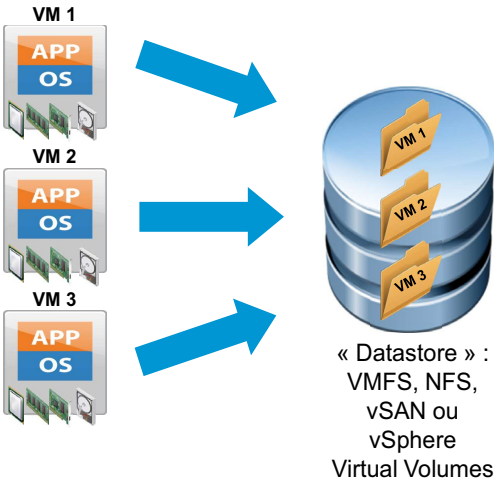
VMFS fournit une interface avec les ressources de stockage de façon à permettre l'utilisation de différents protocoles de stockage (Fibre Channel, Fibre Channel over Ethernet et iSCSI) pour accéder aux datastores susceptibles d'héberger des machines virtuelles. La croissance dynamique des banques de données VMFS par agrégation de ressources de stockage et expansion dynamique d'une banque de données VMFS vous permet de redimensionner un pool de ressources de stockage partagé sans interruption de service.

À l’aide des méthodes de verrouillage distribué, VMFS fait le lien entre la machine virtuelle et les ressources de stockage sous-jacentes. Les fonctionnalités exclusives de VMFS permettent aux machines virtuelles de rejoindre un cluster de manière transparente et sans nécessiter de gestion complexe.

2-19 Encapsulation des machines virtuelles

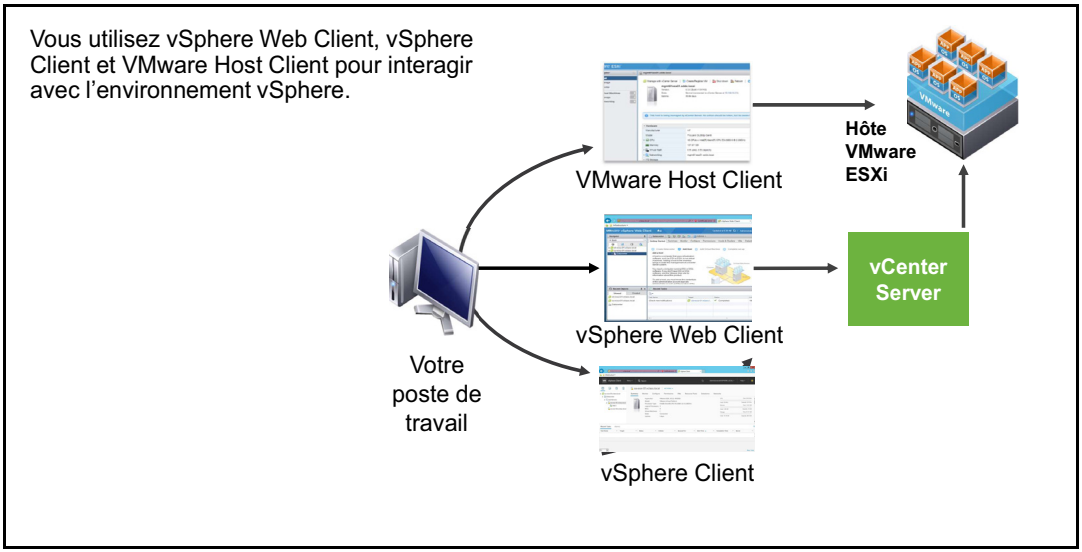
vSphere encapsule chaque machine virtuelle dans un ensemble de fichiers des machines virtuelles.

Les fichiers des machines virtuelles sont stockés dans des répertoires d'une banque de données VMFS, NFS, VMware vSAN™ ou VMware vSphere® Virtual Volumes™.



vSphere encapsule chaque machine virtuelle dans un petit nombre de fichiers ou objets, afin de faciliter la gestion et la migration des machines virtuelles. Les fichiers et objets de chaque machine virtuelle sont stockés dans un dossier séparé, qui est placé dans une banque de données.

2-20 À propos des clients vSphere Client



VMware Host Client™, qui a été lancé avec vSphere 6.0 U2, permet de gérer directement les hôtes VMware ESXi individuels. Dans vSphere 6.5, il remplace VMware vSphere® Client™ basé sur Windows. En général, VMware Host Client est utilisé uniquement lorsque la gestion via VMware vCenter Server® est impossible.

VMware vSphere® Web Client est une interface utilisateur de type navigateur pleinement extensible et indépendante de la plate-forme. vSphere Web Client repose sur Adobe Flex. vSphere Web Client prend en charge toutes les opérations requises pour interagir avec vSphere, VMware ESXi et VMware vCenter Server.

La version actuelle de vSphere Client est un client basé sur HTML5 qui peut être utilisé avec vSphere Web Client.

VMware Host Client, vSphere Client et vSphere Web Client offrent les avantages suivants :

- interface utilisateur épurée et modernisée ;
- aucun plug-in de navigateur à installer ou à gérer ;
- intégration avec vCenter Server et VMware ESXi.

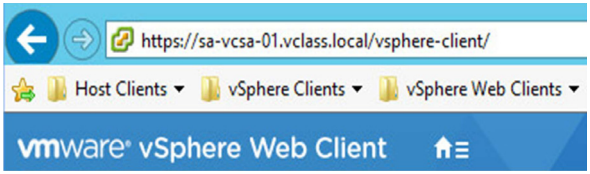
2-21 À propos de vSphere Web Client

vSphere Web Client comprend les composants suivants :

- Application client Adobe Flex exécutée dans un navigateur
- Serveur Java intégré dans vCenter Server Appliance et vCenter Server
- Un client léger, qui requiert seulement un navigateur sur lequel le plug-in Adobe a été installé

vSphere Web Client est accessible à l'adresse https*://your_vCenter_Server_Appliance/* vsphere-client.

Un plug-in d'authentification amélioré est disponible en option : il fournit une authentification Windows intégrée et une fonctionnalité de carte à puce basée sur Windows.



Le bandeau bleu reproduit sur cette diapositive est le seul élément signalétique qui vous est présenté, dans le coin supérieur gauche de l'écran, lorsque vous affichez vSphere Web Client. Cette image vous permet de différencier instantanément vSphere Web Client des autres clients.

vSphere Web Client fournit toutes les fonctionnalités requises pour gérer VMware vCenter® Server Appliance™ via un navigateur Web. vSphere Web Client est conçu pour remplacer la fonctionnalité client de vSphere Client pour Windows.

Lorsque vous utilisez l'adresse https://*votre_vCSA*/vsphere-client pour accéder à vSphere Web Client, celle-ci est redirigée en interne vers le port 9443 de votre système vCenter Server.

L'interface utilisateur de vSphere Web Client offre plusieurs fonctionnalités, telles que les attributs personnalisés, les onglets d'objet et l'actualisation en direct, ainsi que diverses améliorations en termes de performances et de facilité d'utilisation.

La structure des onglets de la plupart des objets vSphere a été réorganisée de façon à permettre une utilisation plus simple et plus intuitive.

Le plug-in Client Integration, qui était auparavant nécessaire pour assurer un ensemble de fonctionnalités de vSphere Web Client, ne l'est plus. Les fonctions suivantes de vSphere Web Client sont désormais entièrement indépendantes :

- Chargement/téléchargement de fichiers dans/depuis la banque de données
- Exportation/déploiement de fichiers OVF
- Importation/exportation de bibliothèques de contenu

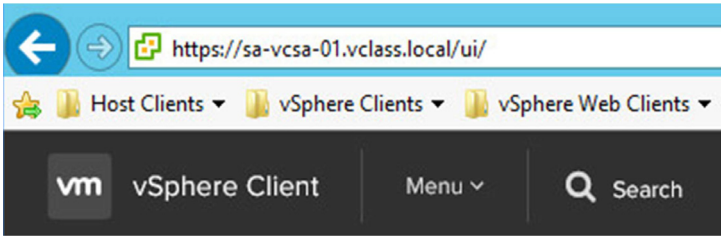
La seule fonction à conserver une dépendance est Windows Session Authentication. Vous gérez cette exception en installant le plug-in d'authentification amélioré.

2-22 À propos de vSphere Client

Le client vSphere Client repose sur HTML5 et ne requiert pas l'installation d'Adobe Flex.

vSphere Client utilise le même serveur Java que vSphere Web Client.

Pour accéder à vSphere Client depuis un navigateur compatible, connectez-vous à l'adresse suivante : https*://your_vCenter_Server_Appliance/*ui.



Le bandeau noir reproduit sur cette diapositive est le seul élément signalétique qui vous est présenté, dans le coin supérieur gauche de l'écran, lorsque vous affichez vSphere Client. Cette image vous permet de différencier instantanément vSphere Client des autres clients.

Lorsque vous utilisez l'adresse https://*votre_vCSA*/ui pour accéder à vSphere Client, celle-ci est redirigée en interne vers le port 9443 de votre système vCenter Server.

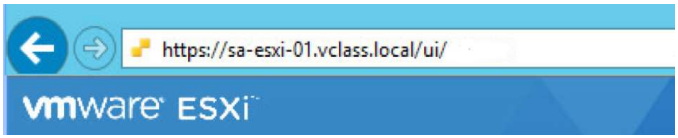
vSphere Client vous permet de gérer vCenter Server Appliance via un navigateur Web, mais ne requiert pas l'activation d'Adobe Flex dans ce navigateur.

Pour obtenir une liste de comparaison entre les fonctionnalités prises en charge par vSphere Client et celles prises en charge par vSphere Web Client, consultez la page https://docs.vmware.com/en/VMware-vSphere/6.5/rn/vsphere-client-65-html5-functionality-support.html.

2-23 À propos de VMware Host Client

VMware Host Client est un client léger basé sur HTML5 que vous pouvez utiliser pour gérer directement les hôtes lorsque vCenter Server n'est pas disponible.

Le service VMware Host Client est assuré depuis VMware ESXi via l'adresse suivante : https*://votre_hôte_VMware_ESXi*/ui.



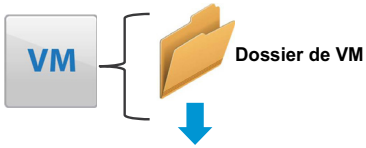
VMware Host Client permet d'accéder directement à la gestion des hôtes VMware ESXi individuels. Il est utilisé dans les cas où vCenter Server Appliance n'est pas disponible. VMware Host Client repose sur HTML5, et est accessible via un navigateur.

Le bandeau bleu reproduit sur cette diapositive est le seul élément signalétique qui vous est présenté, dans le coin supérieur gauche de l'écran, lorsque vous affichez VMware Host Client. Cette image vous permet de différencier instantanément VMware Host Client des autres clients.

VMware Host Client remplace la fonctionnalité de client hôte de vSphere Client pour Windows. La disposition de l'interface utilisateur HTML5 est similaire à celle de vSphere Web Client afin de garantir une navigation homogène dans les workflows. Nous avons cependant simplifié l'interface pour les domaines qui ne requièrent pas la fonctionnalité vCenter Server.

2-24 À propos des fichiers de machine virtuelle

Une machine virtuelle comprend un ensemble de fichiers corrélés.



Fichier de configuration	*nom_VM*.vmx
Fichiers d'échange	*nom_VM*.vswp vmx-*nom_VM*.vswp
Fichier BIOS	*nom_VM*.nvram
Fichiers journaux	vmware.log
Exemple de fichier de configuration	*nom_VM*.vmtx
Fichier de descripteur de disque	*nom_VM*.vmdk
Fichier de données de disque	*nom_VM*-flat.vmdk
Fichier de mappage de périphérique brut	*nom_VM*-rdm(p).vmdk
Fichier de disque de snapshot	*nom_VM*-######.vmdk
Fichier de données de snapshot	*nom_VM*.vmsd
Fichier d'état de snapshot	*nom_VM*-*Snapshot#*.vmsn
Fichier de mémoire active de snapshot	*nom_VM*-*Snapshot#*.vmem
Fichier d'état d'interruption	*nom_VM*-*.vmss
État suspendu de mémoire de snapshot	*nom_VM*-*.vmem

Cette diapositive répertorie certains des fichiers qui constituent une machine virtuelle. À l'exception des fichiers journaux, le nom de chaque fichier commence par celui de la machine virtuelle : *nom_VM*. Une machine virtuelle comprend les fichiers suivants :

- un fichier de configuration (.vmx) ;
- un ou plusieurs fichiers de disque virtuel (le premier disque virtuel est constitué des fichiers *nom_VM*.vmdk et *nom_VM*-flat.vmdk) ;
- un fichier contenant les paramètres du BIOS de la machine virtuelle (.nvram) ;
- un fichier journal actuel de la machine virtuelle (.log), ainsi qu'un ensemble de fichiers utilisés pour archiver les anciennes entrées de journal (-#.log).
- des fichiers d'échange (.vswp) utilisés pour récupérer de la mémoire en cas de contention ;
- un fichier de description de snapshot (.vmsd), qui est vide lorsque la machine virtuelle n'inclut aucun snapshot.

REMARQUES

La liste des fichiers mentionnés dans cette diapositive n'est pas exhaustive. Pour accéder à une liste complète de tous les types de fichiers de machine virtuelle, consultez la page https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-CEFF6D89-8C19-4143-8C26-4B6D6734D2CB.html.

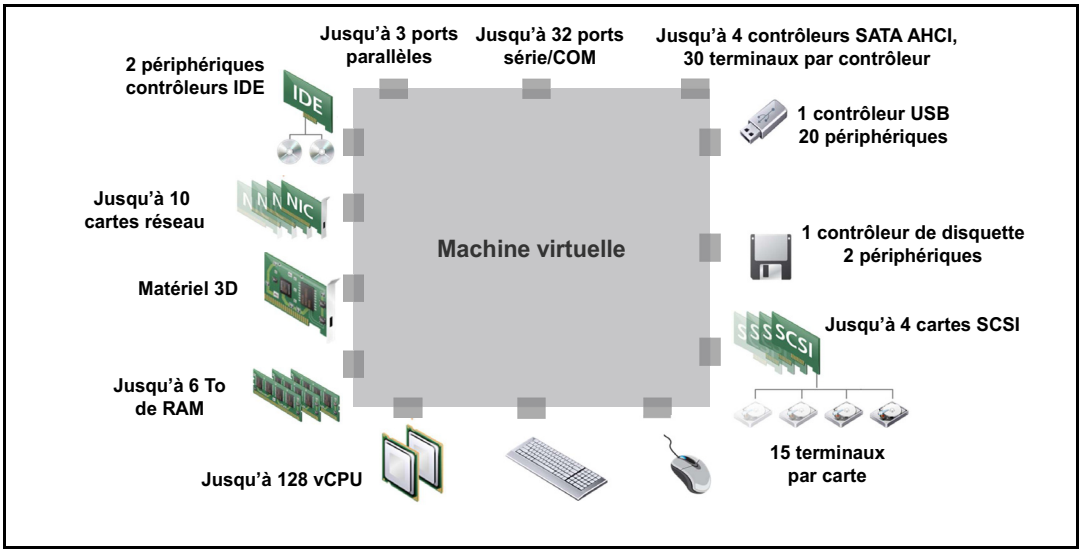
Si la machine virtuelle est convertie en modèle, un fichier de configuration de ce modèle (`.vmtx`) remplace le fichier de configuration de la machine virtuelle (`.vmx`). Un modèle de machine virtuelle correspond à une copie maître d'une machine virtuelle.

Si cette machine virtuelle comprend plusieurs fichiers de disque, les deux fichiers correspondant au deuxième fichier de disque (et aux suivants) portent les noms *nom_VM_#*`.vmdk` et `nom_VM_#-flat.vmdk`, où # correspond à un numéro de séquence incrémenté à partir de 1. Prenons l'exemple d'une machine virtuelle appelée Test01 et comprenant deux disques virtuels. Cette machine inclut alors les fichiers `Test01_0.vmdk`, `Test01_0-flat.vmdk`, `Test01_1.vmdk` et `Test01_1-flat.vmdk`.

En plus du fichier journal actuel, nommé `vmware.log`, jusqu'à six fichiers journaux d'archivage sont conservés en même temps. Par exemple, supposons que les fichiers `-1.log` à `-6.log` soient présents au départ. Lorsqu'un fichier journal d'archivage est créé par la suite (par exemple, lorsque la machine virtuelle est mise hors tension, puis remise sous tension), voici ce qui se produit : le fichier `-6.log` est supprimé, le fichier `-5.log` est renommé en `-6.log`, etc. Pour finir, l'ancien fichier journal vmware.log est renommé en `-1.log`.

Une machine virtuelle peut inclure d'autres fichiers, notamment en cas de création d'un ou de plusieurs snapshots, ou d'ajout de mappages de périphériques bruts (RDM). Une machine virtuelle inclut un fichier de verrouillage supplémentaire lorsqu'elle se trouve dans une banque de données NFS. Elle peut comprendre un fichier de suivi des blocs modifiés (`.ctk`), qui est utilisé pour effectuer un suivi des modifications des sauvegardes différentielles, si elle est sauvegardée par l'appliance VMware vSphere® Data Protection™ ou un autre logiciel de sauvegarde utilisant la fonction CDP.

2-25 À propos du matériel virtuel de la machine virtuelle



Les machines virtuelles utilisent du matériel virtuel. Chaque système d'exploitation client détecte des périphériques matériels classiques ; il ne sait pas que ces périphériques sont virtuels. Toutes les machines virtuelles utilisent un matériel uniforme, à l'exception de quelques variations pouvant être appliquées par l'administrateur système. L'utilisation de composants matériels uniformes permet de garantir la portabilité des machines virtuelles sur les plates-formes de virtualisation VMware.

Vous pouvez configurer les paramètres relatifs aux CPU et à la mémoire des machines virtuelles. vSphere prend en charge la plupart des fonctionnalités de CPU les plus récentes, notamment les compteurs de performances des CPU virtuels. Vous pouvez ajouter des cartes d'interface réseau et des disques durs virtuels. Il est également possible d'ajouter et de configurer du matériel virtuel, par exemple des lecteurs de CD/DVD ou de disquette et des périphériques SCSI. Certains périphériques ne peuvent pas être ajoutés et configurés. Par exemple, vous ne pouvez pas ajouter de périphériques vidéo, mais il est possible de configurer les périphériques vidéo et cartes vidéo disponibles.

Vous avez la possibilité d'ajouter plusieurs périphériques USB (tels que des dongles de sécurité et des périphériques de stockage de masse) à une machine virtuelle résidant sur un hôte VMware ESXi auquel les périphériques sont connectés physiquement. Lorsque vous connectez un périphérique USB à un hôte physique, ce périphérique est uniquement accessible aux machines virtuelles qui résident sur cet hôte. Ces machines virtuelles ne peuvent pas se connecter à un périphérique se trouvant sur un autre hôte dans le Data Center. Un périphérique USB est accessible à une seule machine virtuelle à la fois. Lorsque vous retirez un périphérique d'une machine virtuelle, il devient accessible aux autres machines virtuelles résidant sur le même hôte.

Vous pouvez ajouter jusqu'à 16 périphériques PCI VMware vSphere® DirectPath I/O™ à une machine virtuelle. Les périphériques doivent être réservés pour le passthrough PCI sur l'hôte hébergeant la machine virtuelle. Les snapshots ne sont pas pris en charge par les périphériques passthrough vSphere DirectPath I/O.

L'interface VMCI (Virtual Machine Communication Interface) offre un canal de communication haut débit entre une machine virtuelle et l'hyperviseur. Vous ne pouvez pas ajouter ou retirer de périphériques VMCI.

Le contrôleur SATA fournit un accès aux disques virtuels et aux lecteurs de DVD/CD. Du point de vue de la machine virtuelle, le contrôleur virtuel SATA se présente comme un contrôleur SATA AHCI.

L'interface VMCI est une infrastructure qui permet une communication rapide et efficace entre une machine virtuelle et le système d'exploitation hôte. Le kit de développement logiciel (SDK) VMCI facilite le développement d'applications exploitant l'infrastructure VMCI. En l'absence de VMCI, les machines virtuelles utilisent la couche réseau pour communiquer avec l'hôte, ce qui engendre une charge de communication supplémentaire. L'utilisation de VMCI permet de minimiser la charge de communication et d'optimiser les tâches nécessitant ce type de communication. VMCI est capable d'atteindre près de 10 Gbits/s avec des paires de files d'attente de 128 Ko.

Les types de communication suivants sont pris en charge :

- Communication orientée datagrammes : sans connexion et comparable aux paires de files d'attente UDP.
- Communication orientée connexion : comparable à TCP.

VMCI fournit des API socket qui sont très semblables aux API déjà utilisées pour les applications TCP/UDP. Les adresses IP sont remplacées par des numéros d'identification VMCI. Par exemple, vous pouvez effectuer un portage de l'outil netperf afin d'utiliser les sockets VMCI au lieu de TCP/UDP. Par défaut, l'interface VMCI est désactivée.

Pour en savoir plus sur le matériel virtuel, consultez le *Guide d'administration d'une machine virtuelle vSphere*, disponible à l'adresse suivante : http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

2-26 Versions du matériel virtuel

La version du matériel virtuel détermine les fonctions du système d'exploitation prises en charge par une machine virtuelle. N'utilisez pas une version supérieure à la dernière version prise en charge par le produit VMware.

Compatibilité	Version du matériel
ESXi 6.7	14
VMware ESXi versions 6.5 et ultérieures	13
VMware ESXi versions 6.0 et ultérieures	11
VMware ESXi versions 5.5 et ultérieures	10

Chaque version d'un produit VMware inclut la version du matériel de machine virtuelle qui lui correspond. Le tableau présente le niveau de version du matériel virtuel le plus élevé pris en charge par chaque version du logiciel VMware ESX®/ESXi. Chaque niveau de compatibilité d'une machine virtuelle prend en charge au moins cinq versions de vSphere, majeures ou mineures. Ainsi, une machine virtuelle compatible avec VMware ESX/ESXi versions 4.0 et ultérieures peut s'exécuter sur VMware ESX/ESXi 4.0, ESX/ESXi 4.1, ESXi 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, ESXi 6.5 et ESXi 6.7.

Pour en savoir plus sur la configuration du matériel des machines virtuelles, consultez le *Guide d'administration d'une machine virtuelle vSphere*, disponible à l'adresse suivante : http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

Pour la liste complète des valeurs maximales de configuration de la machine virtuelle, voir la section *Configuration maximum* à l'adresse suivante : http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

2-27 À propos des ressources CPU et de mémoire

Vous avez la possibilité d'améliorer les performances d'une machine virtuelle en ajoutant, en modifiant ou en configurant ses ressources CPU et mémoire.

Le nombre maximal de CPU virtuels (vCPU) que vous pouvez affecter à une machine virtuelle dépend des éléments suivants :

- Le nombre de CPU logiques présents sur l'hôte
- Le type de système d'exploitation client installé

Une machine virtuelle exécutée sur un hôte VMware ESXi 6.x peut accueillir jusqu'à 128 vCPU.

La quantité maximale de mémoire allouée à une machine virtuelle dépend du paramétrage de compatibilité de cette machine virtuelle.

La capacité de mémoire maximale d'une machine virtuelle compatible VMware ESXi 6.7 et exécutée sur VMware ESXi 6.7 est de 6 To.

Les ressources CPU et la mémoire d'une machine virtuelle doivent être dimensionnées en fonction des applications et du système d'exploitation client.

Le nombre maximal de CPU virtuels que vous pouvez affecter à une machine virtuelle dépend du nombre de CPU logiques présents sur l'hôte et du type de système d'exploitation client installé sur la machine virtuelle. La fonctionnalité de vCPU multicœur vous permet de contrôler le nombre de cœurs affectés à chaque socket virtuel d'une machine virtuelle. Un système d'exploitation présentant des restrictions en matière de sockets peut ainsi faire plus largement appel aux cœurs de CPU disponibles sur l'hôte, d'où une amélioration globale des performances.

Le nombre de CPU virtuels configurés sur une machine virtuelle ne peut pas excéder le nombre de CPU logiques présents sur l'hôte. Ce nombre de CPU logiques correspond au nombre total de cœurs des processeurs physiques, ou à deux fois cette quantité en cas d'activation de l'hyperthreading. Par exemple, si un hôte comporte 128 CPU logiques, vous pouvez configurer jusqu'à 128 vCPU sur la machine virtuelle.

La plupart des paramètres de mémoire peuvent être configurés lors de la création de la machine virtuelle ou après l'installation du système d'exploitation client. Pour effectuer certaines actions, vous devrez mettre la machine virtuelle hors tension avant de modifier les paramètres. Les paramètres relatifs aux ressources de mémoire d'une machine virtuelle déterminent la part de la mémoire hôte que vous allouez à cette machine virtuelle. La taille de la mémoire du matériel virtuel détermine la quantité de mémoire disponible pour les applications exécutées sur la machine virtuelle. Les ressources de mémoire dont la machine virtuelle peut bénéficier sont limitées par la taille de mémoire que vous configurez pour le matériel virtuel. Les hôtes VMware ESXi limitent l'utilisation des ressources de mémoire à la quantité maximale utile pour la machine virtuelle ; vous

pouvez par conséquent accepter la valeur par défaut du paramètre « Unlimited memory resources ». Vous pouvez reconfigurer la quantité de mémoire allouée à une machine virtuelle afin d'améliorer les performances. La quantité maximale de mémoire allouée à une machine virtuelle dépend du paramétrage de compatibilité de cette machine virtuelle.

2-28 À propos du stockage virtuel

Les disques virtuels sont connectés à des adaptateurs de stockage virtuels. L'hôte VMware ESXi propose plusieurs options d'adaptateur de stockage pour la connexion à une machine virtuelle :

- BusLogic Parallel
- LSI Logic Parallel
- LSI Logic SAS
- VMware Paravirtual SCSI
- Contrôleur SATA AHCI
- NVMe virtuel

Lorsque vous créez une machine virtuelle, l'assistant sélectionne automatiquement un adaptateur SCSI virtuel en fonction du système d'exploitation client choisi. Le disque virtuel est stocké dans le même dossier que le fichier de configuration de la machine virtuelle. Toutefois, vous pouvez choisir de placer un disque virtuel à un autre endroit, par exemple lorsque vous séparez les disques de données des disques de démarrage. Vous devez alors sélectionner une banque de données VMFS dans laquelle placer le nouveau disque virtuel vierge, et spécifier la taille de ce disque. Vous pouvez également placer le disque en spécifiant un ID de cible SCSI virtuelle et un numéro d'unité logique (LUN).

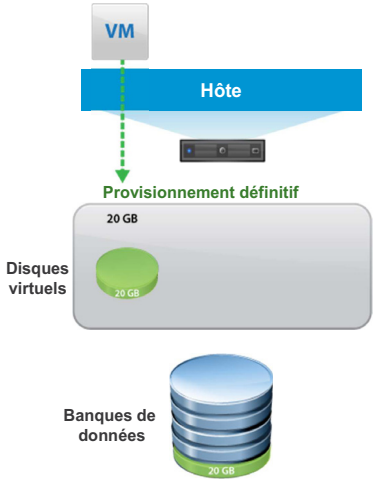
2-29 À propos des disques virtuels à provisionnement définitif

Le provisionnement définitif utilise la totalité de l'espace disque spécifié lors de la création du disque virtuel :

- Les disques de machine virtuelle consomment toute la capacité spécifiée lors de leur création, quel que soit le volume des données présentes dans le système de fichiers du système d'exploitation client.

Mise à zéro immédiate ou différée :

- Dans un disque à provisionnement définitif avec mise à zéro immédiate, chaque bloc est prérempli de zéros.
- Dans un disque à provisionnement définitif avec mise à zéro différée, la mise à zéro n'intervient qu'au moment où des données sont écrites sur les blocs.



Lorsque vous créez un disque virtuel, les types de disque suivants sont disponibles :

- Provisionnement définitif avec mise à zéro différée : l'espace requis pour le disque virtuel est attribué au cours de la création. Les données restant sur le périphérique physique ne sont pas effacées pendant la création, mais mises à zéro ultérieurement et à la demande lors de la première écriture provenant de la machine virtuelle. Il s'agit du type de disque par défaut.
- Provisionnement définitif avec mise à zéro immédiate : l'espace requis pour le disque virtuel est attribué au cours de la création. Les données qui restent sur le périphérique physique sont mises à zéro lors de la création du disque.
- Provisionnement fin : un disque à provisionnement fin utilise uniquement l'espace de banque de données dont il a besoin au départ. S'il lui faut plus d'espace ultérieurement, il peut s'étendre jusqu'à atteindre la capacité maximale qui lui est attribuée.

2-30 À propos des disques virtuels à provisionnement fin

Le provisionnement fin permet aux machines virtuelles d'utiliser l'espace de stockage en fonction de leurs besoins :

- Les disques de machine virtuelle à provisionnement fin utilisent uniquement la capacité requise pour accueillir les fichiers actuels.
- La machine virtuelle détecte à tout moment l'intégralité de la taille de disque attribuée.

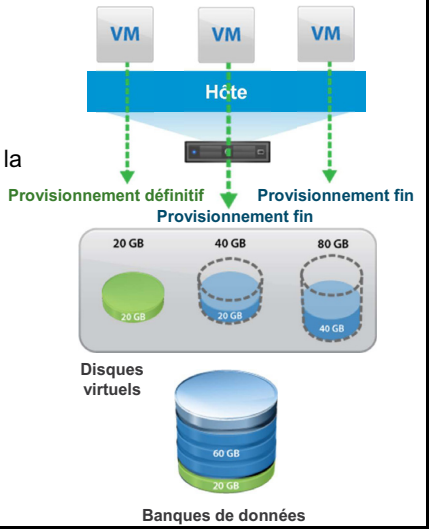
Exécutez la commande unmap pour réclamer l'espace non utilisé de la baie.

Vous pouvez mélanger les formats fin et définitif.

Une fonction très complète de génération de rapports et d'alertes permet de gérer les attributions et la capacité.

Utilisation plus efficace du stockage :

- Attribution de disque virtuel : 140 Go
- Capacité de banque de données disponible : 100 Go
- Capacité de stockage utilisée : 80 Go



La fonction de provisionnement fin génère des alarmes et des rapports permettant un suivi de l'utilisation effective de la capacité de stockage par rapport à la capacité allouée. Le provisionnement fin permet aux administrateurs de stockage d'optimiser l'attribution du stockage au sein des environnements virtuels. Grâce à lui, les utilisateurs peuvent exploiter l'espace de stockage disponible de manière optimale, mais sûre, grâce à la surallocation.

Le provisionnement fin est souvent utilisé lors de la déduplication des baies de stockage, afin d'optimiser l'utilisation du stockage et de sauvegarder les machines virtuelles.

Le tableau ci-dessous identifie les différences entre les options de disque virtuel, et les compare.

	Provisionnement définitif avec mise à zéro différée	**Provisionnement définitif avec mise à zéro immédiate**	**Provisionnement fin**
Durée de la création	Rapide.	Lente et proportionnelle à la taille du disque.	La plus rapide.
Attribution des blocs	Entièrement préalloués.	Entièrement préalloués.	Alloués et mis à zéro à la demande lors de la première écriture sur le bloc.

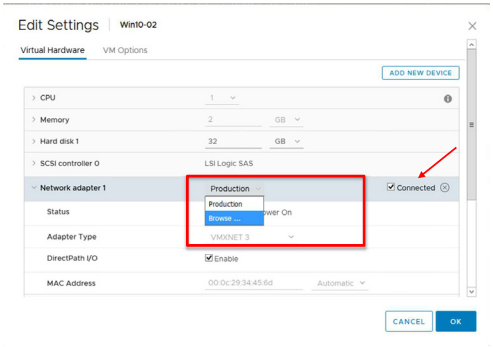
	Provisionnement définitif avec mise à zéro différée	**Provisionnement définitif avec mise à zéro immédiate**	**Provisionnement fin**
Disposition du disque virtuel	Probabilité élevée de contiguïté des blocs de fichiers.	Probabilité maximale de contiguïté des blocs de fichiers.	Disposition variable en fonction de l'état dynamique du volume au moment de l'attribution des blocs.
Mise à zéro des blocs de fichiers attribués	Les blocs de fichiers sont mis à zéro lors de la première écriture sur chaque bloc.	Les blocs de fichiers sont attribués et mis à zéro lors de la création du disque.	Les blocs de fichiers sont mis à zéro lorsque les blocs sont attribués.

2-31 À propos des réseaux virtuels

Un réseau virtuel permet la communication entre des machines virtuelles et des machines physiques.

Lors de la configuration de la mise en réseau d'une machine virtuelle, vous sélectionnez ou modifiez les éléments suivants :

- Le type de carte réseau
- Le groupe de ports auquel se connecter
- L'état de connexion du réseau
- Le paramètre déterminant la connexion de la machine virtuelle au réseau lors de sa mise sous tension



Les adaptateurs de stockage permettent de connecter votre hôte VMware ESXi à une unité ou un réseau de stockage spécifique.

VMware ESXi prend en charge différentes classes d'adaptateurs, y compris SCSI, iSCSI, RAID, Fibre Channel, Fibre Channel over Ethernet (FCoE) et Ethernet. VMware ESXi accède aux adaptateurs directement via les pilotes de périphérique dans VMkernel.

- BusLogic Parallel : le tout nouvel adaptateur de bus hôte compatible Mylex (BusLogic) BT/KT-958.
- LSI Logic Parallel : le contrôleur d'E/S LSI Logic LSI53C10xx Ultra320 SCSI est pris en charge.
- LSI Logic SAS : l'adaptateur LSI Logic SAS intègre une interface série.
- VMware Paravirtual SCSI : l'adaptateur de stockage hautes performances qui permet d'améliorer le débit et de réduire le taux d'utilisation des ressources CPU.
- Contrôleur SATA AHCI : fournit un accès aux disques virtuels et aux lecteurs de DVD/CD. Du point de vue de la machine virtuelle, le contrôleur virtuel SATA se présente comme un contrôleur SATA AHCI. Le contrôleur SATA AHCI est disponible uniquement pour les machines virtuelles compatibles avec VMware ESXi versions 5.5 ou ultérieures.
- NVMe virtuel : NVMe est une spécification Intel permettant d'associer des périphériques de stockage Flash au bus PCI Express et d'y accéder. NVMe est une solution alternative aux protocoles d'accès E/S de stockage sur serveur par blocs.

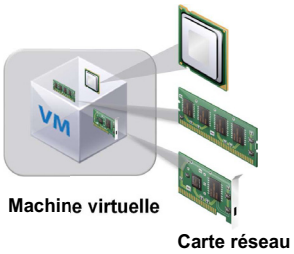
Pour plus d'informations sur la mise en réseau vSphere, consultez le document *Mise en réseau vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

2-32 À propos des cartes réseau virtuelles (1)

Lorsque vous configurez une machine virtuelle, vous pouvez ajouter des cartes réseau et spécifier le type de carte. Si possible, sélectionnez VMXNET3.

Voici les types de carte réseau pris en charge :

- Flexible : peut fonctionner en tant qu'adaptateur Vlance ou VMXNET.
- E1000-E1000E : adaptateur hautes performances disponible pour certains systèmes d'exploitation client seulement.
- VMXNET3 n'est disponible qu'avec les VMware Tools.



Les types de carte réseau disponibles dépendent des facteurs suivants :

- Niveau de compatibilité (ou version du matériel) de la machine virtuelle, déterminé par l'hôte ayant effectué la création de cette dernière ou sa dernière mise à jour. Par exemple, la carte d'interface réseau virtuelle VMXNET3 requiert la version 7 du matériel (VMware ESX/ESXi versions 4.0 ou ultérieures).
- Mise à jour éventuelle de la compatibilité de la machine virtuelle vers la toute dernière version de l'hôte actuel.
- Système d'exploitation client.

Les types de carte d'interface réseau suivants sont pris en charge :

- E1000E : version émulée de la carte réseau Gigabit Ethernet Intel 82574. Le type E1000E est utilisé par défaut pour Windows 8 et Windows Server 2012.
- E1000 : version émulée de la carte réseau Gigabit Ethernet Intel 82545EM, pour laquelle des pilotes sont disponibles dans la plupart des récents systèmes d'exploitation clients (notamment Windows XP et versions ultérieures et Linux versions 2.4.19 et ultérieures).
- Flexible : s'identifie en tant qu'adaptateur Vlance lors du démarrage d'une machine virtuelle, mais s'initialise et fonctionne comme un adaptateur Vlance ou VMXNET, selon l'identité du pilote qui le lance. Lorsque le logiciel VMware Tools est installé, le pilote VMXNET remplace l'adaptateur Vlance par l'adaptateur VMXNET, qui présente des performances plus élevées.

- Vlance : version émulée de la carte d'interface réseau LANCE PCnet32 AMD 79C970, une ancienne carte de 10 Mbits/s associée à des pilotes disponibles dans les systèmes d'exploitation clients 32 bits legacy. Une machine virtuelle configurée avec cette carte réseau peut exploiter immédiatement le réseau associé.
- VMXNET2 (Enhanced) : ce type est basé sur l'adaptateur VMXNET, mais offre des fonctions hautes performances généralement utilisées dans les réseaux actuels (par exemple, trames Jumbo et déchargements matériels). VMXNET2 (Enhanced) est uniquement disponible pour certains systèmes d'exploitation clients sur VMware ESX/ESXi versions 3.5 et ultérieures. Il n'est pas pris en charge sur VMware ESXi versions 6.7 et ultérieures.
- VMXNET3 : cette carte d'interface réseau paravirtualisée est conçue pour offrir des performances élevées. VMXNET3 propose toutes les fonctionnalités de la carte VMXNET2 ainsi que de nouvelles fonctions, telles que la prise en charge de plusieurs files d'attente (également appelée mise à l'échelle côté réception sous Windows), les transferts IPv6 et la gestion des interruptions MSI/MSI-X.

2-33 À propos des cartes réseau virtuelles (2)

- Voici les types de carte réseau pris en charge :
- SR-IOV passthrough : La machine virtuelle et l'adaptateur physique échangent des données sans utiliser VMkernel comme intermédiaire :
  - Restrictions en matière de prise en charge des systèmes d'exploitation client
- VMware vSphere® DirectPath I/O™ : ce type permet aux machines virtuelles d'accéder aux fonctions de réseau PCI physique sur les plates-formes dotées d'une unité de gestion de la mémoire d'E/S.
- PVRDMA : ce type est un appareil paravirtualisé qui permet d'améliorer les performances des périphériques virtuels. Il fournit une interface RDMA pour les clients vSphere.

- SR-IOV passthrough : représentation d'une fonction virtuelle sur une carte d'interface réseau physique, avec prise en charge de SR-IOV. Ce type d'adaptateur peut être utilisé avec les machines virtuelles qui nécessitent davantage de ressources CPU ou pour lesquelles la latence est susceptible d'engendrer des défaillances. La machine virtuelle et l'adaptateur physique échangent des données sans utiliser VMkernel comme intermédiaire. Si certaines machines virtuelles sont sensibles au délai réseau, SR-IOV peut assurer un accès direct aux fonctions virtuelles des cartes d'interface réseau physiques prises en charge, ce qui permet de minimiser la charge en contournant les commutateurs virtuels.

  La technologie SR-IOV passthrough est disponible dans VMware ESXi versions 5.5 et ultérieures, pour les systèmes Red Hat Enterprise Linux versions 6 et ultérieures, et dans Windows Server 2008 R2 avec SP2. Une version d'un système d'exploitation peut contenir un pilote par défaut pour les fonctions virtuelles de certaines cartes d'interface réseau. Dans d'autres cas, vous devrez télécharger ce pilote à partir de l'emplacement indiqué par le fournisseur de la carte d'interface réseau ou de l'hôte, puis l'installer.

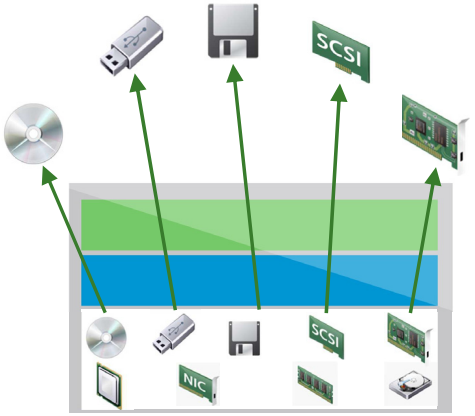
- vSphere DirectPath I/O permet aux machines virtuelles d'accéder aux fonctions de réseau PCI physique sur les plates-formes dotées d'une unité de gestion de la mémoire d'E/S. Les périphériques passthrough vous offrent le moyen d'utiliser plus efficacement les ressources et d'améliorer les performances de votre environnement. Vous pouvez configurer un périphérique PCI passthrough sur une machine virtuelle dans vSphere Web Client. Les fonctionnalités suivantes ne sont pas disponibles pour les machines virtuelles configurées avec vSphere DirectPath I/O :
  - Ajout et suppression à chaud de périphériques virtuels
  - Interruption et reprise
  - Enregistrement et rediffusion

    - Tolérance aux pannes
    - Haute disponibilité
    - VMware vSphere® Distributed Resource Scheduler™ : disponibilité limitée. La machine virtuelle peut faire partie d'un cluster, mais ne peut pas migrer d'un hôte vers un autre.
    - Snapshots.
- vSphere 6.5 et versions ultérieures prend en charge la communication RDMA (Remote Direct Memory Access) entre les machines virtuelles qui disposent de cartes réseau RDMA (PVRDMA) paravirtualisées. PVRDMA fournit une interface RDMA pour les clients vSphere. Il permet à plusieurs clients d'accéder au périphérique RDMA à l'aide d'une API Verbs, une interface standard. Un ensemble de « Verbs » a été mis en œuvre pour mettre un périphérique client compatible avec RDMA (PVRDMA) à la disposition des applications. Les applications peuvent utiliser le pilote client PVRDMA pour communiquer avec le périphérique physique sous-jacent. PVRDMA prend en charge la technologie RDMA (Remote Direct Memory Access) et offre les fonctions suivantes :
    - Contournement du système d'exploitation
    - Zéro-copie
    - Latence faible et bande passante élevée
    - Consommation d'énergie réduite et accès aux données plus rapide

2-34 À propos des périphériques divers

Une machine virtuelle doit disposer d'un vCPU et d'une mémoire virtuelle. Cependant, l'ajout d'autres périphériques virtuels peut lui permettre d'être plus efficace :

- Lecteur CD/DVD : Connexion à un lecteur CD/DVD ou à une image ISO.
- USB 3.0 : Prise en charge avec les terminaux connectés à l'hôte et au client sur Linux ou Windows 8/Server 2012.
- Disquette : Possibilité de connecter une machine virtuelle à un lecteur ou à une image de disquette
- Périphériques SCSI génériques : Possibilité de connecter une machine virtuelle à d'autres adaptateurs SCSI
- vGPU : Permettent à une machine virtuelle d'utiliser les GPU de l'hôte physique pour les activités à calculs intensifs



En matière de matériel virtuel, la configuration minimale requise consiste en un CPU virtuel et une mémoire virtuelle. L'ajout d'un disque dur virtuel et de cartes d'interface réseau virtuelles permet de rendre la machine virtuelle plus efficace. Il existe d'autres composants virtuels destinés aux machines virtuelles : lecteur de CD/DVD virtuel, lecteur de disquette virtuel et périphériques SCSI virtuels. Le lecteur de CD/DVD et le lecteur de disquette virtuels peuvent pointer vers les périphériques suivants :

- Le lecteur de CD/DVD installé sur l'hôte VMware ESXi ;
- Les images ISO de CD/DVD (`.iso`) ou les images de disquette (`.flp`) ;
- Le lecteur de CD/DVD ou le lecteur de disquette de votre système local.

Vous pouvez mapper le lecteur de CD/DVD de votre machine virtuelle à un lecteur physique ou à un fichier ISO correspondant à ce lecteur. Un fichier ISO est la copie octet par octet d'un CD ou d'un DVD dont le contenu a été extrait. Ces DVD et CD virtuels sont accessibles à distance et sont généralement plus rapides que les CD ou DVD physiques.

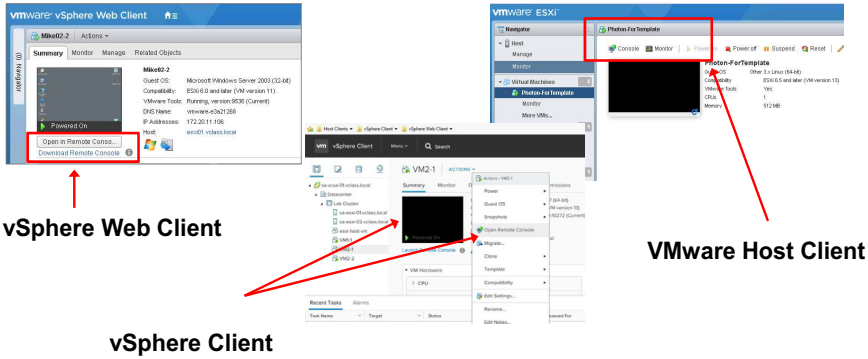
Il est également possible d'ajouter des périphériques SCSI génériques à votre machine virtuelle. Vous pouvez connecter ces périphériques aux adaptateurs SCSI virtuels configurés sur votre machine virtuelle.

Pour en savoir plus sur la création d'une machine virtuelle, consultez le guide *Administration d'une machine virtuelle vSphere*, disponible à l'adresse suivante : http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

2-35 À propos de la console de la machine virtuelle

La console de la machine virtuelle assure les fonctions d'interaction (souris, clavier et affichage à l'écran) nécessaires pour contrôler la machine virtuelle.

Vous pouvez utiliser l'application VMRC (VMware Remote Console Application) autonome pour connecter les terminaux clients.



Vous pouvez ouvrir la console de la machine virtuelle à partir de vSphere Client ou de vSphere Web Client.

La console de la machine virtuelle, disponible dans ces deux interfaces utilisateur, fournit les dispositifs d'interaction requis (souris, clavier et affichage à l'écran) pour contrôler la machine virtuelle. Vous pouvez lancer cette console via l'une des méthodes indiquées sur la diapositive.

vSphere Web Client requiert l'installation d'un plug-in pour activer l'option d'authentification Windows.

Le client VMware Host Client intégré repose sur HTML5 et dispose d'une interface similaire au client vSphere Web Client, mais il est uniquement utilisé pour gérer des hôtes VMware ESXi uniques. Vous utilisez VMware Host Client pour assurer une gestion d'urgence lorsque vCenter Server est momentanément inaccessible.

Cette console vous permet d'accéder au BIOS de la machine virtuelle, d'installer un système d'exploitation sur une machine virtuelle, de la mettre sous tension ou hors tension et de la réinitialiser.

En principe, la console de la machine virtuelle n'est pas utilisée pour se connecter à la machine virtuelle afin d'exécuter des tâches courantes. La connexion au poste de travail virtuel passe habituellement par les fonctions Remote Desktop Connection ou Virtual Network Connection, ou par d'autres options. La console de la machine virtuelle est réservée à certaines tâches, telles que la gestion des redémarrages, la configuration du matériel, et la résolution des problèmes liés au réseau.

2-36 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Montrer comment vSphere s'inscrit dans le Software-Defined Data Center et dans l'infrastructure Cloud
- Expliquer comment vSphere interagit avec les CPU, la mémoire, les réseaux et les systèmes de stockage
- Naviguer dans vSphere Client et examiner les paramètres des VMs
- Utiliser différents clients pour accéder à votre système vCenter Server et à votre hôte VMware ESXi à des fins de gestion
- Comparer les cas d'usage de vSphere Client, VMware vSphere® Web Client et VMware Host Client™
- Identifier les fichiers constituant une machine virtuelle
- Comparer la version 14 du matériel de machine virtuelle avec les autres versions
- Décrire les composants d'une machine virtuelle
- Identifier les méthodes d'accès à la console d'une machine virtuelle
- Identifier les cartes réseau virtuelles et les avantages de l'adaptateur VMXNET3
- Comparer les types de provisionnement du disque virtuel

2-37 Leçon 2 : Ressources partagées : présentation de VMware ESXi

2-38 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire l'architecture des hôtes VMware ESXi
- Naviguer dans la console DCUI (Direct Console User Interface) pour configurer un hôte VMware ESXi
- Utiliser VMware Host Client pour administrer un hôte VMware ESXi
- Discuter des meilleures pratiques en matière de comptes utilisateur
- Installer un hôte VMware ESXi
- Configurer les paramètres d'un hôte VMware ESXi

2-39 À propos de VMware ESXi

La solution VMware ESXi est un hyperviseur offrant les fonctionnalités suivantes :

- Disponible à l'achat avec vSphere ou en tant que version gratuite téléchargeable
- Haut niveau de sécurité :
  - Pare-feu hôte
  - Sécurisation de la mémoire
  - Intégrité des modules du noyau
  - Module TPM (Trusted Platform Module)
  - Démarrage sécurisé UEFI
  - Modes de verrouillage
- Faible encombrement sur un disque
- Installable sur des disques durs, des LUN SAN, des périphériques USB, des cartes SD, un disque SATADOM ou SSD, et des hôtes sans disque

Deux possibilités s'offrent à vous : obtenir la version gratuite de VMware ESXi, appelée VMware vSphere® Hypervisor, ou acheter la version sous licence incluse dans vSphere. La solution VMware ESXi peut être installée sur un disque dur, sur un périphérique USB ou sur une carte SD. Vous avez également la possibilité de l'installer VMware ESXi sur un hôte sans disque (directement dans la mémoire) à l'aide de VMware vSphere® Auto Deploy™.

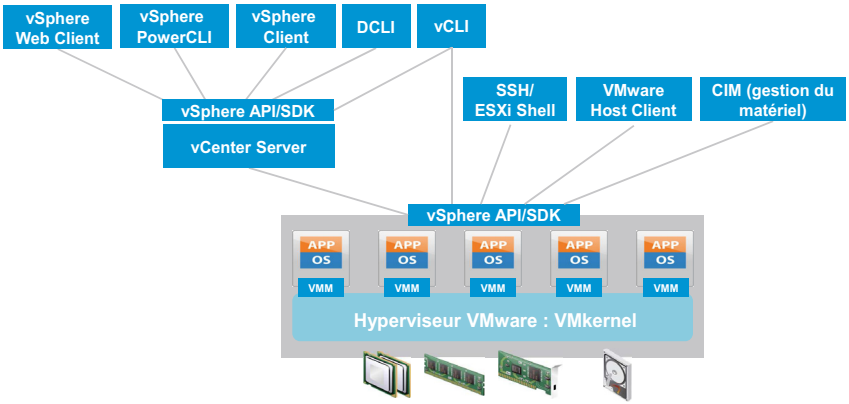
Pour plus de sécurité et de fiabilité, VMware ESXi ne présente qu'un faible encombrement sur un disque. Cette solution offre les fonctionnalités de protection supplémentaires suivantes :

- Pare-feu hôte : afin de réduire les risques d'attaque lancée via l'interface de gestion, VMware ESXi insère un pare-feu entre cette dernière et le réseau.
- Sécurisation de la mémoire : le noyau VMware ESXi, les applications en mode utilisateur et les composants exécutables, tels que les pilotes et les bibliothèques, sont localisés à des adresses mémoire aléatoires et non prédictibles. Associée aux dispositifs de protection de la mémoire non exécutables mis à disposition par les microprocesseurs, la sécurisation de la mémoire protège efficacement contre les tentatives d'exploitation de la mémoire par du code malveillant en vue de profiter des vulnérabilités.
- Intégrité des modules du noyau : un mécanisme de signature numérique garantit l'intégrité et l'authenticité des modules, pilotes et applications chargés par VMkernel.
- Module TPM (Trusted Platform Module) : composant matériel qui permet de créer une plate-forme de confiance. Ce composant confirme l'authenticité du processus de démarrage et de tous les pilotes chargés.

- Démarrage sécurisé UEFI : cette fonctionnalité est destinée aux systèmes prenant en charge le microprogramme de démarrage sécurisé UEFI, qui contient un certificat numérique auquel les offres groupées VMware Infrastructure Bundle (VIB) sont associées. Au démarrage, un vérificateur est lancé avant les autres processus afin de vérifier l'association du composant VIB au certificat intégré dans le microprogramme.
- Modes de verrouillage : le mode de verrouillage est une fonctionnalité de vSphere qui empêche l'exécution directe des fonctions de connexion et d'API sur un hôte VMware ESXi. Avant vSphere 6.0, il n'existait qu'un seul mode de verrouillage. Des retours d'informations émanant de clients avaient souligné le manque de flexibilité de ce mode de verrouillage dans certains cas d'usage. vSphere 6.0 répond à cette préoccupation en proposant deux modes de verrouillage, Normal et Strict.

2-40 Architecture virtuelle

L'hyperviseur VMware ESXi déploie une couche de virtualisation qui permet d'isoler les différentes ressources de l'hôte physique (CPU, mémoire, stockage et réseau) pour les allouer à différentes machines virtuelles.



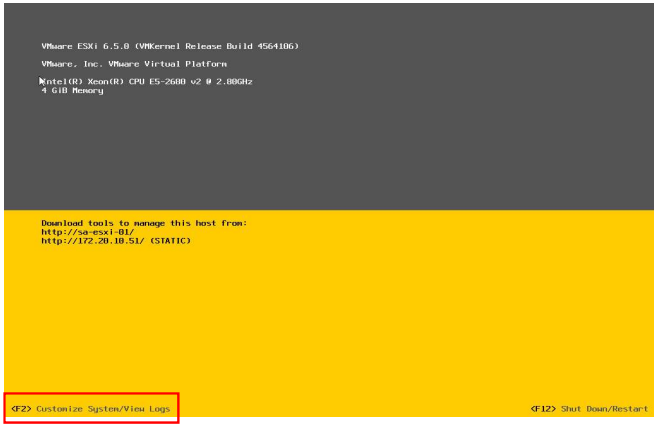
VMware ESXi est un hyperviseur bare-metal offrant la fondation requise pour développer un Data Center dynamique et automatisé. Dans l'architecture VMware ESXi, les applications exécutées sur des machines virtuelles accèdent aux ressources CPU, mémoire et disque ainsi qu'aux interfaces réseau sans interagir directement avec le matériel sous-jacent. L'hyperviseur VMware ESXi est appelé VMkernel. VMkernel reçoit les demandes de ressources émanant des machines virtuelles via le moniteur de machine virtuelle (VMM) et présente ces demandes au matériel physique. Chaque machine virtuelle sous tension dispose de son propre moniteur de machine virtuelle (VMM), qui est chargé de présenter le matériel virtuel à cette machine virtuelle et de recevoir les demandes.

L'accès à un hôte VMware ESXi peut s'effectuer via différentes interfaces :

- vSphere Web Client (connecté à vCenter Server)
- vSphere Client (interface utilisateur HTML5 pour la connexion à vCenter Server)
- VMware Host Client (interface utilisateur HTML5 pour la connexion directe à un hôte)
- VMware vSphere® Command-Line Interface
- VMware vSphere® API et VMware vSphere® Management SDK
- Common Information Model

2-41 Configuration d’un hôte VMware ESXi

DCUI est une interface utilisateur texte autorisant uniquement les interactions clavier.



Vous pouvez utiliser Direct Console User Interface (DCUI) pour configurer certains paramètres des hôtes VMware ESXi. DCUI est une interface de configuration et de gestion de bas niveau accessible via la console du serveur, et principalement utilisée pour la configuration initiale de base. Appuyez sur F2 pour commencer à personnaliser les paramètres système.

2-42 Configuration d'un hôte VMware ESXi : accès root

La console DCUI permet à un administrateur de configurer les paramètres d'accès de l'utilisateur root :

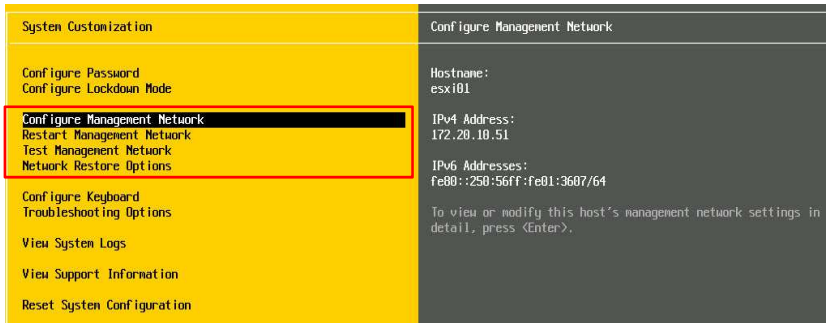
- Définissez un mot de passe root (mots de passe complexes exclusivement).
- Activez ou désactivez le mode verrouillage :
  - Restreint le périmètre de gestion de l'hôte à vCenter Server.
  - Configuration uniquement pour les hôtes gérés par vCenter Server.

Le nom d'administrateur associé à l'hôte VMware ESXi est « root ». Le mot de passe root doit être configuré pendant le processus d'installation de VMware ESXi.

2-43 Configuration d'un hôte VMware ESXi : réseau de gestion

DCUI vous permet de modifier les paramètres réseau :

- Nom d'hôte
- Configuration IP (adresse IP, masque de sous-réseau, passerelle par défaut)
- Serveurs DNS



Votre hôte VMware ESXi ne devient opérationnel que lorsque vous avez configuré votre adresse IP. Par défaut, une adresse affectée par DHCP est configurée pour l'hôte VMware ESXi. Pour modifier ou configurer les paramètres réseau de base, utilisez DCUI.

DCUI vous offre la possibilité de modifier le nom de l'hôte, les paramètres IP (tels que l'adresse IP, le masque de sous-réseau ou la passerelle par défaut) et les serveurs DNS. Vous pouvez également redéfinir la carte réseau utilisé pour le réseau de gestion, configurer les paramètres du VLAN, configurer l'adressage IPv6 ou définir des suffixes DNS personnalisés. Enfin, vous avez la possibilité de redémarrer le réseau de gestion (sans redémarrer le système), de tester le réseau de gestion (à l'aide de commandes ping et DNS) et de désactiver un réseau de gestion.

2-44 Configuration d'un hôte VMware ESXi : autres paramètres

DCUI permet à un administrateur de configurer la disposition de clavier, d'activer les services de dépannage, d'afficher les informations de support et de configurer les journaux système.

DCUI vous permet de changer de disposition de clavier, d'afficher des informations de support telles que le numéro de série de la licence de l'hôte ou de consulter les journaux système. Par défaut, la disposition de clavier est définie sur le clavier anglais.

Les options de dépannage, qui sont désactivées par défaut, vous permettent d'activer ou de désactiver les services de dépannage :

- VMware vSphere® ESXi™ Shell : pour résoudre les problèmes en local.
- SSH : pour résoudre les problèmes à distance via un client SSH, tel que PuTTY.

Il est recommandé de laisser les services de dépannage désactivés jusqu'au moment où vous en avez besoin, par exemple pour résoudre un problème en coopération avec le support technique VMware.

Enfin, cet écran propose l'option **Reset System Configuration**, qui vous permet de rétablir les paramètres de configuration système par défaut du logiciel et de supprimer les extensions ou packages personnalisés que vous avez ajoutés à l'hôte.

2-45 Paramètres d’accès distant : profil de sécurité

Le profil de sécurité contrôle les modalités d’accès à distance à un hôte VMware ESXi :

- VMware ESXi comprend un pare-feu, qui est activé par défaut.
- Le pare-feu VMware ESXi bloque le trafic entrant et sortant, à l’exception du trafic autorisé dans le profil de sécurité de l’hôte.
- Vous pouvez personnaliser de nombreux paramètres de sécurité essentiels d’un hôte VMware ESXi via le volet « Security Profile » de vSphere Client.
- Certains services peuvent être gérés par l’administrateur. Certains processus, tels que DCUI ou les processus client NTP, peuvent démarrer et s’arrêter automatiquement avec l’hôte VMware ESXi.

Chaque hôte VMware ESXi comprend un pare-feu dans son installation par défaut. En règle générale, les clients distants n’ont pas accès aux services disponibles sur un hôte VMware ESXi. De même, les clients locaux n’ont généralement pas la possibilité d’accéder aux services déployés sur des hôtes distants. Afin de garantir l’intégrité de l’hôte, le nombre de ports ouverts par défaut est limité. Si vous souhaitez autoriser ou interdire l’accès à certains services ou clients, vous devez modifier les propriétés du profil de sécurité.

Vous avez la possibilité de configurer les paramètres de pare-feu pour les connexions entrantes et sortantes associées à un service ou à un agent de gestion. Il est possible de gérer les détails de certains services. Par exemple, vous pouvez utiliser les boutons **Start**, **Stop** et **Restart** pour modifier temporairement l’état d’un service. Vous avez également la possibilité de modifier la règle de démarrage (paramètre « Startup Policy ») de sorte que le service démarre avec l’hôte ou en cas d’utilisation d’un port. Pour certains services, vous avez la possibilité d’indiquer explicitement les adresses IP à partir desquelles les connexions sont autorisées.

2-46 Gestion des comptes utilisateur : meilleures pratiques

Soyez vigilant lorsque vous configurez des comptes utilisateur pour l'accès à des hôtes VMware ESXi ou à des systèmes vCenter Server :

- Contrôlez rigoureusement les privilèges root des hôtes VMware ESXi.
- Créez des mots de passe forts comportant au moins huit caractères pour les comptes root. Combinez des caractères spéciaux, des lettres majuscules et minuscules ainsi que des chiffres. Renouvelez régulièrement ces mots de passe.
- Gérez les hôtes VMware ESXi de manière centralisée via le système vCenter Server à l'aide du client vSphere approprié.
- Limitez au minimum l'utilisation des utilisateurs locaux sur les hôtes VMware ESXi :
  - Ajoutez les hôtes VMware ESXi à Active Directory, puis ajoutez les utilisateurs administrateurs au groupe de domaine ESX Admins.
  - Si les utilisateurs locaux sont créés, gérez-les de manière centrale à l'aide de la commande `esxcli` dans vSphere CLI.

Sur un hôte VMware ESXi, le compte utilisateur root est le compte le plus puissant du système. L'utilisateur root a accès à la totalité des fichiers et des commandes. Il dispose de capacités quasi illimitées. La sécurisation de ce compte est donc la mesure la plus importante que vous puissiez prendre pour assurer la sécurité d'un hôte VMware ESXi.

Utilisez autant que possible vSphere Web Client ou vSphere Client pour vous connecter au système vCenter Server et gérer vos hôtes VMware ESXi. Dans certains cas exceptionnels, par exemple lors d'une défaillance du système vCenter Server, vous pouvez utiliser VMware Host Client pour vous connecter directement à l'hôte VMware ESXi. Bien que vous ayez la possibilité de vous connecter à l'hôte VMware ESXi via vSphere CLI ou vSphere ESXi Shell, il convient de réserver ces méthodes d'accès aux tâches de dépannage ou de configuration qui ne peuvent pas être effectuées à l'aide de VMware Host Client. Lorsque vous devez gérer directement un hôte, évitez de créer des utilisateurs locaux sur ce dernier. Si possible, rattachez cet hôte à un domaine Windows, puis connectez-vous à l'aide des informations d'authentification associées à ce domaine.

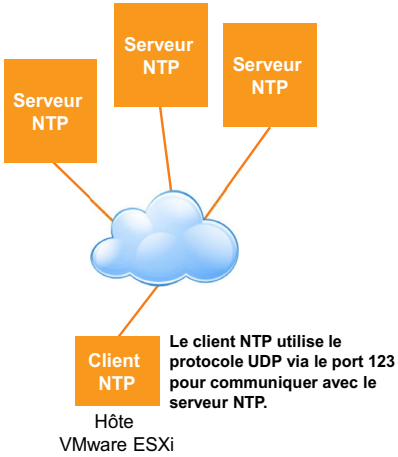
2-47 Hôte VMware ESXi configuré en tant que client NTP

Network Time Protocol (NTP) est un protocole client-serveur servant à synchroniser l'horloge d'un ordinateur avec une référence temporelle.

NTP est important :

- Pour la fiabilité des graphiques de performances
- Pour l'exactitude de l'horodatage des messages journal
- Pour les machines virtuelles, auxquelles il fournit une source avec laquelle se synchroniser

Vous avez la possibilité de configurer un hôte VMware ESXi en tant que client NTP. Cet hôte peut alors synchroniser son horloge avec un serveur NTP présent sur Internet ou avec celui de votre entreprise.



NTP (Network Time Protocol) est un protocole Internet standard servant à synchroniser les horloges des ordinateurs d'un réseau. La synchronisation de l'horloge d'un hôte VMware ESXi offre notamment les avantages suivants :

- Elle permet d'afficher et d'interpréter correctement les données de performances.
- Les journaux d'audit gagnent en pertinence grâce à un horodatage fiable des messages.
- Les machines virtuelles peuvent synchroniser leur horloge avec celle de l'hôte VMware ESXi. La synchronisation des horloges est bénéfique pour les applications exécutées sur les machines virtuelles, telles que les applications de base de données.

NTP est un protocole client-serveur. Lorsque vous le configurez en tant que client NTP, l'hôte VMware ESXi synchronise son horloge avec un serveur NTP présent sur Internet ou avec celui de votre entreprise.

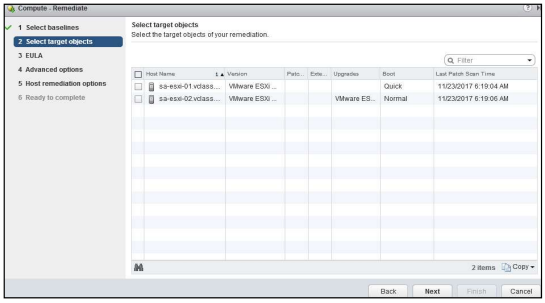
Pour plus d'informations sur le protocole NTP, consultez le site http://www.ntp.org.

Pour en savoir plus sur la synchronisation, consultez les articles 1318 et 1006427 et la base de connaissances VMware, disponibles respectivement à l'adresse http://kb.vmware.com/kb/1318 et à l'adresse http://kb.vmware.com/kb/1006427.

2-48 Démarrage rapide de VMware ESXi

Dans VMware ESX 6.7, le démarrage rapide permet à VMware ESXi de redémarrer sans réinitialiser le BIOS du serveur physique :

- Le démarrage rapide réduit le temps d'exécution pendant les opérations d'application de correctifs ou de mises à niveau sur les hôtes. Le redémarrage peut s'effectuer en une ou deux minutes.
- Le démarrage rapide est intégré au workflow de vSphere Update Manager pendant les opérations d'actions correctives.
- Le démarrage rapide est activé par défaut sur le matériel compatible. Il peut être désactivé si nécessaire.



L'option de démarrage rapide est applicable uniquement avec les plates-formes matérielles suivantes :

- Serveur rack Dell PowerEdge R630
- Serveur rack Dell PowerEdge R640
- Serveur rack Dell PowerEdge R730
- Serveur rack Dell PowerEdge R740
- Serveur HPE ProLiant DL360 Gen9
- Serveur HPE ProLiant DL360 Gen10
- Serveur HPE ProLiant DL380 Gen9
- Serveur HPE ProLiant DL380 Gen10

2-49 Démonstration : Installation et configuration des hôtes VMware ESXi

Votre instructeur va effectuer une démonstration.

2-50 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire l'architecture des hôtes VMware ESXi
- Naviguer dans la console DCUI (Direct Console User Interface) pour configurer un hôte VMware ESXi
- Utiliser VMware Host Client pour administrer un hôte VMware ESXi
- Discuter des meilleures pratiques en matière de comptes utilisateur
- Installer un hôte VMware ESXi
- Configurer les paramètres d'un hôte VMware ESXi

2-51 Points clés

- L'utilisation de machines virtuelles résout nombre de problèmes liés au Data Center.
- Les machines virtuelles sont indépendantes du matériel.
- Les machines virtuelles partagent les ressources de l'hôte VMware ESXi sur lequel elles résident.
- Une machine virtuelle est un ensemble de fichiers facile à transférer et à sauvegarder.
- Les fichiers d'une machine virtuelle sont encapsulés dans un dossier et placés dans une banque de données.
- L'hyperviseur VMware ESXi s'exécute directement sur l'hôte.
- vSphere abstrait les ressources de CPU, de mémoire, de stockage et de réseau pour les mettre à la disposition des machines virtuelles.

Des questions ?

MODULE 3

Création de machines virtuelles

3-2 Vous êtes ici

1. Présentation du cours
2. Présentation de vSphere et du Software-Defined Data Center
3. **Création de machines virtuelles**
4. vCenter Server
5. Configuration et gestion des réseaux virtuels
6. Configuration et gestion du stockage virtuel
7. Gestion des machines virtuelles
8. Gestion et surveillance des ressources
9. vSphere HA, vSphere Fault Tolerance et protection des données
10. vSphere DRS
11. vSphere Update Manager
12. Résolution des problèmes vSphere

3-3 Importance

Il existe différentes méthodes pour créer une machine virtuelle. En choisissant la méthode adéquate pour cette tâche, vous pouvez gagner du temps et rendre le processus de déploiement plus facile à gérer et plus évolutif.

3-4 Objectifs de la formation

À la fin du module, vous devriez être en mesure d'atteindre les objectifs suivants :

- Créer, provisionner et supprimer une machine virtuelle
- Expliquer l'importance de VMware Tools
- Décrire la méthode d'importation d'un modèle OVF d'appliance virtuelle
- Gérer VMware Tools

3-5 À propos du provisionnement des machines virtuelles

Il existe différentes méthodes pour créer une machine virtuelle :

- Vous pouvez utiliser l'assistant « New virtual machine » pour créer des machines virtuelles.
- Vous pouvez déployer de nouvelles machines virtuelles à partir de modèles/clones existants.
- Vous pouvez déployer des machines virtuelles, des appliances virtuelles et des vApps stockées dans un fichier OVF.

VMware offre plusieurs méthodes de provisionnement des machines virtuelles vSphere. La méthode optimale pour votre environnement dépend de facteurs tels que la taille et le type de votre infrastructure, ainsi que des objectifs poursuivis.

Si aucune autre machine virtuelle de votre environnement ne présente la configuration dont vous avez besoin (par exemple un système d'exploitation spécifique ou une configuration matérielle précise), vous pouvez faire appel à l'assistant « New virtual machine » pour créer une machine virtuelle unique. Vous avez notamment la possibilité de créer une machine virtuelle configurée exclusivement à des fins de test. Vous pouvez également créer une machine virtuelle unique, y installer un système d'exploitation et l'utiliser en tant que modèle de clonage pour d'autres machines virtuelles.

Si votre objectif est de disposer de machines virtuelles préconfigurées, vous pouvez déployer des machines virtuelles, des appliances virtuelles et des vApp stockées au format OVF (Open Virtual Machine Format). Une appliance virtuelle est une machine virtuelle généralement équipée d'un système d'exploitation et d'autres logiciels préinstallés. Vous pouvez déployer une machine virtuelle à partir d'un modèle OVF situé sur un système de fichiers local (par exemple, un disque local comme le lecteur C), ou depuis un support amovible (par exemple, lecteur de CD ou clé USB), un lecteur réseau partagé ou une URL.

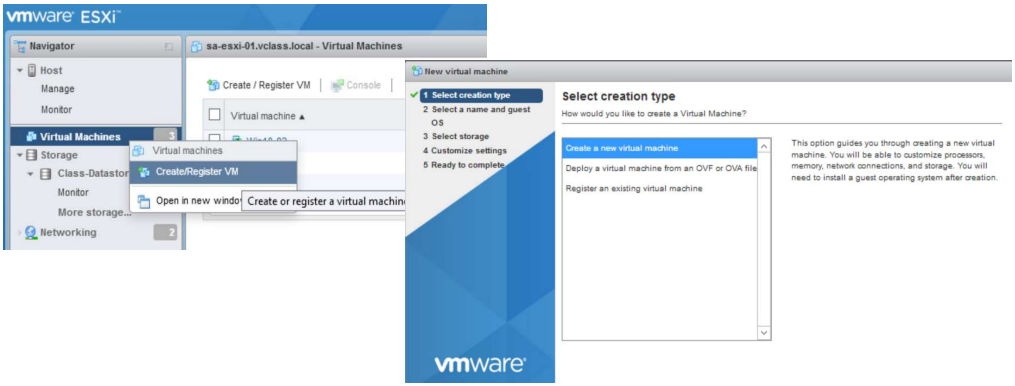
Quel que soit l'emplacement à partir duquel vous l'exécutez, l'assistant « New virtual machine » vous demande de saisir des informations standard :

- Le nom et le dossier de la machine virtuelle. Ressource sur laquelle s'exécutera la machine virtuelle : l'hôte, le cluster, vApp ou le pool de ressources. La machine virtuelle accédera aux ressources de l'objet sélectionné.

- La banque de données dans laquelle les fichiers de la machine virtuelle seront stockés. Chaque banque de données peut avoir des propriétés différentes en matière de taille, de vitesse, de disponibilité, etc. Les banques de données disponibles sont accessibles à partir de la ressource de destination que vous avez sélectionnée.
- Système d'exploitation client à installer sur la machine virtuelle.
- Nombre de cartes réseau, réseau auquel se connecter et type d'adaptateur réseau.
- Mode de provisionnement choisi pour le disque virtuel.

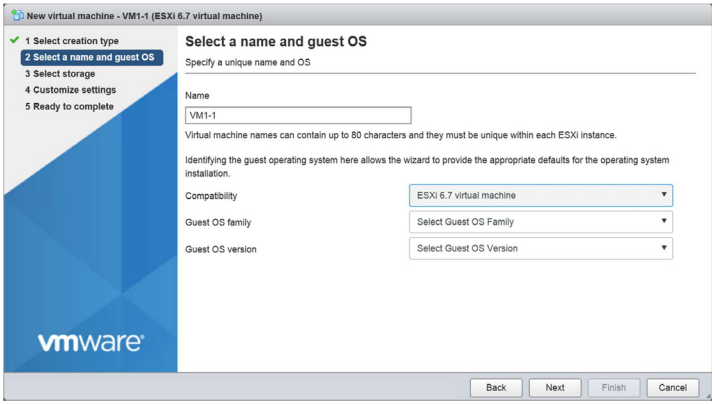
3-6 Création de machines virtuelles avec l'assistant « New virtual machine » (1)

Vous pouvez utiliser l'assistant « New virtual machine » proposé dans vSphere Web Client pour créer une machine virtuelle.



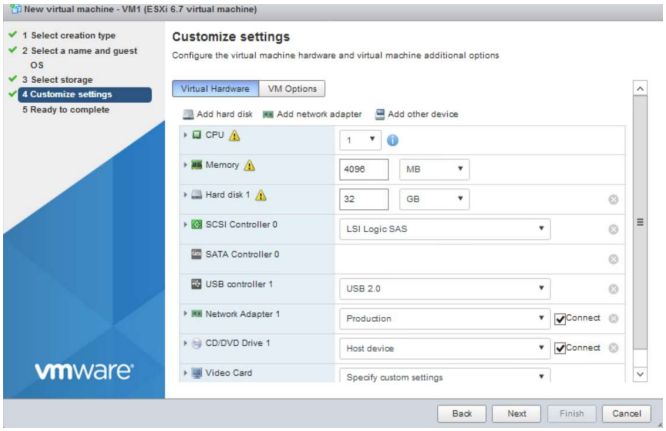
3-7 Création de machines virtuelles avec l’assistant « New virtual machine » (2)

Vous pouvez utiliser l’assistant « New virtual machine » de VMware Host Client pour créer une machine virtuelle.



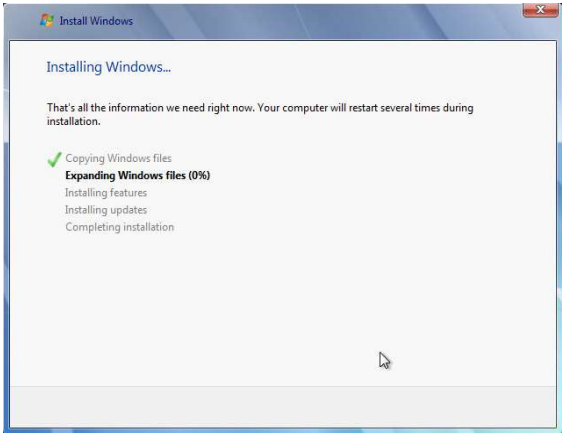
3-8 Paramètres de l’assistant « New virtual machine »

Les paramètres de configuration des machines virtuelles reposent sur vos choix précédents concernant le système d’exploitation.



3-9 Installation du système d'exploitation client

La procédure d'installation d'un système d'exploitation client sur une machine virtuelle est comparable à celle utilisée sur un ordinateur physique.



Pour installer le système d'exploitation client, vous devez interagir avec la machine virtuelle au moyen de la console associée. vSphere Web Client vous permet de connecter un CD, un DVD ou une image ISO contenant l'image d'installation au lecteur de CD/DVD virtuel.

Cette diapositive illustre l'installation d'un système d'exploitation client Windows Server 2008. Vous pouvez utiliser vSphere Web Client pour installer un système d'exploitation client. Il vous est également possible d'installer un système d'exploitation client à partir d'un CD ou d'une image ISO. En général, l'installation à partir d'une image ISO se révèle plus rapide et plus aisée.

Pour en savoir plus sur l'installation des systèmes d'exploitation clients, consultez le Guide *Administration d'une machine virtuelle vSphere*, disponible à l'adresse suivante : http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

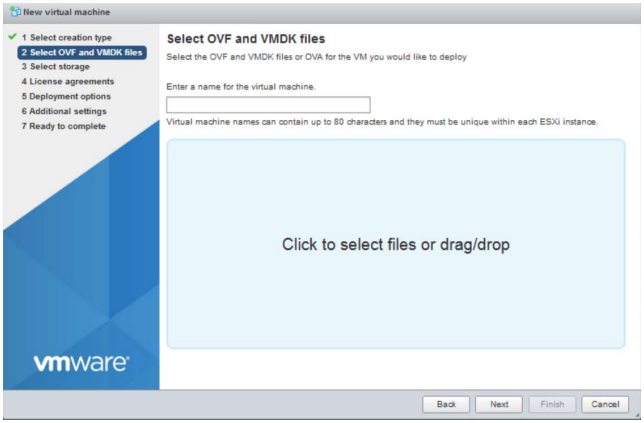
Pour en savoir plus sur les systèmes d'exploitation clients pris en charge, reportez-vous aux *guides de compatibilité du matériel et du système d'exploitation client*, disponibles à l'adresse suivante : http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

3-10 Déploiement de modèles OVF

Vous pouvez déployer une machine virtuelle ou une appliance virtuelle stockées au format OVF (Open Virtual Machine Format).

Les appliances virtuelles sont des machines virtuelles préconfigurées :

- Elles sont généralement dédiées à une fonction unique – par exemple, le navigateur sécurisé ou le pare-feu.
- Elles sont disponibles sur VMware Solution Exchange.



Une appliance virtuelle est une machine virtuelle préconfigurée, qui est généralement dotée d'un système d'exploitation client préinstallé et d'autres logiciels. Elle est habituellement conçue pour répondre à un besoin spécifique, tel que la mise en place d'un navigateur Web sécurisé, d'un pare-feu ou d'un outil de sauvegarde et récupération.

Vous avez la possibilité d'ajouter ou d'importer une appliance virtuelle dans l'inventaire du système vCenter Server ou de VMware ESXi. Vous pouvez importer des appliances virtuelles à partir de différents sites Web, tels que VMware Virtual Appliance Marketplace, disponible à l'adresse suivante : https://marketplace.vmware.com/vsx/.

Les appliances virtuelles sont déployées sous la forme de modèles OVF. OVF (Open Virtual Machine Format) est un format de création de package et de distribution des machines virtuelles indépendant de la plate-forme, à la fois efficace, évolutif et ouvert. Les fichiers OVF sont compressés, ce qui permet d'accélérer les téléchargements. vSphere Web Client valide un fichier OVF avant de l'importer, garantissant ainsi sa compatibilité avec le serveur de destination prévu. Si l'appliance n'est pas compatible avec l'hôte sélectionné, l'importation est impossible.

3-11 À propos de VMware Tools

VMware Tools est une suite d'outils destinés à optimiser les performances du système d'exploitation client de la machine virtuelle.

Avantages de VMware Tools :

- Pilotes de périphériques :
  - Affichage SVGA
  - VMXNET/VMXNET3
  - Pilote ballon pour la gestion de la mémoire
  - Pilote de synchronisation pour la mise au repos des E/S
- Optimisation des performances graphiques
- Amélioration des performances de la souris

Fonctionnalités de VMware Tools :

- Service de pulsation de l'OS client
- Synchronisation de l'heure
- Possibilité d'éteindre la machine virtuelle

VMware Tools améliore la gestion de la machine virtuelle en remplaçant les pilotes génériques du système d'exploitation par des pilotes VMware optimisés pour le matériel virtuel. Vous devez installer VMware Tools dans le système d'exploitation client. Vous pouvez exécuter le système d'exploitation client sans VMware Tools, mais vous perdez alors des fonctionnalités importantes et pratiques. VMware recommande donc l'installation de VMware Tools. Lorsque vous installez ce produit, les fonctions suivantes sont également installées :

- Le service VMware Tools : Ce service synchronise l'heure du système d'exploitation client avec celle du système d'exploitation hôte.
- Un ensemble de pilotes de périphérique VMware associé à des options de surveillance Perfmon supplémentaires.
- Un ensemble de scripts permettant d'automatiser le fonctionnement du système d'exploitation client. Vous pouvez configurer les scripts de sorte qu'ils s'exécutent en cas de changement d'état de fonctionnement de la machine virtuelle.

VMware Tools améliore les performances de la machine virtuelle et permet d'activer de nombreuses fonctionnalités conviviales des produits VMware :

- Les performances graphiques nettement améliorées et la fonction Windows Aero sur les systèmes d'exploitation compatibles
- Les dossiers partagés entre les systèmes de fichiers hôte et client.
- Copier-coller de texte, de graphiques et de fichiers entre la machine virtuelle et le poste de travail client ou hôte.
- L'amélioration des performances de la souris.

- La synchronisation de l'horloge de la machine virtuelle avec celle du poste de travail client ou hôte.
- Les scripts permettant d'automatiser le fonctionnement du système d'exploitation client.
- La possibilité d'arrêter la machine virtuelle.

Bien que le système d'exploitation client puisse s'exécuter sans VMware Tools, de nombreuses fonctionnalités VMware ne sont accessibles qu'une fois ce logiciel installé. Par exemple, si VMware Tools n'est pas installé sur la machine virtuelle, vous ne pouvez pas utiliser les options d'arrêt et de redémarrage à partir de la barre d'outils. Vous pouvez uniquement recourir aux options d'alimentation.

3-12 Gestion de VMware Tools

La version de VMware Tools distribuée avec vSphere 6.5 et les versions ultérieures est la version 10.1.

VMware Tools 10.1 offre les fonctionnalités suivantes :

- Vérification de signature numérique
- Prise en charge de trois images ISO de système d'exploitation client
- Composant Product Locker pour le stockage des images ISO

Vous pouvez télécharger des images ISO pour d'autres systèmes d'exploitation à partir du site de VMware.

vSphere 6.5 et les versions ultérieures ont apporté quelques améliorations à VMware Tools en mettant en place une sécurité renforcée, en réduisant la taille du volume des supports de distribution afin d'exiger moins d'espace, en déchargeant les images ISO sur une instance Product Locker sur disque et en donnant accès aux autres images ISO qui doivent être téléchargées à partir du site Web de VMware.

Pour en savoir plus, consultez l'article 2129825 de la Base de connaissances VMware, disponible à l'adresse suivante : https://kb.vmware.com/s/article/2129825.

3-13 VMware Tools : images ISO prises en charge

Les fichiers ISO fournis avec vSphere 6.5 et les versions ultérieures sont les suivants :

- `windows.iso` : pour les clients Windows Vista et les versions ultérieures
- `winPreVista.iso` : pour les clients Windows 2000, Windows XP et Windows Server 2003
- `linux.iso` : pour les systèmes d'exploitation Linux avec glibc 2.5 ou une version ultérieure (par exemple, RHEL 5 ou une version ultérieure, SLES 11 ou une version ultérieure, Ubuntu 10.04 ou une version ultérieure)

Des versions de VMware Tools destinées à d'autres systèmes d'exploitation clients, tels que Solaris et macOS, sont téléchargeables à partir du portail My VMware à l'adresse suivante : https://download.vmware.com.

VMware a abaissé le nombre d'images ISO distribuées de VMware Tools à seulement trois.

Cette réduction sensible du nombre d'images ISO à conserver et à gérer, alliée à la disponibilité d'une instance Product Locker sur disque, facilite la gestion de vos déploiements d'hôtes et permet d'en réduire la taille.

Si vous avez besoin d'outils pour d'autres systèmes d'exploitation, ceux-ci sont disponibles sur le site Web de VMware, à partir duquel vous pouvez les télécharger et les déployer sur votre instance Product Locker.

3-14 Résolution des problèmes d’installation d’un système d’exploitation sur les machines virtuelles

Problématique : l’installation d’un système d’exploitation 64 bits échoue ou se bloque.

Solution :

1. Vérifiez que le système d’exploitation client que vous tentez d’installer est pleinement certifié par VMware.
2. Assurez-vous que l’hôte VMware ESXi répond aux exigences de matériel et de microprogramme liées à l’exécution d’une machine virtuelle 64 bits.

3-15 Résolution des problèmes d'installation de VMware Tools sur un système d'exploitation client

Problématique : l'installation de VMware Tools échoue ou se bloque.

Solution :

1. Vérifiez que le système d'exploitation client que vous tentez d'installer est pleinement certifié par VMware.
2. Vérifiez que le système d'exploitation approprié est sélectionné.
3. Vérifiez que l'image ISO n'est pas corrompue.
4. Si vous effectuez l'installation sur un système d'exploitation Windows, assurez-vous que le registre Windows ne rencontre aucun problème.
5. En cas d'installation sur un système d'exploitation client Linux 64 bits, vérifiez qu'aucune dépendance ne fait défaut.

Validez chacune des solutions figurant sur la diapositive en référence à votre propre environnement. Ces étapes sont indiquées dans l'ordre le plus approprié pour localiser le problème et déterminer la solution qui convient. Pour en savoir plus, consultez l'article 1003908 de la Base de connaissances VMware, disponible à l'adresse suivante : http://kb.vmware.com/kb/1003908.

3-16 Laboratoire 1 : Déploiement et configuration de machines virtuelles

Créer et préparer une machine virtuelle en vue de son utilisation

1. Accéder au poste de travail étudiant
2. Créer une machine virtuelle
3. Installer VMware Tools
4. Copier des fichiers sur le poste de travail

3-17 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Créer, provisionner et supprimer une machine virtuelle
- Expliquer l'importance de VMware Tools
- Décrire la méthode d'importation d'un modèle OVF d'appliance virtuelle
- Gérer VMware Tools
- Expliquer comment résoudre les problèmes liés à l'installation du système d'exploitation et de VMware Tools

3-18 Points clés

- Vous pouvez provisionner des machines virtuelles de différentes manières :
  - Vous pouvez recourir à l'assistant « New virtual machine » de vSphere Client, de vSphere Web Client ou de VMware Host Client pour créer et cloner des machines virtuelles.
  - Vous pouvez créer une machine virtuelle en déployant un modèle OVF.
- VMware Tools a pour fonction d'optimiser les performances du système d'exploitation client de la machine virtuelle.

Avez-vous des questions ?

MODULE 4

vCenter Server

4-2 Vous êtes ici

1. Présentation du cours
2. Présentation de vSphere et du Software-Defined Data Center
3. Création de machines virtuelles
4. **vCenter Server**
5. Configuration et gestion des réseaux virtuels
6. Configuration et gestion du stockage virtuel
7. Gestion des machines virtuelles
8. Gestion et surveillance des ressources
9. vSphere HA, vSphere Fault Tolerance et protection des données
10. vSphere DRS
11. vSphere Update Manager
12. Résolution des problèmes vSphere

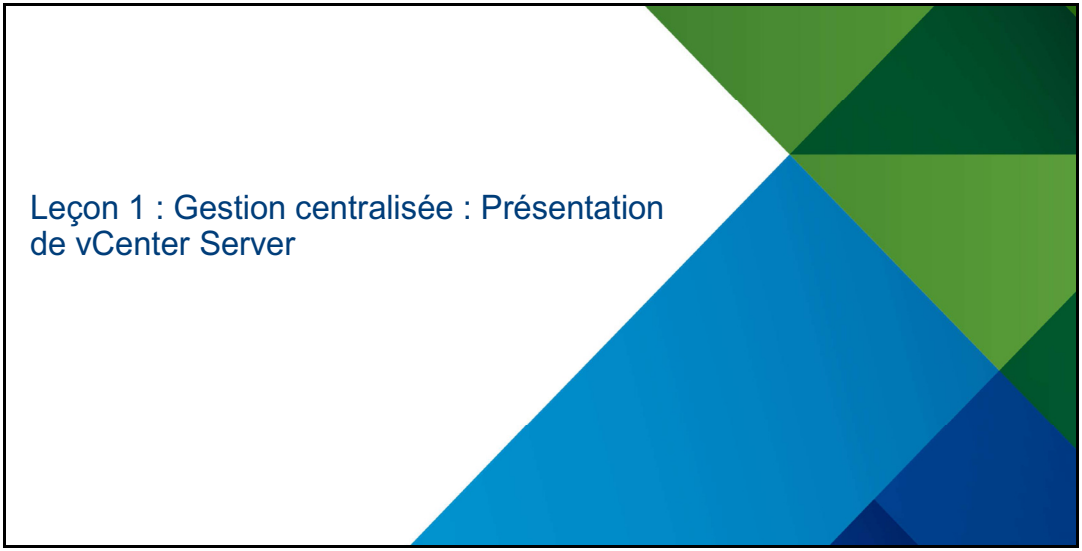
4-3 Importance

vCenter Server vous permet de gérer plusieurs hôtes VMware ESXi et les machines virtuelles associées de manière centralisée. Toute erreur d'installation, de configuration et de gestion de vCenter Server peut compromettre l'efficacité de la gestion, voire entraîner une interruption de service des machines virtuelles et des hôtes VMware ESXi.

4-4 Leçons du module

Leçon 1 :	Gestion centralisée : Présentation de vCenter Server
Leçon 2 :	vCenter Server Appliance
Leçon 3 :	Déploiement de vCenter Server Appliance
Leçon 4 :	Gestion de l'inventaire vCenter Server
Leçon 5 :	Rôles et autorisations de vCenter Server
Leçon 6 :	Sauvegarde et restauration de vCenter Server Appliance
Leçon 7 :	Surveillance de vCenter Server Appliance

4-5 Leçon 1 : Gestion centralisée : Présentation de vCenter Server



4-6 Objectifs de la formation

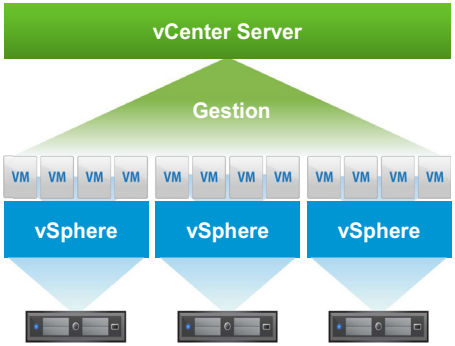
À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire l'architecture de vCenter Server
- Parler de la manière dont les hôtes VMware ESXi communiquent avec vCenter Server
- Identifier les services, les composants et les modules de vCenter Server
- Présenter VMware Platform Services Controller™

4-7 À propos de la plate-forme de gestion vCenter Server

vCenter Server est un service qui joue le rôle de point d'administration centralisée pour les hôtes VMware ESXi et leurs machines virtuelles connectés à un réseau :

- S'exécute sous Windows ou sur une appliance Linux
- Pilote les actions des machines virtuelles et des hôtes



VMware a annoncé que la version 6.7 est la version finale de vCenter Server sur Windows.

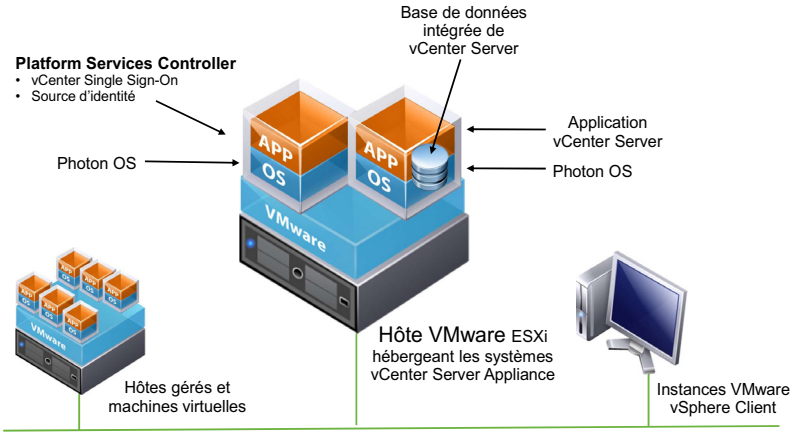
vCenter Server est un service jouant le rôle d'administrateur central des hôtes VMware ESXi connectés à un réseau. Ce service vous permet de regrouper et de gérer les ressources de plusieurs hôtes.

Vous pouvez déployer vCenter Server Appliance sur un hôte VMware ESXi dans votre infrastructure. vCenter Server Appliance est une machine virtuelle basée sur Linux, préconfigurée et optimisée pour exécuter vCenter Server ainsi que les composants vCenter Server.

vCenter Server pour Windows et vCenter Server Appliance fournissent des fonctionnalités avancées, comme VMware vSphere® Distributed Resource Scheduler™, VMware vSphere® High Availability, VMware vSphere® Fault Tolerance, VMware vSphere® vMotion® et VMware vSphere® Storage vMotion®.

4-8 Architecture de vCenter Server

Ce diagramme présente les composants sous-jacents de vCenter Server.



L'architecture de vCenter Server s'appuie sur les composants suivants :

- vSphere Web Client et vSphere Client : Ces clients permettent de vous connecter à vCenter Server afin de gérer vos hôtes VMware ESXi de manière centralisée. Si un hôte VMware ESXi est géré par vCenter Server, les administrateurs doivent toujours utiliser vCenter Server et les clients vSphere pour gérer cet hôte.
- La base de données vCenter Server : La base de données vCenter Server est le composant le plus important. La base de données stocke les éléments d'inventaire, les rôles de sécurité, les pools de ressources, les données de performances et d'autres informations essentielles pour vCenter Server.
- Les hôtes gérés : vCenter Server vous permet de gérer les hôtes VMware ESXi et les machines virtuelles qu'ils hébergent. vCenter Server assure l'accès à l'hôte VMware ESXi via un agent vCenter Server, qui est démarré sur l'hôte lorsque celui-ci est ajouté à l'inventaire vCenter Server.
- VMware vCenter® Single Sign-On : vCenter Single Sign-On est un des services fonctionnant sur Platform Services Controller. Il fournit un domaine de sécurité défini dans votre environnement vSphere. L'authentification est effectuée par le service vCenter Single Sign-On, qui peut être configuré pour effectuer celle-ci selon plusieurs référentiels utilisateur, également appelés « sources d'identités » (par exemple, un domaine Active Directory).

Les services distribués incluent vSphere vMotion, vSphere DRS et vSphere HA, qui sont installés avec vCenter Server.

Plusieurs services supplémentaires sont proposés avec le produit de base – par exemple, VMware vSphere® Update Manager™ et VMware vRealize® Orchestrator™. Aucune licence supplémentaire n’est requise.

4-9 Services vCenter Server

Le groupe de services vCenter Server comprend :

- vCenter Server
- vSphere Web Client (serveur)
- vSphere Update Manager
- VMware vSphere® Auto Deploy™
- VMware vSphere® ESXi™ Dump Collector
- vSphere Client

Platform Services Controller

vCenter Server

Ces fonctions vCenter Server ne peuvent pas être réparties entre différents systèmes. Lorsque vous déployez le composant vCenter Server Appliance, toutes ces fonctions sont comprises dans celui-ci.

Le composant vCenter Server comprend plusieurs systèmes qui étaient déjà présents dans vSphere 5.x :

- vSphere Web Client
- vCenter Server

vSphere Web Client n'est pas une application client. C'est un serveur Web basé sur le serveur Web Apache Tomcat.

Le composant vCenter Server comprend également les services suivants :

- VMware vSphere® ESXi™ Dump Collector
- vSphere Update Manager
- vSphere Auto Deploy

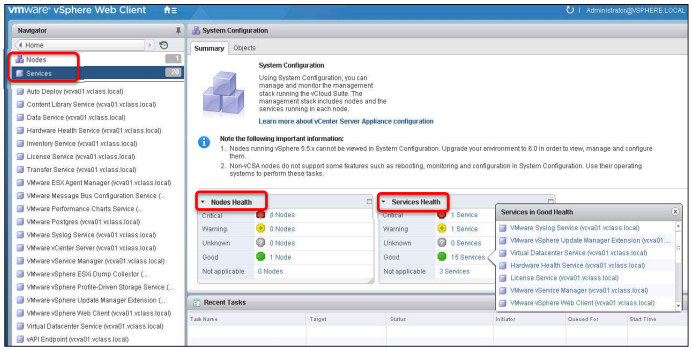
L'installation de ces services n'est pas facultative, mais l'utilisation de leurs fonctionnalités relève de la décision de l'administrateur. Certains services, comme vSphere ESXi Dump Collector, sont installés à l'état désactivé lors de l'installation de vCenter Server sur un serveur Windows.

Vous pouvez utiliser vSphere Update Manager avec la solution vCenter Server sous Windows ou avec vCenter Server Appliance.

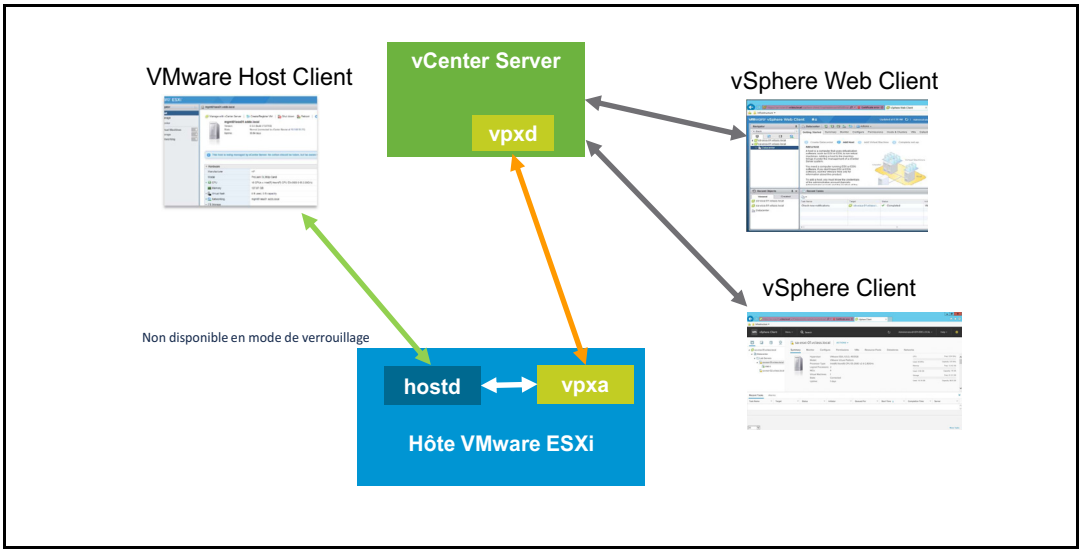
4-10 Surveillance de l'intégrité et de l'état des services et des nœuds dans les systèmes vCenter Server

vSphere Web Client vous permet de surveiller l'état de tous les services et nœuds gérables sur l'ensemble de vos systèmes vCenter Server dans **Administration > Deployment > System Configuration > Services**.

Chaque instance de vCenter Server propose une liste des services par défaut.



4-11 Communication entre VMware ESXi et vCenter Server



vSphere Web Client et vSphere Client communiquent directement avec vCenter Server. Pour communiquer de manière directe avec un hôte VMware ESXi, vous devez utiliser VMware Host Client.

vCenter Server assure un accès direct à l'hôte VMware ESXi via un agent vCenter Server nommé vpxa (agent X de provisionnement). Le processus vpxa est automatiquement installé sur l'hôte et démarré lorsque ce dernier est ajouté à l'inventaire vCenter Server. Le service vCenter Server (vpxd) communique avec le démon de l'hôte VMware ESXi (hostd) via l'agent vCenter Server (vpxa).

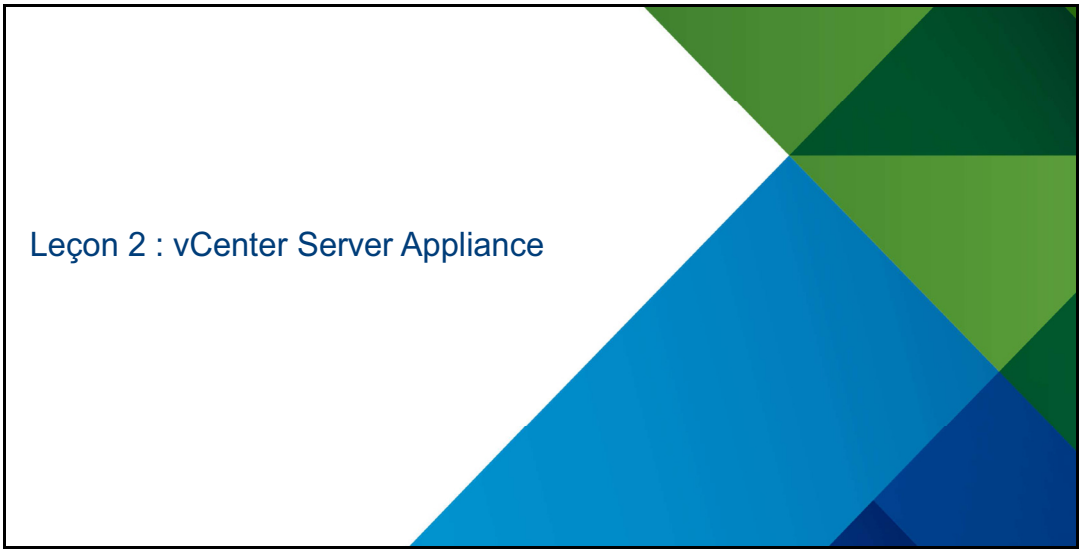
Pour communiquer directement avec l'hôte, en contournant vCenter Server, les clients conversent avec hostd. Ce processus s'exécute directement sur l'hôte VMware ESXi. Il est chargé de gérer la plupart des opérations sur l'hôte VMware ESXi. Il détecte toutes les machines virtuelles enregistrées sur l'hôte VMware ESXi, les volumes de stockage que cet hôte peut voir et l'état de toutes les machines virtuelles. La plupart des commandes ou opérations proviennent de vCenter Server via le processus vpxa. C'est notamment le cas pour la création, la migration et l'activation des machines virtuelles. L'agent vpxa joue le rôle d'intermédiaire entre le processus vpxd, qui s'exécute sur vCenter Server, et le processus hostd, afin de relayer les tâches à exécuter sur l'hôte. Lorsque vous êtes connecté au système vCenter Server via vSphere Web Client, vCenter Server transfère les commandes à l'hôte VMware ESXi via le processus vpxa. La base de données vCenter Server est également mise à jour. Si vous utilisez VMware Host Client pour communiquer directement avec un hôte VMware ESXi, les communications atteignent directement le processus hostd et la base de données vCenter Server n'est pas mise à jour.

4-12 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire l'architecture de vCenter Server
- Parler de la manière dont les hôtes VMware ESXi communiquent avec vCenter Server
- Identifier les services, les composants et les modules de vCenter Server
- Présenter VMware Platform Services Controller™

4-13 Leçon 2 : vCenter Server Appliance



4-14 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Comprendre le but de vCenter Server Appliance
- Décrire l'architecture de vCenter Server
- Décrire l'API REST
- Décrire VMware vCenter Server® High Availability

4-15 Présentation de vCenter Server Appliance (1)

vCenter Server Appliance est une machine virtuelle basée sur Linux, prépackagée et optimisée pour exécuter vCenter Server ainsi que les services associés.

vCenter Server Appliance réduit le temps de déploiement de vCenter Server et des services connexes, et offre une alternative économique à l'installation traditionnelle de vCenter Server basée sur Windows.

Le package de vCenter Server Appliance réunit les composants logiciels suivants :

- VMware Photon™
- Le groupe de services d'infrastructure Platform Services Controller
- Le groupe de services vCenter Server
- PostgreSQL

vCenter Server est un service jouant le rôle d'administrateur central des hôtes VMware ESXi connectés à un réseau. Ce service vous permet de regrouper et de gérer les ressources de plusieurs hôtes. Vous pouvez déployer le système vCenter Server en tant qu'instance VMware vCenter® Server Appliance™. vCenter Server Appliance est une machine virtuelle basée sur Linux, préconfigurée et optimisée pour exécuter vCenter Server ainsi que les composants vCenter Server. Vous pouvez la déployer sur des hôtes exécutant VMware ESXi versions 5.5 ou ultérieures.

4-16 Présentation de vCenter Server Appliance (2)

vCenter Server Appliance exploite la base de données intégrée PostgreSQL, qui affiche une évolutivité verticale allant jusqu'à 2 000 hôtes et 35 000 machines virtuelles enregistrées ou 25 000 machines virtuelles sous tension.

Au cours du déploiement, vous avez la possibilité de dimensionner le système vCenter Server Appliance en fonction de votre environnement vSphere et de spécifier une taille d'espace de stockage adaptée à vos besoins en matière de bases de données.

À partir de vSphere 6.5, vCenter Server Appliance inclut les services vCenter Server suivants :

- L'extension vSphere Update Manager
- La prise en charge de la haute disponibilité par vCenter Server Appliance
- La prise en charge de la sauvegarde et de la restauration en mode fichier par vCenter Server Appliance et Platform Services Controller

vCenter Server propose des fonctionnalités avancées telles que vSphere DRS, vSphere HA, vSphere Fault Tolerance, VMware vSphere® vMotion® et VMware vSphere® Storage vMotion®.

4-17 Évolutivité de vCenter Server Appliance

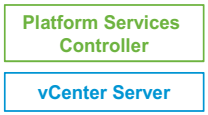
vCenter Server Appliance peut désormais être dimensionné à la même capacité que vCenter Server installé sur un serveur Windows.

Mesure	vCenter Server 6.7 sur Windows	vCenter Server Appliance 6.7
Nombre d'hôtes par système vCenter Server	2 000	2 000
Machines virtuelles mises sous tension par système vCenter Server	25 000	25 000
Hôtes par cluster	64	64
Nombre de machines virtuelles par cluster	8 000	8 000
Base de données	Obligatoirement Oracle ou SQL pour une évolutivité maximale	PostgreSQL
Enhanced Linked Mode	Oui	Oui

4-18 À propos de Platform Services Controller

vCenter Server comprend Platform Services Controller :

- Platform Services Controller comprend un ensemble de services d'infrastructure communs :
  - vCenter Single Sign-On
  - VMware License Server
  - Service de recherche
  - VMware Certificate Authority
  - Magasin de certificats
  - Services d'annuaire VMware
- D'autres fonctionnalités sont installées sous le composant vCenter Server.
- Vous pouvez installer vCenter Server et Platform Services Controller sur une même machine virtuelle ou sur des machines distinctes.
- Lorsque vous installez une instance Platform Services Controller, vous êtes invité à créer un domaine vCenter Single Sign-On ou à rejoindre un domaine existant.



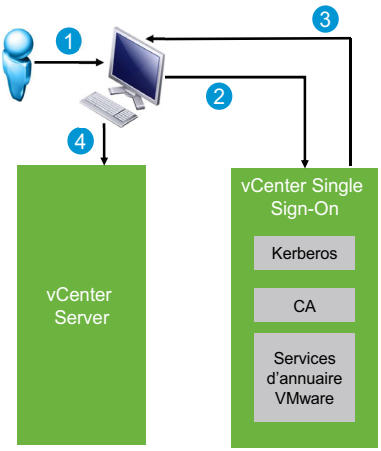
vCenter Server inclut VMware Platform Services Controller. Ce système réunit un ensemble de services d'infrastructure communs. Certains de ces services, comme vCenter Single Sign-On, étaient disponibles sous vCenter Server dans vSphere 5.x. D'autres fonctions, telles que l'autorité de certification et le magasin de certificats internes, sont disponibles dans vSphere 6.x en tant que sous-systèmes destinés à rendre vCenter Server plus robuste.

4-19 À propos de vCenter Single Sign-On

vCenter Single Sign-On permet aux composants vSphere de communiquer entre eux par le biais d'un mécanisme de jetons sécurisés :

- Les utilisateurs s'authentifient sur vCenter Single Sign-On en saisissant leurs informations d'authentification sur la page de connexion.
- vCenter Single Sign-On authentifie les informations d'authentification des utilisateurs avec la source d'identité configurée (par exemple, Active Directory).
- Si l'authentification réussit, vCenter Single Sign-On retourne un jeton représentant l'utilisateur à vSphere Client.
- Le serveur vCenter Single Sign-On retourne le jeton au système vCenter Server en utilisant l'infrastructure d'autorisation vCenter Server pour permettre l'accès à l'utilisateur.

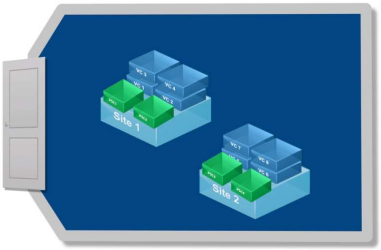
Après s'être connectés à vCenter Server, les utilisateurs authentifiés peuvent consulter toutes les instances vCenter Server ou d'autres objets vSphere pour lesquels leur rôle leur confère des privilèges. Aucune autre authentification n'est requise.

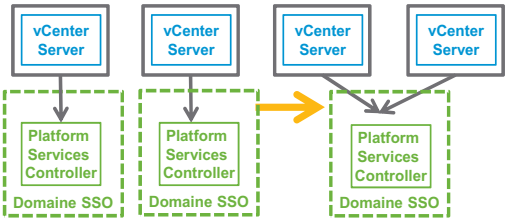


4-20 Domaines et sites multiples vCenter Single Sign-On

Un domaine vCenter Single Sign-On peut être divisé en plusieurs sites :

- Pour garantir une haute disponibilité ou pour les environnements multisites, vous pouvez déployer plusieurs instances Platform Services Controller qui synchronisent toutes leurs configurations et leurs domaines vCenter Single Sign-On.
- Chaque instance Platform Services Controller et vCenter Server ne peut être associée qu'avec un seul site.
- Le repointage entre domaines vCenter Single Sign-On permet à une instance vCenter Server Appliance de migrer vers un nouveau domaine vCenter Single Sign-On.
- Les instances présentes sur différents domaines vCenter Single Sign-On peuvent être regroupées sur un même domaine vCenter Single Sign-On.

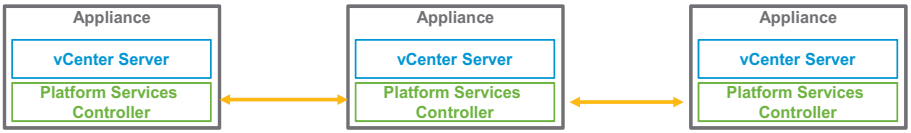




4-21 À propos d'Enhanced Linked Mode

Enhanced Linked Mode vous permet de vous connecter à n'importe quelle instance de vCenter Server Appliance ou vCenter Server, et de gérer les inventaires des deux systèmes vCenter Server dans le groupe :

- Jusqu'à 15 instances vCenter Server peuvent être liées dans un domaine vCenter Single Sign-On. Enhanced Linked Mode intégré prend en charge jusqu'à 10 instances vCenter Server.
- Un groupe Enhanced Linked Mode peut uniquement être créé pendant le déploiement de vCenter Server Appliance ou l'installation de vCenter Server.
- Enhanced Link Mode prend en charge les configurations de déploiement suivantes :
  - vCenter Server avec Platform Services Controller intégré
  - vCenter Server avec Platform Services Controller externe



Vous pouvez uniquement créer un groupe Enhanced Linked Mode pendant le déploiement de vCenter Server Appliance ou l'installation de vCenter Server. Vous ne pouvez pas créer de groupe Enhanced Linked Mode après avoir installé vCenter Server ou après avoir déployé vCenter Server Appliance.

Enhanced Linked Mode propose les fonctionnalités suivantes à la fois pour vCenter Server sur Windows et pour les systèmes vCenter Server Appliance :

- Vous pouvez vous connecter simultanément à tous les systèmes vCenter Server avec le même nom d'utilisateur et le même mot de passe.
- Vous pouvez consulter et interroger les inventaires de tous les systèmes vCenter Server interconnectés dans vSphere Web Client.
- Les rôles, les autorisations, les licences et les règles sont répliqués dans l'ensemble des systèmes vCenter Server interconnectés.

Pour joindre les systèmes vCenter Server dans Enhanced Linked Mode, connectez-les aux mêmes instances Platform Services Controller, ou aux instances Platform Services Controller partageant le même domaine vCenter Single Sign-On.

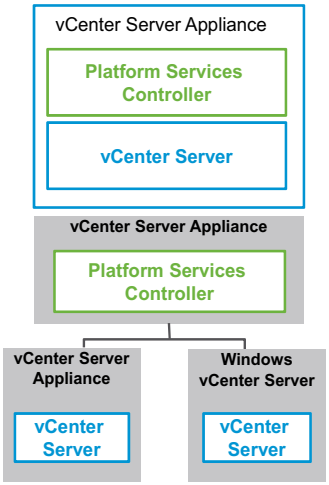
Enhanced Linked Mode nécessite le niveau de licence vCenter Server Standard, et n'est pas pris en charge avec VMware vCenter® Server Foundation™ ou VMware vCenter® Server for Essentials™.

4-22 Options de déploiement de vCenter Server

vCenter Server Appliance équivaut, sur le plan fonctionnel, à vCenter Server installé sur un serveur Windows.

vCenter Server Appliance peut être configuré de différentes manières :

- En tant que système intégré avec une instance interne de Platform Services Controller
- En tant que système distribué avec une instance externe de Platform Services Controller



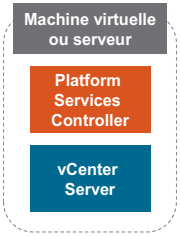
Vous pouvez déployer vCenter Server Appliance sur un hôte VMware ESXi. vCenter Server Appliance est une machine virtuelle préconfigurée basée sur Linux et optimisée pour exécuter vCenter Server.

Vous pouvez télécharger le fichier ISO de vCenter Server Appliance et exécuter le programme d'installation. Des programmes d'installation natifs pour Windows, Linux et macOS sont également disponibles.

4-23 Platform Services Controller intégré

L'utilisation d'une instance Platform Services Controller intégrée crée un déploiement autonome disposant de son propre domaine vCenter Single Sign-On et d'un site unique (même machine virtuelle ou serveur physique) :

- La connexion entre vCenter Server et l'instance intégrée de Platform Services Controller ne se fait pas sur le réseau, et vCenter Server n'est pas soumis aux pannes causées par des problèmes de connectivité et de résolution de noms entre vCenter Server et Platform Services Controller.
- Platform Services Controller intégré convient pour les petits environnements.
- Platform Services Controller intégré ne peut pas rejoindre d'autres instances vCenter Server ou Platform Services Controller.



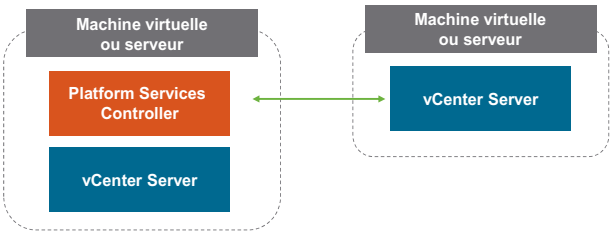
vCenter Server avec Platform Services Controller intégré :

- La machine virtuelle unique contenant les services vCenter Server et Platform Services Controller.
- Le service Platform Services Controller intégré prend en charge VMware vCenter® Server High Availability.
- Chaque instance de vCenter Server avec Platform Services Controller intégré contient un domaine vCenter Single Sign-On isolé.

4-24 Système vCenter Server externe avec une instance intégrée du système vCenter Server

Toutes les instances vCenter Server enregistrées auprès d'une instance Platform Services Controller commune ou de différentes instances rejointes sont connectées via Enhanced Linked Mode :

- Les instances vCenter Server peuvent proposer une haute disponibilité en utilisant vCenter Server High Availability (appliance uniquement).
- Platform Services Controller représente un point unitaire de panne.



Pour une instance de Platform Services Controller intégrée et un système vCenter Server relié à un système vCenter Server externe indépendant, il est possible de relier un second système vCenter Server à un système vCenter Server intégré existant et à l'instance de Platform Services Controller.

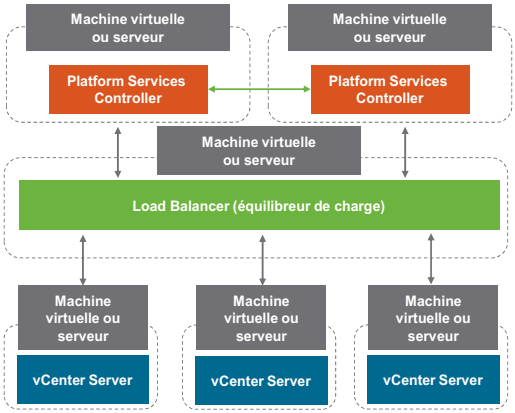
Lorsque vous installez vCenter Server ou déployez vCenter Server Appliance avec une instance de Platform Services Controller externe, vous devez d'abord installer Platform Services Controller. Lors de l'installation de vCenter Server Appliance, vous pouvez choisir de créer un domaine vCenter Single Sign-On ou de rejoindre un domaine existant. Lorsque vous rejoignez un domaine vCenter Single Sign-On existant, les données d'infrastructure de l'instance Platform Services Controller existante sont répliquées sur la nouvelle instance Platform Services Controller.

Pour plus de détails sur les recommandations relatives à Platform Services Controller, consultez l'article 2108548 de la base de connaissances VMware, disponible à l'adresse suivante : http://kb.vmware.com/kb/2108548.

Pour plus d'informations sur la sauvegarde et la restauration des modèles de déploiement externe vCenter Server 6.x, consultez l'article 2147672 de la base de connaissances VMware, disponible à l'adresse suivante : http://kb.vmware.com/kb/2147672.

4-25 Platform Services Controller avec l'équilibreur de charge

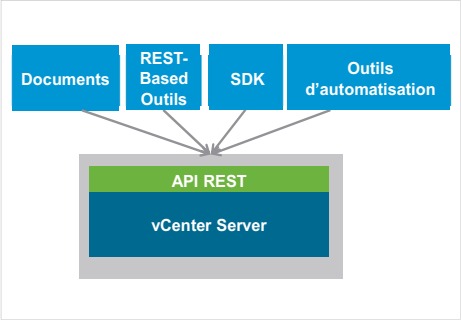
Vous pouvez utiliser un équilibreur de charge tiers par site pour configurer la haute disponibilité de Platform Services Controller et le basculement automatique pour ce site.



Afin de proposer des niveaux de disponibilité supérieurs, il est possible de configurer au moins deux instances Platform Services Controller de manière à ce qu'elles utilisent le même domaine vCenter Single Sign-On derrière un équilibreur de charge. Chacune des instances vCenter Server est configurée pour communiquer avec l'équilibreur de charge, qui utilise des instances Platform Services Controller dans une configuration actif/passif. Si l'instance Platform Services Controller active échoue, l'équilibreur de charge redirige vers la seconde instance Platform Services Controller, et les instances vCenter Server continuent de fonctionner.

4-26 API vCenter Server

vSphere 6.x comprend des API REST et des interfaces conviviales qui simplifient l'automatisation et le développement.



Présentation

- API REST pour la gestion des VMs
- API de conception modernisée et simplifiée
- Facilite l'accès aux fonctions d'automatisation à partir des outils standard
- Conception adaptée à l'automatisation et à DevOps
- SDK complets, interface CLI et accès aux workflows

Avantages

Principal cas d'usage : Automatisation des VMs, développement et bilan d'intégrité des services vCenter Server Appliance

Avantages :

- Réduction de la complexité et du temps de développement des API
- Accès via des processus modernes d'automatisation et de développement pour garantir cohérence et reproductibilité
- Modèle d'API simplifié
- Point d'accès unique pour tous les exemples d'API

VMware fournit des kits de développement logiciel pour plusieurs langages de programmation qui vous permettent d'intégrer des fonctionnalités de service dans votre client API vCenter Server.

Les kits de développement logiciel intégrés dans cette version sont les suivants :

- VMware vSphere Automation SDK for Java
- VMware vSphere Automation SDK for .NET
- VMware vSphere Automation SDK for REST
- VMware vSphere Automation SDK for Python
- VMware vSphere Automation SDK for Perl
- VMware vSphere Automation SDK for Ruby

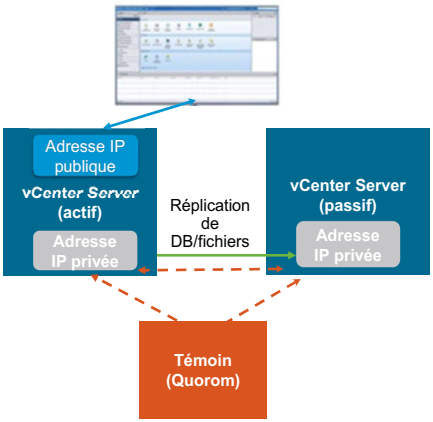
Chacun de ces kits de développement logiciel contient les éléments suivants :

- Liaisons vers l'API d'automatisation vSphere
- vSphere Web Services API
- Guide de référence de l'API
- Guide de programmation
- Exemples

4-27 Haute disponibilité pour vCenter Server Appliance

vCenter Server High Availability offre une protection contre les pannes matérielles et logicielles, et garantit une restauration rapide de votre implémentation, le cas échéant :

- Le nœud protégé est appelé nœud actif.
- Un nœud passif et un nœud témoin sont également créés.
- Si le nœud actif tombe en panne, son rôle est repris par le nœud passif.
- L'état du nœud actif est répliqué sur le nœud passif et capturé dans une base de données PostgreSQL ainsi que dans les fichiers de configuration.



Qu'elles soient planifiées ou non, les interruptions de service engendrent des coûts considérables. Cependant, les solutions permettant d'augmenter les niveaux de disponibilité étaient jusqu'à présent coûteuses, difficiles à mettre en œuvre et complexes à gérer.

Le logiciel VMware offre désormais une alternative plus simple et plus économique pour optimiser la disponibilité des applications essentielles. Grâce à vSphere, les entreprises peuvent aisément garantir la disponibilité de base requise pour toutes leurs applications, mais aussi assurer plus simplement et à moindre coût des niveaux de disponibilité plus élevés.

vCenter Server High Availability protège vCenter Server Appliance contre les défaillances des systèmes hôtes et autres composants matériels. L'architecture active-passive de cette solution permet également une réduction significative des interruptions de service lors du déploiement des correctifs de vCenter Server Appliance.

Après quelques étapes de configuration du réseau, vous créez un cluster contenant trois nœuds : un nœud actif, un nœud passif et un nœud témoin. Vous avez le choix entre plusieurs processus de configuration, selon les caractéristiques de la configuration existante.

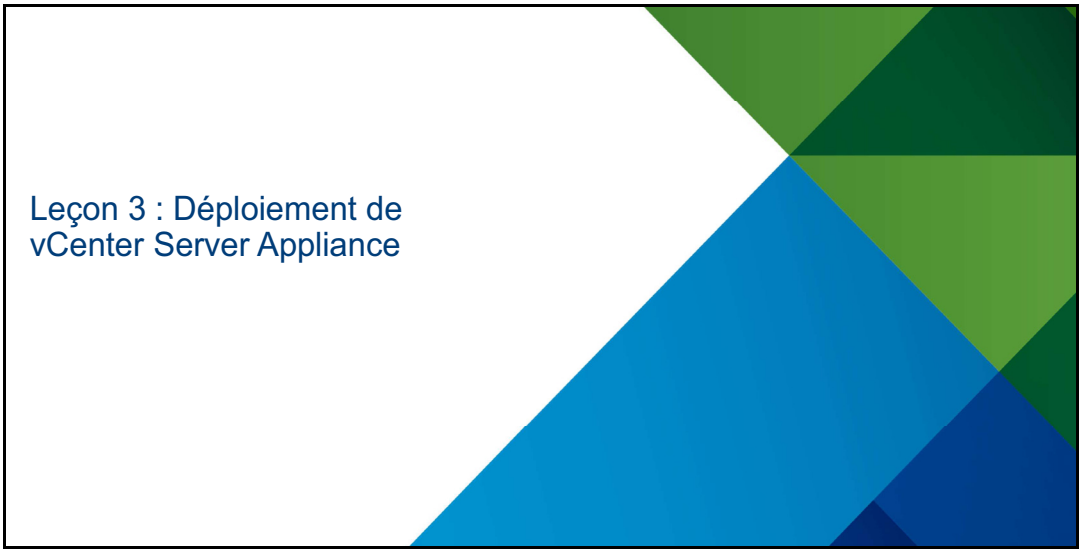
Il convient de prendre plusieurs facteurs en considération avant de procéder à la configuration de vCenter Server High Availability. Un déploiement vCenter Server Appliance peut utiliser une instance Platform Services Controller interne ou externe. Un déploiement sur un réseau existant dont les composants utilisent différentes versions de vSphere ne présente pas les mêmes contraintes qu'un déploiement sur un nouveau réseau comportant exclusivement des composants vSphere 6.x. Les ressources et la configuration logicielle requises doivent être examinées avec soin.

4-28 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Comprendre le but de vCenter Server Appliance
- Décrire l'architecture de vCenter Server
- Décrire l'API REST
- Décrire VMware vCenter Server® High Availability

4-29 Leçon 3 : Déploiement de vCenter Server Appliance



4-30 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Déployer vCenter Server Appliance dans une infrastructure
- Ajouter des clés de licence à vCenter Server
- Configurer les paramètres de vCenter Server

4-31 Préparation du déploiement de vCenter Server Appliance

Avant le déploiement de vCenter Server Appliance, vous devez exécuter différentes tâches :

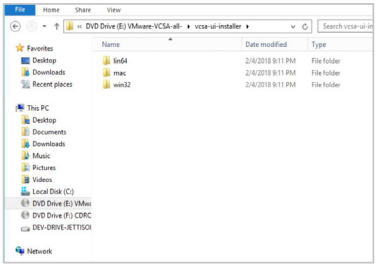
- Vérifiez que l'ensemble des exigences du système vCenter Server Appliance ont été respectées.
- Lors de la première installation de vCenter Server Appliance, Platform Services Controller doit être déployé avant vCenter Server :
  - Si vous déployez vCenter Server Appliance avec une instance intégrée de Platform Services Controller, cette opération s'effectue automatiquement.
  - Si vous installez vCenter Server Appliance avec une instance de Platform Services Controller externe, vous devez d'abord installer cette instance, puis vCenter Server.
  - Vous devez indiquer le nom de domaine complet (FQDN) ou l'adresse IP statique de l'ordinateur hôte sur lequel s'effectue l'installation ou la mise à niveau. Nous vous recommandons d'indiquer le nom de domaine complet.
  - Vous devez vous assurer que les horloges de toutes les machines connectées au réseau vSphere sont synchronisées.

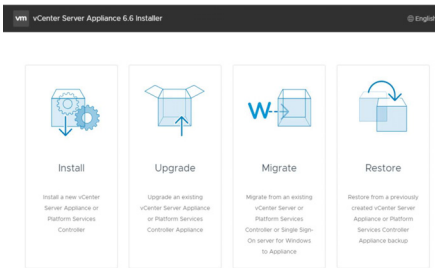
Pour en savoir plus, consultez le document *Guide d'installation et de configuration vSphere*, à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

4-32 Programme d’installation de l’interface utilisateur native de vCenter Server Appliance

vSphere 6.x comprend une application native qui facilite le déploiement de vCenter Server Appliance 6.x :

- Cette application native se décline en versions Windows, Linux et macOS, qui ne présentent aucune dépendance vis-à-vis de navigateurs ou de plug-ins.
- Cette application dotée d’une interface utilisateur effectue un ensemble de validations et de prévérifications au cours du déploiement afin de garantir l’absence d’erreurs et la compatibilité de l’environnement résultant.

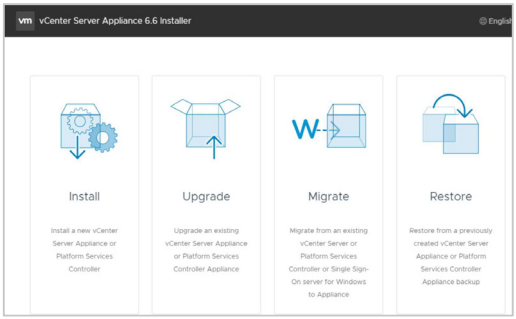




4-33 Installation, mise à niveau, migration et restauration de vCenter Server

L'outil de déploiement doté d'une interface graphique offre les options suivantes :

- **Install :** installe une nouvelle instance de vCenter Server Appliance ou de Platform Services Controller
- **Upgrade :** met à niveau une instance vCenter Server Appliance existante
- **Migrate :** migre une instance existante de vCenter Server pour Windows vers vCenter Server Appliance
- **Restore :** effectue une restauration à partir d'une sauvegarde préalablement créée de vCenter Server Appliance



4-34 Déploiement de vCenter Server Appliance

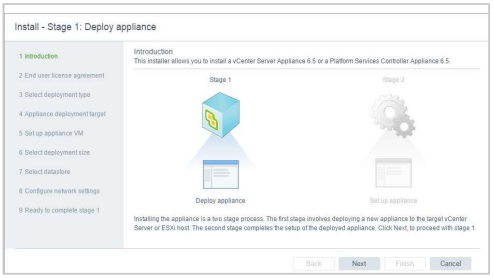
Le programme d'installation est disponible pour Windows, Linux et macOS.

vSphere Update Manager est inclus.

L'installation de vCenter Server Appliance et de Platform Services Controller se déroule en deux phases :

- Phase 1 : Déploiement du fichier OVF
- Phase 2 : Configuration

Le déploiement peut être entièrement automatisé en utilisant des modèles JSON avec le programme d'installation CLI sur Windows, Linux et macOS.



Lorsque vous optez pour le déploiement de vCenter Server Appliance avec une instance intégrée de Platform Services Controller, vous déployez cette dernière et vCenter Server sous la forme d'une seule et même appliance.

Lorsque vous décidez de déployer vCenter Server Appliance avec une instance externe de Platform Services Controller, l'instance de vCenter Server est déployée sous la forme de deux appliances :

1. Vous déployez l'instance de Platform Services Controller.
2. Vous déployez vCenter Server et les composants associés sous la forme d'une appliance virtuelle distincte et connectez vCenter Server Appliance à l'instance de Platform Services Controller externe.

4-35 Déploiement de vCenter Server Appliance en deux phases

Phase 1a, phase d'interface utilisateur :

1. Accepter le contrat EULA
2. Sélectionner le type de déploiement
3. Se connecter à l'hôte VMware ESXi ou au système vCenter Server cible pour déployer vCenter Server Appliance
4. Définir le nom et le mot de passe root de vCenter Server Appliance
5. Sélectionner la taille du déploiement (mémoire/CPU), l'espace de stockage et l'emplacement de la banque de données (disque à provisionnement fin).
6. Définir les paramètres réseau.

Phase 1b, phase de déploiement :

1. Le fichier OVF est déployé sur l'hôte VMware ESXi.
2. Les disques et le réseau sont configurés.

Phase 2, phase de configuration :

1. Créer un domaine vCenter Single Sign-On ou rejoindre un domaine existant.
2. Rejoindre le Programme d'amélioration de l'expérience client.

4-36 Assistant de déploiement de vCenter Server

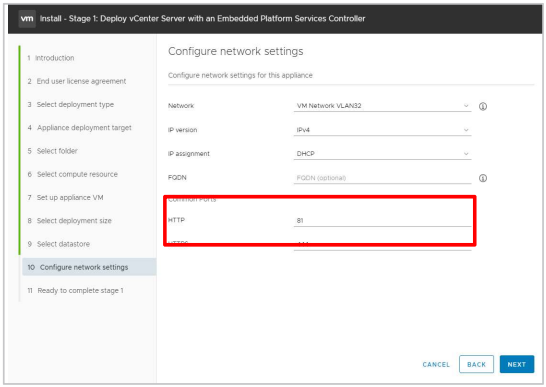
L'assistant de déploiement de vCenter Server vous invite à saisir les informations correspondant à la méthode de déploiement choisie.

	Intégré	Platform Services Controller	vCenter Server
Phase 1			
Cible de déploiement	✓	✓	✓
Type de déploiement	✓	✓	✓
Taille de déploiement	✓	✕	✓
Définition du nom de VM	✓	✓	✓
Définition du mot de passe root	✓	✓	✓
Définition de l'emplacement de la banque de données	✓	✓	✓
Définition du réseau	✓	✓	✓
Phase 2			
Créer un domaine vCenter Single Sign-On	✓	✓	✕
Rejoindre un domaine vCenter Single Sign-On	✕	✓	✓
Configuration CEIP	✓	✓	✓

4-37 Configuration de ports personnalisés pour un déploiement de vCenter Server Appliance

Vous configurez des ports HTTP et HTTPS personnalisés pour vCenter Server Appliance lors de l'installation.

Les ports personnalisés peuvent être obligatoires pour des raisons de sécurité.



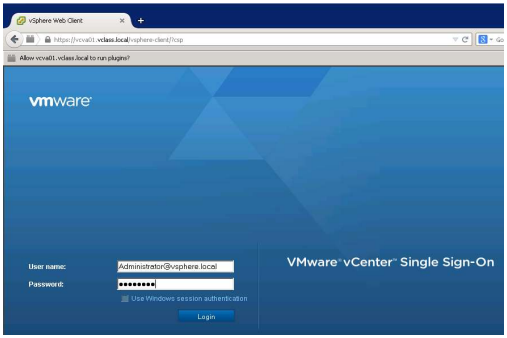
vCenter Server Appliance permet la définition de ports HTTP et HTTPS personnalisés lors de l'installation. Les ports par défaut sont 80 et 443. Les ports ne peuvent pas être changés après l'installation.

Il peut être utile pour le client de définir des ports HTTP/HTTPS personnalisés si une règle de sécurité de l'entreprise interdit l'utilisation des ports par défaut.

4-38 Se lancer avec vCenter Server

Une fois la solution vCenter Server Appliance déployée, connectez-vous à celle-ci via l'un des clients vSphere afin de gérer l'inventaire vCenter Server :

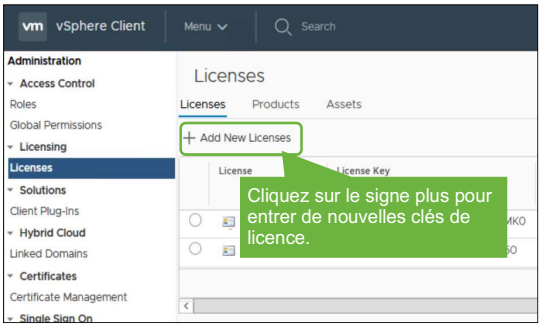
- vSphere Web Client : https:*//FQDN_de_vCenter_Server/*vsphere-client
- vSphere Client : https:*//FQDN_de_vCenter_Server/*ui



4-39 Ajout de clés de licence à vCenter Server

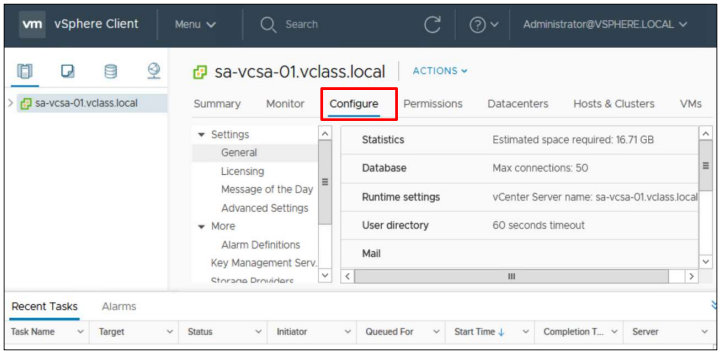
Vous devez attribuer une licence à vCenter Server avant la date d'expiration de la période d'évaluation de 60 jours.

Dans vSphere Client, sélectionnez **Home > Administration > Licenses**.



4-40 Configuration des paramètres de vCenter Server

Vous pouvez configurer le système vCenter Server depuis vSphere Client, notamment pour modifier les paramètres d'attribution de licences, de collecte de statistiques et de journalisation. Pour accéder aux paramètres du système vCenter Server, accédez à celui-ci dans vSphere Client, cliquez sur l'onglet **Configure** et sélectionnez **Settings**.



4-41 Démonstration : Utilisation de vCenter Server Appliance

Votre instructeur va effectuer une démonstration.

4-42 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Déployer vCenter Server Appliance dans une infrastructure
- Ajouter des clés de licence à vCenter Server
- Configurer les paramètres de vCenter Server

4-43 Leçon 4 : Gestion de l’inventaire vCenter Server

4-44 Objectifs de la formation

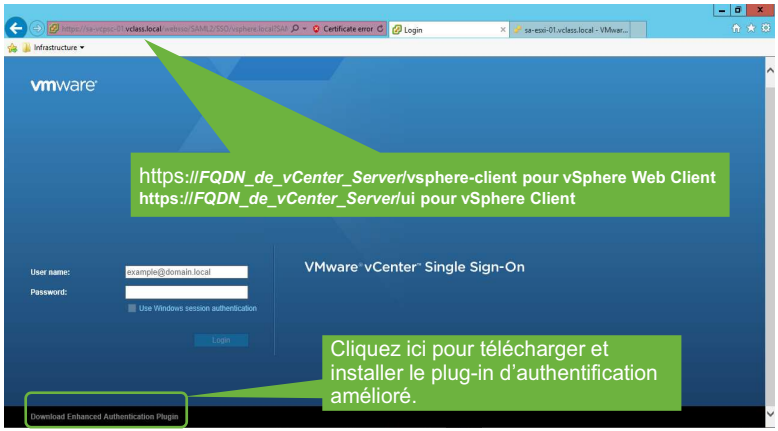
À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Utiliser vSphere Client pour gérer l'inventaire vCenter Server
- Créer et organiser des objets d'inventaire vCenter Server
- Ajouter un Data Center et des objets organisationnels à vCenter Server
- Ajouter des hôtes à vCenter Server
- Parler de la création de balises d'inventaire personnalisées pour les objets d'inventaire

.

4-45 Accès aux clients vSphere

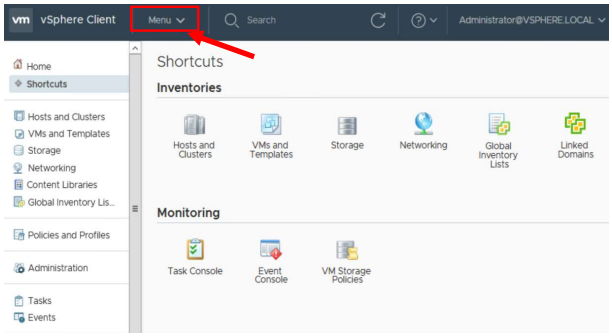
Pour accéder à un client vSphere, ouvrez un navigateur Web et entrez l'URL correspondant au client souhaité.



4-46 Page d’accueil de vSphere Client

Sélectionnez **Menu > Home** pour vous rendre sur la page d’accueil de vSphere Client.

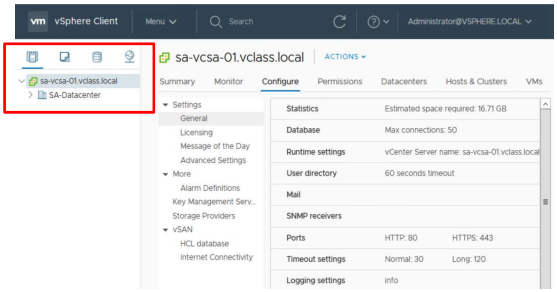
Cette page comprend un volet de navigation sur la gauche et, sur la droite, les volets « Inventories », « Monitoring » et « Administration ».



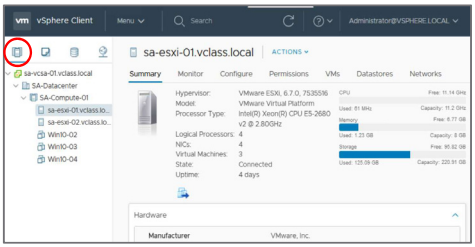
Depuis la page d’accueil de vSphere Client, vous pouvez gérer l’inventaire du système vCenter Server, effectuer le suivi de l’environnement d’infrastructure et exécuter différentes tâches d’administration du système.

4-47 Utilisation du volet de navigation de vSphere Client

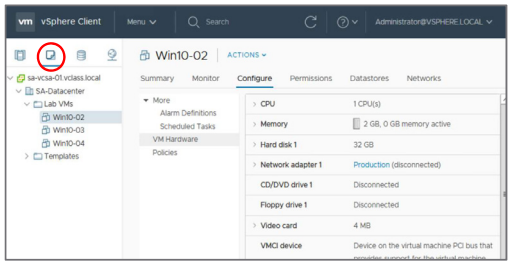
Ce volet de navigation vous permet de parcourir et de sélectionner des objets dans l'inventaire vCenter Server.



4-48 Vues de vCenter Server : « Hosts and Clusters » et « VMs and Templates »



Vue d'inventaire « Hosts and Clusters »

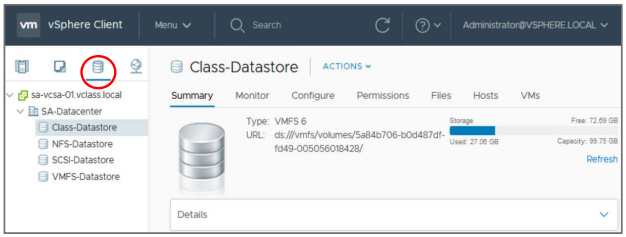


Vue d'inventaire « VMs and Templates »

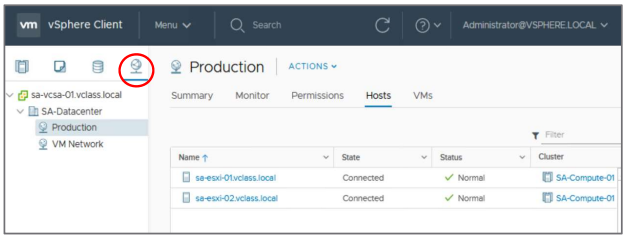
La vue d'inventaire « Hosts and Clusters » affiche tous les objets hôtes ou clusters présents dans un Data Center.

La vue d'inventaire « VMs and Templates » affiche tous les objets machines virtuelles ou modèles présents dans un Data Center.

4-49 Vues de vCenter Server : « Storage » et « Networks »



Vue d'inventaire « Storage »



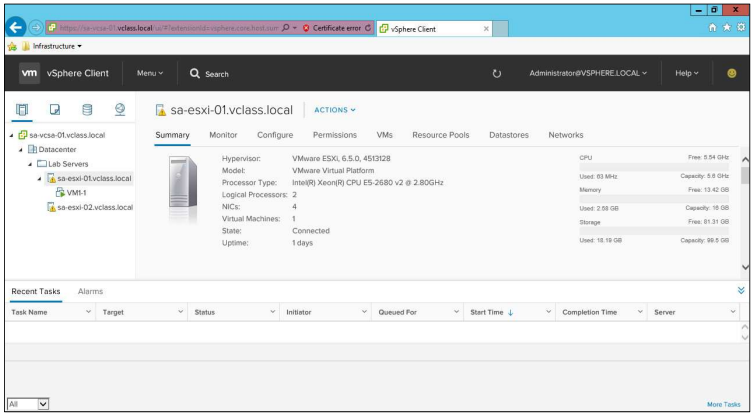
Vue d'inventaire « Networks »

La vue d'inventaire « Storage » affiche tous les détails relatifs aux datastores d'un Data Center. La vue d'inventaire « Networks » affiche tous les groupes de ports de machine virtuelle et les commutateurs distribués.

Comme pour les autres vues d'inventaire, vous avez la possibilité d'organiser vos objets de banque de données et de réseau en dossiers.

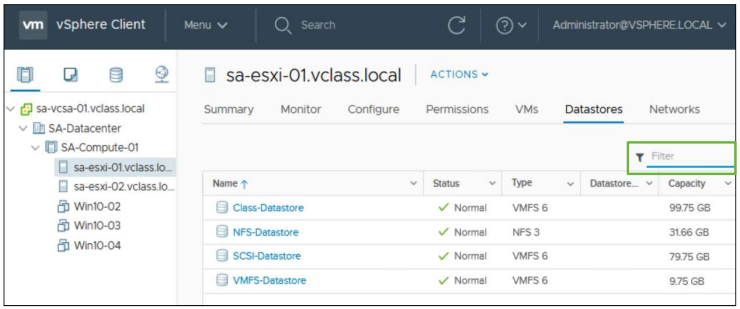
4-50 Affichage des informations relatives aux objets

Vous pouvez vous déplacer pour afficher les informations sur les objets et accéder aux objets associés, ce qui simplifie la surveillance et la gestion des propriétés correspondantes.



4-51 Utilisation des filtres rapides dans vSphere Client

Les filtres rapides de vSphere Client permettent de rechercher un objet ou un ensemble d'objets dans l'inventaire vCenter Server en appliquant certains critères d'affichage.



Les filtres rapides vous permettent de rechercher un objet ou un ensemble d'objets répondant à certains critères dans votre inventaire vCenter Server.

Les filtres rapides figurent dans les vues de liste qui s'affichent dans l'onglet **Objects** de la liste d'inventaire et dans les résultats de recherche.

Par exemple, vous pouvez utiliser ces options pour rechercher dans l'inventaire vSphere toutes les machines virtuelles qui sont sous tension, mais qui ne sont pas dotées de VMware Tools.

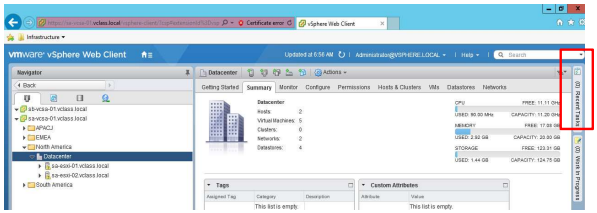
4-52 Glissement d’objets dans vSphere Client

Il est possible de faire glisser un objet de l’inventaire vers un autre emplacement.

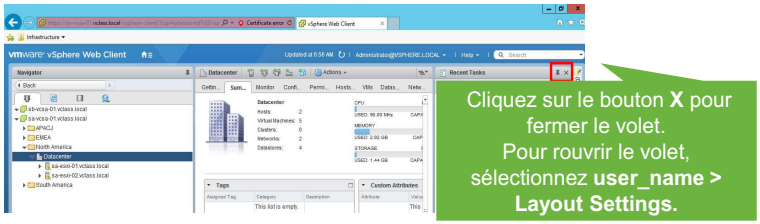
4-53 Utilisation de la fonctionnalité Épingler/Désépingler dans vSphere Web Client

Vous avez la possibilité d'épingler et de désépingler les volets affichés dans l'interface utilisateur.

Volet « Recent Tasks » désépinglé



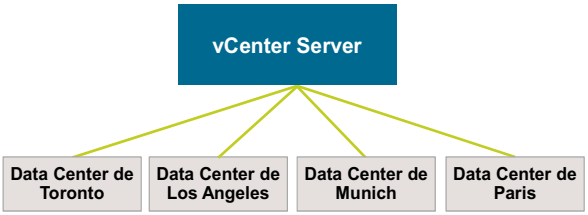
Volet « Recent Tasks » épinglé



4-54 À propos des objets du Data Center

Un Data Center virtuel est une organisation logique de tous les objets d'inventaire nécessaires pour mettre en place un environnement entièrement fonctionnel pour l'exécution des machines virtuelles :

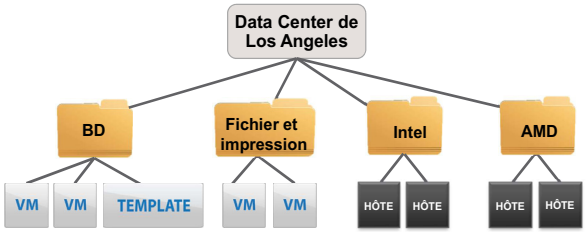
- Vous pouvez créer plusieurs Data Centers pour organiser des ensembles d'environnements.
- Chaque Data Center inclut ses propres hôtes, modèles, banques de données, réseaux et machines virtuelles.



Un Data Center virtuel contient l'ensemble des objets d'inventaire nécessaires pour mettre en place un environnement entièrement fonctionnel pour l'exécution des machines virtuelles. Vous pouvez créer plusieurs Data Centers pour organiser des ensembles d'environnements. Par exemple, vous pouvez créer un Data Center distinct pour chacune des unités organisationnelles de votre entreprise, ou créer des Data Centers pour les environnements hautes performances et d'autres Data Centers pour les machines virtuelles moins exigeantes.

4-55 Organisation des objets de l'inventaire dans des dossiers

Les éléments du Data Center peuvent être regroupés dans des dossiers. Vous pouvez créer des dossiers et des sous-dossiers pour optimiser l'organisation des systèmes.



Commencez par planifier la configuration de votre environnement virtuel. Une implémentation vSphere de grande envergure peut comporter plusieurs Data Centers virtuels mettant en œuvre des configurations complexes de systèmes hôtes, de clusters, de pools de ressources et de réseaux. Elle peut mettre en présence plusieurs systèmes vCenter Server interconnectés en mode Enhanced Linked Mode. Une implémentation plus modeste peut se réduire à un unique Data Center virtuel présentant une topologie plus simple. Quelle que soit la taille de votre environnement virtuel, il importe de déterminer le mode d'utilisation et d'administration des machines virtuelles qu'il devra prendre en charge.

Le remplissage et l'organisation de votre inventaire impliquent les tâches suivantes :

- Créer des Data Centers.
- Ajouter des hôtes à ces Data Centers.
- Organiser les objets de l'inventaire dans des dossiers.
- Configurer la mise en réseau à l'aide de commutateurs standard vSphere ou de commutateurs distribués vSphere. En cas d'utilisation de services tels que vSphere vMotion, le stockage TCP/IP, VMware vSAN™ ou vSphere Fault Tolerance : configurez le réseau VMkernel pour ces services.

  Pour plus d'informations, reportez-vous au guide *Mise en réseau vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

- Configurer les systèmes de stockage et créer des objets d'inventaire de banques de données afin de fournir des conteneurs logiques pour les périphériques de stockage répertoriés dans votre inventaire.

  Pour plus d'informations, reportez-vous au guide *Stockage vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

- Créer des clusters visant à consolider les ressources d'un ensemble d'hôtes et de machines virtuelles. Vous avez la possibilité d'activer vSphere HA et vSphere DRS afin d'améliorer la disponibilité et de permettre une gestion plus flexible des ressources.

  Pour en savoir plus sur la configuration de vSphere HA, consultez le document *Disponibilité vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

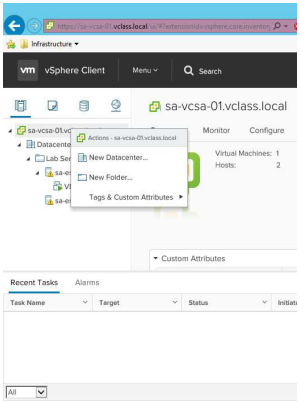
  Pour en savoir plus sur la configuration de vSphere DRS, consultez le document *Gestion des ressources vSphere,* disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

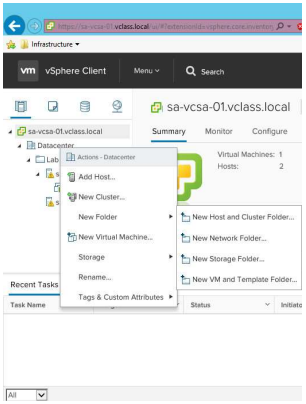
- Créer des pools de ressources, afin de fournir une abstraction logique et de permettre une gestion flexible des ressources disponibles dans vSphere. Les pools de ressources peuvent être regroupés et hiérarchisés, puis utilisés pour le partitionnement hiérarchique des ressources mémoire et CPU disponibles.

  Pour plus d'informations, consultez le document *Gestion des ressources vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

4-56 Ajout d'un Data Center et d'objets organisationnels à vCenter Server

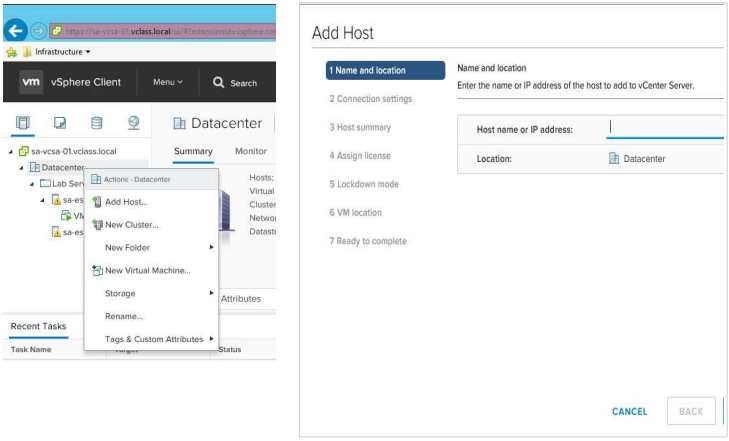
Vous pouvez ajouter un Data Center ainsi que des dossiers d'hôte et de cluster. Créez des dossiers pour regrouper les objets du même type afin de simplifier leur gestion.





4-57 Ajout d'hôtes VMware ESXi à vCenter Server

Vous pouvez ajouter un hôte VMware ESXi à vCenter Server.

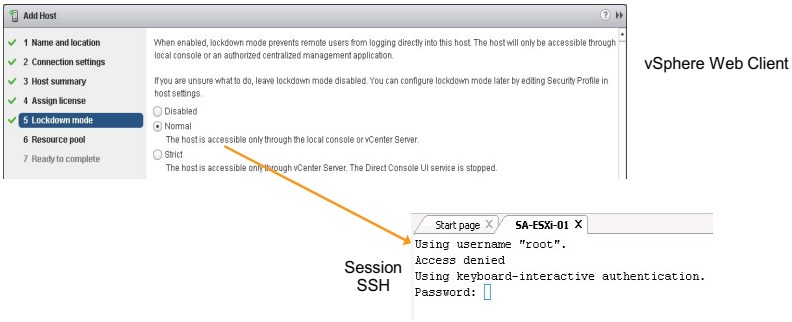


4-58 Configuration du mode verrouillage

Pour améliorer la sécurité de vos hôtes VMware ESXi, vous pouvez les mettre en mode de verrouillage. Deux modes de verrouillage sont disponibles : normal et strict.

Lorsque vous activez le mode de verrouillage normal, seul vpxuser dispose de l'autorisation d'authentification. En outre, les utilisateurs ne peuvent pas effectuer d'opérations directement sur l'hôte.

Seul l'utilisateur root peut se connecter à l'interface DCUI.



Les modes de verrouillage forcent l'exécution de toutes les opérations de gestion des hôtes via vCenter Server. Lorsqu'un hôte est en mode de verrouillage :

- Vous ne pouvez pas le gérer directement via VMware Host Client.
- Vous ne pouvez pas exécuter de commandes sur cet hôte à partir de vSphere CLI.
- Les logiciels ou outils de gestion externes qui accèdent directement à l'hôte ne peuvent pas récupérer ni modifier d'informations provenant de l'hôte VMware ESXi, à moins que les informations d'authentification soient ajoutées à la liste d'exceptions de l'hôte.

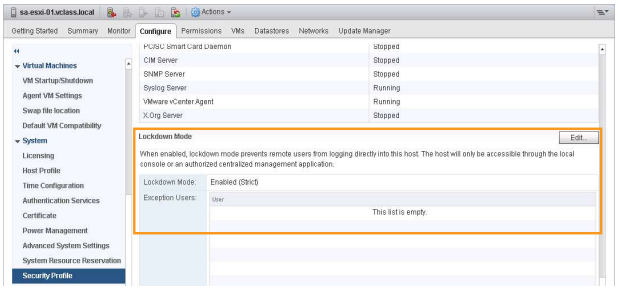
Lorsque le mode de verrouillage normal est activé, seul l'utilisateur root est autorisé à se connecter à l'interface DCUI. Si le mode de verrouillage strict est activé sur un hôte, le service DCUI est automatiquement désactivé. Par conséquent, même l'utilisateur root ne peut pas se connecter à l'hôte.

4-59 Mode de verrouillage strict

En mode de verrouillage strict, le service DCUI est également arrêté.

Si la connexion au système vCenter Server est perdue et que vSphere Client n'est plus disponible, l'hôte VMware ESXi ne peut pas être géré à distance.

Dans ce cas, l'hôte est accessible uniquement si les services VMware vSphere® ESXi™ Shell et SSH sont activés et si les comptes de services autorisés sont ajoutés à la liste d'exceptions.



Dans le mode de verrouillage normal, l'hôte VMware ESXi est accessible via vCenter Server. Seuls les utilisateurs figurant sur la liste d'exceptions et disposant de privilèges d'administrateur peuvent se connecter à l'interface DCUI. Si SSH ou vSphere ESXi Shell sont activés, l'accès est éventuellement possible via ces services.

Dans le mode de verrouillage strict, l'hôte VMware ESXi est uniquement accessible via vCenter Server. Si SSH ou vSphere ESXi Shell sont activés, l'exécution de sessions reste activée pour les comptes spécifiés sous l'option avancée `DCUI.Access` et disposant de privilèges d'administrateur. C'est également le cas pour les sessions des utilisateurs figurant sur la liste d'exceptions et disposant de privilèges d'administrateur. Toutes les autres sessions DCUI sont interrompues.

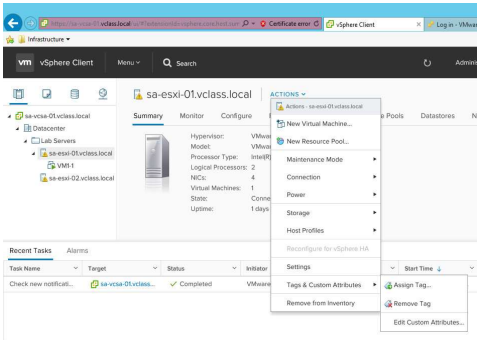
Les utilisateurs figurant sur la liste d'exceptions conservent leurs autorisations lorsque l'hôte VMware ESXi entre en mode de verrouillage. Les comptes sont conçus pour être utilisés par des solutions tierces et des applications externes qui doivent continuer à fonctionner lorsqu'un hôte VMware ESXi est en mode de verrouillage. Seuls les utilisateurs associés à ces applications doivent être ajoutés à la liste d'exceptions.

4-60 Création de balises personnalisées pour les objets de l'inventaire

Grâce aux balises, vous pouvez associer des métadonnées aux objets de l'inventaire vCenter Server afin d'en faciliter le tri.

Vous pouvez associer un ensemble d'objets du même type :

- Recherche d'objets en fonction d'une balise donnée.
- Adapté lorsque les clients souhaitent créer des groupes de machines virtuelles, de clusters et de banques de données afin d'en simplifier la gestion.



Les balises vous permettent d'ajouter des métadonnées aux objets de l'inventaire. Vous avez la possibilité d'enregistrer des informations relatives aux objets de votre inventaire au sein de balises, que vous pourrez ensuite utiliser pour vos recherches.

4-61 Laboratoire 2 : Utilisation de vCenter Server Appliance

Configurer et utiliser vCenter Server Appliance

1. Accéder à votre instance vCenter Server Appliance et configurer les licences
2. Configurer l'authentification unique et créer un objet Data Center
3. Ajouter vos hôtes VMware ESXi à l'inventaire vCenter Server
4. Configurer les hôtes VMware ESXi en tant que clients NTP
5. Créer un dossier d'hôtes et de clusters
6. Créer des dossiers de modèles et de machines virtuelles
7. Naviguer dans vSphere Client

4-62 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Utiliser vSphere Client pour gérer l'inventaire vCenter Server
- Créer et organiser des objets d'inventaire vCenter Server
- Ajouter un Data Center et des objets organisationnels à vCenter Server
- Ajouter des hôtes à vCenter Server
- Parler de la création de balises d'inventaire personnalisées pour les objets d'inventaire

4-63 Leçon 5 : Rôles et autorisations de vCenter Server

4-64 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

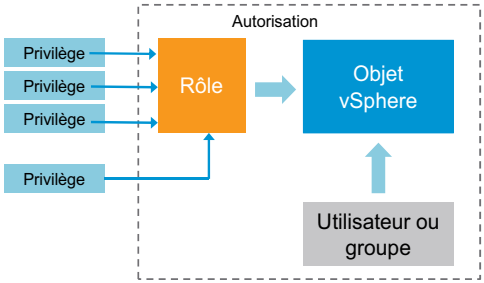
- Définir une autorisation
- Décrire les règles pour l'application des autorisations
- Créer un rôle personnalisé
- Créer une autorisation

4-65 À propos des autorisations vCenter Server

Le système de contrôle d'accès permet à l'administrateur vCenter Server de définir les privilèges des utilisateurs pour accéder aux objets dans l'inventaire.

Voici les concepts clés de ce modèle :

- Autorisations : Le modèle d'autorisations applicable aux systèmes vCenter Server prévoit l'octroi d'autorisations sur les objets de la hiérarchie vSphere. Chaque autorisation confère à un utilisateur ou à un groupe un ensemble de privilèges, ou rôle, vis-à-vis de l'objet sélectionné.
- Privilège : une action pouvant être effectuée.
- Rôle : un ensemble de privilèges.
- Objet : la cible de l'action.
- Utilisateur ou groupe : indique qui peut effectuer l'action.



L'autorisation d'effectuer des tâches dans vCenter Server est régie par un système de contrôle d'accès. Ce système active l'administrateur vCenter Server afin de spécifier plus en détail quels utilisateurs ou groupes peuvent effectuer quelles tâches sur quels objets. Le système de contrôle d'accès est défini selon les concepts suivants :

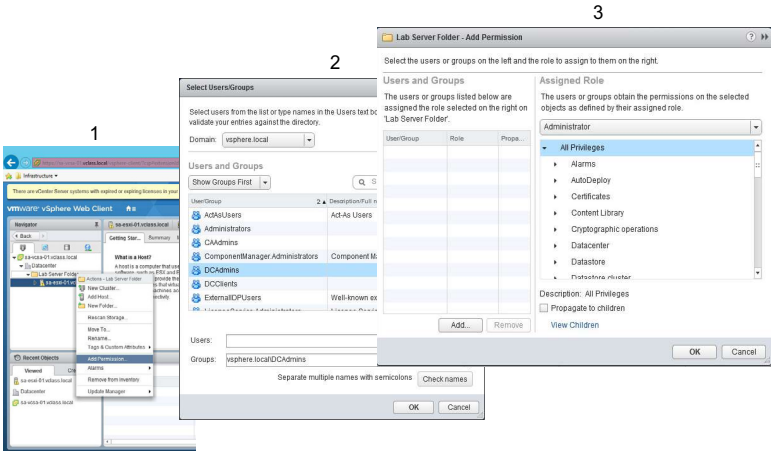
- Le privilège : Une capacité à effectuer une action spécifique ou à lire une propriété spécifique, par exemple, mettre sous tension une machine virtuelle et créer une alarme.
- Le rôle : une collection de privilèges. Les rôles fournissent un moyen de regrouper l'ensemble des privilèges individuels requis pour effectuer une tâche de haut niveau comme administrer une machine virtuelle.
- L'objet : une entité sur laquelle les actions sont effectuées.
- L'utilisateur ou le groupe : un utilisateur ou un groupe qui peut effectuer l'action.

Chaque autorisation est octroyée pour un objet de la hiérarchie vCenter Server. Cette autorisation associe alors l'objet concerné à un utilisateur ou à un groupe d'utilisateurs, ainsi qu'à un rôle d'accès conféré à cet utilisateur ou à ce groupe. Par exemple, vous pouvez sélectionner un objet machine virtuelle, ajouter une autorisation attribuant le rôle ReadOnly au groupe 1, puis ajouter une seconde autorisation attribuant le rôle Administrator à l'utilisateur 2.

En attribuant des rôles distincts pour différents objets à un groupe d'utilisateurs, vous pouvez contrôler les tâches que ces utilisateurs sont autorisés à effectuer au sein de votre environnement vSphere. Par exemple, pour autoriser un groupe à configurer la mémoire de l'hôte, il vous suffit de sélectionner cet hôte et d'ajouter une autorisation qui attribue à ce groupe un rôle incluant le privilège de configuration Host.Configuration.Memory.

4-66 Ajout d'autorisations à l'inventaire vCenter Server

Cliquez avec le bouton droit sur l'objet d'inventaire et sélectionnez **Add Permission**, puis sélectionnez le rôle et cliquez sur **OK**.



Pour gérer les autorisations à partir de vSphere Web Client, il importe de bien maîtriser les concepts suivants :

- L'autorisation : tout objet de la hiérarchie vCenter Server est associé à des autorisations. Chaque autorisation détermine les privilèges que détient un utilisateur ou un groupe d'utilisateurs sur l'objet concerné.
- Les utilisateurs et les groupes : sur les systèmes vCenter Server, vous ne pouvez attribuer des privilèges qu'à des utilisateurs authentifiés ou à des groupes d'utilisateurs authentifiés. L'authentification des utilisateurs est assurée par vCenter Single Sign-On. Les utilisateurs et les groupes doivent donc être définis au sein de la source d'identité sur laquelle vCenter Single Sign-On s'appuie pour gérer l'authentification. Pour définir des utilisateurs et des groupes, recourez aux outils inclus dans votre source d'identité (par exemple, Active Directory).
- Les privilèges : les privilèges sont des contrôles d'accès détaillés. Vous pouvez regrouper ces privilèges en rôles et associer ces rôles à des utilisateurs ou à des groupes.
- Les rôles : un rôle correspond à un ensemble de privilèges. Les rôles vous permettent d'attribuer des autorisations sur un objet en fonction d'un ensemble type de tâches que les utilisateurs sont appelés à effectuer. Plusieurs rôles par défaut, tels que le rôle Administrator, sont prédéfinis dans vCenter Server et ne peuvent pas être modifiés. D'autres rôles, comme Resource Pool Administrator, correspondent à des exemples de rôle prédéfinis. Vous pouvez créer des rôles personnalisés à partir de zéro ou en clonant et en modifiant un exemple de rôle. Pour en savoir plus sur la création d'un rôle personnalisé ou le clonage d'un rôle, consultez le

document *Sécurité vSphere*, disponible à l'adresse
http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

Vous pouvez attribuer des autorisations à des objets de différents niveaux hiérarchiques. Par exemple, vous pouvez attribuer des autorisations à un objet hôte ou un objet dossier contenant tous les objets hôtes. Pour en savoir plus sur l'héritage hiérarchique des autorisations, consultez le document *Sécurité vSphere*, disponible à l'adresse
http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

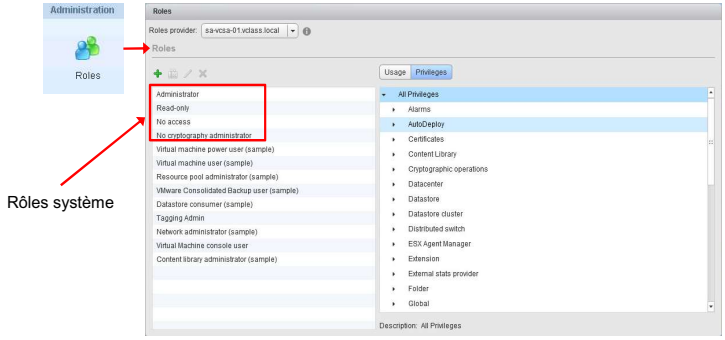
Vous pouvez aussi attribuer des autorisations sur un objet root global, auquel cas ces autorisations s'appliqueront à tous les objets de toutes les solutions. Pour plus d'informations sur les autorisations globales, consultez le document *Sécurité vSphere*, disponible à l'adresse
http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

4-67 À propos des rôles

Les privilèges sont regroupés sous la forme de rôles :

- Les rôles permettent aux utilisateurs d'effectuer des tâches.
- Les rôles sont regroupés en catégories pour simplifier leur configuration.

vCenter Server fournit quelques rôles par défaut, que vous n'avez pas la possibilité de modifier.



Un rôle est un jeu de privilèges. Un privilège permet d'accéder à une tâche spécifique et est regroupé avec d'autres privilèges qui lui sont associés. Ainsi, l'exemple de rôle « Virtual Machine Power User » est composé de plusieurs privilèges dans des catégories telles que « Datastore » et « Global ». Un rôle est affecté à un utilisateur ou à un groupe et détermine le niveau d'accès de cet utilisateur ou de ce groupe.

Il n'est pas possible de modifier les privilèges associés aux rôles par défaut :

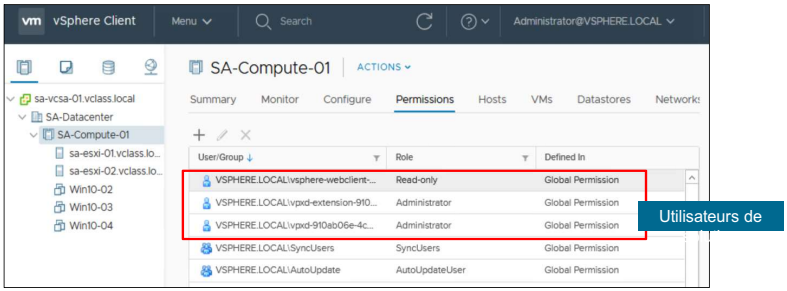
- Le rôle « Administrator » : les utilisateurs dotés du rôle « Administrator » pour un objet sont autorisés à consulter cet objet et à effectuer toutes les actions sur celui-ci.
- Le rôle « No cryptography administrator » : les utilisateurs dotés du rôle « No cryptography administrator » pour un objet ont les mêmes privilèges que les utilisateurs possédant le rôle « Administrator » à l'exception des privilèges relatifs aux opérations de chiffrement.
- Le rôle « No access » : les utilisateurs dotés du rôle « No access » pour un objet ne sont pas autorisés à consulter cet objet ni à le modifier de quelque façon que ce soit.
- Le rôle « Read-only » : les utilisateurs dotés du rôle « Read-only » pour un objet sont autorisés à consulter l'état de cet objet et les détails relatifs à celui-ci.

Tous les rôles sont indépendants les uns des autres. Il n'existe pas de hiérarchie ou de mécanisme d'héritage entre eux.

4-68 À propos des objets

Les objets sont des entités sur lesquelles des actions sont effectuées. Les objets incluent des Data Centers, des dossiers, des pools de ressources, des clusters, des hôtes, des banques de données, des réseaux et des machines virtuelles.

Tous les objets ont un onglet **Permissions**. L'onglet **Permissions** affiche quel utilisateur ou groupe et quel rôle sont associés avec l'objet sélectionné.



Un utilisateur ou un groupe indique qui peut effectuer l'action. L'objet est la cible de l'action. Chaque combinaison d'utilisateurs ou de groupes, de rôles et d'objets doit être spécifiée.

L'utilisation d'un rôle permet d'affecter une ou plusieurs autorisations sur tout objet de l'inventaire vCenter Server.

Sur la diapositive, le rôle « Administrator » a été accordé à l'utilisateur VSPHERE.LOCAL\Administrator. L'association de l'utilisateur (ou du groupe d'utilisateurs) avec le rôle a été appliquée au niveau de vCenter Server. Cette autorisation couvre ainsi l'ensemble des Data Centers répertoriés dans l'inventaire vCenter Server.

Les trois premières entrées figurant sur cette diapositive se rapportent à des utilisateurs de solution. Un utilisateur de solution représente un ou plusieurs services vCenter Server :

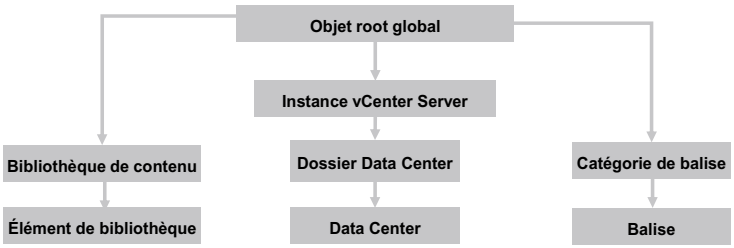
- vpxd : utilisateur de solution pour vCenter Server
- vpxd-extension : utilisateur de solution associé à des services tels que le service d'inventaire ou vSphere Auto Deploy
- vsphere-webclient : utilisateur de solution associé à des services tels que vSphere Web Client

Ces utilisateurs de solution sont dotés du rôle « Administrator » et disposent d'autorisations globales.

4-69 À propos des autorisations globales

Les autorisations globales prennent en charge l'affectation de privilèges sur les solutions à partir d'un objet root global :

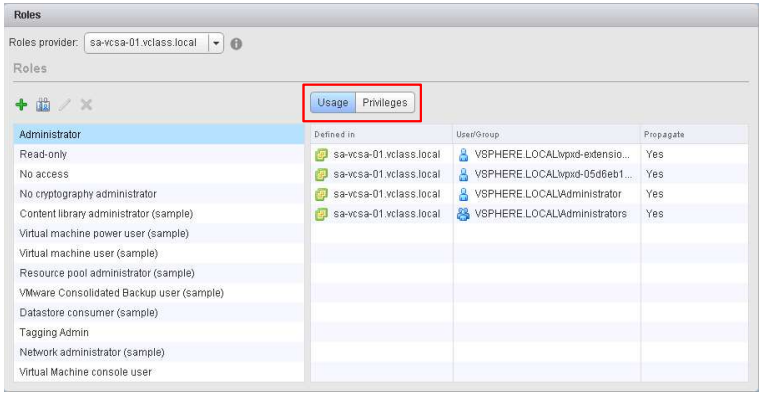
- Les autorisations globales couvrent des solutions telles que vCenter Server et VMware vRealize® Orchestrator™.
- Les autorisations globales accordent à un utilisateur ou à un groupe des privilèges pour tous les objets dans toutes les hiérarchies d'objet.



Le plus souvent, vous appliquez une autorisation à un objet d'inventaire vCenter Server, tel qu'un hôte VMware ESXi ou une machine virtuelle. Lorsque vous appliquez une autorisation, vous spécifiez qu'un utilisateur ou un groupe dispose d'un jeu de privilèges, appelé rôle, sur l'objet. Les autorisations globales accordent à un utilisateur ou à un groupe des privilèges pour afficher ou gérer l'ensemble des objets dans chacune des hiérarchies de l'inventaire dans votre déploiement. L'exemple de la diapositive montre que l'objet root global dispose d'autorisations sur l'ensemble des objets vCenter Server, y compris sur les bibliothèques de contenu, les instances vCenter Server et les balises. Par ailleurs, les autorisations vCenter Server sont valables uniquement sur les objets dans l'instance vCenter Server.

4-70 Affichage des rôles et des affectations

Le volet « Roles » affiche quels utilisateurs sont affectés au rôle sélectionné sur un objet particulier.

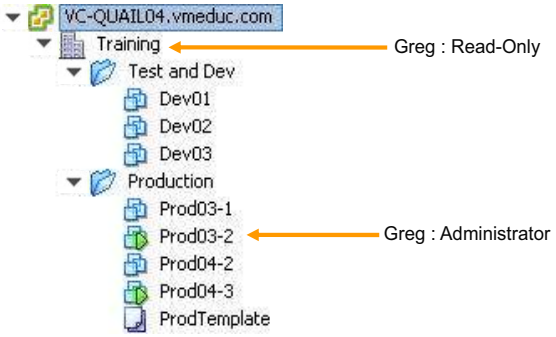


Vous pouvez afficher tous les objets auxquels un rôle a été affecté, ainsi que tous les utilisateurs ou groupes auxquels le rôle a été accordé.

Pour consulter les informations relatives au rôle, cliquez sur **Usage** dans le volet « Roles », puis sélectionnez un rôle dans la liste des rôles. Le volet d'informations montre chaque objet auquel le rôle est affecté et les utilisateurs et groupes auxquels le rôle a été accordé.

4-71 Application des autorisations : Scénario 1

Une autorisation peut se propager vers le bas de la hiérarchie à tous les sous-objets de l'objet spécifié, ou s'appliquer uniquement à ce dernier.

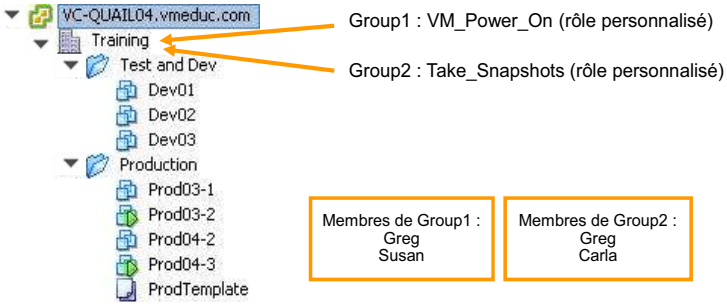


Outre le fait de spécifier si les autorisations se propagent ou non vers le bas, vous pouvez remplacer les autorisations définies à un niveau supérieur en définissant de manière explicite des autorisations différentes pour un objet de niveau inférieur.

Sur la diapositive, l'utilisateur Greg bénéficie d'un accès Read-Only dans le Data Center « Training ». Ce rôle est propagé à tous les objets enfants sauf un, la machine virtuelle Prod03-2. Pour cette machine virtuelle, Greg est un administrateur.

4-72 Application des autorisations : Scénario 2

Lorsqu'un utilisateur est membre de plusieurs groupes avec des autorisations sur le même objet, l'utilisateur reçoit l'union de privilèges affectée aux groupes pour cet objet.



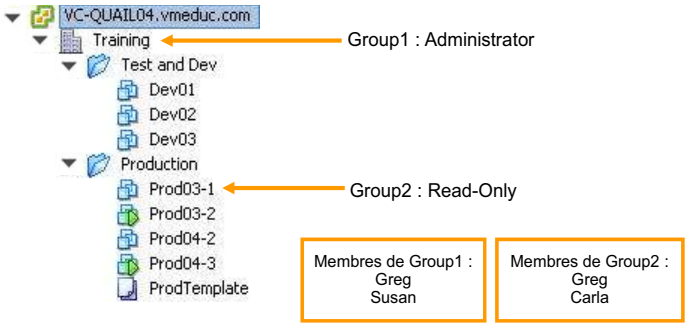
Lorsqu'un utilisateur est membre de plusieurs groupes et que ces groupes ont des autorisations sur le même objet dans l'inventaire, l'utilisateur reçoit l'union de privilèges affectée aux groupes pour cet objet.

Sur la diapositive, Group1 reçoit le rôle VM_Power_On, un rôle personnalisé qui contient uniquement un privilège : la capacité de mettre sous tension une machine virtuelle. Group2 reçoit le rôle Take_Snapshots, un autre rôle personnalisé qui contient les privilèges permettant de créer et de supprimer les snapshots. Les deux rôles se propagent sur les objets enfants.

Parce que Greg appartient à Group1 et à Group2, il bénéficie à la fois des privilèges VM_Power_On et Take_Snapshots pour tous les objets se trouvant dans le Data Center « Training ».

4-73 Application des autorisations : Scénario 3

Lorsqu'un utilisateur est membre de plusieurs groupes avec des autorisations sur différents objets, les mêmes autorisations s'appliquent pour chaque objet sur lequel le groupe dispose d'autorisations, comme si elles étaient directement accordées à l'utilisateur.



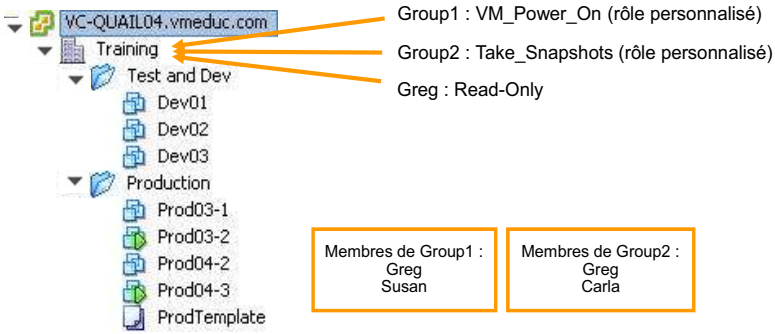
Un utilisateur peut être membre de plusieurs groupes et disposer d'autorisations sur différents objets dans l'inventaire. Pour chaque objet sur lequel le groupe dispose d'autorisations, les mêmes autorisations s'appliquent comme si elles avaient été accordées à l'utilisateur directement. Vous pouvez remplacer les autorisations définies pour un objet de niveau supérieur en définissant de manière explicite des autorisations différentes pour un objet de niveau inférieur.

Sur la diapositive, Group1 reçoit le rôle « Administrator » dans le Data Center « Training », et Group2 le rôle « Read-Only » sur l'objet de machine virtuelle, Prod03-1. L'autorisation accordée à Group1 est propagée aux objets enfants.

Puisque Greg est membre de Group1 et de Group2, il reçoit des privilèges d'administrateur sur l'intégralité du Data Center « Training » (l'objet de niveau supérieur), sauf pour la machine virtuelle Prod03-1 (l'objet de niveau inférieur), pour lequel il bénéficie uniquement d'un accès en lecture seule.

4-74 Application des autorisations : Scénario 4

Les autorisations définies explicitement pour l'utilisateur sur un objet sont prioritaires sur l'ensemble des autorisations de groupe sur ce même objet.



Sur la diapositive, trois autorisations sont affectées au Data Center « Training » :

- Group1 reçoit le rôle VM_Power_On.
- Group2 reçoit le rôle Take_Snapshots.
- Greg reçoit le rôle Read-Only.

Puisque Greg est membre de Group1 et de Group2, supposons également que la propagation aux objets enfants soit activée sur tous les rôles. Bien que Greg soit membre de Group1 et de Group2, il bénéficie du privilège de lecture seule sur le Data Center « Training » et sur tous les objets qui en dépendent. Greg reçoit le privilège de lecture seule, car des autorisations explicites des utilisateurs sur un objet sont prioritaires sur l'ensemble des autorisations de groupe sur ce même objet.

4-75 Création d'un rôle

Créez des rôles activant uniquement les tâches nécessaires :

- Par exemple, « Virtual Machine Creator ».

Utilisez des dossiers pour limiter la portée des autorisations :

- Par exemple, affectez le rôle « Virtual Machine Creator » à l'utilisateur Nancy et appliquez-le au dossier « Finance ».

Rôle « Virtual Machine Creator » :

Datastore > Allouer de l'espace

Réseau > Affecter un réseau

Ressource > Affecter une machine virtuelle au pool de ressources

Machine virtuelle > Inventaire > Créer

Machine virtuelle > Configuration > Ajouter un nouveau disque

Machine virtuelle > Configuration > Ajouter ou supprimer un périphérique

Le rôle « Virtual Machine Creator » n'est qu'un exemple parmi de nombreux autres des rôles qui peuvent être créés. Il est fortement recommandé de définir un rôle en utilisant le moins de privilèges possible, de manière à optimiser la sécurité et le contrôle sur votre environnement. En outre, nommez les rôles d'une manière indiquant explicitement ce qu'ils autorisent, en faisant ressortir clairement leur objectif.

Utilisez des dossiers pour limiter la portée des autorisations. Par exemple, pour limiter la création de machines virtuelles, créez un dossier dans la vue d'inventaire « VMs and Templates ». Appliquez le rôle « Virtual Machine Creator » à ce dossier pour les utilisateurs.

4-76 Laboratoire 3 : Utilisateurs, groupes et autorisations

Attribuer des rôles et des autorisations à des utilisateurs Active Directory pour leur permettre d'effectuer des opérations dans vCenter Server Appliance

1. Joindre vCenter Server Appliance au domaine vclass.local
2. Ajouter vclass.local en tant que source d'identité
3. Afficher les utilisateurs Active Directory
4. Attribuer des autorisations sur les objets à un utilisateur Active Directory
5. Attribuer des autorisations globales au niveau root
6. Se connecter avec l'authentification de session Windows
7. Gérer une machine virtuelle en tant qu'utilisateur Active Directory

4-77 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Définir une autorisation
- Décrire des règles pour l'application des autorisations
- Créer un rôle personnalisé
- Créer une autorisation

4-78 Leçon 6 : Sauvegarde et restauration de vCenter Server Appliance

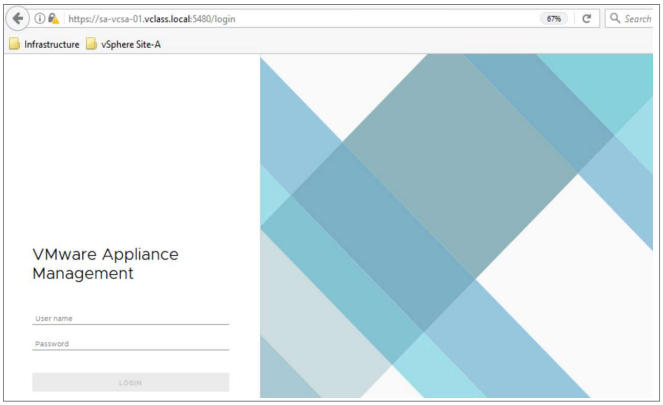
4-79 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Créer un planning de sauvegarde vCenter Server Appliance
- Restaurer vCenter Server Appliance à partir d'une sauvegarde

4-80 Connexion à l'interface de gestion de vCenter Server Appliance

Pour sauvegarder ou restaurer vCenter Server Appliance, connectez-vous à l'interface de gestion de vCenter Server Appliance à l'adresse suivante : https:*//FQDN_ou_adresse_IP*:5480.

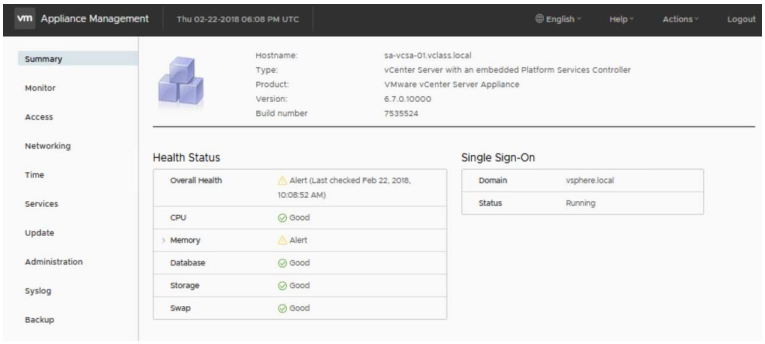


L'interface de gestion de vCenter Server Appliance est un client HTML spécifiquement conçu pour configurer l'appliance.

L'interface de gestion de vCenter Server Appliance se connecte directement au port 5480 de l'appliance et est utilisée lors de sa configuration initiale. L'interface de gestion de vCenter Server Appliance donne accès à toutes les API de service de l'appliance.

4-81 Fonctions de l’interface de gestion de vCenter Server Appliance Management

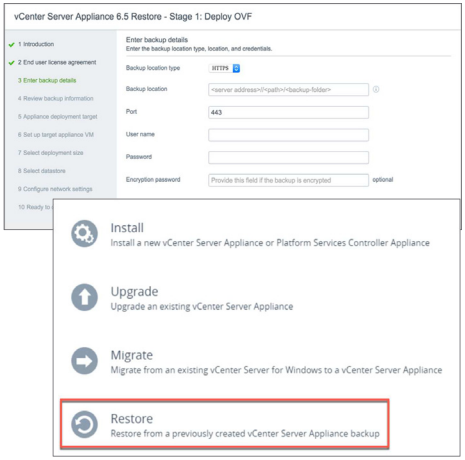
Une fois connecté à l’interface de gestion de vCenter Server Appliance, vous pouvez voir les différentes fonctions disponibles.



4-82 À propos des fonctions natives de sauvegarde et de restauration de vCenter Server

Les fonctions natives de sauvegarde et de restauration de vCenter Server offrent plusieurs fonctionnalités :

- L'indépendance vis-à-vis de toute solution de sauvegarde tierce
- La restauration d'une instance vCenter Server dans une toute nouvelle appliance
- La prise en charge de la sauvegarde et de la restauration de vCenter Server Appliance et de Platform Services Controller
- La prise en charge des protocoles HTTP/S, SCP et FTP/S
- L'option de chiffrement disponible
- La restauration effectuée directement depuis l'image ISO de vCenter Server Appliance



L'interface de gestion de vCenter Server Appliance permet de sauvegarder les composants essentiels de l'appliance. Vous avez ainsi la possibilité de protéger les données vCenter Server et de réduire le temps nécessaire à la restauration des opérations de Data Center.

Le processus de sauvegarde recueille les fichiers importants dans un fichier d'archive TAR et compresse celui-ci de façon à réduire la charge réseau. Afin de minimiser l'impact sur les capacités de stockage, les données sont transmises sans mise en cache sur l'appliance. Pour réduire le temps nécessaire à l'opération, le processus de sauvegarde traite les différents composants en parallèle.

Vous pouvez demander le chiffrement du fichier compressé avant sa transmission à l'emplacement de stockage de la sauvegarde. Si vous sélectionnez cette option de chiffrement, vous devez indiquer le mot de passe qui permettra de déchiffrer le fichier lors de la restauration.

L'opération de sauvegarde inclut obligatoirement la base de données et les fichiers de configuration de vCenter Server, de sorte que le processus de restauration dispose de toutes les données requises pour recréer une appliance opérationnelle. Vous avez également la possibilité d'étendre la sauvegarde aux statistiques, aux événements et aux tâches correspondant à l'état actuel du Data Center. Les alarmes en cours sont systématiquement incluses dans les sauvegardes.

4-83 Méthodes de sauvegarde et de restauration de vCenter Server Appliance

Vous pouvez utiliser les méthodes suivantes pour sauvegarder et restaurer vCenter Server Appliance :

- Sauvegarde et restauration en mode fichier :
  - Utilisez l'interface de gestion de vCenter Server Appliance pour créer une sauvegarde en mode fichier de l'instance vCenter Server Appliance et de l'appliance Platform Services Controller.
  - Après avoir créé la sauvegarde, vous pouvez la restaurer en utilisant le programme d'installation de l'interface utilisateur de l'appliance.
  - La sauvegarde et la restauration en mode fichier peuvent être planifiées.
- Sauvegarde et restauration en mode image :
  - Utilisez un produit tiers pour sauvegarder et restaurer une machine virtuelle contenant vCenter Server, vCenter Server Appliance ou Platform Services Controller.
  - API de stockage VMware vSphere® - Data Protection est une infrastructure de protection des données permettant aux produits de sauvegarde d'effectuer des sauvegardes efficaces, centralisées, hors hôte et hors LAN de machines virtuelles vSphere.

4-84 Sauvegarde de vCenter Server Appliance en mode fichier

Vous pouvez configurer un planning de sauvegarde en mode fichier pour effectuer des sauvegardes périodiques :

- Un planning peut être configuré en renseignant l'emplacement, la fréquence et la conservation des sauvegardes.
- Vous ne pouvez configurer qu'un planning à la fois.

L'interface de gestion de vCenter Server Appliance vous permet d'effectuer une sauvegarde en mode fichier des données de configuration de base de vCenter Server, des données d'inventaire et des données historiques de votre choix. Les données sauvegardées sont transmises à un système distant via FTP, FTPS, HTTP, HTTPS ou SCP. La sauvegarde n'est pas stockée sur vCenter Server Appliance.

4-85 Restauration de vCenter Server Appliance en mode fichier

Vous pouvez utiliser le programme d'installation de vCenter Server Appliance pour restaurer une instance vCenter Server Appliance sur un hôte VMware ESXi ou une instance vCenter Server.

La procédure de la restauration se déroule par phases :

1. Le fichier OVA inclus dans le programme d'installation de vCenter Server Appliance est déployé.
2. L'instance vCenter Server Appliance fraîchement déployée est remplie avec les données stockées dans la sauvegarde en mode fichier.

Lorsque vous utilisez la restauration en mode fichier, le rapprochement est automatiquement effectué.

Vous pouvez uniquement effectuer une restauration en mode fichier d'une instance vCenter Server Appliance que vous avez préalablement sauvegardée avec l'interface de gestion de vCenter Server Appliance. Vous pouvez effectuer ce type de restauration en utilisant le programme d'installation de l'interface utilisateur de vCenter Server Appliance. Cette opération consiste à déployer une nouvelle instance vCenter Server Appliance et à copier les données de la sauvegarde en mode fichier vers la nouvelle appliance.

Vous pouvez également effectuer une restauration en déployant une nouvelle instance vCenter Server Appliance et en utilisant l'interface de gestion vCenter Server Appliance pour copier les données de la sauvegarde en mode fichier vers la nouvelle appliance.

4-86 Planification des sauvegardes

vCenter Server Appliance offre la possibilité de planifier des sauvegardes automatiques en mode fichier.

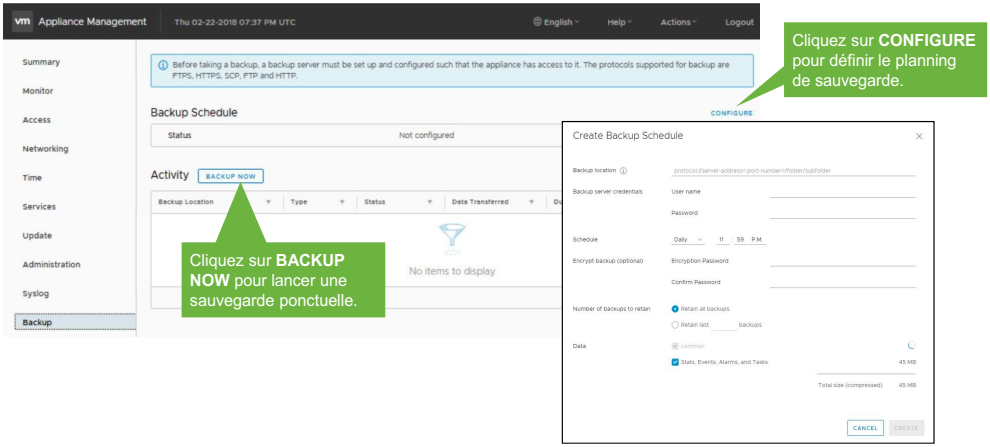
Le planificateur de sauvegarde prend en charge :

- FTPS, HTTPS, SCP, FTP et HTTP
- Le chiffrement des sauvegardes planifiées
- La règle de conservation pour garder toutes les sauvegardes ou le nombre défini de sauvegardes
- Les plannings quotidiens, hebdomadaires et personnalisés

Les sauvegardes qui échouent déclenchent une alarme dans vSphere Client.

4-87 Création d'un planning de sauvegarde

Pour créer un planning de sauvegarde, rendez-vous dans l'interface de gestion de vCenter Server Appliance et sélectionnez **Backup**.



La création d'un planning de sauvegarde nécessite les informations suivantes :

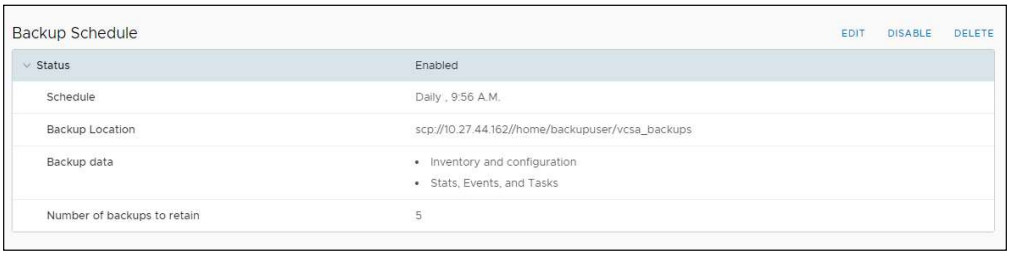
- Backup location : le protocole, l'emplacement et le répertoire du serveur de sauvegarde
- Backup server credentials : le nom d'utilisateur et le mot de passe du serveur de sauvegarde
- Schedule : la fréquence des sauvegardes
- Encrypt backup : le mot de passe de chiffrement (facultatif)
- Number of backups to retain : retenir toutes les sauvegardes ou retenir un nombre défini de sauvegardes
- Data : vous pouvez choisir de sauvegarder les données SEAT

Si un planning est déjà défini, cliquez sur **BACKUP NOW** pour réutiliser les paramètres précédemment définis ou remplacer les paramètres pour une sauvegarde ponctuelle.

4-88 Affichage du planning de sauvegarde

Vous pouvez consulter le planning de sauvegarde actuellement défini à partir de l'interface de gestion de vCenter Server Appliance.

Le planning de sauvegarde peut être modifié, désactivé ou supprimé.



4-89 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Créer un planning de sauvegarde vCenter Server Appliance
- Restaurer vCenter Server Appliance à partir d'une sauvegarde

4-90 Leçon 7 : Surveillance de vCenter Server Appliance

4-91 Objectifs de la formation

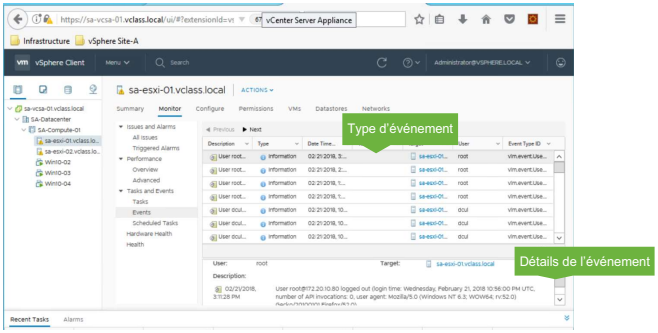
À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Savoir comment afficher les journaux et les événements de vCenter Server
- Gérer les services de vCenter Server
- Surveiller vCenter Server Appliance
- Surveiller l'utilisation des services et de l'espace disque de vCenter Server Appliance
- Utiliser les alarmes vSphere pour détecter les ressources épuisées et les défaillances de services

4-92 Événements de vCenter Server

Les fonctions de conservation des événements et de pistes d'audit de vCenter Server permettent de configurer une période de conservation par incréments de 30 jours :

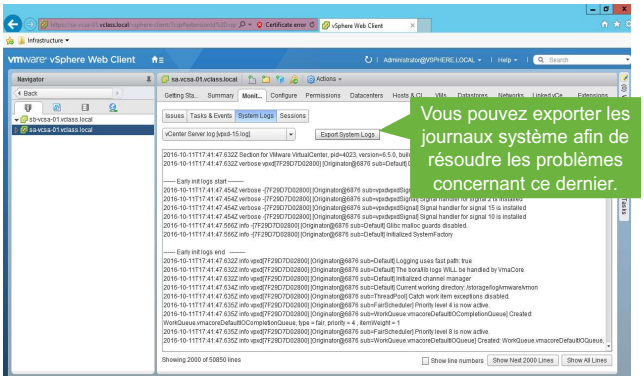
- Les informations relatives à une action utilisateur incluent le compte utilisateur et les détails spécifiques de l'événement.
- Toutes les actions sont consignées avec l'ID et le chemin de fichier, ainsi que la source, le nom, et la date et l'heure de l'opération.



4-93 Journaux du système vCenter Server

vSphere enregistre les événements dans la base de données vCenter Server.

Les informations consignées dans une entrée de journal système incluent notamment l'auteur, la date et l'heure de création, ainsi que le type d'énènement.



4-94 À propos des niveaux de journalisation

Vous pouvez définir des niveaux de journalisation pour contrôler la quantité et le type des informations consignées.

Voici quelques situations justifiant ce type de définition :

- Lorsque vous cherchez à corriger des problèmes complexes, définissez le niveau de journalisation sur la valeur « Verbose » ou « Trivia ». Effectuez le dépannage, puis redéfinissez ce niveau sur « Info ».
- Lorsque vous voulez contrôler la quantité d'informations stockées dans les fichiers journaux.

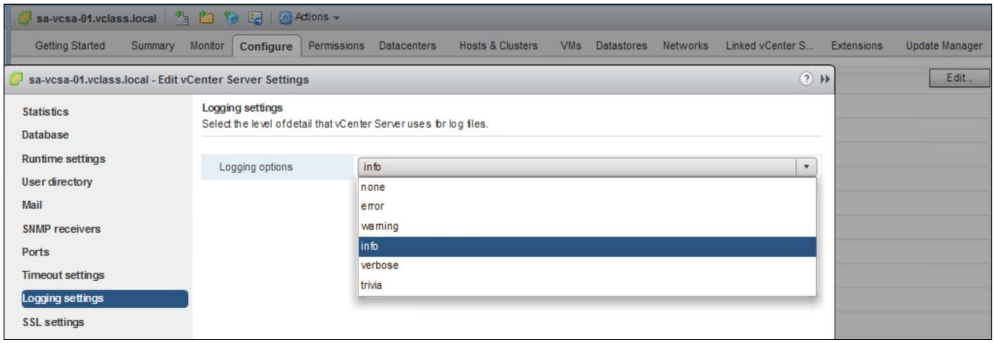
Option	Description
None	Désactive la journalisation.
Error (errors only)	Affiche uniquement les entrées du journal correspondant à des erreurs.
Warning (errors and warnings)	Affiche uniquement les entrées du journal correspondant à des erreurs et à des avertissements.
Info (normal logging)	Affiche uniquement les entrées du journal correspondant à des avertissements, des erreurs et des informations.
Verbose	Affiche uniquement les entrées du journal correspondant à des commentaires, des avertissements, des erreurs et des informations.
Trivia (extended verbose)	Affiche uniquement les entrées du journal correspondant à des trivia, des commentaires, des avertissements, des erreurs et des informations.

Les modifications apportées aux paramètres de journalisation sont appliquées immédiatement ; vous n'êtes pas obligé de redémarrer le système vCenter Server.

4-95 Définition des niveaux de journalisation

Vous pouvez configurer le niveau de détail des fichiers journaux générés par vCenter Server.

- Vous pouvez modifier les niveaux de journalisation dans vSphere Web Client.
- Une journalisation plus exhaustive nécessite beaucoup plus d'espace sur votre système vCenter Server ou dans vSphere Syslog Collector.



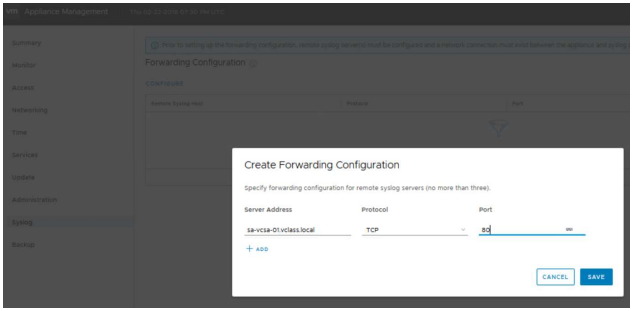
Pour configurer les niveaux de journalisation

1. Dans vSphere Client, naviguez jusqu'à l'instance vCenter Server.
2. Cliquez sur l'onglet **Configure**.
3. Sous Settings, sélectionnez **General**.
4. Cliquez sur **Edit**.
5. Dans le volet de gauche, sélectionnez **Logging settings**.
6. Sélectionnez les options de journalisation.

4-96 Transmission de fichiers journaux vCenter Server Appliance vers une autre machine hôte

vCenter Server est capable de diffuser les informations de ses journaux vers un serveur syslog distant :

- Cette fonction peut être activée dans l'interface de gestion de vCenter Server Appliance à l'adresse suivante : https://*FQDN_de_vCenter_Server_Appliance*:5480.
- Cette fonctionnalité permet d'éviter une saturation du système de fichiers de vCenter Server Appliance due aux fichiers journaux. Elle permet aussi une analyse approfondie des fichiers journaux de vCenter Server Appliance avec des produits d'analyse comme VMware vRealize® Log Insight™.



4-97 Intégrité de la base de données vCenter Server

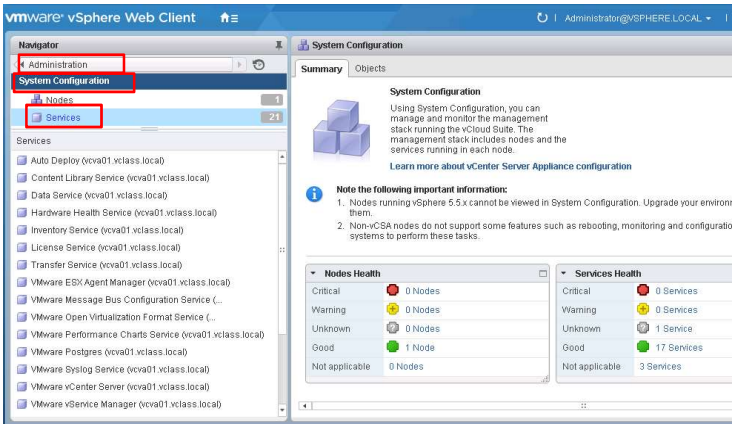
vCenter Server vérifie l'intégrité de la base de données toutes les 15 minutes :

- Par défaut, les avertissements relatifs à l'intégrité de la base de données déclenchent une alarme lorsque le l'espace utilisé par la base de données atteint 80 %.
- L'avertissement se transforme en erreur lorsque l'espace utilisé par la base de données atteint le seuil de 95 %. Les services vCenter Server se ferment alors pour permettre à l'utilisateur de configurer plus d'espace disque ou de supprimer le contenu inutile.

Ces fonctionnalités sont disponibles pour les bases de données PostgreSQL et Microsoft SQL Server. Elles ne sont pas disponibles pour les bases de données Oracle.

4-98 Gestion des services de vCenter Server

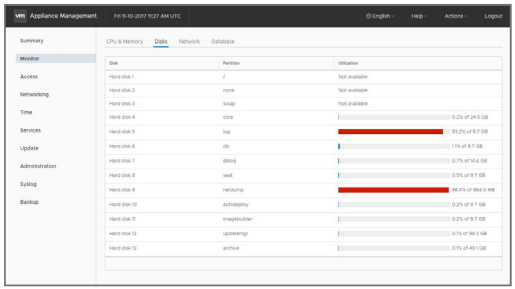
Vous pouvez gérer les services de vCenter Server en sélectionnant **Administration > System Configuration** dans la page d'accueil, puis en cliquant sur **Services**.



4-99 Surveillance de vCenter Server Appliance

L’interface de gestion de vCenter Server Appliance comprend une interface de surveillance.

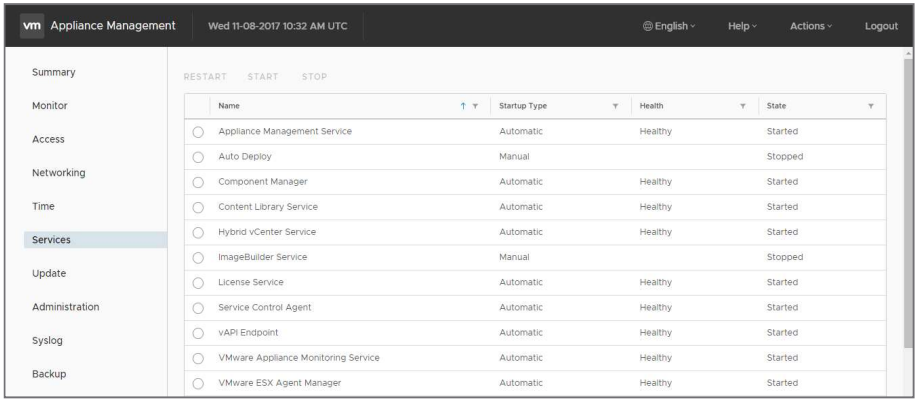
« CPU & Memory » fournit une vue historique de l’utilisation CPU et de la mémoire.



Il est possible de surveiller les disques de vCenter Server Appliance pour contrôler l’espace disponible.

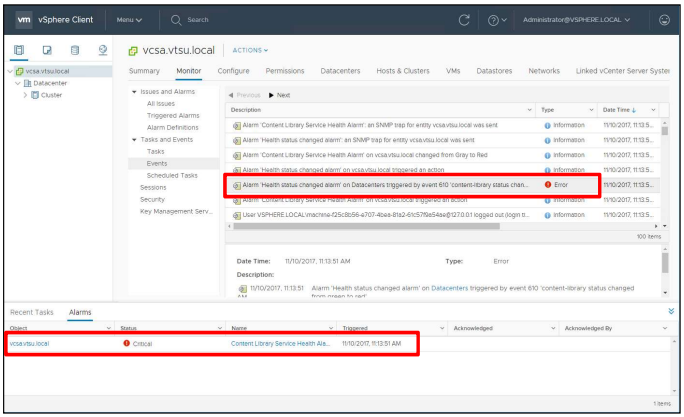
4-100 Surveillance des services vCenter Server Appliance

Vous pouvez utiliser l'interface de gestion de vCenter Server Appliance pour surveiller l'intégrité et l'état des services vCenter Server Appliance. Vous pouvez redémarrer, démarrer ou arrêter des services à partir de l'interface de gestion de vCenter Server Appliance.



4-101 Alarmes vSphere pour la détection d'épuisement des ressources et de défaillances de services

vSphere Client affiche les événements et les alarmes pour alerter l'utilisateur des changements relatifs à l'intégrité des services et d'éventuelles défaillances.



4-102 Mises à jour correctives mensuelles pour vCenter Server Appliance

VMware publie chaque mois des correctifs de sécurité pour vCenter Server Appliance :

- Des correctifs de vulnérabilités critiques sont publiés chaque mois.
- Les vulnérabilités importantes et mineures sont corrigées avec la mise à jour ou le correctif vCenter Server suivant.
- Si une mise à jour ou un correctif vCenter Server est publié dans la même période que le correctif de sécurité mensuel, ce dernier est intégré à la mise à jour ou au correctif vCenter Server.

4-103 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Savoir comment afficher les journaux et les événements de vCenter Server
- Gérer les services de vCenter Server
- Surveiller vCenter Server Appliance
- Surveiller l'utilisation des services et de l'espace disque de vCenter Server Appliance
- Utiliser les alarmes vSphere pour détecter les ressources épuisées et les défaillances de services

4-104 Points clés

- L’architecture de vCenter Server comprend les composants suivants :
  - vCenter Server
  - La base de données vCenter Server
  - Les hôtes VMware ESXi gérés
- vCenter Server propose les types de modèle de déploiement suivants :
  - Platform Services Controller intégré
  - Système Platform Services Controller externe
- Les clients vSphere vous permettent de vous connecter aux systèmes vCenter Server et de gérer les objets de l’inventaire vCenter Server.
- Vous avez la possibilité de gérer l’inventaire vCenter Server.
- Vous pouvez sauvegarder et restaurer nativement le système vCenter Server Appliance.

Des questions ?

MODULE 5

Configuration et gestion des réseaux virtuels

5-2 Vous êtes ici

1. Présentation du cours
2. Présentation de vSphere et du Software-Defined Data Center
3. Création de machines virtuelles
4. vCenter Server
5. **Configuration et gestion des réseaux virtuels**
6. Configuration et gestion du stockage virtuel
7. Gestion des machines virtuelles
8. Gestion et surveillance des ressources
9. vSphere HA, vSphere Fault Tolerance et protection des données
10. vSphere DRS
11. vSphere Update Manager
12. Résolution des problèmes vSphere

5-3 Importance

Les machines virtuelles doivent pouvoir communiquer entre elles ainsi qu'avec d'autres machines virtuelles physiques. Il importe d'assurer le bon fonctionnement de la gestion à distance des hôtes et du stockage basé sur IP.

Une configuration incorrecte de la mise en réseau VMware ESXi peut avoir un impact négatif sur les opérations de votre infrastructure virtuelle.

5-4 Leçons du module

Leçon 1 :	Présentation des commutateurs vSphere Standard
Leçon 2 :	Configuration des règles de commutateur standard

5-5 Leçon 1 : Présentation des commutateurs vSphere Standard

5-6 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

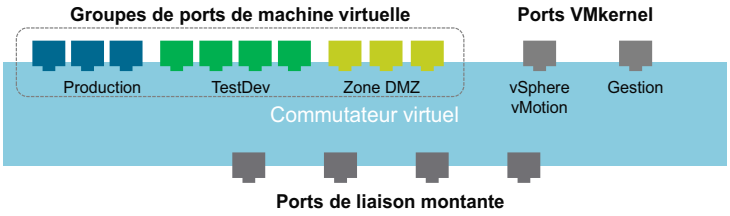
- Décrire les types de connexion d'un commutateur virtuel
- Configurer et consulter les paramètres de configuration d'un commutateur standard, comme les groupes de ports de machine virtuelle, les ports VMkernel, les paramètres VLAN et les fonctionnalités de sécurité
- Comparer les fonctionnalités des commutateurs standard et des commutateurs distribués

5-7 Types de connexion de commutateurs virtuels

Les commutateurs virtuels assurent la connectivité entre les machines virtuelles déployées sur un même hôte ou sur des hôtes distincts. Ils garantissent également l'accès au réseau VMkernel pour la gestion à distance des hôtes, la migration vSphere vMotion, iSCSI et NFS.

Un commutateur virtuel présente des types de connexion spécifiques :

- Les groupes de ports de machine virtuelle
- Le Port VMkernel : pour le stockage IP, la migration vSphere vMotion, VMware vSphere® Fault Tolerance, vSAN, VMware vSphere® Replication™ et le réseau de gestion VMware ESXi.
- Les ports de liaison montante



Un commutateur virtuel propose les types de connexion suivants aux hôtes et aux machines virtuelles :

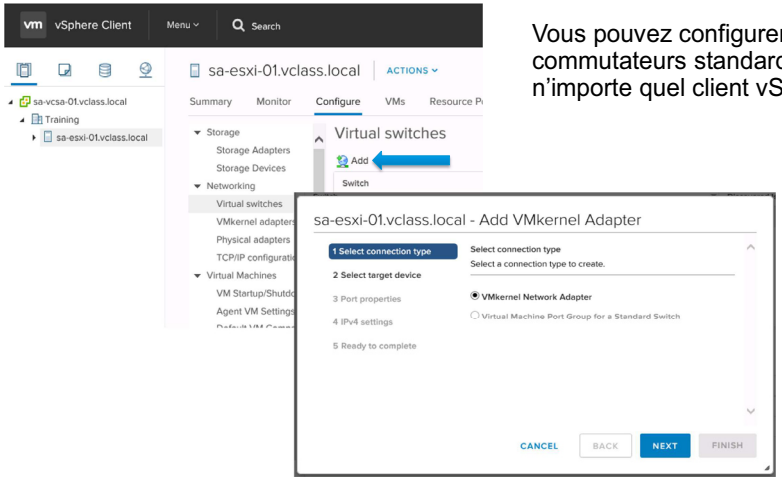
- La connexion de machines virtuelles au réseau physique
- La connexion de services VMkernel au réseau physique Les services VMkernel incluent l'accès au stockage IP (par exemple, NFS ou iSCSI), la migration via vSphere vMotion et l'accès au réseau de gestion.

Le port du réseau de gestion VMware ESXi est utilisé pour la connexion aux services distants et réseau, notamment vpxd sur vCenter Server et VMware Host Client. Chaque port du réseau de gestion VMware ESXi ou chaque port VMkernel peut être configuré avec sa propre adresse IP, son propre masque de réseau et sa propre passerelle.

Pour faciliter la configuration des commutateurs virtuels, vous pouvez créer des groupes de ports. Un groupe de ports est un modèle qui stocke les informations de configuration afin de permettre la création de ports de commutateur virtuel sur un commutateur virtuel. Les groupes de ports de machine virtuelle servent à assurer la connexion des machines virtuelles entre elles avec des propriétés de mise en réseau communes.

Les groupes de ports de machine virtuelle et les ports VMkernel permettent la connexion au monde extérieur via des adaptateurs Ethernet physiques connectés aux ports de liaison montante des commutateurs virtuels.

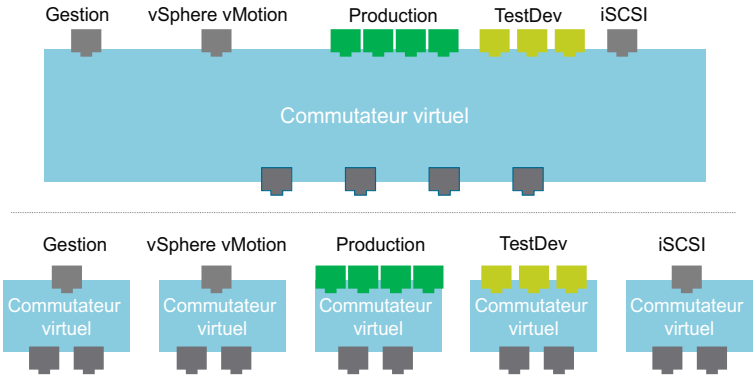
5-8 Ajout de la mise en réseau VMware ESXi



Vous pouvez configurer des commutateurs standard avec n'importe quel client vSphere.

5-9 Exemples de connexions de commutateurs virtuels

Plusieurs réseaux peuvent coexister sur le même commutateur virtuel. Les réseaux peuvent également être configurés sur des commutateurs virtuels distincts.

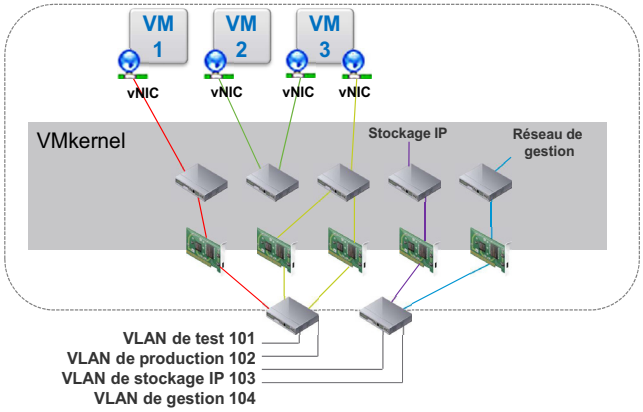


Lorsque vous concevez votre environnement de mise en réseau, vSphere vous permet de placer l'ensemble de vos réseaux sur un commutateur virtuel unique. Vous pouvez également choisir de configurer plusieurs commutateurs virtuels dotés chacun d'un réseau distinct. Cette décision dépend en partie de la disposition de vos réseaux physiques. Par exemple, il se peut que vous ne disposiez pas d'un nombre suffisant d'adaptateurs réseau pour créer un commutateur virtuel distinct pour chaque réseau. Dans ce cas, vous pouvez plutôt associer les adaptateurs réseau au sein d'un commutateur virtuel unique et isoler ces réseaux via des VLAN.

Les cartes d'interface réseau physiques étant affectées au niveau du commutateur virtuel, l'ensemble des ports et des groupes de ports définis pour un commutateur donné partagent le même matériel.

5-10 À propos des commutateurs standard

Un commutateur standard fournit des connexions aux machines virtuelles pour leur permettre de communiquer entre elles, qu'elles soient installées sur un même hôte ou sur des hôtes distincts.

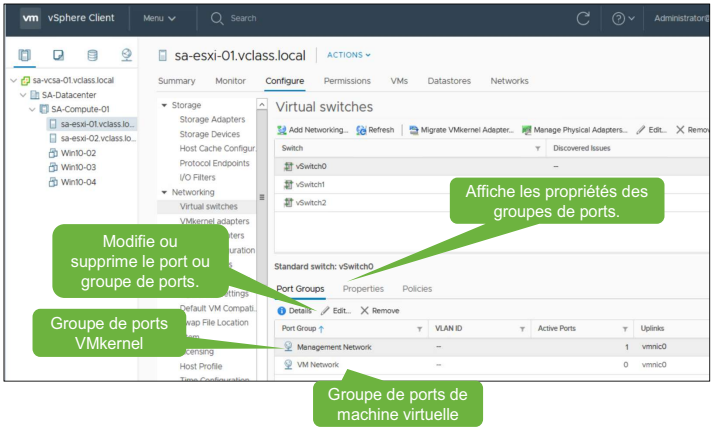


Cette diapositive représente cinq commutateurs standard destinés chacun à un usage distinct. De gauche à droite, ces commutateurs sont placés par ordre numérique :

1. Un commutateur standard associé à un seul adaptateur sortant. Ce commutateur est utilisé uniquement par VM1.
2. Un commutateur standard interne uniquement, qui permet à toutes les machines virtuelles d'un même hôte VMware ESXi de communiquer directement avec d'autres machines virtuelles connectées au même commutateur standard. VM2 et VM3 peuvent utiliser ce commutateur pour communiquer entre elles.
3. Un commutateur standard associé à plusieurs cartes d'interface réseau. Une association de cartes d'interface réseau assure la distribution automatique des paquets, ainsi que le basculement.
4. Un commutateur standard utilisé par VMkernel pour accéder au stockage iSCSI ou NAS.
5. Un commutateur standard utilisé par VMkernel pour activer les fonctions de gestion à distance.

5-11 Affichage de la configuration des commutateurs standard

Vous pouvez afficher la configuration du commutateur standard d'un hôte en sélectionnant « Virtual switches » dans l'onglet « Configure ».



La diapositive montre un commutateur standard nommé vSwitch0 et configuré sur un hôte VMware ESXi. Par défaut, l'installation de VMware ESXi crée un groupe de ports de machine virtuelle nommé « VM Network » et un port VMkernel nommé « Management Network ». Il est recommandé de supprimer le groupe de ports « VM Network » et de séparer les réseaux de machines virtuelles et les réseaux de gestion, à des fins de sécurité et d'optimisation des performances.

Pour supprimer un commutateur standard, sélectionnez-le dans la liste des commutateurs, puis cliquez sur la croix rouge en regard. Pour afficher les propriétés d'un commutateur virtuel, cliquez sur l'icône en forme de crayon au-dessus.

Vous pouvez afficher les propriétés de groupe de port associées à un port ou à un groupe de ports. Le cas échéant, les informations du protocole CDP (Cisco Discovery Protocol) peuvent être affichées pour un adaptateur physique.

Ce protocole permet aux administrateurs VMware ESXi de déterminer quel port de commutateur Cisco est connecté à un commutateur virtuel donné. Si CDP est activé pour un commutateur virtuel spécifique, vous pouvez afficher les propriétés du commutateur Cisco à partir de VMware vSphere® Web Client. Les propriétés incluent le type de périphérique, l'ID de port, les fonctionnalités matérielles, etc.

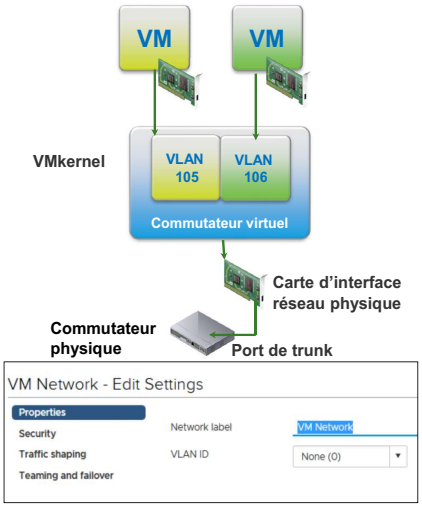
5-12 À propos des VLAN

VMware ESXi prend en charge le marquage VLAN 802.1Q.

Le marquage VLAN de commutateur virtuel correspond à l'une des règles de marquage prises en charge :

- Les trames d'une machine virtuelle sont marquées lorsque le commutateur virtuel les envoie au réseau physique.
- Les trames marquées reçues par un commutateur virtuel perdent leur marquage avant d'être envoyées à la machine virtuelle de destination.
- L'impact sur les performances est minime.

VMware ESXi assure la prise en charge des VLAN en attribuant un ID VLAN à un groupe de ports.



Un réseau local virtuel (VLAN) assure le regroupement logique des ports de commutateur, ce qui permet aux communications de se dérouler comme si tous les ports ou machines virtuelles du VLAN se trouvaient sur le même segment LAN physique. Un VLAN est un domaine de diffusion configuré par logiciel. L'utilisation d'un VLAN présente les avantages suivants :

- La création de réseaux logiques indépendamment de la topologie physique
- L'amélioration des performances grâce à la restriction du trafic de diffusion à un sous-ensemble des ports d'un commutateur
- La réduction des coûts via le partitionnement du réseau, sans surcharge liée au déploiement de nouveaux routeurs

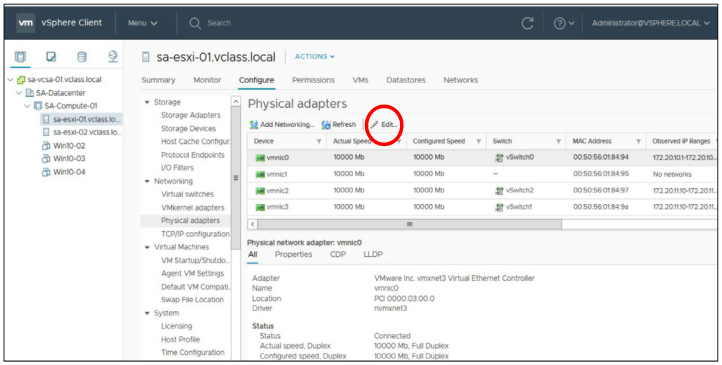
Les VLAN peuvent être configurés au niveau du groupe de ports. L'hôte VMware ESXi assure la prise en charge des VLAN par l'intermédiaire du marquage de VLAN des commutateurs virtuels, qui est effectué grâce à l'association d'un ID VLAN à un groupe de ports. Par défaut, l'ID VLAN est facultatif. VMkernel gère le marquage et la suppression du marquage lorsque les paquets traversent le commutateur virtuel.

Le port d'un commutateur physique auquel un hôte VMware ESXi est connecté doit être défini comme un port de trunk statique. Un port de trunk est un port de switch Ethernet physique configuré pour envoyer et recevoir des paquets balisés avec un ID VLAN. Aucune configuration du VLAN n'est requise sur la machine virtuelle. De fait, celle-ci ignore qu'elle est connectée à un VLAN.

Pour en savoir plus sur la mise en œuvre des VLAN, consultez l'article 1003806 de la base de connaissances VMware, disponible à l'adresse suivante : http://kb.vmware.com/kb/1003806.

5-13 Propriétés des adaptateurs réseau

L'adaptateur physique peut constituer un goulot d'étranglement pour le trafic réseau si son débit ne répond pas aux exigences des applications.



Vous pouvez modifier la vitesse de connexion et le duplex d'un adaptateur physique afin de transférer les données en fonction du débit du trafic.

Si l'adaptateur physique prend en charge la fonction SR-IOV, vous pouvez l'activer et configurer le nombre de fonctions virtuelles à utiliser pour la mise en réseau des machines virtuelles.

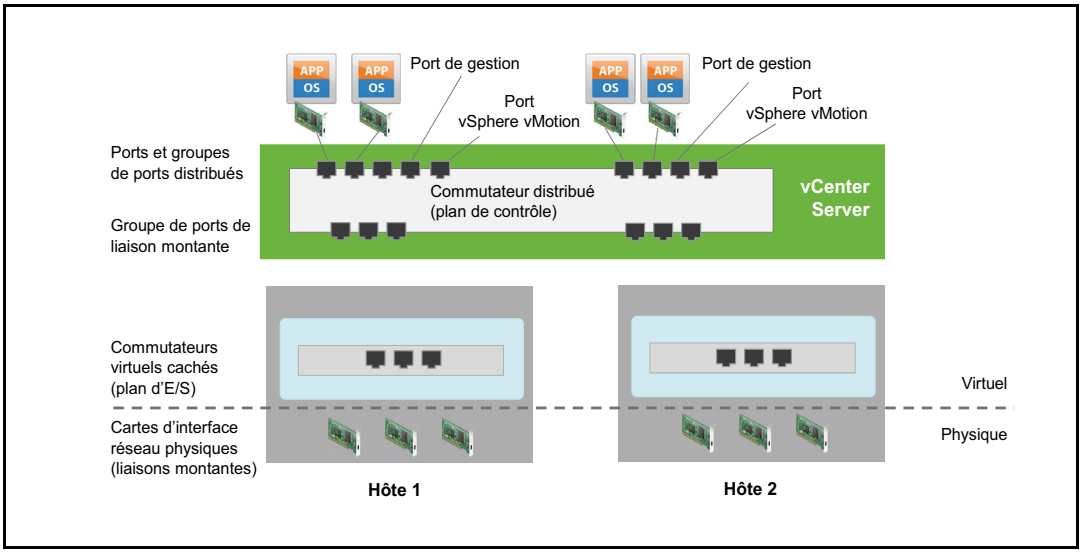
5-14 Types de commutateur virtuel

Un réseau virtuel prend en charge les types de commutateurs virtuels suivants :

- Les commutateurs standard :
  - La configuration des commutateurs virtuels pour un hôte unique.
- Les commutateurs distribués :
  - Le commutateur virtuel configuré pour l'ensemble d'un Data Center.
  - Jusqu'à 2 000 hôtes peuvent être reliés au même commutateur distribué.
  - La configuration cohérente sur tous les hôtes reliés.
  - Les hôtes doivent avoir une licence Enterprise Plus ou appartenir à un cluster vSAN.

Les deux types de commutateurs sont élastiques : les ports sont automatiquement créés et supprimés.

5-15 Architecture de commutateur distribué



vCenter Server est responsable de la configuration du commutateur distribué. La configuration est cohérente sur l'ensemble des hôtes utilisant le commutateur distribué.

5-16 Comparatif entre les commutateurs standard et les commutateurs distribués

Fonction	Commutateur standard	Distributed Switch
Commutateur de couche 2	✓	✓
Segmentation du VLAN	✓	✓
Prise en charge du protocole IPv6	✓	✓
Balisage 802.1Q	✓	✓
Association de cartes d'interface réseau	✓	✓
Paramétrage du trafic sortant	✓	✓
Paramétrage du trafic entrant		✓
Blocage de ports réseau des VMs		✓
VLAN privés		✓
Association en fonction de la charge		✓
Gestion au niveau du Data Center		✓
Migration vSphere vMotion du réseau		✓
Paramètres des règles par port		✓
Surveillance de l'état des ports		✓
NetFlow		✓
Mise en miroir des ports		✓

5-17 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les types de connexion d'un commutateur virtuel
- Configurer et consulter les paramètres de configuration d'un commutateur standard, comme les groupes de ports de machine virtuelle, les ports VMkernel, les paramètres VLAN et les fonctionnalités de sécurité
- Comparer les fonctionnalités des commutateurs standard et des commutateurs distribués

5-18 Leçon 2 : Configuration des règles de commutateur standard

5-19 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Expliquer comment configurer les règles de sécurité pour un groupe de ports de commutateur standard
- Expliquer comment configurer les règles de paramétrage du trafic pour un groupe de ports de commutateur standard
- Expliquer comment configurer les règles d'association de cartes d'interface réseau et de basculement pour un groupe de ports de commutateur standard

5-20 Règles relatives aux commutateurs et aux ports réseau

Les règles définies au niveau d'un commutateur standard s'appliquent par défaut à tous les groupes de ports de ce commutateur.

Les règles de réseau disponibles :

- La sécurité
- Le paramétrage du trafic
- L'association de cartes d'interface réseau et basculement

Les règles sont définies aux niveaux suivants :

- Le niveau du commutateur standard :
  - Les règles par défaut pour l'ensemble des ports sur le commutateur standard.
- Le niveau du groupe de ports :
  - Les règles applicables : les règles créées à ce niveau remplacent les règles par défaut spécifiées pour le commutateur standard.

La règle de sécurité réseau assure la protection du système contre toute tentative d'usurpation d'adresse MAC ou d'analyse de ports frauduleuse.

La fonction de paramétrage du trafic est utile si vous souhaitez limiter le volume de trafic à destination d'une machine virtuelle ou d'un groupe de machines virtuelles. Le paramétrage du trafic permet de protéger une machine virtuelle ou le trafic au sein d'un réseau suralloué.

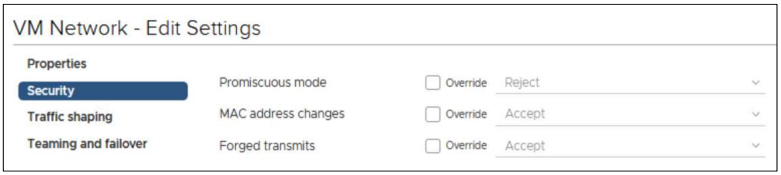
La règle d'association et de basculement vous permet de déterminer le mode de distribution du trafic réseau des machines virtuelles et des adaptateurs VMkernel connectés au commutateur entre les adaptateurs physiques, ainsi que le mode de réacheminement du trafic en cas de défaillance d'un adaptateur.

Ces règles sont définies pour l'ensemble du commutateur standard, mais peuvent également porter sur un port VMkernel ou sur un groupe de ports de machine virtuelle. Lorsqu'une règle est définie au niveau d'un port ou d'un groupe de ports donnés, elle remplace les règles par défaut définies pour le commutateur standard.

5-21 Configuration de règles de sécurité

Les administrateurs peuvent définir les règles de sécurité au niveau du commutateur standard et du groupe de ports :

- **Promiscuous mode :** permet à un commutateur virtuel ou à un groupe de ports virtuels de transmettre l'ensemble du trafic vers toutes ses vNIC, sans tenir compte de la destination.
- **MAC address changes :** détermine si le trafic entrant doit être accepté ou rejeté lorsque l'adresse MAC est modifiée par le client.
- **Forged transmits :** détermine si le trafic sortant doit être accepté ou rejeté lorsque l'adresse MAC est modifiée par le client.



Pour un commutateur vSphere standard, vous pouvez configurer la règle de sécurité de façon à rejeter les changements relatifs aux adresses MAC et au mode de proximité dans le système d'exploitation client d'une machine virtuelle.

La règle de sécurité réseau contient les exceptions suivantes :

- **Promiscuous mode** : le mode de proximité permet à un commutateur virtuel ou à un groupe de ports virtuels de transmettre l'ensemble du trafic, sans tenir compte de la destination. La valeur par défaut est « Reject ».
- **MAC address changes** : si cette option est définie sur « Reject », le client cesse de recevoir des trames s'il tente de modifier l'adresse MAC affectée à la carte d'interface réseau virtuelle. La valeur par défaut est « Accept ».
- **Forged transmits** : le champ d'adresse source d'une trame peut avoir été modifié par le client et contenir une adresse MAC autre que celle affectée à la carte d'interface réseau virtuelle. Vous pouvez définir le paramètre « Forged Transmits » de façon à accepter ou à rejeter de telles trames. La valeur par défaut est « Accept ».

De façon générale, ces règles vous permettent d'interdire certains comportements susceptibles d'affecter la sécurité du système. En effet, un pirate pourrait utiliser un périphérique en mode de proximité pour capturer le trafic réseau à des fins frauduleuses. De même, un utilisateur malveillant pourrait emprunter l'identité d'un nœud et obtenir un accès non autorisé en usurpant son adresse MAC.

Définissez l'option **Promiscuous mode** sur **Accept** afin d'utiliser une application d'analyse ou d'examen des paquets (« sniffing ») exécutée sur la machine virtuelle – par exemple, un système de détection des intrusions exploitant le réseau.

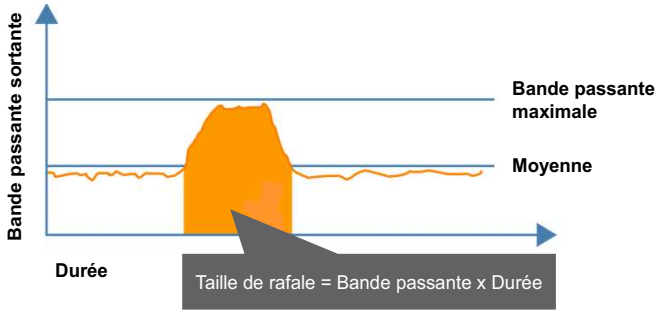
Définissez les options **MAC Address Changes** et **Forged Transmits** sur **Reject** pour optimiser la protection du système contre certaines attaques lancées par un système d'exploitation client frauduleux.

Dans le cas des options **MAC Address Changes** et **Forged Transmits**, laissez la valeur par défaut (**Accept**) si vos applications modifient l'adresse MAC mappée, comme le font certains pare-feu basés sur le système d'exploitation client.

5-22 Règles de paramétrage du trafic

Le mécanisme de paramétrage du trafic réseau permet de limiter la bande passante réseau disponible consommée par une machine virtuelle.

Les bandes passantes moyenne, maximale et la taille de rafale peuvent être configurées.

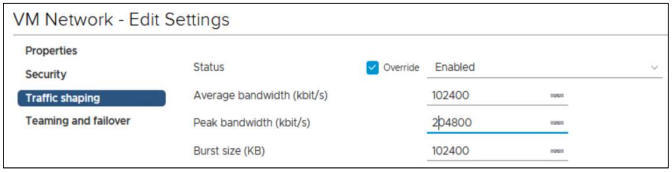


La bande passante réseau d'une machine virtuelle peut être contrôlée via l'activation d'un régulateur de trafic réseau. Lorsqu'il est utilisé sur un commutateur standard, ce régulateur porte uniquement sur le trafic réseau sortant. Pour contrôler le trafic entrant, utilisez un système d'équilibrage de charge ou activez les fonctions de limitation de débit sur votre routeur physique.

5-23 Configuration du paramétrage du trafic

Une règle de paramétrage du trafic se définit en termes de bande passante moyenne, maximale et de taille de rafale. Vous pouvez mettre en place une règle de paramétrage du trafic pour chaque groupe de ports ainsi que pour chaque port ou groupe de ports distribués :

- L'option de paramétrage du trafic est désactivée par défaut.
- Les paramètres s'appliquent à chaque carte d'interface réseau virtuelle du commutateur standard.
- Sur un commutateur standard, le paramétrage du trafic permet uniquement de contrôler le trafic sortant, c'est-à-dire le trafic transitant des machines virtuelles au commutateur virtuel et sortant sur le réseau physique.



L'hôte VMware ESXi paramètre uniquement le trafic sortant, en établissant des valeurs pour les caractéristiques suivantes du trafic :

- **Average bandwidth** (Kbit/s) : cette option définit le nombre de kilobits par seconde autorisés à transiter par un port, sous la forme d'une moyenne sur une période définie. La bande passante moyenne correspond à la charge moyenne autorisée.
- **Peak bandwidth** (Kbit/s) : Le nombre maximal de kilobits par seconde autorisés à transiter par un port en cas d'envoi d'une surcharge de trafic. Ce nombre limite la bande passante utilisée par un port chaque fois que ce dernier utilise le bonus de surcharge configuré en utilisant le paramètre « Burst size ».
- **Burst size** (Ko) : Le nombre maximal de kilooctets autorisés lors d'une surcharge. Si ce paramètre est défini, un port peut obtenir un bonus de surcharge s'il n'utilise pas toute sa bande passante allouée. Chaque fois que le port a besoin d'une quantité de bande passante supérieure à celle que spécifie l'option **Average bandwidth**, il peut être autorisé à transmettre temporairement des données à une vitesse plus élevée si un bonus de surcharge est disponible. Ce paramètre limite le nombre de kilooctets qui peuvent être cumulés dans le bonus de surcharge et seront donc transférés à une vitesse plus élevée.

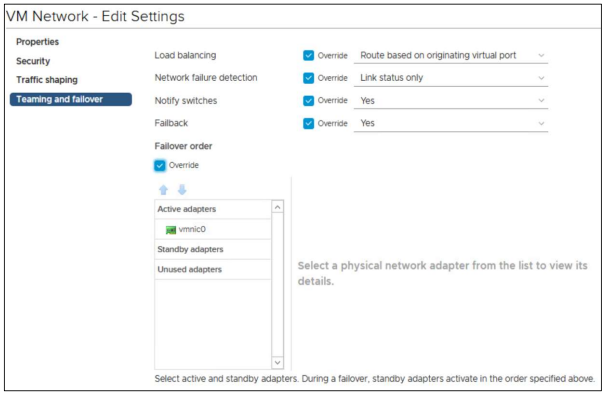
Par défaut, la fonction de paramétrage du trafic réseau est désactivée.

Pour plus d'informations sur la configuration de la règle de paramétrage du trafic dans vSphere Web Client, reportez-vous au document *VMware PowerCLI User's Guide*, disponible à l'adresse suivante : https://www.vmware.com/support/developer/PowerCLI/.

Bien que vous ayez la possibilité d'établir une règle de paramétrage du trafic au niveau du commutateur virtuel ou du groupe de ports, les paramètres définis au niveau du groupe de ports remplacent ceux qui sont spécifiés au niveau du commutateur virtuel.

5-24 Règle d’association de cartes d’interface réseau et de basculement

Les administrateurs peuvent modifier la règle d’association de cartes d’interface réseau et de basculement en configurant des options spécifiques.



L’association de cartes d’interface réseau vous permet d’augmenter la capacité réseau d’un commutateur virtuel en lui adjoignant plusieurs cartes d’interface réseau physiques formant une association. Afin de déterminer le mode de réacheminement du trafic en cas de panne de l’adaptateur, vous spécifiez un ordre de basculement pour les cartes d’interface réseau physiques. Vous déterminez la façon dont le commutateur virtuel distribue le trafic réseau entre les cartes d’interface réseau physiques d’une association en sélectionnant des algorithmes d’équilibrage de charge adaptés aux besoins et aux capacités de votre environnement :

- La règle d’association de cartes d’interface réseau : l’association de cartes d’interface réseau vous permet de connecter un commutateur virtuel à plusieurs cartes d’interface réseau d’un même hôte en vue d’augmenter la bande passante de ce commutateur et d’assurer la redondance. Une association de cartes d’interface réseau est capable de distribuer le trafic entre ses membres et d’opérer un basculement passif en cas de panne d’adaptateur ou de réseau. Vous pouvez configurer les règles d’association de cartes d’interface réseau au niveau du commutateur virtuel ou du groupe de ports dans le cas d’un commutateur standard vSphere, et au niveau du groupe de ports ou du port dans le cas d’un commutateur distribué vSphere.
- La règle d’équilibrage des charges : la règle d’équilibrage de charge détermine le mode de distribution du trafic réseau entre les membres d’une association de cartes d’interface réseau. Dans le cas d’un commutateur virtuel vSphere, l’équilibrage de charge s’applique uniquement au trafic sortant. Le trafic entrant est contrôlé par la règle d’équilibrage de charge définie pour le commutateur physique.

- La règle de retour arrière : par défaut, une règle de retour arrière est activée sur une association de cartes d'interface réseau. Si une carte d'interface réseau physique est remise en ligne après une défaillance, le commutateur virtuel réactive cette carte d'interface réseau en la substituant à la carte d'interface réseau de secours qui avait pris sa place.

  Si la carte d'interface réseau physique qui figure en première position dans l'ordre de basculement connaît des pannes intermittentes, la règle de retour arrière peut entraîner de fréquentes substitutions de l'adaptateur actif. De fréquents changements d'adresse MAC sont alors détectés par le commutateur physique, dont le port risque de ne pas accepter immédiatement le trafic survenant après la remise en ligne d'un adaptateur. Afin de limiter au minimum ces retards, vous pouvez envisager de redéfinir les paramètres indiqués ci-après sur le commutateur physique.

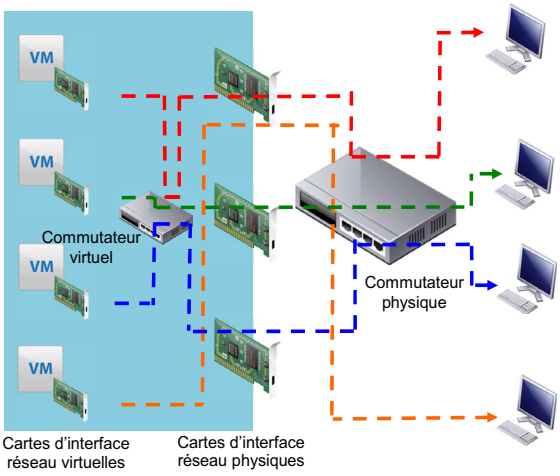
- La règle de notification des commutateurs : la règle de notification des commutateurs détermine la façon dont l'hôte VMware ESXi communique les événements de basculement. Lorsqu'une carte d'interface réseau physique se connecte au commutateur virtuel ou que le trafic est réacheminé vers une autre carte physique de l'association, le commutateur virtuel envoie des notifications sur le réseau afin de mettre à jour les tables de recherche présentes sur les commutateurs physiques. Le fait d'avertir le commutateur physique garantit une latence minimale en cas de basculement ou de migration via vSphere vMotion.

  Les règles d'association de cartes d'interface réseau et de basculement permettent de déterminer le mode de distribution du trafic réseau entre les adaptateurs ainsi que le mode de réacheminement du trafic en cas de défaillance d'un adaptateur. Les règles d'association de cartes d'interface réseau incluent des paramètres d'équilibrage de charge et de basculement. Des règles d'association de cartes d'interface réseau et de basculement par défaut sont définies pour le commutateur standard dans son ensemble. Ces paramètres par défaut peuvent être remplacés au niveau du groupe de ports. Les règles indiquent les valeurs héritées des paramètres définis au niveau du commutateur.

Pour plus d'informations sur la configuration de l'association de cartes d'interface réseau, du basculement et de l'équilibrage de charge dans vSphere Web Client, consultez le guide *Mise en réseau vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

5-25 Méthode d'équilibrage de charge : ID du port virtuel d'origine

Routage basé sur l'ID du port d'origine, ou « équilibrage de charge en fonction de l'ID de port virtuel ».



Grâce à cette méthode d'équilibrage de charge, le trafic sortant d'une machine virtuelle est mappé vers une carte d'interface réseau physique spécifique déterminée par l'ID du port virtuel auquel la machine virtuelle est connectée. C'est une méthode simple et rapide, qui évite à VMkernel de devoir analyser la trame pour obtenir les informations nécessaires.

Lorsque la charge est distribuée dans l'association de cartes d'interface réseau au moyen de la méthode basée sur des ports, une machine virtuelle disposant d'une unique carte d'interface réseau ne peut pas bénéficier d'une bande passante supérieure à celle que peut offrir un seul adaptateur physique.

Les avantages :

- La distribution uniforme du trafic si le nombre de cartes d'interface réseau virtuelles est supérieur au nombre de cartes d'interface réseau physiques de l'association.
- La faible consommation de ressources, étant donné que dans la plupart des cas, le commutateur virtuel calcule une seule fois les liaisons montantes pour les machines virtuelles.
- Aucune modification du commutateur physique n'est requise.

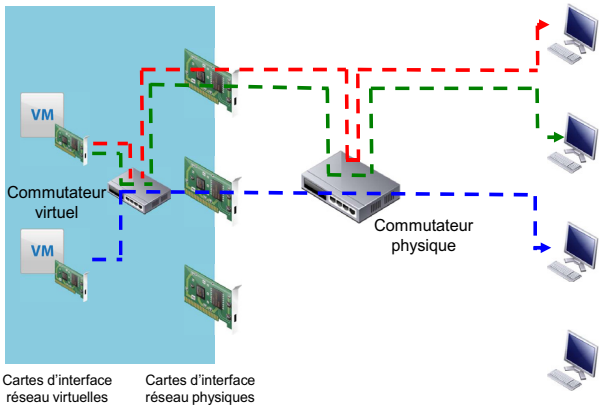
Les inconvénients :

- Le commutateur virtuel ne connaît pas la charge de trafic sur les liaisons montantes et ne redirige par conséquent pas le trafic vers les liaisons montantes moins utilisées.

- La bande passante disponible pour une machine virtuelle est limitée au débit de la liaison montante associée à l'ID de port correspondant, à moins que la machine virtuelle ne soit équipée de plusieurs cartes d'interface réseau virtuelles.

5-26 Méthode d'équilibrage de charge : Le hachage MAC source

Ce diagramme représente le routage basé sur le hachage MAC source.



Avec cette méthode, le trafic sortant de chaque machine virtuelle est mappé vers une carte d'interface réseau physique spécifique, déterminée en fonction de l'adresse MAC de la carte d'interface réseau virtuelle.

Cette méthode présente une surcharge faible et est compatible avec l'ensemble des commutateurs. Cependant, il se peut qu'elle ne puisse pas répartir le trafic de manière égale sur toutes les cartes d'interface réseau physiques.

Lorsque la charge est distribuée sur l'association de cartes d'interface réseau au moyen de la méthode basée sur des adresses MAC, une machine virtuelle disposant d'une unique carte d'interface réseau ne peut pas bénéficier d'une bande passante supérieure à celle que peut offrir un seul adaptateur physique.

Vous pouvez également baser l'équilibrage du trafic sur la charge de trafic actuelle des différentes cartes d'interface réseau physiques. La carte d'interface réseau présentant la charge la plus faible sera sélectionnée en priorité.

Les avantages :

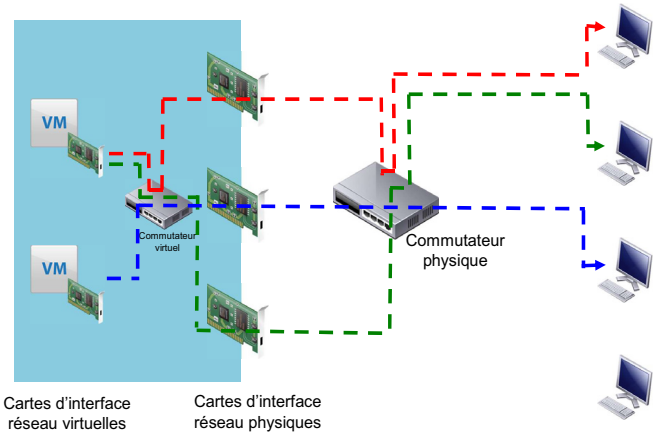
- Une distribution du trafic plus uniforme que le routage basé sur l'ID du port virtuel d'origine, car le commutateur virtuel calcule une liaison montante pour chaque paquet.
- Les machines virtuelles utilisent la même liaison montante, car l'adresse MAC est statique. La mise sous tension ou hors tension d'une machine virtuelle ne permet pas de changer la liaison montante utilisée par la machine virtuelle.
- Aucune modification du commutateur physique n'est requise.

Les inconvénients :

- La bande passante disponible pour une machine virtuelle est limitée au débit de la liaison montante associée à l'ID de port correspondant, à moins que la machine virtuelle n'utilise plusieurs adresses MAC sources.
- Une consommation de ressources plus élevée comparée au routage basé sur l'ID du port virtuel d'origine, car le commutateur virtuel calcule une liaison montante pour chaque paquet.
- Le commutateur virtuel ne connaît pas la charge des liaisons montantes, ces dernières peuvent donc être surchargées.

5-27 Méthode d'équilibrage de charge : Le hachage IP source et de destination

Ce diagramme représente le routage basé sur le hachage IP.



Avec la méthode d'équilibrage de charge, une carte d'interface réseau est sélectionnée pour chaque paquet sortant, en fonction de ses adresses IP d'origine et de destination.

La méthode basée sur l'adresse IP nécessite la prise en charge de l'agrégation de liens 802.3ad ou la technologie EtherChannel sur le commutateur. Le protocole LACP (Link Aggregation Control Protocol) permet de contrôler l'aggrégat constitué de différents ports physiques pour créer un canal logique unique. Ce protocole fait partie de la spécification IEEE 802.3ad.

EtherChannel est une technologie d'agrégation de ports principalement utilisée sur les commutateurs Cisco. Cette technologie permet de regrouper plusieurs liens Ethernet physiques dans le but de créer un lien Ethernet logique capable d'assurer des liaisons haut débit et tolérantes aux pannes entre les commutateurs, les routeurs et les serveurs.

Lorsque la charge est distribuée dans l'association de cartes d'interface réseau en utilisant la méthode basée sur des adresses IP, une machine virtuelle disposant d'une seule carte d'interface réseau peut utiliser la bande passante offerte par plusieurs adaptateurs physiques.

La méthode d'équilibrage basée sur les adresses IP affecte uniquement le trafic sortant. Par exemple, une machine virtuelle pourrait choisir une carte d'interface réseau particulière pour communiquer avec une machine virtuelle de destination donnée. Il est alors possible que le trafic de retour n'emprunte pas la même carte d'interface réseau que le trafic sortant, mais sur une autre carte d'interface réseau de la même association de cartes d'interface réseau. Pour obtenir la liste des exigences de l'hôte VMware ESXi pour l'agrégation de liens, consultez l'article 1001938 de la base de connaissances VMware, disponible à l'adresse suivante : http://kb.vmware.com/kb/1001938.

Les avantages :

- Une distribution de la charge plus uniforme comparée au routage basé sur l'ID du port virtuel d'origine et au routage basé sur le hachage MAC source, car le commutateur virtuel calcule la liaison montante pour chaque paquet.
- Un débit potentiellement supérieur pour les machines virtuelles qui communiquent avec plusieurs adresses IP.

Les inconvénients :

- La consommation de ressources plus élevée comparée aux autres algorithmes d'équilibrage de charge.
- Le commutateur virtuel ne connaît pas la charge réelle des liaisons montantes.
- Nécessite des modifications sur le réseau physique.
- Le dépannage complexe.

5-28 Détection et gestion des défaillances réseau

VMkernel peut utiliser l'état des liens et/ou la fonction de sondage pour détecter une défaillance réseau.

Ce type de défaillance est détecté par VMkernel, qui effectue la surveillance de l'état des liens et mets en place des paquets de sondage.

VMkernel informe les commutateurs physiques de tout déplacement physique d'une adresse MAC.

Le basculement est mis en œuvre par VMkernel sur la base des paramètres configurables suivants :

- Le retour arrière : détermine de quelle manière un adaptateur physique est remis en service lors de la reprise après une panne.
- L'option d'équilibrage de charge : utilise un ordre de basculement explicite. Utilise toujours la liaison montante de la vmnic figurant en haut de la liste des adaptateurs actifs.

La surveillance de l'état des liens assurée par l'adaptateur réseau permet de détecter certaines défaillances, telles qu'un câble débranché ou une panne d'un commutateur physique. Cette fonction ne peut cependant pas détecter les problèmes de configuration, tels que le blocage d'un port de commutateur physique par le protocole STP (Spanning Tree Protocol) ou une mauvaise configuration du VLAN d'appartenance. Cette méthode ne détecte pas non plus les défaillances affectant les commutateurs physiques ou les câbles situés en amont et non directement connectés.

Le sondage introduit la charge d'un paquet de 62 octets toutes les secondes environ, pour chaque carte d'interface réseau physique. Lorsque cette fonction est activée, VMkernel envoie et écoute les paquets de sondage sur toutes les cartes d'interface réseau configurées dans l'association. Cette technique permet de détecter les défaillances que la fonction de surveillance de l'état des liens ne peut pas identifier à elle seule. Demandez au fabricant du commutateur de vérifier la prise en charge du sondage (beacon probing) au sein de votre environnement. Consultez l'article 1005577 de la base de connaissances VMware, disponible à l'adresse suivante : http://kb.vmware.com/kb/1005577.

Un commutateur physique peut recevoir des notifications de VMkernel chaque fois qu'une carte d'interface réseau virtuelle est connectée à un commutateur virtuel. Il peut également recevoir des notifications lorsqu'un événement de basculement entraîne l'acheminement du trafic d'une carte d'interface réseau virtuelle via une autre carte d'interface réseau physique. La notification est envoyée via le réseau pour mettre à jour les tables d'adresses MAC sur les commutateurs physiques. Dans la plupart des cas, ce processus de notification est une option souhaitable, car les machines virtuelles risquent sinon de rencontrer une latence plus importante après un basculement et lors du fonctionnement de vSphere vMotion. Ne définissez pas cette option lorsque les machines virtuelles connectées au groupe de ports exécutent la fonction d'équilibrage de la charge réseau de Microsoft en mode monodiffusion. Lorsqu'elle est en mode multidiffusion, cette fonction n'est pas affectée. Pour en savoir plus sur ce problème, consultez l'article 1556 de la base de connaissances VMware , disponible à l'adresse suivante : http://kb.vmware.com/kb/1556.

Si vous avez recours à un ordre de basculement explicite, le système utilise toujours la liaison montante présentant l'ordre le plus élevé de la liste des adaptateurs actifs répondant aux critères de détection de basculement.

L'option de retour arrière détermine les modalités de remise en service d'un adaptateur physique lors de la reprise après une panne. Si l'option **Failback** est définie sur **Yes**, l'adaptateur qui a connu une défaillance est remis en service lors la reprise, remplaçant ainsi l'adaptateur de secours qui avait pris sa place lors de la défaillance. Si l'option **Failback** a la valeur **No**, l'adaptateur qui a connu une défaillance reste inactif même après la reprise, jusqu'à ce qu'un autre adaptateur actif subisse une défaillance nécessitant son remplacement.

5-29 Considérations relatives au réseau physique

Votre environnement de réseau virtuel repose sur l'infrastructure de réseau physique. En tant qu'administrateur vSphere, vous devez évaluer vos besoins en fonctionnalités de réseau vSphere en concertation avec votre équipe d'administration réseau.

Il convient notamment d'aborder les aspects suivants :

- Le nombre de commutateurs physiques
- La bande passante réseau requise
- La configuration des commutateurs physiques prenant en charge la technologie 802.3ad pour l'association de cartes d'interface réseau
- La configuration des commutateurs physiques prenant en charge la technologie 802.1Q, pour le marquage de VLAN
- La configuration des commutateurs physiques prenant en charge le protocole LACP (Link Aggregation Control Protocol)
- La sécurité des ports du réseau
- Les protocoles LLDP (Link Layer Discovery Protocol) et CDP (Cisco Discovery Protocol), ainsi que leurs modes de fonctionnement, par exemple : listen, broadcast, listen et broadcast, et disabled

5-30 Laboratoire 4 : Utilisation de commutateurs standard

Créer un commutateur standard et un groupe de ports

1. Afficher la configuration des commutateurs standard
2. Créer un commutateur standard avec un groupe de ports de machine virtuelle
3. Connecter vos machines virtuelles au groupe de ports de la nouvelle machine virtuelle

5-31 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Expliquer comment configurer les règles de sécurité pour un groupe de ports de commutateur standard
- Expliquer comment configurer les règles de paramétrage du trafic pour un groupe de ports de commutateur standard
- Expliquer comment configurer les règles d'association de cartes d'interface réseau et de basculement pour un groupe de ports de commutateur standard

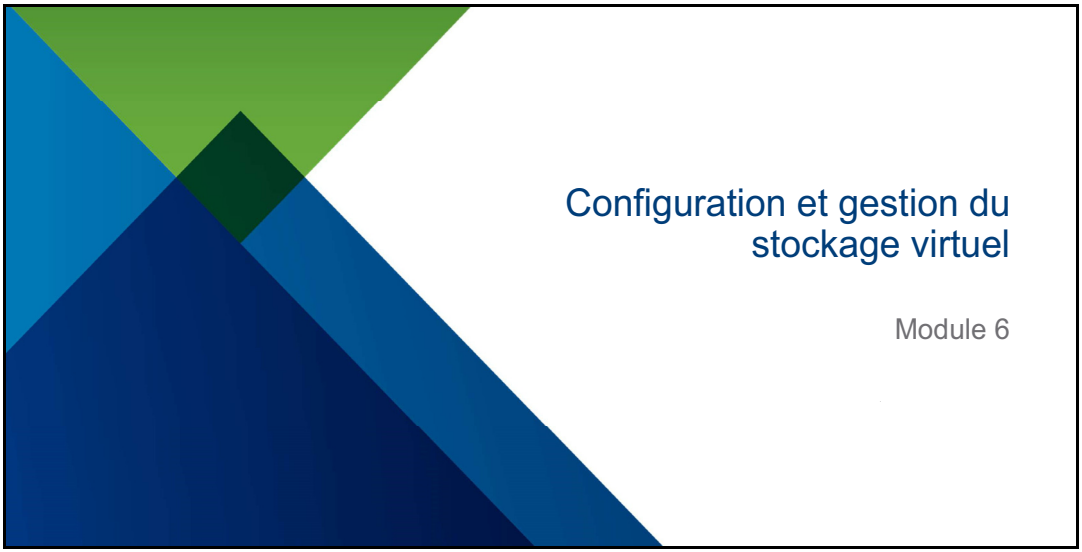
5-32 Points clés

- Les types de connexion pouvant être définis sur un commutateur virtuel sont les suivants : Le groupe de ports de machine virtuelle, la connexion VMkernel et les liaisons montantes physiques.
- Un commutateur standard correspond à une configuration de commutateur virtuel associée à un hôte unique.
- Des règles de réseau définies au niveau du commutateur standard peuvent être remplacées au niveau du groupe de ports.
- Un commutateur distribué assure la gestion centralisée et la surveillance de la configuration de la mise en réseau pour tous les hôtes associés au commutateur.

Des questions ?

MODULE 6

Configuration et gestion du stockage virtuel



6-2 Vous êtes ici

1. Présentation du cours
2. Présentation de vSphere et du Software-Defined Data Center
3. Création de machines virtuelles
4. vCenter Server
5. Configuration et gestion des réseaux virtuels
6. **Configuration et gestion du stockage virtuel**
7. Gestion des machines virtuelles
8. Gestion et surveillance des ressources
9. vSphere HA, vSphere Fault Tolerance et protection des données
10. vSphere DRS
11. vSphere Update Manager
12. Résolution des problèmes vSphere

6-3 Importance

Les options de stockage vous offrent la liberté de configurer votre stockage selon vos besoins en termes de coûts, de performances et de gérabilité.

Le stockage partagé s'avère particulièrement utile pour la reprise d'activité, la haute disponibilité et le transfert de machines virtuelles entre les hôtes.

6-4 Leçons du module

Leçon 1 :	Concepts liés au stockage
Leçon 2 :	Stockage Fibre Channel
Leçon 3 :	Stockage iSCSI
Leçon 4 :	Banques de données VMFS
Leçon 5 :	Banques de données NFS
Leçon 6 :	Banques de données vSAN

6-5 Leçon 1 : Concepts liés au stockage

6-6 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les technologies de stockage et les banques de données vSphere

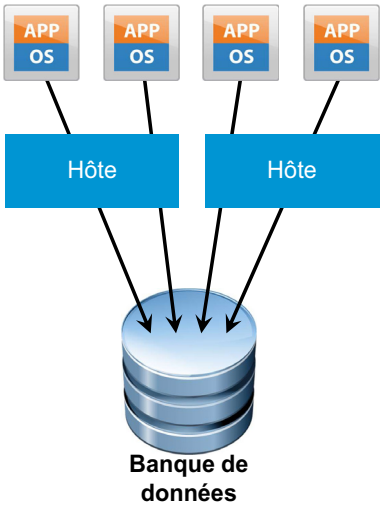
6-7 À propos des banques de données

Une banque de données est une unité de stockage logique qui peut occuper l'espace disque d'un ou plusieurs périphériques physiques.

Les banques de données sont destinées à héberger les fichiers, les modèles et les images ISO des machines virtuelles.

vSphere prend en charge les types de banque de données suivants :

- VMFS
- NFS
- vSAN
- vSphere Virtual Volumes

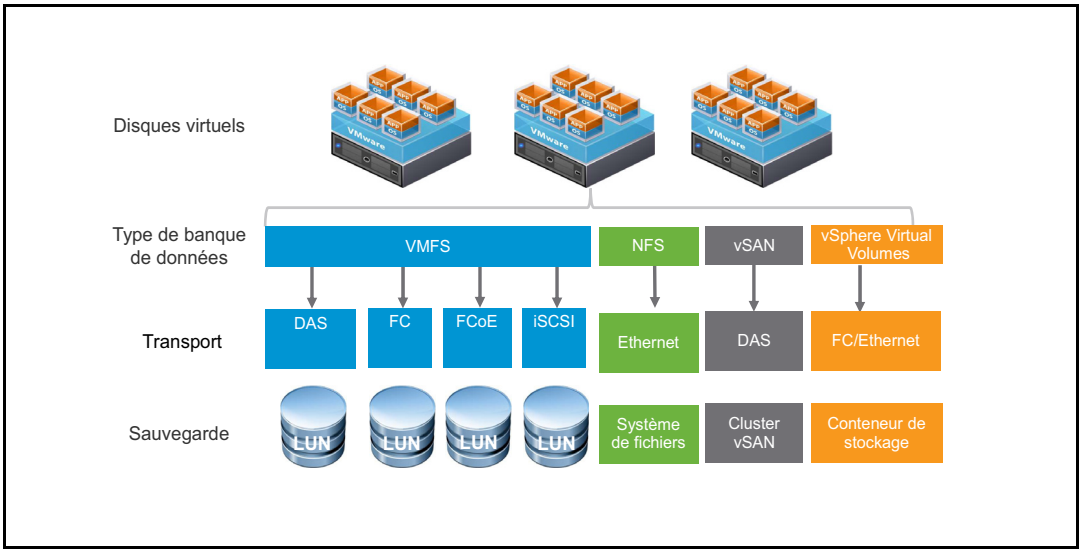


Le concept générique de banque de données désigne un conteneur renfermant des fichiers et des objets. Les banques de données sont des conteneurs logiques comparables à des systèmes de fichiers, qui servent à masquer les spécificités des différents périphériques de stockage de façon à proposer un modèle uniforme pour le stockage des fichiers de machine virtuelle.

Vous avez la possibilité d'afficher toutes les banques de données disponibles pour vos hôtes et d'en analyser les propriétés.

Chaque machine virtuelle est stockée sous la forme d'un ensemble de fichiers dans son propre répertoire ou d'un groupe d'objets rassemblés dans une banque de données. Les banques de données peuvent également être utilisées pour stocker des images ISO, des images de disquette, des modèles de machine virtuelle, etc.

6-8 Généralités sur le stockage



Les hôtes VMware ESXi doivent être configurés de façon à partager l'accès aux banques de données. Selon le type de stockage utilisé, les banques de données peuvent être formatées à l'aide de VMFS ou selon le système de fichiers natif d'un périphérique de stockage partagé via le protocole NFS.

Différentes technologies de stockage sont prises en charge par les hôtes VMware ESXi dans l'environnement vSphere :

- DAS (Direct-Attached Storage) : Les disques ou les baies de stockage internes ou externes connectés à l'hôte via une connexion directe (et non une connexion réseau).
- Fibre Channel : Le protocole de transport haut débit utilisé pour les SAN. Fibre Channel encapsule les commandes SCSI qui sont transmises entre les différents nœuds Fibre Channel. De façon générale, un nœud Fibre Channel correspond à un serveur, à un système de stockage ou à un lecteur de bande. Un commutateur Fibre Channel permet d'interconnecter plusieurs nœuds pour former le fabric d'un réseau Fibre Channel.
- FCoE : le trafic Fibre Channel est encapsulé dans des trames FCoE (Fibre Channel over Ethernet). Ces trames FCoE sont mises en convergence avec d'autres types de trafic empruntant le réseau Ethernet. Le transport du trafic Ethernet et du trafic Fibre Channel sur une même liaison Ethernet augmente considérablement le taux d'utilisation de l'infrastructure physique. FCoE permet également de réduire la quantité totale de ports réseau et de câblage mise en œuvre.

- iSCSI : Le protocole de transport SCSI donnant accès aux périphériques et au câblage de stockage à travers les réseaux TCP/IP standard. iSCSI assure le mappage du stockage par blocs SCSI via TCP/IP. Des initiateurs, tels qu'un adaptateur de bus hôte iSCSI ou un hôte VMware ESXi, envoient des commandes SCSI à des cibles localisées au sein des systèmes de stockage iSCSI.
- NAS : Le stockage partagé via des réseaux TCP/IP standard au niveau du système de fichiers. Le stockage NAS est utilisé pour contenir les banques de données NFS. Le protocole NFS ne prend pas en charge les commandes SCSI.

Les technologies iSCSI, NAS et FCoE peuvent fonctionner avec des connexions 1 Gigabit Ethernet ou 10 Gigabit Ethernet. Le 10GbE assure des performances de stockage plus élevées, ainsi qu'une bande passante suffisante pour permettre la coexistence et accélérer l'exécution de différents types de trafic de protocole haut débit sur un même réseau.

6-9 Présentation des protocoles de stockage

Type de banque de données	Protocole de stockage	Prise en charge du démarrage à partir du SAN	Prise en charge de vSphere vMotion	Prise en charge de vSphere HA	Prise en charge de vSphere DRS	Prise en charge du mappage de périphériques bruts
VMFS	Fibre Channel	•	•	•	•	•
	FCoE	•	•	•	•	•
	iSCSI	•	•	•	•	•
	NFS		•	•	•	
DAS	DAS		•			•
vSphere Virtual Volumes	FC/ Ethernet		•	•	•	
	vSAN		•	•	•	

Le stockage DAS (Direct-Attached Storage), par opposition au stockage SAN, est le type de stockage choisi par de nombreux administrateurs pour l'installation de VMware ESXi. Le stockage local est également idéal pour les petits environnements, dans la mesure où il permet de faire l'économie des coûts d'achat et de gestion d'un SAN. En revanche, ce type de stockage vous prive de nombre des fonctionnalités qui justifient l'investissement dans la virtualisation, notamment l'équilibrage de la charge d'un hôte VMware ESXi déterminé. Le stockage DAS peut également être utilisé pour stocker des données non stratégiques, par exemple :

- Les images ISO de CD/DVD
- Les machines virtuelles mises hors service
- Les modèles de machine virtuelle

En comparaison, les numéros d'unité logique (LUN) de stockage ne sont accessibles aux hôtes VMware ESXi qu'une fois regroupés et partagés. Le stockage partagé permet d'activer certaines fonctionnalités de vSphere, telles que :

- vSphere vMotion
- vSphere HA
- vSphere DRS

Le stockage SAN partagé permet quant à lui de déployer de puissantes fonctionnalités de vSphere, telles que :

- Les référentiels centralisés pour les fichiers et les modèles de machine virtuelle

- Le clustering de machines virtuelles résidant sur différents hôtes VMware ESXi
- L'allocation de grands volumes de mémoire (plusieurs téraoctets) à vos hôtes VMware ESXi

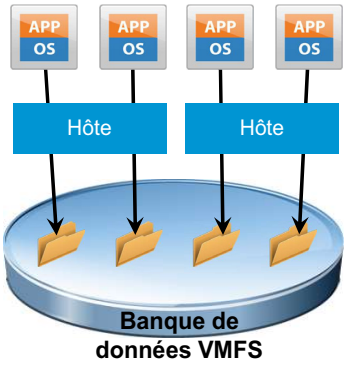
VMware ESXi prend en charge différentes méthodes de démarrage à partir du SAN, ce qui permet d'éviter la maintenance de stockage local supplémentaire, mais aussi d'utiliser des configurations matérielles sans disque telles que des systèmes lames. Lorsque vous configurez un hôte pour démarrer à partir d'un SAN, l'image de démarrage de cet hôte est stockée sur un ou plusieurs LUN du système de stockage SAN. Lors de son lancement, l'hôte démarre à partir d'un LUN du réseau SAN plutôt que d'un disque local.

Les hôtes VMware ESXi permettent le démarrage à partir de l'iSCSI logiciel, à partir d'un adaptateur SCSI matériel indépendant pris en charge, ou à partir d'un adaptateur iSCSI matériel dépendant pris en charge. L'adaptateur réseau doit uniquement prendre en charge le format iBFT (iSCSI Boot Firmware Table), qui définit une méthode pour communiquer les paramètres concernant le périphérique de démarrage iSCSI à un système d'exploitation.

6-10 À propos de VMFS

Les hôtes VMware ESXi versions 6.5 et ultérieures prennent en charge VMFS5 et VMFS6 :

- Les fonctionnalités prises en charge conjointement par VMFS5 et VMFS6 :
  - Permettent les accès simultanés au stockage partagé
  - Peuvent être étendues de manière dynamique
  - Utilisent des tailles de bloc de 1 Mo et de 512 Mo, optimales pour le stockage des grands fichiers de disque virtuel
  - Fournissent un mécanisme de verrouillage sur disque
- Les fonctionnalités prises en charge conjointement par VMFS6 :
  - Les périphériques prenant en charge le stockage natif 4k
  - La récupération automatique de l'espace



VMFS est un système de fichiers en cluster qui permet à plusieurs hôtes VMware ESXi d'accéder simultanément en lecture ou en écriture à un même périphérique de stockage. Ce système de fichiers en cluster permet d'activer des services exclusifs basés sur la virtualisation – entre autres :

- La migration de machines virtuelles en cours d'exécution d'un hôte VMware ESXi à un autre sans interruption de service
- Le redémarrage automatique d'une machine virtuelle défaillante sur un nouvel hôte VMware ESXi
- Le clustering de machines virtuelles résidant sur différents serveurs physiques

VMFS permet au département informatique de simplifier considérablement le provisionnement des machines virtuelles en centralisant efficacement le stockage de l'état complet des machines. VMFS permet à plusieurs hôtes VMware ESXi d'accéder simultanément au stockage partagé des machines virtuelles.

Il est possible de redimensionner dynamiquement la taille d'une banque de données VMFS alors que les machines virtuelles résidant sur cette banque de données sont sous tension et en cours d'exécution. Une banque de données VMFS permet un stockage efficace des fichiers de toute taille appartenant à une machine virtuelle. Les banques de données VMFS prennent en charge les fichiers de disque virtuel. La taille maximale d'un fichier de disque virtuel est de 62 To. Les banques de données VMFS ont recours à l'adressage de sous-blocs pour optimiser l'utilisation du stockage dans le cas de petits fichiers.

VMFS utilise un mécanisme de verrouillage distribué en mode bloc pour éviter qu'une même machine virtuelle soit mise sous tension par plusieurs serveurs au même moment. Si un hôte

VMware ESXi tombe en panne, le verrouillage sur disque de chaque machine virtuelle est levé, afin de permettre le redémarrage de la machine virtuelle sur d'autres hôtes VMware ESXi.

Sur cette diapositive, chaque hôte VMware ESXi héberge deux machines virtuelles en cours d'exécution. Les lignes qui relient les machines virtuelles aux disques de machine virtuelle (VMDK) sont une représentation logique du processus d'association et d'allocation de la banque de données VMFS prise dans son ensemble. Une banque de données VMFS comprend un ou plusieurs LUN. Du point de vue des machines virtuelles, le volume de stockage alloué se présente comme une simple cible SCSI, perçue depuis l'intérieur du système d'exploitation client. Le contenu de la machine virtuelle se résume à un ensemble de fichiers stockés sur le volume VMFS.

VMFS peut être déployé sur des périphériques de stockage SCSI de l'un de ces trois types :

- Le stockage DAS
- Le stockage Fibre Channel
- Le stockage iSCSI

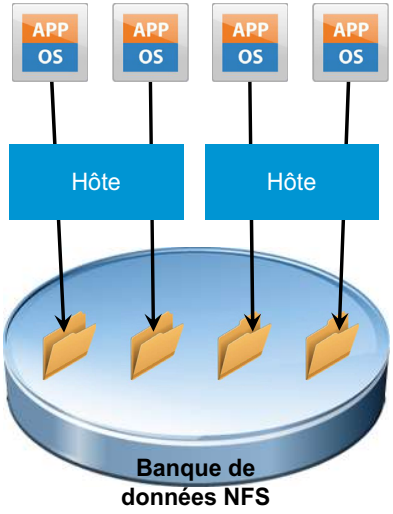
Pour la machine virtuelle, un disque virtuel stocké dans une banque de données VMFS se présente toujours comme un périphérique SCSI monté. Le disque virtuel masque la couche de stockage physique vis-à-vis du système d'exploitation de la machine virtuelle.

Pour le système d'exploitation de la machine virtuelle, VMFS préserve la sémantique du système de fichiers interne. Le système d'exploitation exécuté sur la machine virtuelle perçoit par conséquent un système de fichiers natif, et non le système de fichiers VMFS. Cette sémantique garantit un comportement correct des applications exécutées sur les machines virtuelles, ainsi que l'intégrité de leurs données.

6-11 À propos de NFS

NFS offre un stockage partagé sur le réseau au niveau du système de fichiers.

- NFS prend en charge NFS versions 3 et 4.1 sur TCP/IP.



NFS est un protocole de partage de fichiers utilisé par les hôtes VMware ESXi pour communiquer avec un périphérique NAS. Un périphérique NAS est un périphérique de stockage spécialisé capable de se connecter à un réseau et de fournir aux hôtes VMware ESXi des services d'accès aux fichiers.

Les banques de données NFS sont traitées comme des banques de données VMFS dans la mesure où elles peuvent être utilisées pour stocker des fichiers, des modèles et des images ISO de machine virtuelle. De plus, à l'instar d'une banque de données VMFS, un volume NFS permet de migrer via vSphere vMotion des machines virtuelles dont les fichiers résident dans une banque de données NFS. Le client NFS intégré dans VMware ESXi utilise les versions 3 et 4.1 du protocole NFS pour communiquer avec les serveurs NAS/NFS.

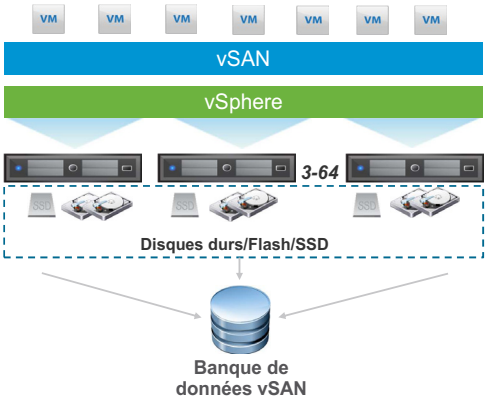
Les hôtes VMware ESXi ne font pas appel à Network Lock Manager, un protocole standard utilisé pour la prise en charge du verrouillage de fichiers montés via NFS. VMware dispose en effet de son propre protocole de verrouillage. Les verrous de NFS version 3 sont implémentés via la création de fichiers de verrouillage sur le serveur NFS. NFS 4.1 utilise quant à lui des réservations de partage comme mécanisme de verrouillage.

Dans la mesure où les clients NFS 3 et NFS 4.1 n'exploitent pas le même mécanisme de verrouillage, vous n'avez pas la possibilité d'utiliser différentes versions de NFS pour monter une même banque de données sur plusieurs hôtes. Le fait d'accéder à un même disque virtuel via deux clients incompatibles peut entraîner des erreurs de fonctionnement et une altération des données.

6-12 Présentation de vSAN

vSAN est une solution de software-defined storage convergé par hyperviseur pour les environnements virtuels.

Le clustering des disques durs traditionnels et/ou des disques SSD connectés à l'hôte permet à vSAN de regrouper ces ressources pour créer une banque de données partagée par les machines virtuelles.



Lorsque vSAN est activé sur un cluster, une banque de données vSAN unique est créée. Cette banque de données exploite les composants de stockage de chacun des hôtes du cluster.

Le montage du stockage fait appel au système de fichiers OSFS (Object Store File System). vSAN stocke et gère les données résidant au sein de la banque de données vSAN sous la forme de conteneurs flexibles appelés objets. Un objet est un volume logique dont les données et métadonnées sont réparties et accessibles sur l'ensemble du cluster. Dans la pile de stockage de VMware ESXi, ces objets apparaissent sous la forme de périphériques.

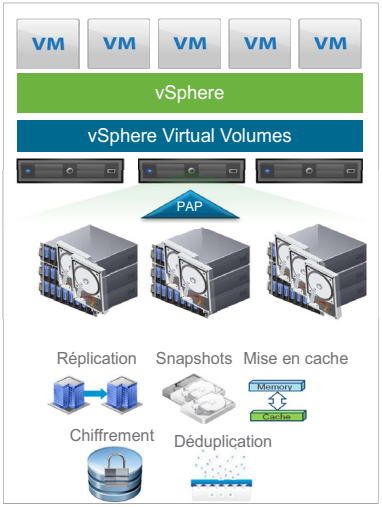
Bien qu'une seule banque de données vSAN soit créée pour l'ensemble du cluster vSAN, cette banque de données peut se voir associer plusieurs stratégies de stockage, qui peuvent être configurées de façon à solliciter différentes fonctionnalités de stockage.

vSAN peut être configuré comme un système de stockage hybride ou 100 % Flash. Dans une architecture de stockage hybride, vSAN regroupe les disques durs et les disques SSD des serveurs de manière à créer une banque de données partagée et distribuée qui isole le matériel de stockage pour fournir un niveau de software-defined storage dédié aux machines virtuelles. La technologie Flash sert de cache de lecture/tampon d'écriture pour accélérer les performances. En outre, les disques magnétiques offrent une capacité de stockage assurant la persistance des données. Autre possibilité : vSAN peut être déployé sous la forme d'une architecture de stockage 100 % Flash dans laquelle des périphériques Flash sont utilisés comme un cache d'écriture, tandis que les disques SSD fournissent une capacité de stockage garantissant la persistance des données, ainsi que des temps de réponse rapides et constants. L'architecture 100 % Flash permet la hiérarchisation des disques SSD dans le cadre d'une implémentation à coûts optimisés : un niveau de cache SSD d'entreprise à écriture intensive, et un niveau économique de capacité SSD à lecture intensive.

6-13 À propos de vSphere Virtual Volumes

vSphere Virtual Volumes offre les fonctionnalités suivantes :

- La représentation native des disques de machine virtuelle sur le SAN/NAS : Pas de LUN ni de gestion de volumes
- Fonctionne avec les systèmes SAN/NAS existants
- Un nouveau chemin de contrôle pour les opérations de données au niveau des VMs/disques de machine virtuelle
- Les snapshots, les réplications et les autres opérations effectuées au niveau des VMs sur le stockage externe
- Automatise le contrôle des niveaux de service VM par VM
- Le point d'accès de protocole (PAP) VMware vSphere® API for Storage Awareness™ fournit un accès au stockage par protocole standard.
- Les conteneurs de stockage extensibles à la totalité de la baie



VMware vSphere® Virtual Volumes™ virtualise les périphériques SAN et NAS grâce à l'abstraction des ressources matérielles physiques et à leur regroupement en pools logiques de capacité. Le paradigme de stockage de vSphere Virtual Volumes est conçu pour répondre aux besoins en stockage nouvelle génération suscités par le Software-Defined Data Center.

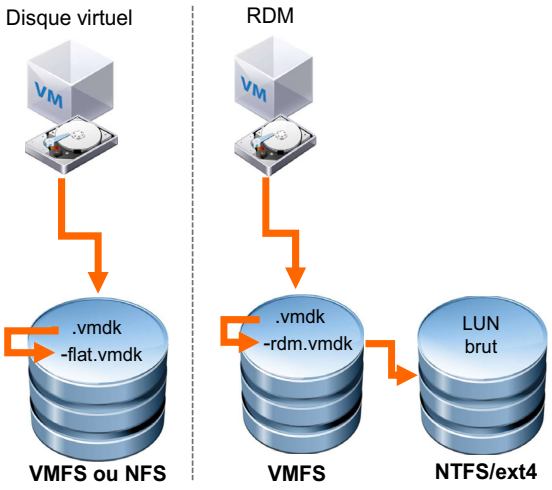
vSphere Virtual Volumes offre les avantages suivants :

- La réduction du coût de stockage
- La réduction du temps système de gestion lié au stockage
- L'évolutivité accrue
- La meilleure prise en charge des besoins en matière d'accès aux données et de capacités analytiques

6-14 À propos du mappage de périphériques bruts (RDM)

Un mappage de périphériques bruts (RDM) ne constitue pas une banque de données, mais il permet à une machine virtuelle d'accéder directement à un LUN physique.

Le fichier de mappage (`-rdm.vmdk`) faisant pointer une VM vers un LUN doit être stocké dans une banque de données VMFS.



Un mappage de périphériques bruts (RDM) est un fichier stocké sur un volume VMFS qui agit comme proxy pour un périphérique physique brut.

Au lieu de stocker les données d'une machine virtuelle sur un disque virtuel stocké dans une banque de données VMFS, vous pouvez stocker les données du système d'exploitation client directement sur un LUN brut. Le stockage direct des données est utile si vos machines virtuelles exécutent des applications qui ont besoin de connaître les caractéristiques du périphérique de stockage. Le mappage d'un LUN brut vous permet d'utiliser les commandes SAN existantes pour gérer le stockage sur ce disque.

Un RDM est recommandé dans les cas où une machine virtuelle doit interagir avec un disque réel sur le SAN. C'est notamment le cas lorsque vous créez des snapshots de baie de disques, ou lorsque vous disposez de grands volumes de données que vous ne souhaitez pas transférer vers un disque virtuel dans le cadre d'une conversion P2V (physique vers virtuel).

6-15 Considérations relatives au stockage physique

Veillez à évaluer vos besoins en stockage vSphere en concertation avec votre équipe d'administration du stockage, notamment pour ce qui concerne les aspects suivants :

- La taille des LUN
- La bande passante d'E/S
- Le nombre de demandes d'E/S par seconde qu'un LUN doit être capable d'effectuer
- Les paramètres de cache disque
- Le zonage et le masquage
- La présentation identique des LUN pour tous les hôtes VMware ESXi
- Les baies en mode actif-actif ou actif-passif
- Les propriétés d'exportation pour les banques de données NFS

En tant qu'administrateur vSphere, vous devez évaluer vos besoins en stockage avec votre équipe d'administration du stockage avant de déployer l'environnement vSphere :

- La taille des LUN
- La bande passante d'E/S requise pour vos applications
- Les paramètres, le zonage et le masquage des caches disque
- La présentation identique des LUN auprès de chaque hôte VMware ESXi (dans le cas où ce ne sont pas les noms canoniques qui sont présentés)
- Le paramètre de multipathing à utiliser pour vos baies de stockage (actif-actif ou actif-passif)
- Les paramètres NFS à utiliser

Pour plus d'informations sur la planification de vos besoins en matière de stockage, reportez-vous au guide *Stockage vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

6-16 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les technologies de stockage et les banques de données vSphere

6-17 Leçon 2 : Stockage Fibre Channel

6-18 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les utilisations possibles de la technologie Fibre Channel avec VMware ESXi
- Décrire les composants et l'adressage Fibre Channel
- Expliquer le fonctionnement du multipathing avec Fibre Channel

6-19 À propos de Fibre Channel

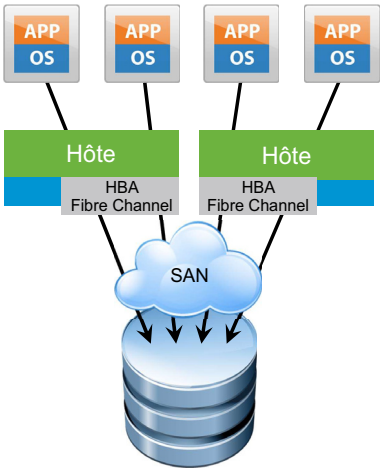
Fibre Channel stocke les fichiers de machine virtuelle à distance sur un SAN Fibre Channel.

Un SAN Fibre Channel est un réseau haut débit spécialisé qui connecte vos hôtes à des périphériques de stockage hautes performances.

Ce réseau utilise le protocole Fibre Channel pour transporter le trafic SCSI des machines virtuelles vers les périphériques SAN Fibre Channel.

VMware ESXi prend en charge les fonctionnalités suivantes :

- Fibre Channel 32 Gbit/s
- Fibre Channel over Ethernet (FCoE)



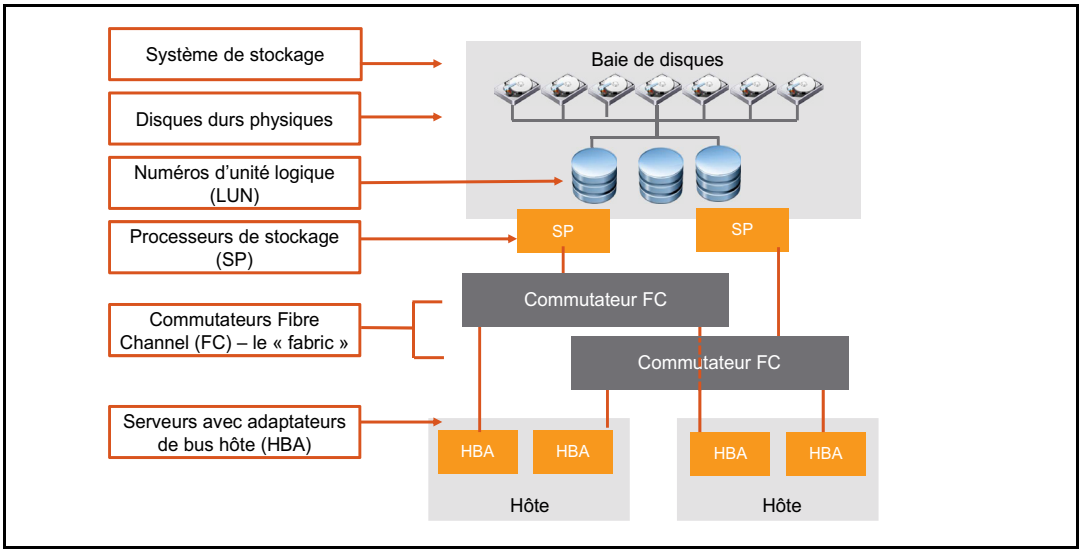
Banque de données VMFS ou vSphere Virtual Volumes sur une baie Fibre Channel

Pour se connecter au SAN Fibre Channel, votre hôte doit être équipé d'adaptateurs de bus hôte (HBA) Fibre Channel.

À moins de disposer de stockage Fibre Channel à connexion directe, vous aurez besoin de commutateurs Fibre Channel pour acheminer le trafic de stockage. Si votre hôte est doté d'adaptateurs FCoE (Fibre Channel over Ethernet), vous pouvez connecter ceux-ci à vos périphériques Fibre Channel partagés via un réseau Ethernet.

Dans cette configuration, un hôte se connecte à un fabric SAN qui comprend des commutateurs et des baies de stockage Fibre Channel à l'aide d'un adaptateur Fibre Channel. Les LUN d'une baie de stockage deviennent disponibles pour l'hôte. Vous pouvez ainsi accéder à ces LUN afin de créer des banques de données répondant à vos besoins en stockage. Ces banques de données utilisent le format VMFS. Vous avez également la possibilité d'accéder à une baie de stockage compatible avec vSphere Virtual Volume et de créer des banques de données vSphere Virtual Volumes utilisant les conteneurs de stockage de cette baie.

6-20 Composants d'un SAN Fibre Channel

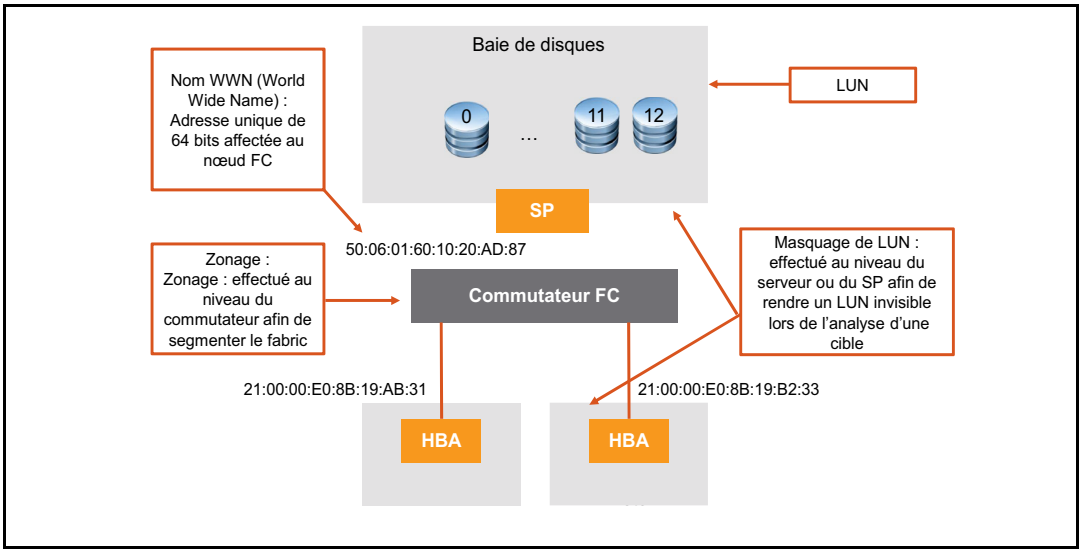


Dans sa forme la plus simple, un SAN consiste en un ou plusieurs serveurs connectés à une baie de stockage via un ou plusieurs commutateurs SAN. Chaque serveur est susceptible d'héberger de nombreuses applications, auquel cas le traitement de ces charges applicatives nécessite des ressources de stockage dédiées.

Les composants mis en œuvre sont les suivants :

- Les commutateurs SAN : ceux-ci assurent l'interconnexion des différents éléments du SAN. Ils peuvent notamment servir à connecter les hôtes aux baies de stockage. Les commutateurs SAN permettent également aux administrateurs de configurer la redondance des chemins d'accès pour parer à toute panne de chemin entre le serveur ou la baie de stockage et le commutateur.
- Le fabric : le fabric SAN correspond à la partie réseau du SAN. Un fabric est créé dès lors que plusieurs commutateurs SAN sont interconnectés. Le protocole Fibre Channel assure la communication à l'échelle du réseau tout entier. Un SAN peut englober plusieurs fabrics interconnectés. Même dans le cas d'un SAN simple, il est fréquent de déployer deux fabrics pour assurer la redondance.
- Les connexions (adaptateurs de bus hôte et processeurs de stockage) : les serveurs hôtes et les systèmes de stockage sont connectés au fabric SAN par l'intermédiaire des ports du fabric.
    - La connexion d'un hôte à un port du fabric fait appel à un adaptateur de bus hôte.
    - Les périphériques de stockage sont connectés aux ports du fabric via leurs processeurs de stockage.

6-21 Adressage et contrôle d'accès Fibre Channel



Un port assure la connexion d'un périphérique au SAN. Chaque nœud du SAN inclut chacun des hôtes, des périphériques de stockage ou des composants de fabric (routeur ou commutateur). Chaque nœud du SAN dispose d'un ou plusieurs ports assurant sa connexion au SAN. Les ports peuvent être identifiés de différentes manières :

- Le nom de port mondial (WWPN) : cet identifiant unique à l'échelle mondiale permet à certaines applications d'accéder au port concerné. Les commutateurs Fibre Channel détectent le WWPN d'un périphérique ou d'un hôte et attribuent une adresse de port au périphérique.
- L'ID de port : au sein du SAN, chaque port est identifié par un ID de port unique qui constitue son adresse Fibre Channel. Les commutateurs FC attribuent l'ID de port lors de la connexion du périphérique au fabric. L'ID de port ne reste valide que durant la période de connexion du périphérique.

Vous pouvez recourir au zonage et au masquage de LUN pour séparer les activités SAN et restreindre l'accès aux périphériques de stockage.

Vous avez également la possibilité de protéger l'accès au stockage au sein de votre environnement vSphere en appliquant le zonage et le masquage de LUN à vos ressources SAN. Vous avez notamment la possibilité de gérer les zones définies à des fins de test de manière indépendante au sein du SAN de sorte qu'elles n'interfèrent pas avec l'activité des zones de production. De même, vous pouvez configurer des zones distinctes pour différents départements.

Lorsque vous configurez des zones, tenez compte des groupes d'hôtes éventuellement configurés sur le périphérique SAN.

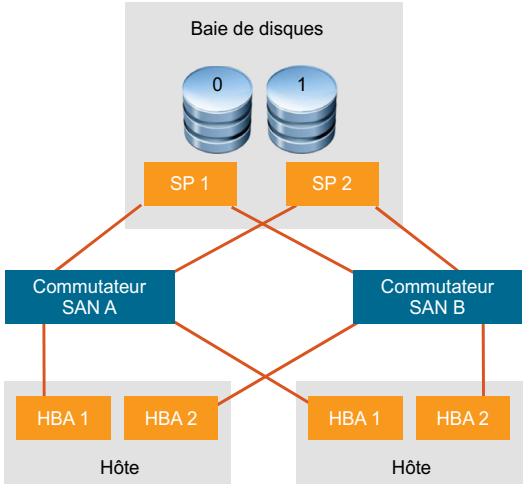
Les fonctionnalités de zonage et de masquage disponibles pour chaque commutateur ou baie de disques SAN, de même que les outils de gestion du masquage de LUN, varient selon les fournisseurs.

Reportez-vous à la documentation du fournisseur de votre solution SAN, ainsi qu'au guide *Stockage vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

6-22 Multipathing avec Fibre Channel

Le multipathing permet de maintenir l'accès aux LUN d'un SAN en cas de défaillance matérielle.

Il assure également l'équilibrage de charge.



Chaque chemin d'accès Fibre Channel décrit un itinéraire :

- qui part d'un port HBA déterminé sur l'hôte,
- qui traverse les commutateurs du fabric et
- qui aboutit à un port de stockage déterminé sur la baie de stockage.

Tout hôte doit disposer de plusieurs chemins pour accéder à un LUN d'une baie de stockage. L'établissement de plusieurs chemins d'accès entre un hôte et un LUN est appelé multipathing.

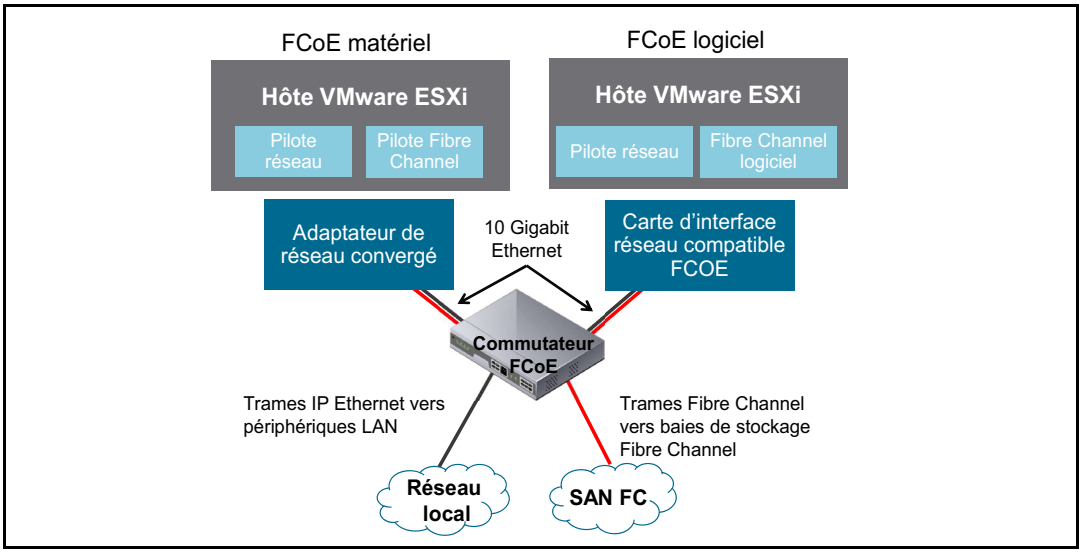
Par défaut, les hôtes VMware ESXi n'utilisent à un moment donné qu'un seul chemin d'accès pour relier un hôte à un LUN déterminé. En cas de panne du chemin d'accès activement utilisé par l'hôte VMware ESXi, le serveur sélectionne l'un des autres chemins disponibles. Le processus consistant à détecter un chemin défaillant puis à en activer un autre est appelé « basculement de chemin d'accès ». Un chemin d'accès est en panne lorsque l'un de ses composants (adaptateur de bus hôte, câble, port de commutateur ou processeur de stockage) est défaillant.

Les baies de disques en mode actif-actif ou actif-passif : Il est utile de bien comprendre la distinction entre les baies de disques en mode actif-actif et en mode actif-passif :

- Une baie de disques en mode actif-actif permet l'accès simultané aux LUN via tous les processeurs de stockage disponibles sans dégradation significative des performances. Tous les chemins d'accès sont actifs à tout moment (excepté en cas de panne d'un chemin).
- Sur une baie de disques en mode actif-passif, chaque LUN est activement desservi par un seul processeur de stockage. Les autres processeurs de stockage jouent le rôle de processeurs de secours pour le LUN, et peuvent éventuellement assurer la desserte active des E/S d'autres

LUN. Les E/S ne peuvent être envoyées qu'à un processeur actif. En cas de défaillance du processeur de stockage principal, l'un des processeurs de stockage secondaires est promu en tant que processeur actif, de manière automatique ou sur intervention de l'administrateur.

6-23 Adaptateurs FCoE



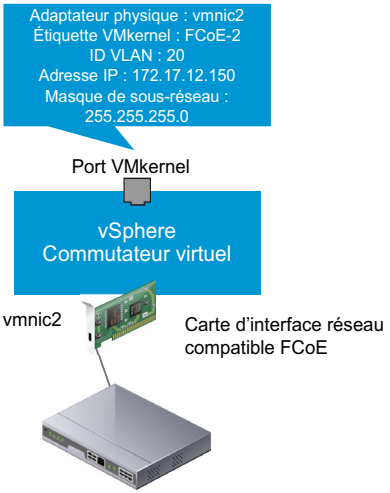
6-24 Configuration d'un FCoE logiciel : La création de ports VMkernel

Étape 1 :

Connectez VMkernel aux cartes d'interface réseau FCoE physiques installées sur votre hôte.

L'ID VLAN et la classe de priorité sont détectés au cours de l'initialisation FCoE. La classe de priorité n'est pas configurée dans vSphere.

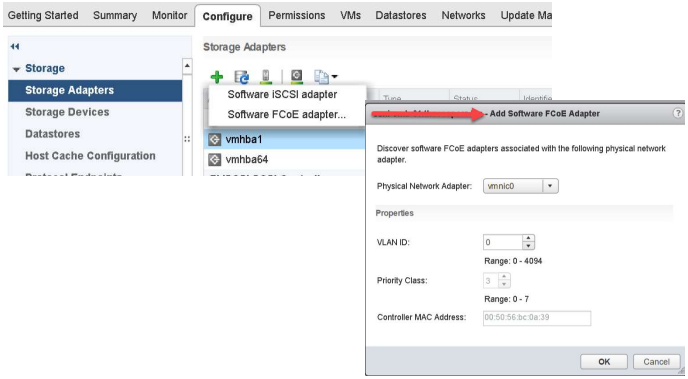
VMware ESXi prend en charge le nombre maximal de quatre ports d'adaptateur réseau utilisés pour le FCoE logiciel.



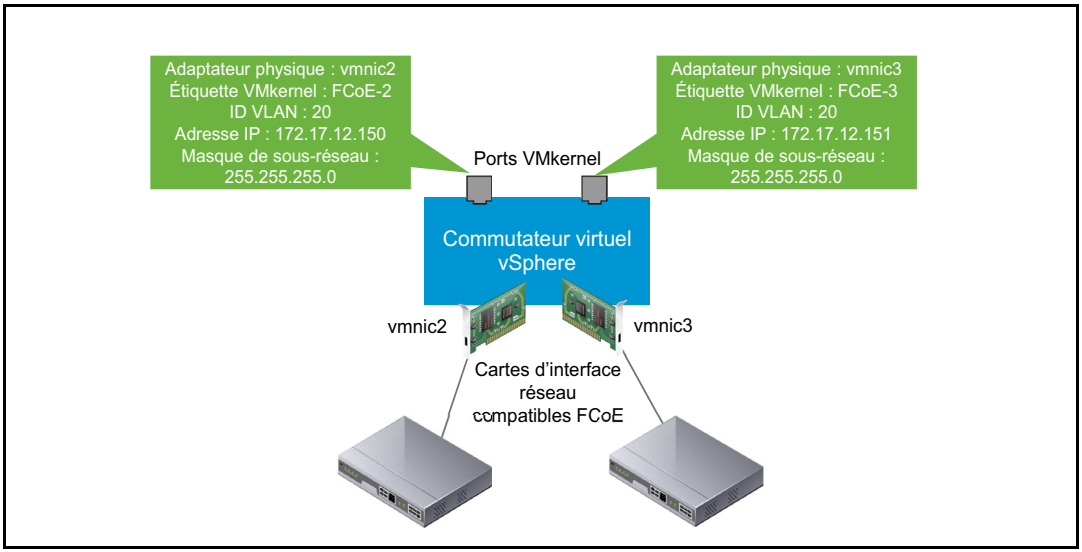
6-25 Configuration d’un FCoE logiciel : l’activation d’adaptateurs FCoE logiciels

Étape 2 :

Ajoutez l’adaptateur FCoE logiciel. Sélectionnez l’hôte, cliquez sur l’onglet **Configure**, sélectionnez **Storage Adapters**, cliquez sur le signe plus vert, sélectionnez **Software FCoE adapter**, puis saisissez les paramètres de configuration appropriés.



6-26 Multipathing avec FCoE logiciel



Le multipathing est une technique permettant d'utiliser plusieurs chemins d'accès physiques pour le transfert de données entre l'hôte et un périphérique de stockage externe.

Pour assurer la commutation de chemins sur un SAN Fibre Channel, un hôte VMware ESXi dispose généralement de deux adaptateurs de bus hôte pour atteindre la baie de stockage via un ou plusieurs commutateurs. La configuration peut également comporter un adaptateur de bus hôte et deux processeurs de stockage, de sorte que l'adaptateur de bus hôte puisse utiliser un chemin alternatif pour accéder à la baie de disques.

Dans le cas du multipathing Fibre Channel, plusieurs chemins relient chaque hôte au périphérique de stockage. Par exemple, en cas de défaillance de l'adaptateur HBA1 ou de la liaison entre celui-ci et le commutateur, l'adaptateur HBA2 prend le relais et assure la connexion entre le serveur et le commutateur. Le processus de bascule entre deux adaptateurs de bus hôte se nomme basculement HBA.

Pour configurer un adaptateur FCoE de type logiciel, vous devez disposer d'un adaptateur VMkernel dédié. L'adaptateur FCoE logiciel transmet les informations de configuration via le protocole Data Center Bridging Exchange (DCBX) en s'appuyant sur le module VMkernel Cisco Discovery Protocol (CDP).

6-27 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les utilisations possibles de la technologie Fibre Channel avec VMware ESXi
- Décrire les composants et l'adressage Fibre Channel
- Expliquer le fonctionnement du multipathing avec Fibre Channel

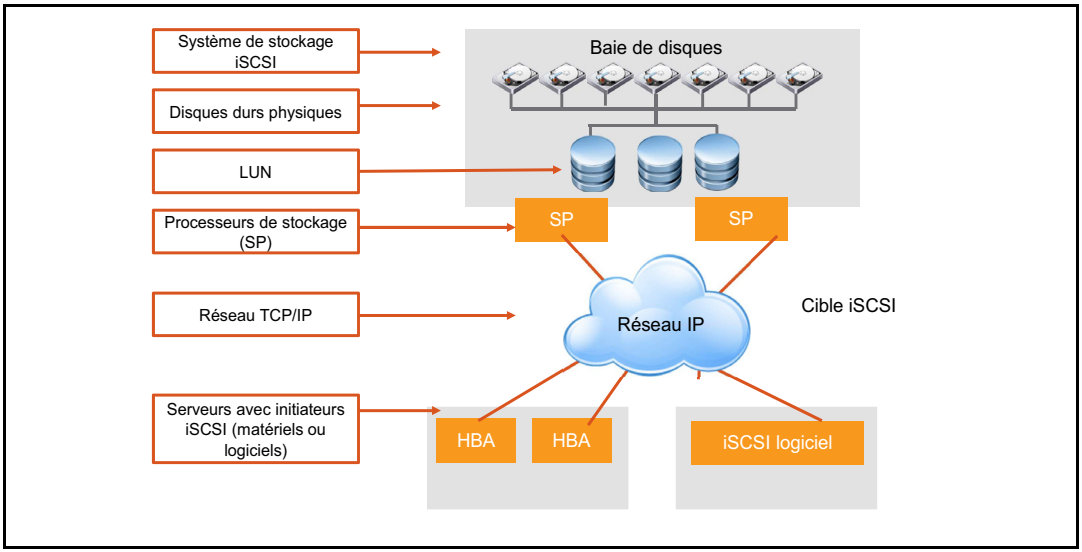
6-28 Leçon 3 : Stockage iSCSI

6-29 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les utilisations possibles du stockage IP avec VMware ESXi
- Décrire les composants et l'adressage iSCSI
- Configurer les initiateurs iSCSI
- Identifier les conventions de nommage des périphériques de stockage

6-30 Composants iSCSI



Un SAN iSCSI correspond à un système de stockage iSCSI, constitué d'une ou plusieurs LUN et d'un ou plusieurs processeurs de stockage (SP). La communication entre l'hôte et la baie de stockage s'effectue via un réseau TCP/IP.

L'hôte VMware ESXi est configuré avec un initiateur iSCSI. Cet initiateur peut être un composant matériel, ou un adaptateur de bus hôte (HBA) iSCSI. Il peut également s'agir d'un composant logiciel, ou un initiateur iSCSI logiciel.

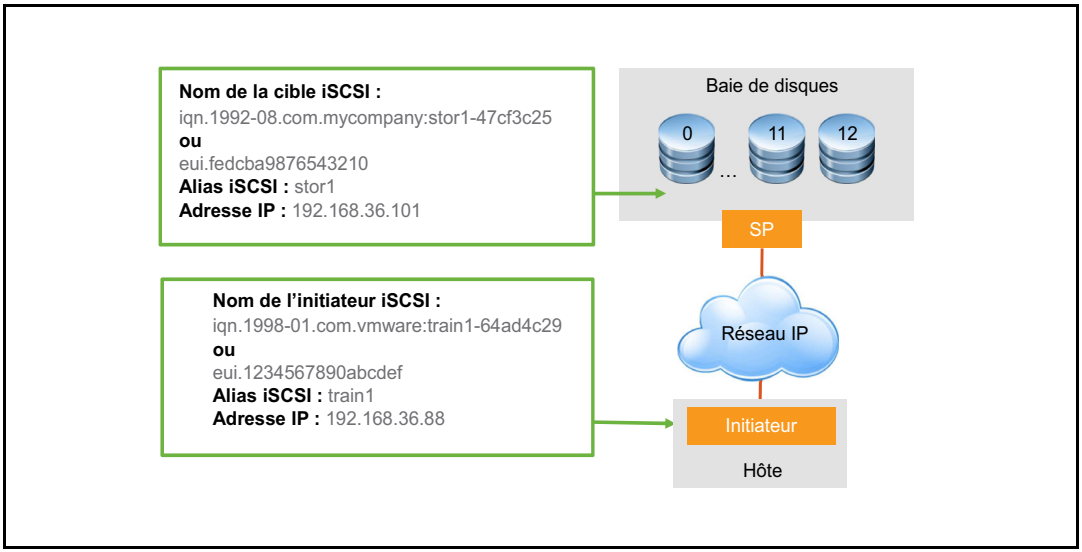
Le rôle de l'initiateur est de transmettre les commandes SCSI via le réseau IP. Une cible reçoit les commandes SCSI transmises par le réseau IP. Votre réseau iSCSI peut comporter plusieurs initiateurs et plusieurs cibles. La technologie iSCSI est orientée SAN dans la mesure où :

- L'initiateur localise une ou plusieurs cibles.
- La cible présente des LUN à l'initiateur.
- L'initiateur envoie des commandes SCSI à une cible.

Un initiateur réside sur l'hôte VMware ESXi. Les cibles résident dans les baies de stockage prises en charge par l'hôte VMware ESXi.

Les baies iSCSI peuvent mettre en œuvre différents dispositifs, tels qu'une adresse IP, sous-réseaux ou authentification, pour restreindre l'accès aux cibles depuis les hôtes.

6-31 Adressage iSCSI



La principale entité adressable et détectable est un nœud iSCSI. Un nœud iSCSI peut être soit un initiateur, soit une cible. Un nœud iSCSI doit être identifié par un nom, de façon à permettre la gestion du stockage indépendamment de l'adresse.

Le nom iSCSI peut emprunter le format IQN (iSCSI Qualified Name) ou le format EUI (Extended Unique Identifier).

Un nom IQN peut comporter jusqu'à 255 caractères. La convention de nommage utilisée est la suivante :

- Le préfixe « iqn »
- Le code de date indiquant l'année et le mois d'enregistrement du nom de domaine ou de sous-domaine utilisé dans la chaîne désignant l'autorité de nommage
- La chaîne désignant l'autorité de nommage, constituée d'un nom de domaine ou de sous-domaine valide énoncé en syntaxe inverse
- (Facultatif) Le signe deux-points (:) suivi d'une chaîne choisie par l'autorité de nommage de telle sorte que chaque nom iSCSI constitue un identifiant univoque

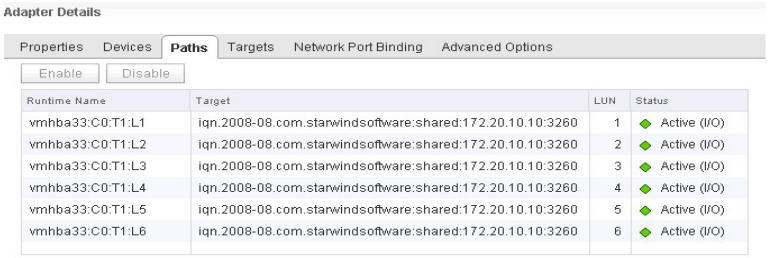
La convention de nommage EUI prévoit les éléments suivants :

- Le préfixe « eui » suivi d'un nom à 16 caractères. Ce nom comprend 24 bits dans le cas d'un nom de société attribué par l'IEEE, et 40 bits dans le cas d'un identifiant unique tel qu'un numéro de série

6-32 Conventions de nommage des périphériques de stockage

Les périphériques de stockage peuvent être identifiés de différentes manières :

- Le nom d'exécution : conforme à la convention vmhbaN:C:T:L. Ce nom n'est pas permanent d'un redémarrage sur l'autre.
- La cible : identifie l'adresse et le port de la cible iSCSI.
- Le LUN : identifiant unique assigné à un ou plusieurs périphériques de disques durs. L'adressage d'une unité logique s'effectue via le protocole SCSI ou via les protocoles SAN encapsulant SCSI, tels qu'iSCSI ou Fibre Channel.



Sur les hôtes VMware ESXi, les périphériques de stockage SCSI utilisent divers identifiants, dont chacun répond à un besoin spécifique. Par exemple, VMkernel requiert un identifiant généré par le périphérique de stockage et garantissant une identification univoque de chaque LUN. Si le périphérique de stockage n'est pas en mesure de le lui fournir, VMkernel doit générer un identifiant unique représentant chaque LUN ou disque.

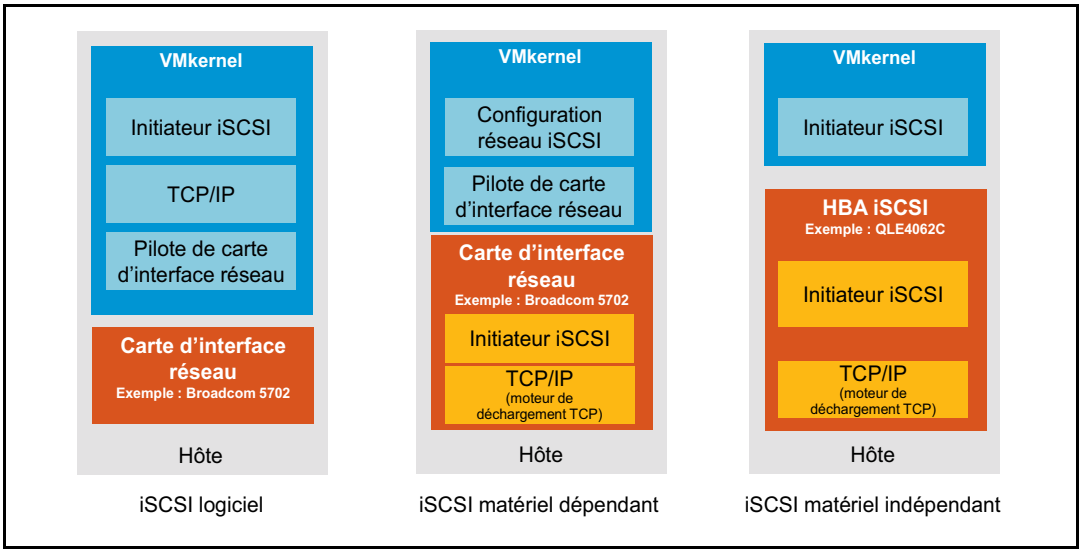
Les identifiants de disque qui apparaissent sur cette diapositive étant difficilement reconnaissables par les utilisateurs, une troisième convention de nommage, plus conviviale, est créée après chaque redémarrage pour désigner chacun des disques. Vous pouvez utiliser ces noms lorsque vous vous servez d'utilitaires de ligne de commande pour interagir avec des ressources de stockage reconnues par un hôte VMware ESXi.

Les identifiants disponibles pour les périphériques de stockage SCSI sont les suivants :

- Le nom d'exécution : Le nom du premier chemin d'accès au périphérique. Le nom d'exécution est créé par l'hôte. Ce nom ne constitue pas un identifiant fiable pour le périphérique dans la mesure où il n'est pas permanent. Le nom d'exécution peut être modifié lorsque vous ajoutez des adaptateurs de bus hôte (HBA) à l'hôte VMware ESXi.
- Le nom iSCSI : Le nom permettant d'identifier le nœud de manière univoque à l'échelle mondiale. iSCSI utilise les formats IQN et EUI. IQN utilise le format suivant : *iqn.aaaa-mm.autorité_de_dénomination:nom_unique*.

Les noms de périphérique de stockage apparaissent dans différents volets de vSphere Web Client et de vSphere Client.

6-33 Adaptateurs iSCSI



Pour accéder aux cibles iSCSI, votre hôte fait appel à des initiateurs iSCSI. Ces initiateurs transportent les demandes et les réponses SCSI, encapsulées dans le protocole iSCSI, entre l'hôte et la cible iSCSI. Votre hôte prend en charge les initiateurs iSCSI de type logiciel et de type matériel.

Un initiateur iSCSI logiciel est constitué de code VMware intégré dans VMkernel. Cet initiateur permet à votre hôte de se connecter au périphérique de stockage iSCSI par l'intermédiaire d'adaptateurs réseau standard. L'initiateur iSCSI logiciel prend en charge le traitement iSCSI lié aux communications avec l'adaptateur réseau. Cet initiateur vous permet d'exploiter la technologie iSCSI sans acheter de matériel spécialisé.

Un initiateur iSCSI matériel est un adaptateur tiers spécialisé capable d'accéder au stockage iSCSI via TCP/IP. Les initiateurs iSCSI matériels existent en deux catégories : dépendants et indépendants.

Un initiateur iSCSI matériel dépendant, ou un adaptateur de bus hôte (HBA) iSCSI, est un adaptateur réseau standard intégrant la fonction de déchargement iSCSI. Pour utiliser ce type d'adaptateur, vous devez configurer les communications réseau pour le trafic iSCSI et lier l'adaptateur à un port iSCSI VMkernel approprié.

Un adaptateur iSCSI matériel indépendant décharge entièrement votre hôte VMware ESXi du traitement et de la gestion iSCSI et réseau.

6-34 Configuration des adaptateurs iSCSI

Vous devez configurer des adaptateurs logiciels ou matériels avant de pouvoir faire fonctionner un hôte ESXi avec un SAN.

Types d'adaptateur iSCSI pris en charge (vmhba) :

- L'adaptateur logiciel
- Les adaptateurs matériels (indépendants ou dépendants)

L'adaptateur iSCSI logiciel utilise des cartes d'interface réseau standard pour connecter l'hôte VMware ESXi à une cible iSCSI distante située sur le réseau IP. Dans ce cas, la configuration réseau VMkernel est requise.

L'adaptateur iSCSI matériel indépendant fourni par un tiers décharge l'hôte VMware ESXi du traitement et de la gestion iSCSI et réseau. Dans ce cas, la configuration réseau VMkernel n'est pas nécessaire.

L'adaptateur iSCSI matériel dépendant fourni par un tiers est tributaire des interfaces de gestion de la mise en réseau et de la configuration iSCSI. Dans ce cas, la configuration réseau VMkernel est requise.

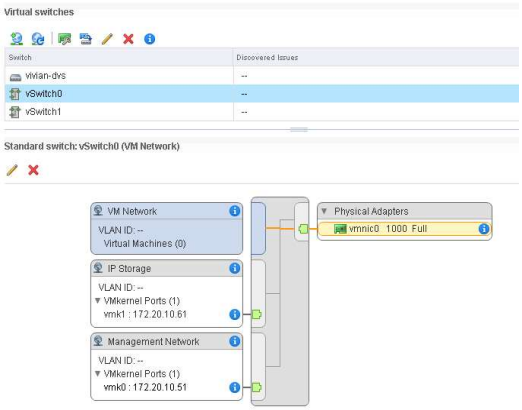
Pour plus d'informations sur la configuration, reportez-vous au guide *Stockage vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

6-35 Configuration réseau de VMware ESXi pour le stockage IP

Vous devez créer un port VMkernel pour que VMware ESXi puisse accéder à l'iSCSI logiciel. Ce même port peut être utilisé pour l'accès au stockage NAS/NFS.

Pour optimiser la configuration réseau de vSphere, séparez les réseaux iSCSI des réseaux NAS/NFS :

- Une séparation physique est préférable.
- Si une séparation physique n'est pas possible, utilisez des VLAN.



La configuration réseau de l'iSCSI logiciel comprend la création d'un port VMkernel destiné au traitement du trafic iSCSI sur un commutateur virtuel.

Différentes configurations réseau sont envisageables, selon le nombre d'adaptateurs physiques que vous souhaitez affecter au trafic iSCSI :

- Si vous n'avez qu'un adaptateur réseau physique, il vous suffit de disposer d'un port VMkernel sur un commutateur virtuel.
- Si vous disposez de plusieurs adaptateurs réseau physiques pour l'iSCSI, ceux-ci peuvent être utilisés pour le multipathing hôte.

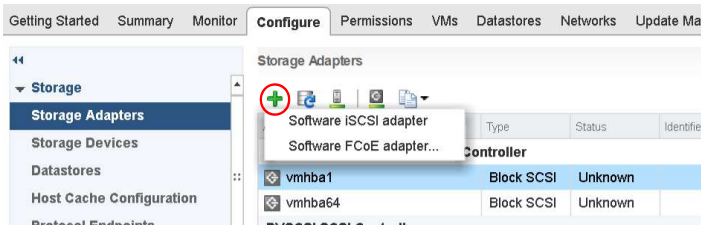
Pour des raisons de performances et de sécurité, il est recommandé d'isoler le réseau iSCSI des autres réseaux. Le mieux est de séparer physiquement ces réseaux. Si cela s'avère impossible, séparez-les logiquement sur le commutateur virtuel en configurant un VLAN distinct pour chaque réseau.

Pour connaître le détail de la procédure de configuration permettant d'ajouter un port VMkernel à un commutateur virtuel, reportez-vous au guide *Stockage vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

6-36 Activation de l'adaptateur iSCSI logiciel

Pour ajouter l'adaptateur iSCSI logiciel :

1. Sélectionnez l'hôte et cliquez sur l'onglet **Configure**.
2. Sélectionnez **Storage Adapters** et cliquez sur le signe plus vert.
3. Sélectionnez **Software iSCSI adapter**.



Vous devez activer votre adaptateur iSCSI logiciel de telle sorte que votre hôte puisse l'utiliser pour accéder au stockage iSCSI.

Vous ne pouvez activer qu'un seul adaptateur iSCSI logiciel

REMARQUES

Si vous démarrez un hôte à partir d'iSCSI via l'adaptateur iSCSI logiciel, l'activation de cet adaptateur et la création de la configuration réseau interviennent lors du premier démarrage. Si vous désactivez cet adaptateur, il est réactivé à chaque nouveau démarrage de l'hôte.

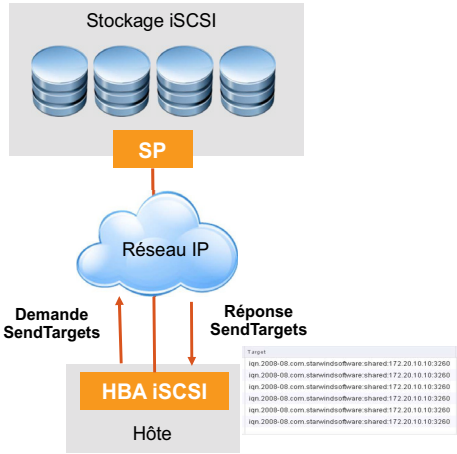
6-37 Détection des cibles iSCSI

L'adaptateur iSCSI détecte les ressources de stockage présentes sur le réseau et détermine celles qui sont accessibles.

Un hôte VMware ESXi prend en charge les méthodes de détection suivantes :

- La méthode statique
- La méthode dynamique, appelée SendTargets

La réponse fournie par SendTargets indique le nom IQN et l'ensemble des adresses IP disponibles.



L'hôte VMware ESXi prend en charge les méthodes suivantes pour la détection des cibles iSCSI :

- La détection statique : l'initiateur n'a aucune opération de détection à effectuer. Il connaît à l'avance toutes les cibles à contacter, et utilise leur adresse IP et leur nom de domaine pour communiquer avec elles.
- La détection dynamique, ou « SendTargets » : chaque fois que l'initiateur contacte un serveur iSCSI spécifié, il envoie à celui-ci une demande SendTargets. Le serveur répond à l'initiateur en lui fournissant la liste des cibles disponibles. Les noms et les adresses IP de ces cibles apparaissent en tant que cibles statiques dans vSphere Client. Vous avez la possibilité de supprimer une cible statique ajoutée par détection dynamique. Si vous supprimez une cible, il se peut qu'elle soit réintroduite dans la liste à la prochaine opération de réanalyse. Cette cible peut également être réintroduite dans la liste en cas de réinitialisation du HBA ou de redémarrage de l'hôte.

6-38 Sécurité iSCSI : l'authentification CHAP

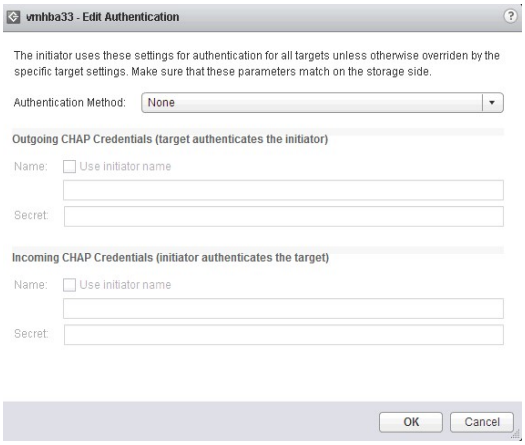
Les initiateurs iSCSI utilisent CHAP à des fins d'authentification.

Par défaut, l'authentification CHAP n'est pas configurée.

VMware ESXi prend en charge deux types d'authentification CHAP :

- CHAP unidirectionnelle
- CHAP bidirectionnelle

VMware ESXi prend également en charge l'authentification CHAP en fonction de la cible.



Vous pouvez mettre en œuvre le protocole CHAP, afin de fournir un mécanisme d'authentification entre les initiateurs et les cibles iSCSI.

VMware ESXi prend en charge les méthodes d'authentification CHAP ci-après :

- CHAP unidirectionnelle : la cible authentifie l'initiateur, mais celui-ci n'authentifie pas la cible. Vous devez indiquer votre secret CHAP pour permettre à vos initiateurs d'accéder à la cible.
- CHAP bidirectionnelle (ou mutuelle) : un niveau de sécurité supplémentaire permet à l'initiateur d'authentifier la cible. Vous devez spécifier des secrets différents pour la cible et pour l'initiateur.

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 prédéfinie, dite secret CHAP, partagée par l'initiateur et par la cible. L'implémentation de CHAP dans VMware ESXi est conforme à la norme RFC 1994.

VMware 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 initiateurs iSCSI logiciels et matériels dépendants, VMware ESXi prend également en charge l'authentification CHAP en fonction de la cible.

Avant de configurer CHAP, vérifiez qu'il est activé dans le système de stockage iSCSI et vérifiez la méthode d'authentification CHAP prise en charge par le système. Si le protocole CHAP est activé dans ce système, activez-le également pour vos initiateurs, en veillant à ce que les informations d'authentification CHAP concordent avec celles du stockage iSCSI. Bien que VMware vous

recommande d'utiliser CHAP dans votre implémentation SAN iSCSI, assurez-vous auprès de votre fournisseur de stockage que les meilleures pratiques sont respectées.

Plusieurs autres méthodes sont à votre disposition pour assurer une protection supplémentaire de vos données. Par exemple, vous pouvez protéger votre SAN iSCSI en lui attribuant un commutateur standard dédié. Vous pouvez également configurer le SAN iSCSI sur son propre VLAN, de façon à améliorer les performances et la sécurité. Enfin, le déploiement de certains périphériques réseau en ligne permet d'assurer le chiffrement et de renforcer la protection des données.

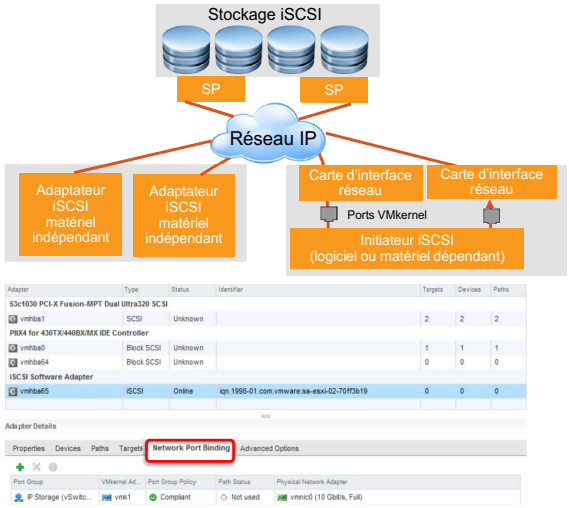
Pour plus d'informations sur la sécurité, consultez le guide *Stockage vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

6-39 Stockage iSCSI et multipathing

Le stockage iSCSI logiciel ou iSCSI matériel dépendant :

- Utilise plusieurs cartes d'interface réseau
- Connecte chaque carte d'interface réseau à un port VMkernel distinct
- Lie les ports VMkernel à l'initiateur iSCSI

L'iSCSI matériel indépendant utilise plusieurs adaptateurs iSCSI matériels.



Lorsque vous configurez votre hôte VMware ESXi pour le multipathing et le basculement, vous avez la possibilité d'utiliser plusieurs adaptateurs iSCSI matériels ou plusieurs cartes d'interface réseau. Ce choix dépend du type des initiateurs iSCSI configurés sur votre hôte.

Avec l'iSCSI logiciel et l'iSCSI matériel dépendant, vous pouvez utiliser plusieurs cartes d'interface réseau pour assurer la protection par basculement des connexions iSCSI entre votre hôte et les systèmes de stockage iSCSI. Pour cette configuration, étant donné que les plug-ins de multipathing n'ont pas un accès direct aux cartes d'interface réseau physiques installées sur votre hôte, vous devez tout d'abord connecter chaque carte d'interface 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 d'interface réseau séparée devient ainsi un chemin distinct utilisable par la pile de stockage iSCSI et son plug-in de multipathing. Pour l'iSCSI matériel dépendant, vérifiez que la carte d'interface réseau physique est correctement installée et apparaît sous l'onglet **Configure** de l'hôte dans la vue **Networking** > **Virtual Switches** .

Dans le cas de l'iSCSI matériel indépendant, l'hôte dispose généralement de plusieurs adaptateurs iSCSI matériels donnant accès au système de stockage via un ou plusieurs commutateurs. Une autre solution consiste à configurer un adaptateur et deux processeurs de stockage, afin que l'adaptateur ait un chemin distinct à sa disposition pour atteindre le système de stockage.

Une fois le multipathing iSCSI configuré, chacun des ports du système VMware ESXi dispose de sa propre adresse IP, mais tous partagent le même IQN d'initiateur iSCSI. Lorsque le multipathing iSCSI est configuré, la table de routage VMkernel n'est pas consultée pour l'identification de la carte d'interface réseau sortante à utiliser : ce sont les modules de multipathing

de vSphere qui sont utilisés pour la gestion du multipathing iSCSI. VMware ne recommande pas le routage du trafic iSCSI en raison de la latence qui pourrait en résulter. Pour en savoir plus sur la configuration du multipathing iSCSI, reportez-vous au guide *Stockage vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

6-40 Laboratoire 5 : Accès au stockage iSCSI

Configurer l'accès à une banque de données iSCSI

1. Vérifier la configuration iSCSI d'un hôte VMware ESXi
2. Ajouter un groupe de ports VMkernel à un commutateur standard
3. Configurer l'adaptateur iSCSI logiciel
4. Connecter les adaptateurs iSCSI logiciels au stockage

6-41 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les utilisations possibles du stockage IP avec VMware ESXi
- Décrire les composants et l'adressage iSCSI
- Configurer les initiateurs iSCSI
- Identifier les conventions de nommage des périphériques de stockage

6-42 Leçon 4 : Banques de données VMFS

6-43 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Créer une banque de données VMFS
- Expliquer les mécanismes de verrouillage VMFS
- Augmenter la taille d'une banque de données VMFS
- Supprimer une banque de données VMFS

6-44 Utiliser des banques de données avec des hôtes VMware ESXi

Utilisez des banques de données VMFS ou vSphere Virtual Volumes pour l'accès au stockage de niveau bloc :

- VMFS est optimisé pour le stockage de fichiers volumineux et pour l'accès à de tels fichiers.
- Une banque de données VMFS peut accueillir des volumes d'une taille maximale de 64 To.
- vSphere Virtual Volumes est capable d'utiliser des services de stockage avancés, qui incluent des fonctions de réplication, de chiffrement, de déduplication et de compression sur des disques virtuels individuels.
- vSphere Virtual Volumes prend en charge des fonctionnalités vSphere telles que VMware vSphere® vMotion™, vSphere Storage vMotion, snapshots, clones liés, Flash Read Cache et vSphere DRS.

Utilisez des RDM si votre machine virtuelle vérifie l'une des conditions suivantes :

- Cette VM prend des snapshots au niveau de la baie de stockage.
- Elle est configurée en cluster avec une machine physique.
- Elle héberge de grandes quantités de données que vous ne souhaitez pas convertir en disque virtuel.

Les banques de données VMFS sont principalement utilisées comme référentiels pour les fichiers des machines virtuelles. Les banques de données VMFS sont optimisées pour le stockage de grands fichiers, tels que disques virtuels ou images mémoire de machines virtuelles interrompues, ainsi que pour l'accès à ces fichiers. La taille maximale d'une banque de données VMFS est de 64 To.

Une banque de données Virtual Volumes correspond à un conteneur de stockage de vCenter Server ou de vSphere Web Client. Du point de vue d'un administrateur vSphere, la banque de données Virtual Volumes est une banque de données comme une autre permettant d'accueillir des machines virtuelles. La capacité de la banque de données Virtual Volumes peut être configurée par l'administrateur de stockage en dehors de vSphere.

Vous pouvez utiliser une banque de données NFS pour stocker vos machines virtuelles, vos modèles et vos images ISO, sachant que certaines fonctionnalités ne sont pas prises en charge. Par exemple, vous ne pouvez pas stocker un mappage de périphériques bruts (RDM) dans une banque de données NFS. Le stockage des fichiers de mappage RDM (`-*-rdm.vmdk`) requiert obligatoirement une banque de données VMFS.

Optez pour des RDM de préférence à des banques de données VMFS dans les situations suivantes :

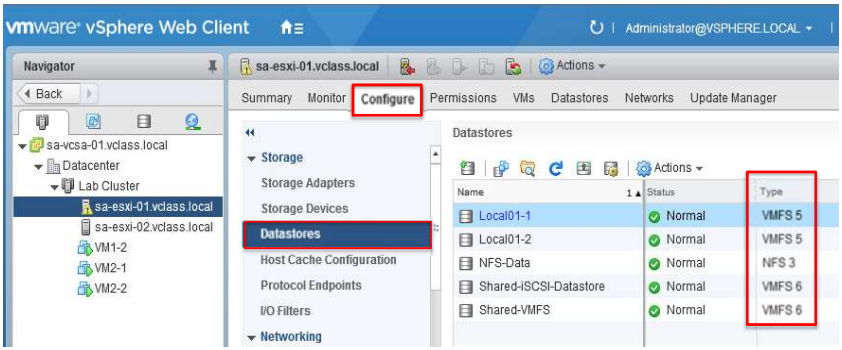
- Une machine virtuelle utilise des applications de snapshot exécutées au niveau de la baie de stockage.
- Une machine virtuelle est mise en cluster avec une machine physique.

- Vous souhaitez maintenir les données d'une machine virtuelle sur un disque brut plutôt que les convertir en disque virtuel – par exemple, parce que le disque de données est très volumineux.

6-45 Création et affichage des banques de données VMFS

Les banques de données VMFS sont utilisées comme référentiels pour les machines virtuelles.

L'assistant « New Datastore » vous permet de créer des banques de données VMFS sur n'importe quel périphérique de stockage SCSI détecté par l'hôte, y compris les périphériques de type Fibre Channel, iSCSI ou local.



L'affichage des banques de données vous permet de savoir quel type de banques de données vous utilisez – par exemple, NFS, VMFS ou un autre type de banque de données.

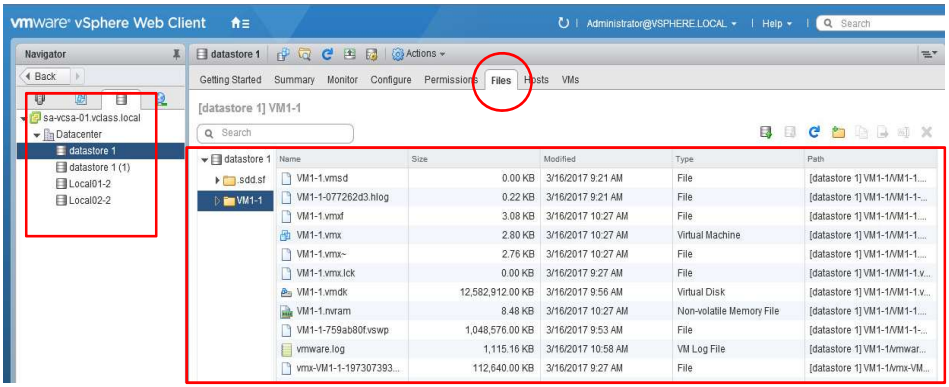
Le mécanisme ATS+SCSI : Une banque de données VMFS qui prend en charge le verrouillage ATS+SCSI est configurée pour tirer parti du mécanisme ATS et tente d'utiliser celui-ci lorsque c'est possible. En cas d'échec du verrouillage ATS, la banque de données VMFS se rabat sur les réservations SCSI. Contrairement au verrouillage ATS, les réservations SCSI verrouillent entièrement le périphérique de stockage durant l'exécution d'une opération nécessitant la protection des métadonnées. Une fois cette opération terminée, VMFS lève la réservation et les autres opérations peuvent reprendre leur cours.

Les banques de données qui utilisent le mécanisme ATS+SCSI comprennent notamment les banques de données VMFS5 issues d'une mise à niveau à partir de VMFS3. Les nouvelles banques de données VMFS5 ou VMFS6 déployées sur des périphériques non compatibles ATS exploitent également le mécanisme ATS+SCSI.

Si votre banque de données VMFS se rabat sur les réservations SCSI, vous constaterez une dégradation des performances liée à la portée excessive des réservations SCSI. Pour plus d'informations sur la réduction des réservations SCSI, consultez le document *Dépannage vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

6-46 Exploration du contenu des banques de données

Le navigateur de fichiers de banque de données vous permet de gérer le contenu de vos banques de données.



Le volet « Datastores » vous présente les banques de données qui sont disponibles dans de nombreuses vues. Cet onglet répertorie toutes les banques de données actuellement configurées pour l'hôte VMware ESXi.

Cet exemple présente le contenu de la banque de données VMFS nommée datastore1, c'est-à-dire les dossiers des machines virtuelles. Les fichiers de chaque machine virtuelle apparaissent dans le dossier de machine virtuelle correspondant.

6-47 Gestion des banques de données surprovisionnées

Une banque de données est surprovisionnée lorsque l'espace total provisionné pour les disques à provisionnement fin excède la taille de cette banque de données.

Surveillez activement la capacité de votre banque de données :

- Appuyez-vous sur les notifications émises par les alertes :
  - La surallocation des disques de la banque de données
  - L'utilisation des disques de machine virtuelle
- Recourez au reporting pour visualiser l'utilisation de l'espace.

Gérez activement la capacité de votre banque de données :

- Augmentez la capacité de la banque de données en cas de besoin.
- Faites appel à vSphere Storage vMotion pour limiter les problèmes d'utilisation de l'espace sur une banque de données donnée.

Le provisionnement fin des disques virtuels des machines virtuelles est un moyen d'optimiser la capacité d'une banque de données. Cette banque de données risque cependant d'être surprovisionnée si elle n'a pas été dimensionnée correctement. Il y a surprovisionnement lorsque la capacité totale des disques virtuels à provisionnement fin est supérieure à celle de la banque de données. Une bonne gestion de la capacité des disques permettra à l'administrateur vSphere d'éviter de se trouver à court d'espace en dépit des problématiques externes d'ordre budgétaire ou autre.

Lorsque la pleine capacité d'une banque de données est atteinte, vSphere Web Client vous invite à augmenter l'espace disponible dans la banque de données VMFS sous-jacente, et gèle la capacité des machines virtuelles jusqu'à ce que vous ayez fait le nécessaire. Vous devez surveiller la capacité de votre banque de données à l'aide d'alertes indiquant dans quelle mesure les disques d'une banque de données sont suralloués, ou quelle est la quantité d'espace disque consommée par une machine virtuelle.

Gérez la capacité de votre banque de données. Augmentez dynamiquement la taille de votre banque de données selon les besoins. Vous pouvez également faire appel à vSphere Storage vMotion pour limiter les problèmes liés à l'utilisation de l'espace disque. Par exemple, vSphere Storage vMotion vous permet de délester une banque de données en migrant une machine virtuelle vers une autre banque de données. Une telle migration peut s'accompagner du remplacement du format définitif par le format fin pour les disques virtuels de la banque de données cible.

6-48 Augmentation de la taille des banques de données VMFS

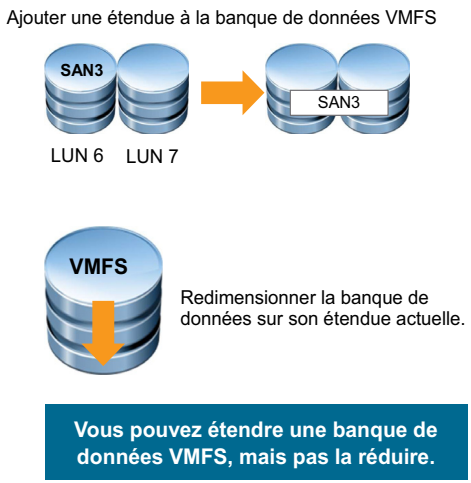
De façon générale, avant de modifier l'allocation du stockage :

- Relancez une analyse pour vous assurer que tous les hôtes ont accès à la vue actuelle du stockage.
- Notez l'identifiant unique.

Augmentez la taille d'une banque de données VMFS afin d'étendre l'espace disponible ou, dans certains cas, d'améliorer ses performances.

Les deux façons d'augmenter dynamiquement la taille d'une banque de données VMFS :

- Ajouter une étendue (LUN)
- Redimensionner la banque de données sur son étendue actuelle



Vous pouvez étendre une banque de données VMFS, mais pas la réduire.

De façon générale, avant de modifier l'allocation du stockage, il est recommandé de relancer une analyse pour s'assurer que tous les hôtes ont accès à la vue actuelle du stockage. Prenez également soin de noter l'identifiant unique du volume à étendre – par exemple, son identifiant NAA. Cette information vous est indispensable pour identifier la banque de données VMFS dont vous souhaitez augmenter la taille.

Vous pouvez augmenter dynamiquement la capacité des banques de données VMFS présentant un espace disque insuffisant. Un manque d'espace disque peut apparaître lorsque vous créez une machine virtuelle ou tentez d'ajouter de l'espace disque à une machine virtuelle existante.

Recourez à l'une des méthodes suivantes :

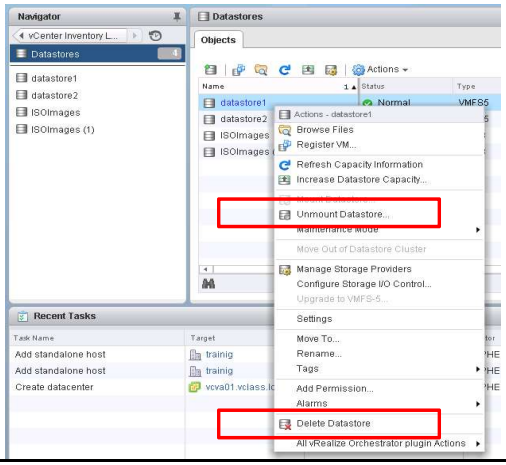
- Ajouter une étendue à la banque de données VMFS : une étendue correspond à une partition d'un LUN. Vous pouvez ajouter des étendues à n'importe quelle banque de données VMFS, dans la limite de 32 étendues.
- Étendre la banque de données VMFS : augmentez la taille de la banque de données VMFS sur son étendue actuelle. Seules les étendues immédiatement suivies d'espace libre sont extensibles. Plutôt que d'ajouter une nouvelle étendue, vous pouvez par conséquent augmenter la taille d'une étendue existante de façon à remplir la capacité adjacente disponible.

Pour plus d'informations sur le redimensionnement ou l'extension d'un volume ou d'une banque de données VMFS, consultez l'article 1017662 de la base de connaissances VMware, disponible à l'adresse suivante : http://kb.vmware.com/kb/1017662.

6-49 Suppression ou démontage de banques de données VMFS

Les banques de données que vous démontez restent intactes, mais elles ne sont plus visibles depuis les hôtes que vous spécifiez. Elles restent toutefois visibles sur les hôtes où elles sont toujours montées.

Une banque de données supprimée est détruite et disparaît de tous les hôtes qui y ont accès. Toutes les machines virtuelles présentes sur cette banque de données sont définitivement supprimées.



Les banques de données que vous démontez restent intactes, mais elles ne sont plus visibles depuis les hôtes que vous spécifiez. Le démontage d'une banque de données VMFS conserve les fichiers au sein de cette banque de données mais rend celle-ci inaccessible à l'hôte VMware ESXi. Cette banque de données reste visible et continue à desservir les autres hôtes sur lesquels elle est toujours montée. N'effectuez aucune opération de configuration pouvant entraîner des E/S avec une banque de données en cours de démontage.

Vous pouvez supprimer n'importe quel type de banque de données VMFS, y compris les copies que vous avez montées sans nouvelle signature. Lorsque vous supprimez une banque de données, celle-ci est définitivement détruite et disparaît de tous les hôtes qui y ont accès. Cette opération supprime de façon définitive l'ensemble des fichiers associés aux machines virtuelles hébergées dans la banque de données. Bien qu'il soit possible de supprimer une banque de données sans la démonter, il est préférable de commencer par le démontage de la banque de données. La suppression d'une banque de données VMFS détruit les pointeurs référençant les fichiers stockés dans la banque de données, de sorte que ces fichiers disparaissent de tous les hôtes qui y ont accès.

Avant de supprimer ou de démonter une banque de données VMFS, vous devez arrêter toutes les machines virtuelles dont les disques résident dans cette banque de données. Si vous tentez de poursuivre l'opération sans avoir mis les machines virtuelles hors tension, un message d'erreur vous signale que la ressource est occupée. Avant de démonter une banque de données VMFS, recourez à vSphere Web Client pour vérifier les points suivants :

- Aucune machine virtuelle ne réside sur la banque de données.
- La banque de données ne fait pas partie d'un cluster de banques de données.
- La banque de données n'est pas gérée par VMware vSphere® Storage DRS™.
- La fonctionnalité VMware vSphere® Storage I/O Control est désactivée.

- La banque de données n’est pas utilisée pour les signaux de pulsation vSphere HA.

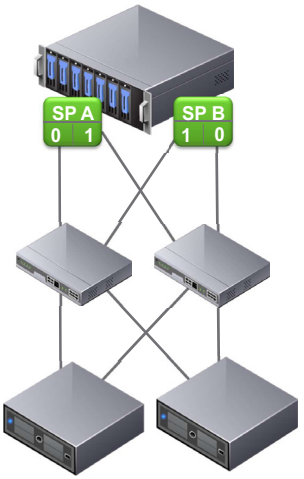
Pour conserver vos données, sauvegardez le contenu de la banque de données VMFS avant de supprimer celle-ci.

6-50 Algorithmes de multipathing

Les fonctionnalités offertes par les baies sont très diverses. Certaines offrent des processeurs de stockage (SP) en mode actif-actif. D'autres présentent des processeurs de stockage en mode passif-passif.

vSphere fournit des mécanismes natifs de sélection de chemin, d'équilibrage de charge et de basculement.

Les fournisseurs tiers ont la possibilité de créer leur propre logiciel pour installation sur les hôtes VMware ESXi. Ce logiciel tiers permet aux hôtes d'interagir correctement avec les baies de stockage.



Baie de stockage

Processeurs de stockage (SP)

Commutateurs

Hôtes VMware ESXi.

L'architecture PSA (Pluggable Storage Architecture) est une couche de VMkernel responsable de la gestion des liens de stockage multiples et de l'équilibrage de charge. Pour sa connexion aux baies de stockage, un hôte VMware ESXi prend en charge ces deux modes de configuration du processeur de stockage :

- Actif-actif
- Actif-passif

VMware offre des mécanismes natifs d'équilibrage de charge et de basculement. Les règles de sélection de chemin fournies par VMware incluent notamment :

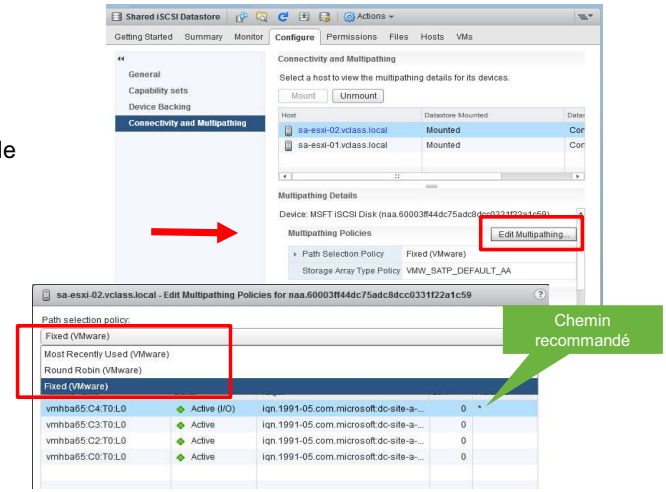
- Round Robin
- Most Recently Used (MRU)
- Fixed

Les fournisseurs tiers ont également la possibilité de concevoir leurs propres techniques d'équilibrage de charge et mécanismes de basculement adaptés à certains types de baie, de façon à permettre la prise en charge de nouvelles baies. Les fournisseurs tiers ne sont pas tenus de divulguer à VMware des informations internes ou des éléments de propriété intellectuelle relatifs à la baie.

6-51 Configuration de l'équilibrage de la charge de stockage

Les règles de sélection de chemin visent deux objectifs principaux :

- L'évolutivité :
  - Round Robin : La règle de multipathing assurant l'équilibrage de charge entre les différents chemins
- La disponibilité :
  - Most Recently Used (MRU)
  - Fixed



Un hôte VMware ESXi peut disposer de plusieurs chemins vers une même banque de données. Vous pouvez afficher ces chemins dans les propriétés de la banque de données en cliquant sur l'onglet **Manage**, puis sur l'onglet **Settings**.

Les règles de sélection de chemin prises en charge pour le multipathing avec Fibre Channel ou iSCSI sont les suivantes :

- La règle de sélection de chemin « Fixed » : l'hôte utilise systématiquement le chemin préféré pour l'accès au disque dès lors que ce chemin est disponible. Si l'hôte ne peut pas accéder au disque via le chemin préféré, il tente d'utiliser les chemins alternatifs. Il s'agit de la règle activée par défaut pour les périphériques de stockage en mode actif-actif.
- La règle de sélection de chemin « Most Recent Used » (MRU) : l'hôte utilise le chemin d'accès le plus récent pour accéder au disque, jusqu'à ce que ce chemin devienne indisponible. Autrement dit, l'hôte ne revient sur sa sélection que si le chemin n'est plus disponible, auquel cas il procède à un basculement vers un nouveau chemin. Si le chemin initial redevient disponible, l'hôte ne rebascule pas sur ce chemin. La règle « Most Recent Used (MRU) » est celle qui est activée par défaut pour les périphériques de stockage en mode actif-passif, avec lesquels elle est obligatoire.
- La règle de sélection de chemin « Round Robin » : l'hôte utilise un algorithme de sélection de chemin déterminant une rotation sur l'ensemble des chemins disponibles. Outre le basculement d'un chemin à un autre, la règle « Round Robin » assure un équilibrage de charge entre les différents chemins. Avant d'utiliser cette règle, vérifiez auprès des fournisseurs de stockage que la configuration Round Robin est prise en charge sur leurs systèmes de stockage.

6-52 Laboratoire 6 : Gestion des banques de données VMFS

Créer et gérer des banques de données VMFS

1. Créer des banques de données VMFS pour l'hôte VMware ESXi
2. Étendre une banque de données VMFS pour tirer parti de l'espace inutilisé sur un LUN
3. Supprimer une banque de données VMFS
4. Étendre une banque de données VMFS
5. Créer une seconde banque de données VMFS via iSCSI

6-53 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Créer une banque de données VMFS
- Expliquer les mécanismes de verrouillage VMFS
- Augmenter la taille d'une banque de données VMFS
- Supprimer une banque de données VMFS

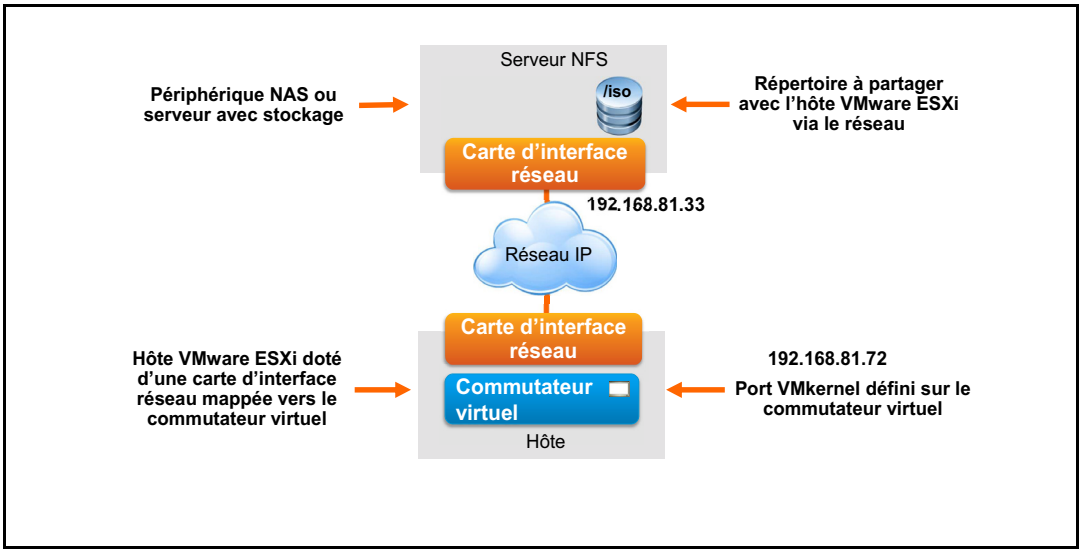
6-54 Leçon 5 : Banques de données NFS

6-55 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d’atteindre les objectifs suivants :

- Décrire les composants NFS
- Expliquer les différences entre NFS v3 et NFS v4.1
- Créer et gérer des banques de données NFS.

6-56 Composants NFS



Un système de fichiers NFS réside sur un périphérique NAS appelé « serveur NFS ». Le serveur NFS contient un ou plusieurs répertoires partagés avec l'hôte VMware ESXi via un réseau TCP/IP. Un hôte VMware ESXi accède au serveur NFS via un port VMkernel défini sur un commutateur virtuel.

6-57 Configuration des banques de données NFS

Créez un port VMkernel :

- Pour des performances et une sécurité optimales, séparez votre réseau NFS du réseau iSCSI.

Fournissez les informations suivantes :

- La version de NFS : v3 ou v4.1
- Le nom de la banque de données
- Les noms ou les adresses IP des serveurs NFS
- Le dossier sur le serveur NFS – par exemple : `/templates` ou `/nfs_share`
- Les hôtes appelés à monter la banque de données
- L'option indiquant si le système de fichiers NFS doit ou non être monté en lecture seule
- Les paramètres d'authentification

Afin que chaque hôte ESXi puisse accéder à une banque de données NFS via le réseau, il convient de configurer un port VMkernel sur un commutateur virtuel. Le choix du nom de ce port est entièrement libre. Pour des raisons de performances et de sécurité, il est recommandé d'isoler le réseau NFS des autres réseaux, tels que votre réseau iSCSI et vos réseaux de machines virtuelles.

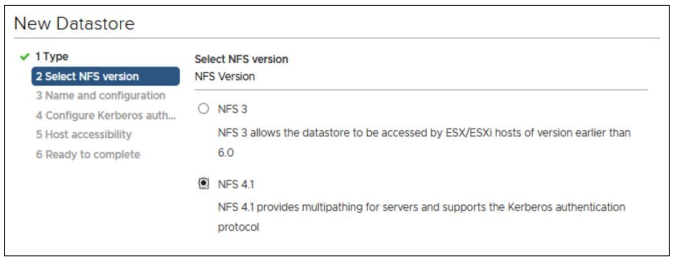
6-58 NFS v3 et NFS v4.1

NFS v3 :

- Le multipathing géré VMware ESXi
- L'authentification AUTH_SYS (root)
- Le mécanisme de verrouillage de fichiers propriétaire de VMware
- Suivi des erreurs côté client

NFS v4.1 :

- Le multipathing natif et la jonction de sessions
- L'authentification Kerberos facultative
- Le mécanisme de verrouillage de fichier intégré
- Suivi des erreurs côté serveur



Les banques de données NFS que vous créez peuvent être en NFS v3 ou en NFS v4.1. En raison de divers problèmes de compatibilité entre les deux versions de NFS, il n'est pas possible d'accéder aux banques de données depuis des hôtes distincts en utilisant simultanément les deux protocoles. Si une banque de données est configurée en NFS v4.1, tous les hôtes qui accèdent à cette banque de données doivent obligatoirement monter le partage en NFS 4.1. L'accès à une banque de données par un hôte utilisant une version erronée de NFS peut entraîner la corruption des données.

À compter de vSphere 6.5, NFS v4.1 n'est plus compatible avec vSphere Storage DRS, VMware vSphere® Storage I/O Control et VMware Site Recovery Manager™ en raison du verrouillage de protocole serveur.

6-59 Compatibilité des versions de NFS avec les autres technologies vSphere

	NFS v3	NFS v4.1
vSphere vMotion et vSphere Storage vMotion	Oui	Oui
vSphere HA	Oui	Oui
vSphere Fault Tolerance	Oui	Oui
vSphere DRS et vSphere DPM	Oui	Oui
VMware ESXi sans état et Host Profiles	Oui	Oui
vSphere Storage DRS et Storage I/O Control	Oui	Non
Site Recovery Manager	Oui	Non
vSphere Virtual Volumes	Oui	Oui

vSphere 6.x prend en charge la version 4.1 de NFS, conçue pour surmonter nombre des restrictions liées à l'utilisation de NFS v3. vSphere 6.x permet l'utilisation conjointe de partages NFS v3 et NFS v4.1, sachant toutefois que de fortes contraintes s'appliquent à la conception d'un environnement vSphere associant ces deux versions.

NFS v4.1 apporte les améliorations suivantes :

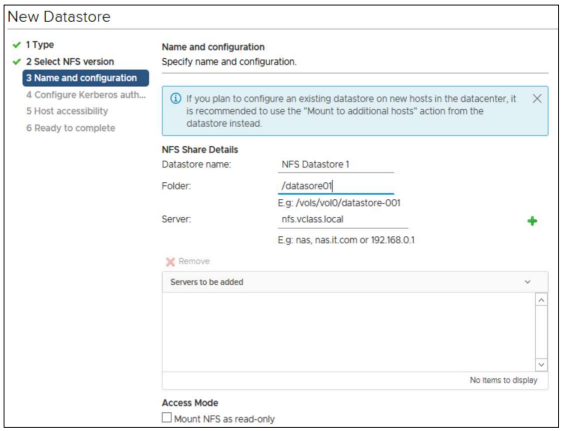
- Le multipathing natif et la jonction de sessions : NFS v4.1 assure le multipathing pour les serveurs prenant en charge la jonction de sessions. Lorsque la jonction de sessions est disponible, vous pouvez utiliser plusieurs adresses IP pour accéder à un même volume NFS. La jonction d'ID de client n'est pas prise en charge.
- L'authentification Kerberos : NFS v4.1 introduit l'authentification Kerberos en complément de la méthode AUTH_SYS traditionnellement utilisée par NFS v3.
- L'amélioration du mécanisme de verrouillage de fichier intégré.
- Les reprise après sinistre améliorée grâce au suivi des fichiers ouverts et des délégations côté serveur.
- Les nombreux gains d'efficience d'ordre général, dont les baux de session et la réduction de la surcharge liée au protocole.

Le client NFS v4.1 présente les nouvelles fonctionnalités ci-après :

- Les verrous à état avec réservation de partage selon une sémantique de verrouillage obligatoire
- L'intégration du protocole : plus besoin de recourir à un protocole de bande latérale (auxiliaire) pour le verrouillage et le montage
- La jonction de sessions (vrai multipathing NFS), avec possibilité de création de plusieurs chemins (sessions) vers la baie NAS et de répartition de la charge entre ces sessions
- La reprise après sinistre améliorée en vue de limiter les pannes serveur et la perte de connectivité

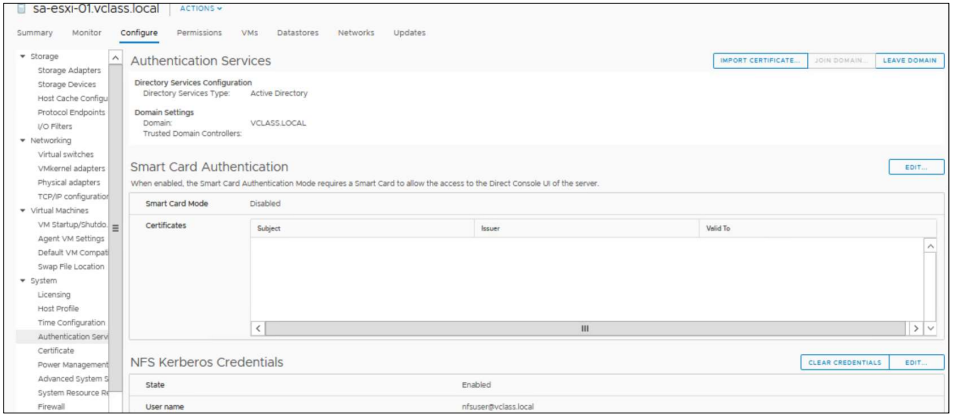
6-60 Nom et configuration d'une banque de données NFS

Vous allez affecter un nom à la banque de données NFS et modifier les paramètres de banque de données.



6-61 Configuration de l'authentification et des informations d'authentification NFS Kerberos des hôtes VMware ESXi

Conformément aux exigences liées à l'authentification Kerberos, commencez par ajouter chacun des hôtes VMware ESXi au domaine AD. Configurez ensuite les informations d'authentification NFS Kerberos.



Chaque hôte VMware ESXi doit être ajouté au domaine Active Directory.

Plusieurs étapes de configuration doivent être effectuées pour préparer chacun des hôtes VMware ESXi à l'utilisation de l'authentification Kerberos. L'authentification Kerberos présuppose la synchronisation de tous les nœuds concernés (le serveur Active Directory, les serveurs NFS et les hôtes VMware ESXi), de telle sorte que l'écart temporel entre ces nœuds soit minime ou nul. Tout écart significatif entre les nœuds entraîne l'échec de l'authentification Kerberos. Pour préparer votre hôte VMware ESXi à l'utilisation de l'authentification Kerberos, configurez les paramètres du client NTP de sorte qu'ils fassent référence à un serveur NTP commun (ou, le cas échéant, au contrôleur de domaine).

Les administrateurs qui envisagent l'utilisation de NFS Kerberos doivent tenir compte de ce qui suit :

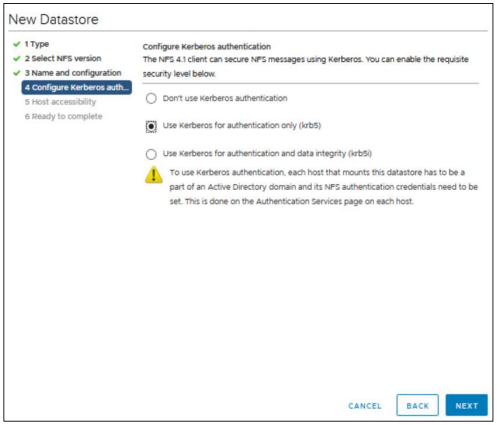
- NFS v3 et NFS v4.1 n'utilisent pas les mêmes informations d'authentification, ce qui les amène à configurer des identifiants UID/GID incompatibles sur les fichiers.
- L'utilisation de comptes d'utilisateur Active Directory différents sur des hôtes distincts accédant au même partage NFS peut faire échouer la migration via vSphere vMotion.
- Il est possible d'automatiser la configuration de NFS Kerberos via Host Profiles de façon à réduire les conflits de configuration.

Il est nécessaire de synchroniser les horloges de tous les composants impliqués.

6-62 Configuration des banques de données pour l'utilisation de Kerberos

Vous devez activer l'authentification Kerberos lors de la création de chaque nouvelle banque de données, avant de sélectionner le mode de sécurité :

- L'authentification Kerberos 5
- L'authentification Kerberos 5i et l'intégrité des données



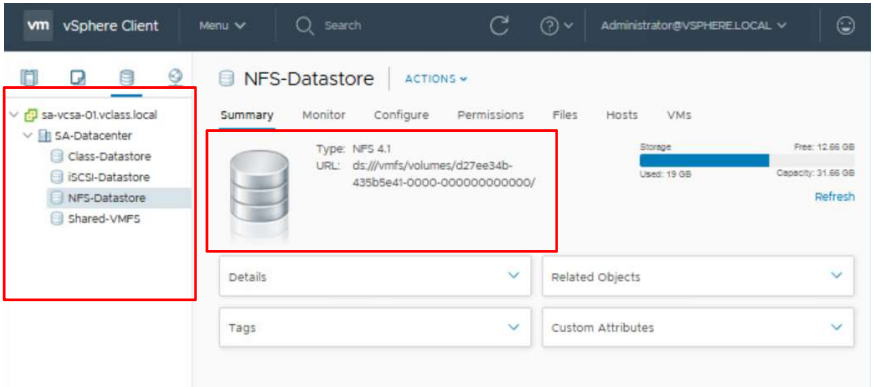
Une fois les étapes de configuration menées à bien, vous pouvez configurer la banque de données pour l'utilisation de l'authentification Kerberos.

La capture d'écran présente le choix entre l'authentification Kerberos seule (krb5) et l'authentification avec intégrité des données (krb5i). Selon l'option retenue, c'est l'en-tête seul ou l'en-tête et le corps de chaque opération NFS qui seront signés à l'aide d'un total de contrôle sécurisé.

Pour plus d'informations sur la configuration des hôtes VMware ESXi hosts pour l'authentification Kerberos, voir https://docs.vmware.com/fr/VMware-vSphere/6.7/com.vmware.vsphere.storage.doc/GUID-BDCB7500-72EC-4B6B-9574-CFAEAF95AE81.html.

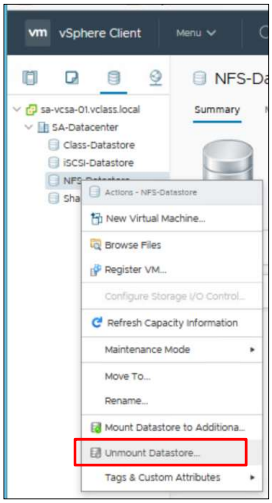
6-63 Affichage d’informations relatives au stockage IP

Vous pouvez afficher les détails des banques de données VMFS ou NFS que vous avez créées.



6-64 Démontage des banques de données NFS

Le démontage d'une banque de données NFS rend les fichiers stockés dans celle-ci inaccessibles pour l'hôte VMware ESXi.

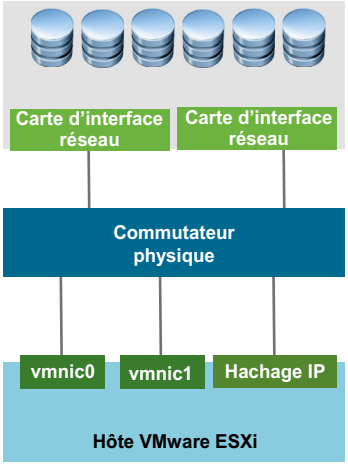


Lorsque vous démontez une banque de données NFS, les fichiers stockés dans celle-ci deviennent inaccessibles pour l'hôte VMware ESXi. Avant de démonter une banque de données NFS, vous devez arrêter toutes les machines virtuelles dont les disques résident dans cette banque de données.

6-65 Multipathing et stockage NFS

Exemple de configuration pour le multipathing NFS :

- Configurez un port VMkernel.
- Pour configurer une association de cartes d'interface réseau, utilisez des adaptateurs connectés à un même commutateur physique.
- Configurez le serveur NFS avec plusieurs adresses IP. Ces adresses IP peuvent se trouver sur un même sous-réseau.
- Pour utiliser efficacement plusieurs liens, configurez les associations de cartes d'interface réseau avec la règle d'équilibrage de charge avec hachage IP.



Lors de la création d'une architecture NAS à haute disponibilité, vous devez éviter tout point unitaire de panne, tel qu'une carte d'interface réseau unique installée sur un hôte VMware ESXi, ou le câble reliant cette carte au commutateur. Cette diapositive présente un exemple de point unique de panne. Pour éviter les points unitaires de panne en vue de créer une architecture NAS à haute disponibilité, il convient de configurer l'hôte VMware ESXi avec des cartes d'interface réseau et des commutateurs physiques redondants.

La meilleure méthode consiste à installer plusieurs cartes d'interface réseau sur un hôte VMware ESXi, puis à les configurer en associations de cartes d'interface réseau. Les associations de cartes d'interface réseau doivent être configurées sur des commutateurs externes distincts, chaque paire de cartes étant configurée comme une association sur son commutateur externe respectif. Vous avez en outre la possibilité d'appliquer un algorithme d'équilibrage de charge correspondant au type de protocole d'agrégation de liens pris en charge sur le commutateur externe – par exemple, 802.3ad ou EtherChannel.

Il est par ailleurs possible d'atteindre des niveaux encore plus élevés de performances et de haute disponibilité au moyen de commutateurs compatibles Cross-Stack EtherChannel. Certains commutateurs réseau permettent d'associer des ports appartenant à plusieurs commutateurs physiques distincts gérés comme un seul commutateur logique. L'association de cartes d'interface réseau relevant de commutateurs virtuels distincts offre une résilience supplémentaire, ainsi qu'un certain degré d'optimisation des performances. Le fait de mettre plusieurs chemins à la disposition de l'hôte VMware ESXi permet d'améliorer les performances via un partage distribué de la charge.

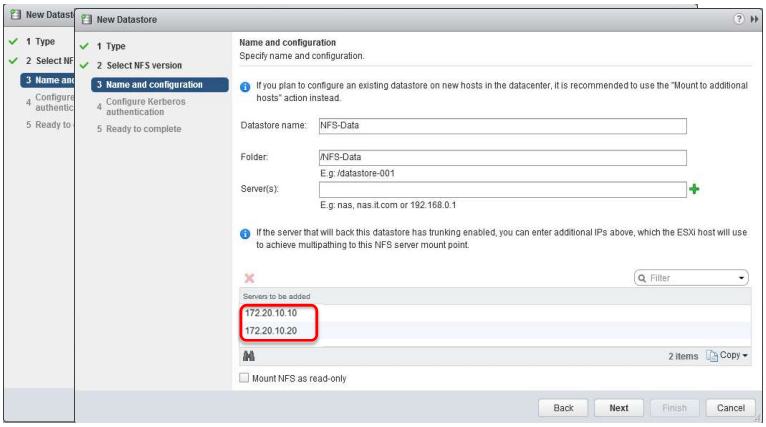
Un seul chemin actif est disponible pour la connexion entre l'hôte VMware ESXi et une cible de stockage déterminée (LUN ou point de montage). Même lorsque des connexions de basculement sont disponibles, la bande passante exploitable entre une banque de données donnée et le stockage sous-jacent est limitée à la capacité d'une connexion unique. Pour augmenter la bande passante utilisable, un hôte VMware ESXi aurait besoin de disposer de plusieurs connexions avec les cibles de stockage. Il vous faudra éventuellement configurer plusieurs banques de données utilisant chacune une connexion distincte entre l'hôte VMware ESXi et le stockage.

Ce tableau indique la configuration recommandée pour le multipathing NFS

Les commutateurs externes sont compatibles Cross-Stack EtherChannel.	**Les commutateurs externes ne sont pas compatibles Cross-Stack EtherChannel.**
Configurez un port VMkernel.	Configurez plusieurs ports VMkernel sur des commutateurs virtuels différents se trouvant sur des sous-réseaux distincts.
Configurez l'association de cartes d'interface réseau à l'aide d'adaptateurs connectés à des commutateurs physiques distincts.	Configurez l'association de cartes d'interface réseau à l'aide d'adaptateurs connectés à un même commutateur physique.
Configurez le serveur NFS avec plusieurs adresses IP. Ces adresses IP peuvent se trouver sur un même sous-réseau.	Configurez le serveur NFS avec plusieurs adresses IP. Ces adresses IP peuvent se trouver sur un même sous-réseau.
Pour utiliser plusieurs liens, configurez les associations de cartes d'interface réseau avec la règle d'équilibrage de charge avec hachage IP.	Pour utiliser plusieurs liens, autorisez la table de routage VMkernel à décider du lien à utiliser pour l'envoi de paquets (nécessite plusieurs banques de données).

6-66 Activer la jonction de sessions NFS 4.1

Plusieurs adresses IP sont configurées pour chaque banque de données NFS v4.1.



NFS v4.1 prend en charge le multipathing natif et la jonction de sessions. Pour activer le multipathing, l'administrateur entre plusieurs adresses IP lors de la configuration de la banque de données.

6-67 Laboratoire 7 : Accès au stockage NFS

Configurer l'accès à une banque de données NFS

1. Configurer l'accès à des banques de données NFS
2. Afficher des informations sur le système de stockage NFS

6-68 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les composants NFS
- Expliquer les différences entre NFS v3 et NFS v4.1
- Créer et gérer des banques de données NFS.

6-69 Leçon 6 :Banques de données vSAN

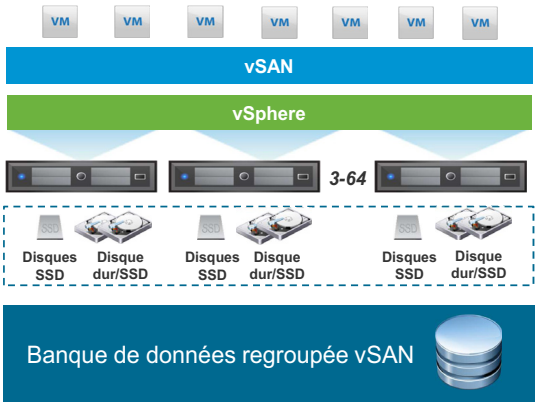
6-70 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Expliquer le rôle d'une banque de données vSAN
- Décrire l'architecture et les contraintes de configuration de vSAN
- Décrire les étapes de la configuration de vSAN
- Expliquer la création et l'utilisation des stratégies de stockage vSAN

6-71 À propos de vSAN

La création d'une seule et unique banque de données vSAN exploitant la capacité de stockage de plusieurs hôtes et disques du cluster.



À partir de vSphere 5.5, VMware a introduit le software-defined storage avec les banques de données vSAN. VMware vSAN regroupe les périphériques de stockage locaux (dispositifs Flash et disques magnétiques) de manière à fournir une banque de données en cluster utilisable par les machines virtuelles.

vSAN 6.x propose deux modèles de configuration : le modèle hybride et le modèle 100 % Flash. La configuration hybride s'appuie sur des périphériques Flash côté serveur pour constituer une couche de cache hautes performances, ainsi que sur des disques magnétiques pour fournir une capacité de stockage assurant la persistance de données. Dans une configuration 100 % Flash, la couche de cache et la couche de capacité reposent toutes deux sur des dispositifs Flash.

Dans un environnement vSAN, plusieurs hôtes VMware ESXi sont configurés de façon à former un cluster vSAN. Tous les hôtes VMware ESXi communiquent entre eux via un réseau vSAN dédié. Les hôtes dépourvus de stockage local peuvent partager leurs ressources de calcul tout en exploitant les ressources de stockage disponibles dans le cluster. Les périphériques de stockage local présents sur un hôte sont combinés de façon à constituer jusqu'à cinq groupes de disques locaux. Chaque groupe de disques comprend un dispositif de cache Flash et jusqu'à sept dispositifs de capacité.

Les groupes de disques de tous les hôtes VMware ESXi d'un cluster vSAN sont combinés pour former une banque de données vSAN. Une seule banque de données est autorisée par cluster vSAN. Le système de fichiers OSFS (Object Store File System) permet la combinaison des volumes VMFS des différents hôtes et leur montage sous la forme d'une banque de données unique. Cette banque de données contient l'ensemble des fichiers de machine virtuelle, y compris les fichiers VMDK. Chacun de ces fichiers VMDK peut être assorti de sa propre stratégie de stockage pour machine virtuelle, définissant les modalités de stockage des données

sur les disques de la banque de données. Les stratégies de stockage pour machine virtuelle sont configurées pour optimiser l'utilisation des fonctionnalités du cluster vSAN.

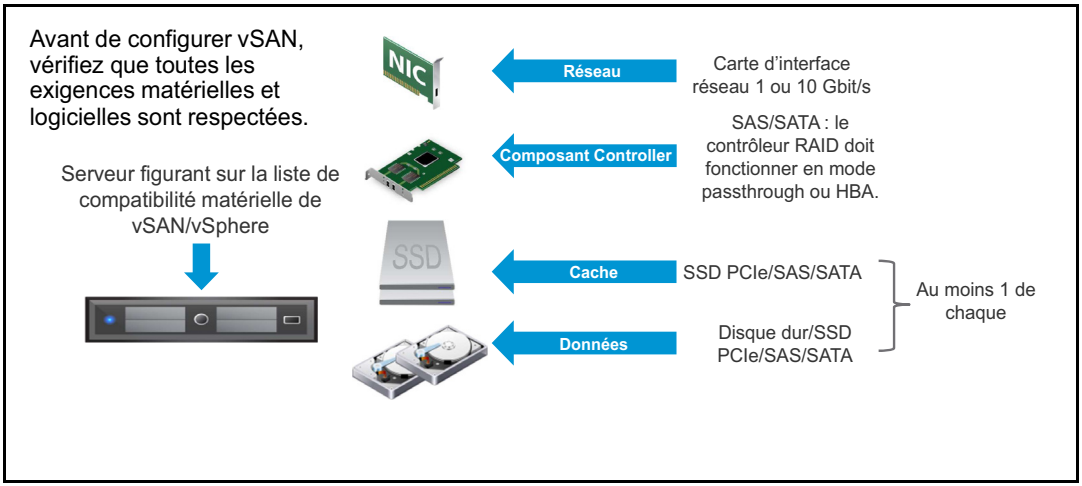
Les banques de données vSAN offrent plusieurs fonctionnalités permettant aux administrateurs d'utiliser plus efficacement le software-defined storage :

- L'architecture à stratégie de stockage différenciée pour chaque machine virtuelle : grâce à la possibilité de créer plusieurs stratégies par banque de données, chaque machine virtuelle peut disposer d'un stockage distinct.
- L'intégration de vSphere avec vCenter Server : la fonctionnalité vSAN est intégrée et ne requiert aucune appliance. Vous créez un cluster vSAN en procédant comme pour un cluster vSphere HA ou vSphere DRS.
- Le stockage à évolutivité horizontale : un cluster peut contenir jusqu'à 64 hôtes VMware ESXi. Pour une évolutivité horizontale, il suffit d'ajouter de nouveaux nœuds au cluster, ou de configurer vSAN pour lancer une analyse afin de détecter les disques vides et de les ajouter automatiquement.
- La résilience intégrée : une stratégie par défaut met en miroir tous les objets correspondant à des machines virtuelles non configurées pour vSAN.

vSAN 6.x introduit plusieurs nouvelles fonctionnalités et améliorations :

- Le nouveau format sur disque
- La nouvelle méthodologie de snapshots garantissant de meilleures performances
- Les domaines de pannes conçus pour résister aux défaillances de baie
- La stratégie de stockage par machine virtuelle affectable comme stratégie par défaut au niveau de la banque de données
- La visualisation de l'utilisation de la banque de données vSAN
- La projection de l'utilisation en fonction d'une configuration possible des stratégies de stockage
- L'état de resynchronisation affiché dans l'interface de vSphere Web Client
- Les nouvelles fonctions facilitant la maintenance des disques

6-72 Exigences liées à vSAN



Le premier composant requis pour vSAN est une machine exécutant vCenter Server. Celle-ci est nécessaire à la gestion dans la mesure où vSAN est pleinement intégré dans vSphere.

Un cluster vSAN doit comporter un minimum de trois hôtes contribuant à sa capacité. Un hôte inclus dans le cluster vSAN ne peut pas faire partie d'autres clusters.

Chaque cluster vSAN requiert un réseau dédié avec lequel chacun des hôtes est en mesure de communiquer :

- Un réseau dédié 1 Gbit/s (10 Gbit/s recommandés) pour les groupes de disques hybrides
- Un réseau dédié 10 Gbit/s pour les groupes de disques 100 % Flash

VMware recommande d'utiliser à cet effet un réseau 10 Gbit/s avec, si possible, une association de deux cartes d'interface réseau 10 Gbit/s permettant d'assurer la tolérance aux pannes. Les tests ont montré qu'un réseau 1 Gbit/s peut s'avérer suffisant, mais ce type de réseau n'est pas pris en charge. Le réseau vSAN doit être configuré pour IPv4 et IPv6, et doit prendre en charge la multidiffusion.

Tous les hôtes d'un cluster ne doivent pas nécessairement disposer d'une capacité de stockage locale. Un hôte sans stockage est utilisé pour ses ressources de calcul et bénéficie pour sa part de la banque de données vSAN. Tous les hôtes dotés de stockage local doivent être équipés des dispositifs suivants :

- Un disque dur électronique SSD SAS (Serial Attached SCSI) ou SATA ou un dispositif Flash PCIe, et un ou plusieurs disques magnétiques pour chaque groupe de disques hybride
- Un disque SSD SAS/SATA ou un dispositif Flash PCIe et un ou plusieurs disques Flash avec capacité Flash activée pour les groupes de disques 100 % Flash

De plus, chaque hôte doit disposer d'un minimum de 32 Go de mémoire pour prendre en charge un maximum de cinq groupes de disques et un maximum de sept dispositifs de capacité par groupe de disques.

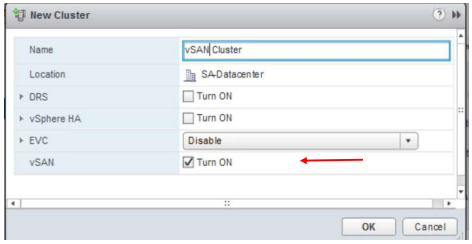
Pour plus d'informations, consultez le guide *Administration de VMware vSAN*, disponible à l'adresse https://www.vmware.com/support/pubs/virtual-san-pubs.html.

6-73 Configuration de vSAN

Pour utiliser vSAN, vous devez créer un cluster hôte, puis activer vSAN sur ce cluster.

Pour autoriser l'échange de données au sein du cluster vSAN, vous devez fournir un adaptateur réseau VMkernel dédié au trafic vSAN sur chaque hôte VMware ESXi.

Vous pouvez activer vSAN lors de la création d'un cluster. Vous avez également la possibilité de modifier les propriétés d'un cluster existant de manière à activer vSAN pour ce cluster.



Les banques de données vSAN sont totalement intégrées avec vSphere 6.x.

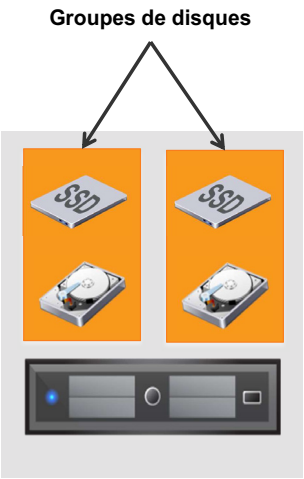
Pour plus d'informations sur l'activation ou la désactivation d'un cluster vSAN, consultez l'article 2058322 de la base de connaissances VMware, disponible à l'adresse suivante : http://kb.vmware.com/kb/2058322.

La configuration pour vSAN ne peut s'effectuer que via vSphere Web Client.

6-74 Groupes de disques

Les groupes de disques vSAN composés de périphériques Flash et de disques magnétiques requièrent les composants suivants :

- Un périphérique Flash :
  - Un périphérique Flash au maximum par groupe de disques
- Un disque dur/SSD :
  - Jusqu'à sept périphériques pris en charge par groupe de disques
- Cinq groupes de disques au maximum par hôte

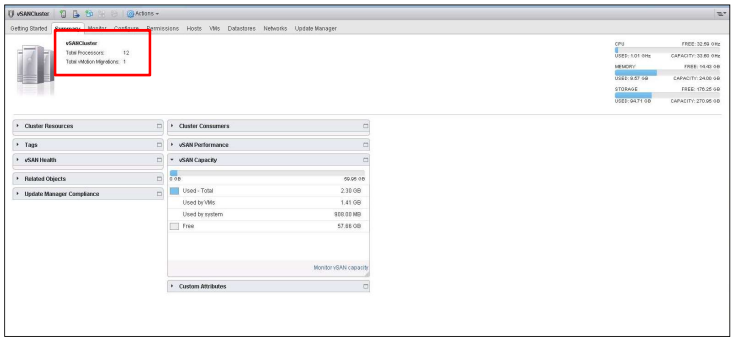


Sur chaque hôte VMware ESXi dont les périphériques locaux participent à un cluster vSAN, les périphériques sont organisés en groupes de disques. Un groupe de disques correspond à une unité de capacité de stockage physique définie sur un hôte, ainsi qu'à un ensemble de périphériques physiques contribuant aux performances et à la capacité du cluster vSAN.

Les groupes de disques de tous les hôtes VMware ESXi d'un cluster vSAN sont combinés pour former une banque de données vSAN. La taille de la banque de données vSAN dépend du nombre de dispositifs de capacité par hôte VMware ESXi et du nombre d'hôtes VMware ESXi présents dans le cluster. La banque de données vSAN stocke les fichiers des machines virtuelles, y compris les fichiers de disque de machine virtuelle (VMDK).

6-75 Affichage de l’onglet « vSAN Cluster Summary »

Dans vSphere Web Client, l’onglet **Summary** associé au cluster vSAN présente des informations d’ordre général sur la configuration de vSAN.

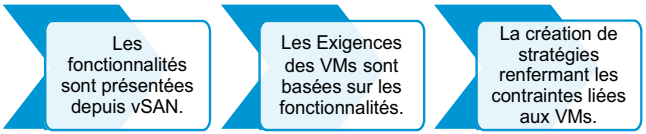


6-76 Utilisation de vSAN

Les fonctionnalités définissent les caractéristiques de capacité, de performances et de disponibilité du stockage physique sous-jacent. Le cluster vSAN présente ces fonctionnalités à vCenter Server, afin qu'elles puissent être utilisées par les machines virtuelles.

Les exigences correspondent aux besoins d'une machine virtuelle

Les stratégies de stockage pour machine virtuelle spécifient les exigences des machines virtuelles en vue de déterminer leur placement optimal dans la banque de données vSAN.



Lorsque vSAN est activé sur un cluster, une banque de données vSAN unique est créée. Cette banque de données apparaît en tant que type distinct dans la liste des banques de données éventuellement disponibles (vSphere Virtual Volumes, VMFS et/ou NFS).

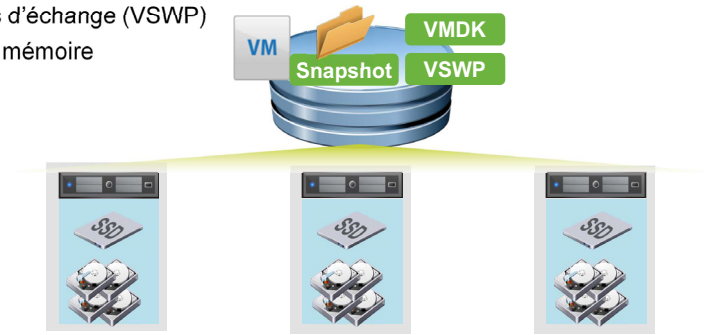
Une même banque de données vSAN peut offrir des niveaux de service distincts à chacune des machines virtuelles ou à chacun des disques virtuels. Dans vCenter Server, les caractéristiques de stockage de la banque de données vSAN sont présentées comme un ensemble de fonctionnalités,

auxquelles vous pouvez faire référence pour définir une stratégie de stockage applicable aux machines virtuelles. vSAN s'appuie sur cette stratégie pour déterminer le placement optimal des machines virtuelles que vous déploierez par la suite en fonction de leurs exigences spécifiques.

6-77 Objets présents dans les banques de données vSAN

Dans une banque de données vSAN, les fichiers sont regroupés sous les types d'objet suivants :

- Les dossiers de base (« espaces de nommage ») des machines virtuelles :
- Les disques virtuels
- Les snapshots
- Les fichiers d'échange (VSWP)
- L'état de la mémoire

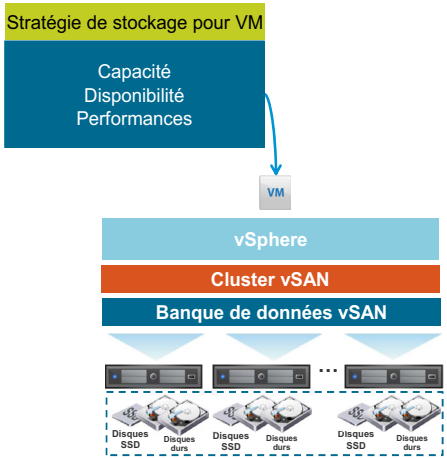


Un cluster vSAN stocke et gère les données sous la forme de conteneurs flexibles appelés objets. Le provisionnement d'une machine virtuelle sur une banque de données VMware vSAN se traduit par la création d'un ensemble d'objets. Ces objets sont de plusieurs types :

- Le dossier de base (« espace de nommage ») de la machine virtuelle : contient les métadonnées (fichiers de configuration) de la machine virtuelle.
- VMDK : Le disque de machine virtuelle.
- Les deltas de snapshot : créés lors des prises de snapshot de la machine virtuelle.
- VM Swap : le fichier d'échange de machine virtuelle, créé lors de la mise sous tension de la machine virtuelle.
- La mémoire de la VM : l'état de la mémoire de la machine virtuelle lors de l'interruption de cette machine, ou lors de la création d'un snapshot avec préservation de l'état de la mémoire de la machine virtuelle.

6-78 Stratégies de stockage pour machine virtuelle

- Les stratégies de stockage pour machine virtuelle sont créées préalablement au déploiement des machines virtuelles. Elles reflètent les exigences liées aux applications exécutées sur ces machines virtuelles.
- Ces stratégies se fondent sur les fonctionnalités vSAN.
- La stratégie de stockage applicable à la machine virtuelle est sélectionnée en fonction des besoins de cette VM, après quoi des objets de stockage répondant à cette stratégie sont créés pour la machine virtuelle.



Les stratégies de stockage pour machine virtuelle constituent un ensemble de propriétés de stockage qui sont configurées par un administrateur en vue d'être utilisées par les machines virtuelles. Chacune des stratégies de stockage que vous créez reflète un ensemble de fonctionnalités répondant aux exigences en termes de disponibilité, de performances et de stockage des machines virtuelles déployées dans un environnement. La création de ces stratégies de stockage intervient préalablement au déploiement des machines virtuelles.

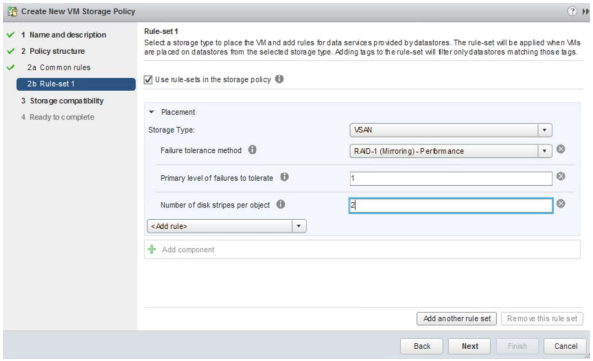
Au moment de déployer une machine virtuelle, l'administrateur choisit la stratégie de stockage pour machine virtuelle qui répond à ses exigences en vue de la création du fichier de disque de machine virtuelle.

6-79 Configuration des stratégies de stockage pour machine virtuelle

Les stratégies de stockage pour machine virtuelle jouent un rôle clé dans le provisionnement d'une machine virtuelle.

Ces stratégies contrôlent les éléments suivants :

- Le type de stockage fourni pour la machine virtuelle
- Le placement de la machine virtuelle au sein du stockage
- Les services de données proposés pour la machine virtuelle

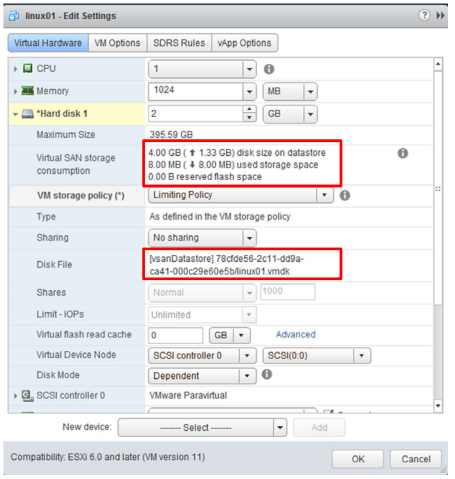


6-80 Affichage des banques de données vSAN des machines virtuelles

L'utilisation du stockage vSAN est déterminée par la stratégie de stockage associée à la machine virtuelle.

La vue des disques durs de la machine virtuelle fournit les informations suivantes :

- Le récapitulatif de la taille de l'espace de stockage total et utilisé
- La présentation de la stratégie de stockage pour machine virtuelle
- L'emplacement des fichiers de disque au sein d'une banque de données vSAN



6-81 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Expliquer le rôle d'une banque de données vSAN
- Décrire l'architecture et les contraintes de configuration de vSAN
- Décrire les étapes de la configuration de vSAN
- Expliquer la création et l'utilisation des stratégies de stockage vSAN

6-82 Points clés

- Les banques de données servent à héberger les fichiers des machines virtuelles.
- Le stockage partagé est essentiel à la prise en charge de fonctionnalités vSphere telles que vSphere vMotion, vSphere HA et vSphere DRS.
- Les clusters vSAN regroupent les disques serveur en attachement direct afin de créer un stockage partagé exploitable par les machines virtuelles.
- VMware vSAN permet d'utiliser vSphere HA, vSphere vMotion et vSphere DRS sans stockage partagé externe.

Des questions ?

MODULE 7

Gestion des machines virtuelles

7-2 Vous êtes ici

1. Présentation du cours
2. Présentation de vSphere et du Software-Defined Data Center
3. Création de machines virtuelles
4. vCenter Server
5. Configuration et gestion des réseaux virtuels
6. Configuration et gestion du stockage virtuel
7. **Gestion des machines virtuelles**
8. Gestion et surveillance des ressources
9. vSphere HA, vSphere Fault Tolerance et protection des données
10. vSphere DRS
11. vSphere Update Manager
12. Résolution des problèmes vSphere

7-3 Importance

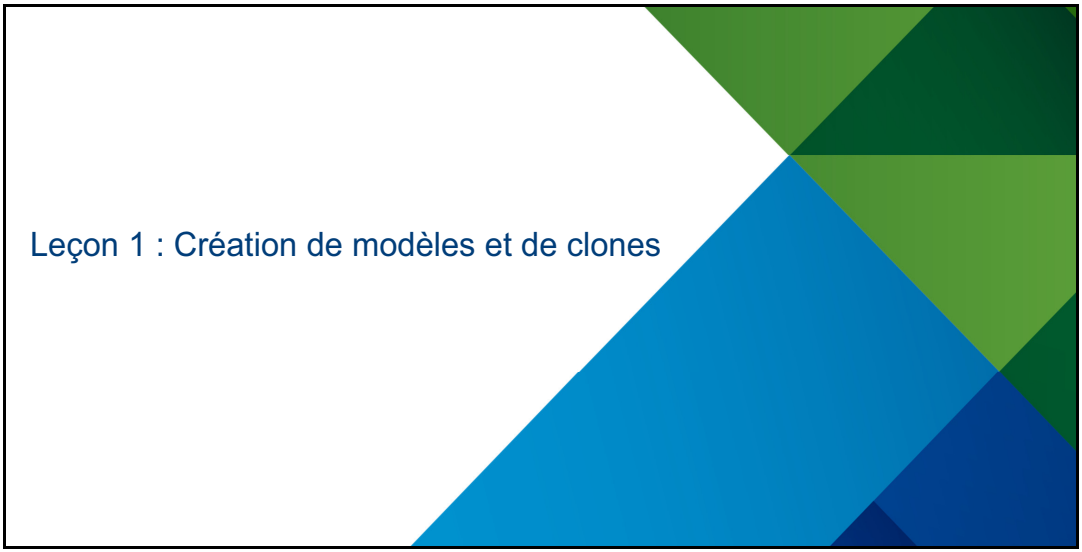
Les machines virtuelles jouant un rôle fondamental dans l'ensemble des opérations informatiques d'une infrastructure virtuelle, il importe de bien maîtriser leur déploiement, leur configuration et leur gestion.

Un remplissage incorrect de votre inventaire de machines virtuelles peut entraîner des résultats insatisfaisants.

7-4 Leçons du module

Leçon 1 :	Création de modèles et de clones
Leçon 2 :	Utilisation des bibliothèques de contenu
Leçon 3 :	Modification de machines virtuelles
Leçon 4 :	Migration de machines virtuelles
Leçon 5 :	Création de snapshots de machine virtuelle

7-5 Leçon 1 : Création de modèles et de clones



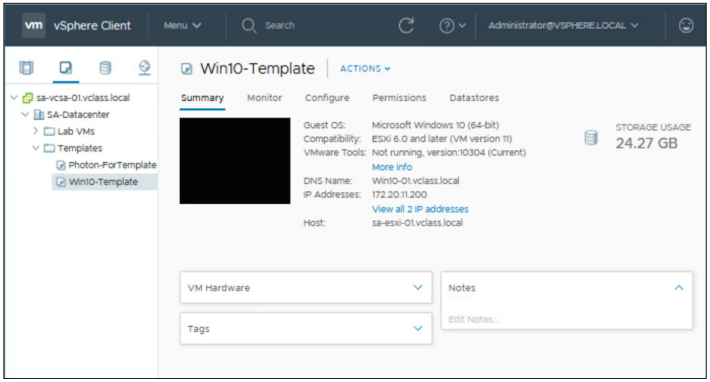
7-6 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Créer un modèle
- Déployer une machine virtuelle à partir d'un modèle
- Cloner une machine virtuelle
- Activer la personnalisation d'un système d'exploitation client par vCenter Server
- Mettre à niveau le matériel d'une machine virtuelle
- Créer un clone instantané d'une machine virtuelle

7-7 Utilisation de modèles

Un modèle est une copie d'une machine virtuelle. Les modèles servent à créer et à provisionner de nouvelles machines virtuelles.



Un modèle est une image contenant habituellement :

- Un système d'exploitation client
- Un ensemble d'applications
- Une configuration de machine virtuelle spécifique, qui fournit l'équivalent virtuel d'un ensemble de composants matériels

La création de modèles permet de provisionner des machines virtuelles beaucoup plus rapidement et avec un risque d'erreur sensiblement diminué par rapport au provisionnement de machines physiques et à la création individuelle de machines virtuelles via l'assistant « Create New Virtual Machine ».

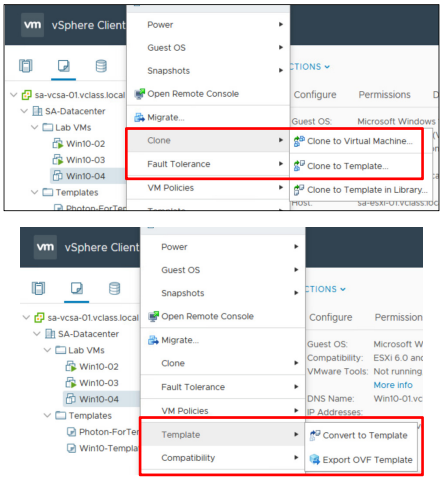
Les modèles côtoient les machines virtuelles au sein de l'inventaire. Vous pouvez organiser à votre guise des ensembles de machines virtuelles et de modèles dans des dossiers, et appliquer des autorisations aux machines virtuelles comme aux modèles. Vous avez la possibilité de transformer une machine virtuelle en modèle sans copier l'intégralité de ses fichiers ni créer de nouvel objet.

Vous pouvez déployer une machine virtuelle à partir d'un modèle. La machine virtuelle ainsi déployée vient s'ajouter au dossier sélectionné par l'utilisateur lors de la création du modèle.

7-8 Création de modèles

Vous disposez de plusieurs méthodes pour créer un modèle :

- Cloner la machine virtuelle sous la forme d'un modèle : cette machine virtuelle peut être sous tension ou hors tension.
- Convertir la machine virtuelle en modèle : la machine virtuelle doit être hors tension.
- Cloner un modèle : cette méthode permet de créer un nouveau modèle à partir d'un modèle existant.



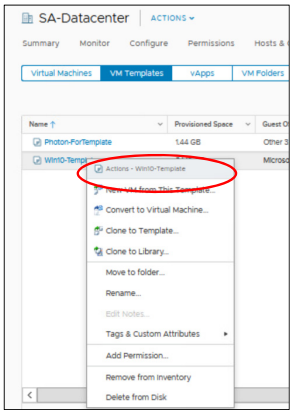
L'option **Clone to Template** vous permet de choisir le format dans lequel les disques virtuels de la machine virtuelle seront stockés :

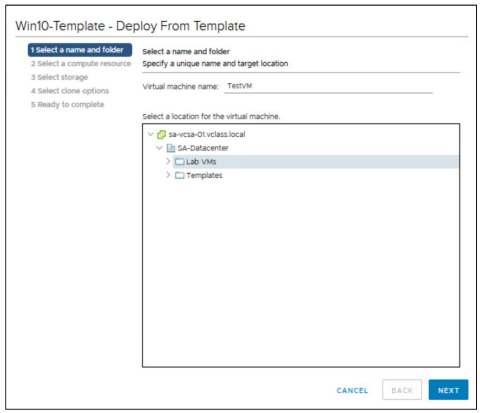
- Le même format que la source
- Le format à provisionnement fin
- Le format à provisionnement définitif avec mise à zéro différée
- Le format à provisionnement définitif avec mise à zéro immédiate

L'option **Convert to Template** ne propose pas de spécifier le format et laisse les fichiers de la machine virtuelle intacts.

7-9 Déploiement des machines virtuelles à partir d'un modèle

Lors du déploiement d'une machine virtuelle, vous êtes invité à fournir un ensemble d'informations, telles que son nom, son emplacement dans l'inventaire, l'hôte et la banque de données associés, ainsi que les données de personnalisation du système d'exploitation client.

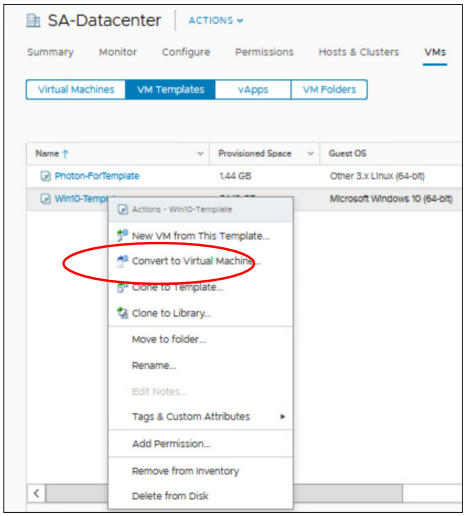




7-10 Mise à jour des modèles

La mise à jour d'un modèle permet d'inclure de nouveaux correctifs, d'apporter des changements au système ou d'installer de nouvelles applications.

- Commencez par convertir le modèle en machine virtuelle.
- Placez cette machine virtuelle sur un réseau isolé de façon à la soustraire aux accès utilisateur.
- Apportez les modifications requises à cette machine virtuelle.
- Convertissez la machine virtuelle en modèle.



La mise à jour d'un modèle permet d'ajouter des correctifs ou des logiciels sans créer un nouveau modèle. Commencez par convertir le modèle en machine virtuelle. Cette conversion vous permet de mettre la machine virtuelle sous tension.

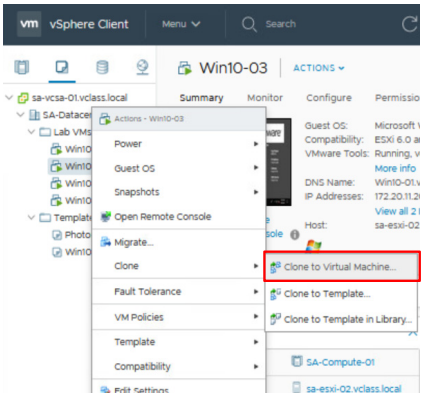
Pour plus de sécurité, interdisez l'accès des autres utilisateurs à la machine virtuelle pendant la mise à jour. Pour ce faire, déconnectez la machine virtuelle du réseau, ou placez-la sur un réseau isolé.

Connectez-vous au système d'exploitation client de la machine virtuelle et appliquez le correctif ou installez le logiciel. Lorsque vous avez terminé, mettez la machine virtuelle hors tension et convertissez-la de nouveau en modèle.

7-11 Clonage des machines virtuelles

Le clonage d'une machine virtuelle permet de créer une réplique exacte de l'original.

- Le clonage offre une alternative au déploiement d'une machine virtuelle.
- La machine virtuelle que vous clonez peut être sous tension ou hors tension.



Le clonage d'une machine virtuelle offre une alternative au déploiement d'une machine virtuelle à partir d'un modèle. Cette opération crée une réplique de la machine virtuelle présentant la même configuration et les mêmes logiciels installés que l'original.

Vous pouvez personnaliser le système d'exploitation client du clone de façon à modifier le nom, les paramètres réseau et les autres propriétés de la machine virtuelle. Vous évitez ainsi les conflits susceptibles de se produire en cas de déploiement simultané d'une machine virtuelle et d'un clone présentant des paramètres de système d'exploitation client identiques.

Pour pouvoir cloner une machine virtuelle, vous devez être connecté à vCenter Server. Vous ne pouvez pas cloner de machine virtuelle si vous utilisez VMware Host Client pour gérer directement un hôte.

La machine virtuelle que vous clonez peut être sous tension ou hors tension. Lorsque vous clonez une machine virtuelle sous tension, les services et les applications ne sont pas automatiquement mis à l'arrêt.

7-12 Personnalisation du système d'exploitation client

L'option « Customize guest OS » vous permet de différencier des machines virtuelles créées à partir d'un même modèle ou générées par clonage.

La personnalisation d'un système d'exploitation client vous permet de modifier les éléments suivants :

- Le nom de l'ordinateur
- Les paramètres réseau
- Les paramètres de licence
- L'identifiant de sécurité Windows (WSI)

Durant le clonage de machines virtuelles ou leur déploiement à partir d'un modèle :

- Vous pouvez créer une spécification afin de préparer les systèmes d'exploitation clients.
- Les spécifications sont stockées dans la base de données vCenter Server.
- Vous pouvez modifier les spécifications dans le volet « Customization Specifications Manager ».
- Les systèmes d'exploitation Windows et Linux sont pris en charge.

Lorsque vous clonez une machine virtuelle ou que vous la déployez à partir d'un modèle, vous avez la possibilité de personnaliser son système d'exploitation client afin de modifier certaines propriétés, notamment :

- Le nom de l'ordinateur
- Les paramètres réseau
- Les paramètres de licence

La personnalisation de système d'exploitation client permet d'éviter des conflits liés au déploiement simultané de plusieurs machines virtuelles présentant des propriétés identiques, telles qu'une adresse IP ou un nom d'ordinateur redondants.

Les paramètres de personnalisation peuvent être spécifiés via l'assistant « Guest Customization » durant le clonage ou le déploiement. Vous pouvez également créer des spécifications de personnalisation, c'est-à-dire des paramètres de personnalisation stockés dans la base de données VMware vCenter Server®. Lors d'un clonage ou d'un déploiement, vous avez la possibilité de sélectionner une spécification de personnalisation pour l'appliquer à la nouvelle machine virtuelle. Recourez au gestionnaire de spécifications de personnalisation pour gérer les spécifications créées via l'assistant « Guest Customization ».

VMware Tools doit être installé sur le système d'exploitation client que vous personnalisez. Ce système d'exploitation client doit de plus être installé sur un disque connecté au nœud SCSI 0:0 dans la configuration de la machine virtuelle.

La personnalisation du système d'exploitation client n'est possible que si vCenter Server a été préalablement configuré pour cette tâche. Pour être à même de personnaliser des machines virtuelles exécutant un système d'exploitation antérieur à Windows 2008 et Windows Vista, vous devez au préalable installer les outils Microsoft Sysprep sur le système vCenter Server. Les outils Sysprep sont intégrés dans les systèmes d'exploitation Windows 2008, Windows Vista et ultérieurs.

La personnalisation des systèmes d'exploitation client Linux présuppose l'installation de Perl sur le système d'exploitation client Linux.

La personnalisation du système d'exploitation client est prise en charge dans de nombreuses distributions de Linux. Pour vérifier si la personnalisation est prise en charge par certaines distributions de Linux et déterminer les hôtes VMware ESXi compatibles, consultez le *Guide de compatibilité VMware*, disponible à l'adresse suivante : http://www.vmware.com/resources/compatibility.

Pour en savoir plus sur la personnalisation du système d'exploitation client, consultez le *Guide d'administration d'une machine virtuelle vSphere*, disponible à l'adresse suivante : http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

7-13 À propos des clones instantanés

Le mécanisme de clone instantané permet de générer rapidement une machine virtuelle à partir d'une machine virtuelle source dont elle reprend exactement l'état.

L'état du processeur, l'état du périphérique virtuel, l'état de la mémoire et l'état des disques de la machine virtuelle de destination sont identiques à ceux de la machine virtuelle source.

L'efficacité du stockage est garantie par un mécanisme de partage de disque basé sur des snapshots et similaire à celui des clones liés.

Cas d'usage des clones instantanés :

- L'infrastructure de postes de travail virtuels
- Les déploiements à évolution horizontale rapide : Les hôtes de conteneur, Big Data et les nœuds de travail Hadoop
- Dév./Test : la réplication rapide et efficace de VM et de bancs d'essai présentant un même état d'exécution
- DevOps : la capacité à répliquer des VMs de la préproduction à la production, ou inversement, sans modifier leur état d'exécution

Dans vSphere 6.7, la création de clones instantanés de machines virtuelles passe bligatoirement par des appels d'API.

Avec le clonage instantané, les utilisateurs ont la possibilité de créer des machines virtuelles sous tension reprenant l'état d'exécution d'une autre machine virtuelle sous tension. Le processus de clonage n'altère pas l'état de la machine virtuelle source. Compte tenu de la rapidité et de la capacité de conservation d'état de cette opération, l'utilisateur peut évoluer vers un modèle de provisionnement en flux tendu.

Le clonage instantané est particulièrement intéressant dans les déploiements d'applications à grande échelle, car il garantit une utilisation efficace de la mémoire et permet de créer un grand nombre de machines virtuelles sur un hôte unique.

Afin d'éviter des conflits réseau, la fonction de clonage instantané permet de personnaliser le matériel virtuel de la machine virtuelle de destination durant l'opération de clonage. Vous avez notamment la possibilité de personnaliser les adresses MAC des cartes d'interface réseau virtuelles, ou la configuration des ports série et parallèles de la machine virtuelle de destination.

Lors d'une opération de clonage instantané, la machine virtuelle source est paralysée pendant une courte période de temps n'excédant pas une seconde. Durant cette période de paralysie de la machine virtuelle source, un nouveau disque delta inscriptible est généré pour chaque disque virtuel et un point de contrôle est prélevé et transféré sur la machine virtuelle de destination. La machine virtuelle de destination se met alors sous tension à l'aide du point de contrôle de VM source. Une fois la mise sous tension machine virtuelle de destination entièrement effectuée, la machine virtuelle source reprend son exécution.

Les machines virtuelles créées par clonage instantané sont des objets d'inventaire vCenter Server totalement indépendants. Les machines virtuelles créées par clonage instantané peuvent être gérées comme des VMs normales sans aucune restriction.

7-14 Suppression d’une machine virtuelle

Vous disposez de deux méthodes pour supprimer une machine virtuelle :

- La suppression dans l’inventaire :
  - Ce mode de suppression annule l’enregistrement de la machine virtuelle.
  - Les fichiers de la machine virtuelle restent stockés sur le disque.
  - Vous conservez la possibilité de réenregistrer (ajouter) ultérieurement la machine virtuelle dans l’inventaire.
- La suppression sur le disque :
  - Tous les fichiers de la machine virtuelle sont définitivement supprimés de sa banque de données.

Le fait de supprimer une machine virtuelle de l’inventaire vCenter Server annule son enregistrement auprès de l’hôte et de vCenter Server. Ce processus ne supprime pas les fichiers de la machine virtuelle de la banque de données. Les fichiers de la machine virtuelle restent stockés au même emplacement, et vous conservez la possibilité d’enregistrer à nouveau cette machine virtuelle dans le navigateur de la banque de données.

Toutefois, la fonction de suppression « Delete » supprime définitivement les fichiers de la machine virtuelle de la banque de données, et annule l’enregistrement de la machine virtuelle auprès de l’hôte et de vCenter Server.

7-15 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Créer un modèle
- Déployer une machine virtuelle à partir d'un modèle
- Cloner une machine virtuelle
- Activer la personnalisation d'un système d'exploitation client par vCenter Server
- Mettre à niveau le matériel d'une machine virtuelle
- Créer un clone instantané d'une machine virtuelle

7-16 Leçon 2 : Utilisation des bibliothèques de contenu

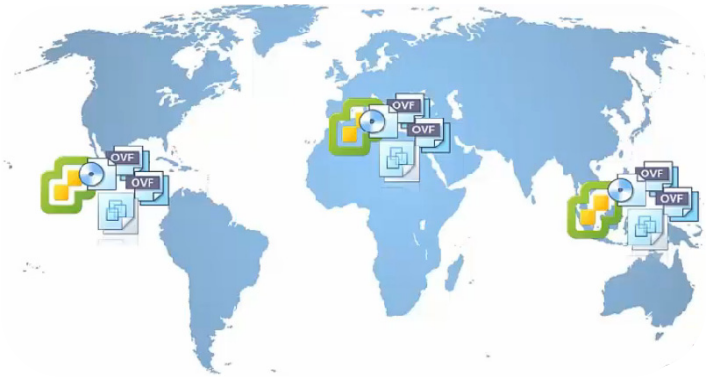
7-17 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Identifier les avantages liés aux bibliothèques de contenu
- Décrire les différents types de bibliothèque de contenu
- Déployer une machine virtuelle à partir de la bibliothèque de contenu

7-18 À propos des bibliothèques de contenu

Les bibliothèques de contenu sont des référentiels de modèles OVF et d'autres fichiers pouvant être partagés et synchronisés à l'échelle de plusieurs systèmes vCenter Server.

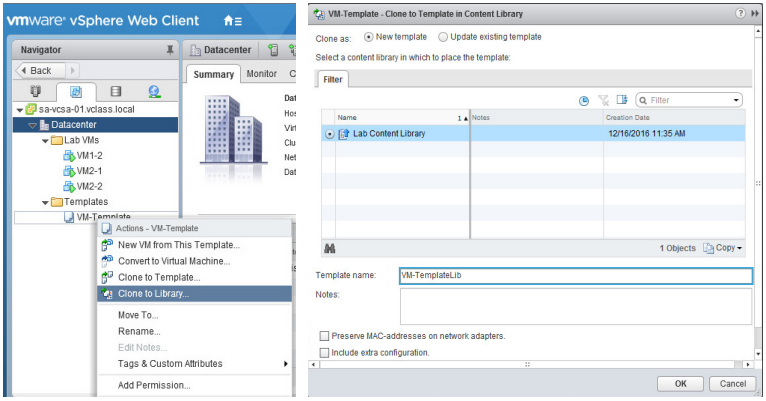


La bibliothèque de contenu permet de gérer les modèles et les autres types de fichiers utilisés dans les instances de vCenter Server dans le monde entier. Certaines entreprises ont déployé de nombreuses instances de vCenter Server dans leurs Data Centers à travers le monde. Pour chacune de ces instances de vCenter Server, elles disposent généralement d'une collection de modèles, d'images ISO, etc. Le problème est que tous ces éléments sont indépendants les uns des autres, et qu'il existe plusieurs versions distinctes de ces fichiers et modèles sur les différentes instances de vCenter Server.

La solution réside dans la bibliothèque de contenu, qui permet au département informatique de centraliser le stockage des modèles OVF, des images ISO ou des fichiers de tous types. Il est dès lors possible de publier ces modèles, images et fichiers divers, auxquels les autres bibliothèques de contenu pourront s'abonner en vue de les télécharger. La bibliothèque de contenu permet d'actualiser ces contenus en effectuant régulièrement une synchronisation avec l'éditeur de façon à disposer à tout moment de la version la plus récente.

7-19 Ajout de modèles à une bibliothèque de contenu

Les types d'éléments pouvant être chargés dans une bibliothèque de contenu sont les modèles de VM et les modèles VMware vSphere® vApp™, ainsi que d'autres objets VMware.



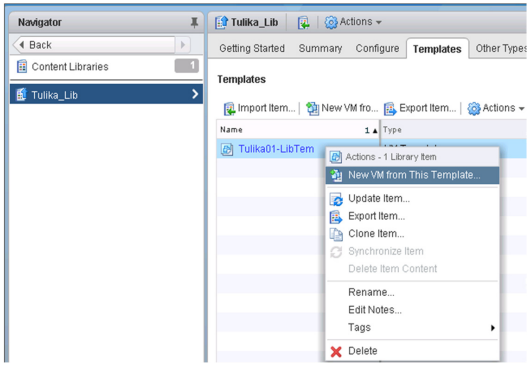
Les types d'éléments pouvant être chargés dans une bibliothèque de contenu sont les modèles de VM et les modèles VMware vSphere® vApp™, ainsi que d'autres objets VMware. Chaque VM ou vApp comporte plusieurs fichiers, tels que les fichiers journaux,les fichiers de disque, les fichiers de mémoire et les fichiers de snapshot, qui sont tous réunis dans un même élément de bibliothèque. Vous pouvez créer des éléments de bibliothèque dans une bibliothèque locale déterminée, ou supprimer des éléments d'une telle bibliothèque. Vous pouvez également charger des fichiers dans un élément d'une bibliothèque locale, afin que les bibliothèques abonnées à cette dernière puissent télécharger ces fichiers vers leur serveur NFS, leur serveur SMB ou leur banque de données.

7-20 Déploiement de machines virtuelles à partir de modèles stockés dans une bibliothèque de contenu

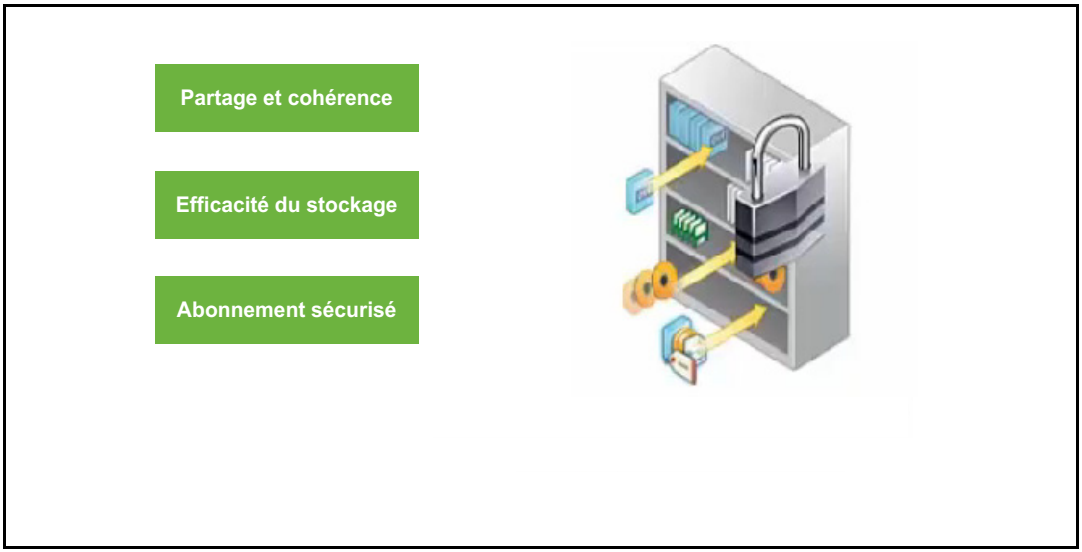
Les modèles publiés dans la bibliothèque peuvent être utilisés pour déployer des machines virtuelles et des vApps.

Les modèles de VM ou de vApp et les autres types de fichiers présents dans une bibliothèque constituent des éléments de bibliothèque.

Vous pouvez monter un fichier ISO directement depuis une bibliothèque de contenu.



7-21 Avantages liés aux bibliothèques de contenu



L'API de bibliothèque de contenu fournit un ensemble de services permettant de créer et de gérer des bibliothèques de contenu par programmation. Vous avez la possibilité de créer une bibliothèque de contenu locale et de la publier à l'échelle de l'environnement virtuel tout entier.

Les bibliothèques de contenu permettent aux administrateurs d'effectuer les actions suivantes :

- Stocker et partager les contenus en assurant le suivi des versions : l'installation et l'utilisation d'une bibliothèque de contenu répondent principalement à des besoins de stockage et d'homogénéité. Le partage et l'actualisation des contenus représentent un effort considérable. Par exemple, supposons que vous disposiez d'une instance principale de vCenter Server et que vous ayez créé une bibliothèque de contenu afin de stocker une copie maître de vos divers modèles OVF, images ISO et autres fichiers. En publiant cette bibliothèque de contenu, vous offrez aux autres bibliothèques localisées dans le monde entier la possibilité de s'abonner et de télécharger une copie exacte de ces données. Chaque fois qu'un modèle OVF est ajouté, modifié ou supprimé dans le catalogue publié, les bibliothèques abonnées peuvent se synchroniser avec l'éditeur de façon à actualiser leurs contenus.
- Gérer des fichiers distribués.
- Publier des contenus disponibles publiquement ou sur abonnement.
- Synchroniser des contenus entre différents sites ou différents systèmes vCenter Server.
- Sauvegarder des bibliothèques de contenu à l'aide de banques de données vSphere, du répertoire vCenter ou de NFS.
- Monter un fichier ISO directement depuis une bibliothèque de contenu.

Les abonnés ne souhaiteront pas nécessairement télécharger et stocker l'intégralité des contenus de la bibliothèque publiée : il se peut en effet qu'ils n'aient pas l'utilité de tous les contenus mis à leur disposition, ou qu'ils ne disposent pas de l'espace nécessaire. Les bibliothèques de contenu résolvent cette problématique en proposant des mécanismes d'optimisation de l'efficacité du stockage.

Chaque fois qu'un éditeur met à jour ses contenus, les modifications sont notifiées aux abonnés. Chaque abonné peut alors choisir de recevoir l'intégralité des données, ou uniquement les métadonnées. Lorsqu'il opte pour la réception de l'intégralité des données, deux possibilités s'offrent à lui : télécharger l'ensemble de la bibliothèque ou sélectionner les éléments voulus.

Dans la mesure où elles sont disponibles à l'abonnement dans le monde entier, les bibliothèques de contenu soulèvent des problèmes potentiels de sécurité, d'où la possibilité de les protéger par mot de passe lors de la publication.

7-22 Types de bibliothèque de contenu

Une bibliothèque de contenu peut être de trois types : locale, publiée et abonnée.

Vous pouvez créer des bibliothèques locales et des bibliothèques abonnées :

- Vous pouvez créer une bibliothèque locale afin de l'utiliser comme source d'un ensemble de contenus à enregistrer ou à partager. Créez cette bibliothèque locale sur une seule instance de vCenter Server. Vous pouvez ajouter ou supprimer des éléments dans une bibliothèque locale.
- Vous avez également la possibilité de publier une bibliothèque locale afin d'en faire un point d'accès du service de bibliothèque de contenu accessible à d'autres instances vCenter Server déployées dans votre environnement virtuel. Lors de la publication d'une bibliothèque, vous pouvez configurer la méthode d'authentification que les bibliothèques abonnées devront utiliser pour s'authentifier auprès de cette bibliothèque.
- Vous pouvez créer une bibliothèque abonnée et y charger des contenus par synchronisation avec une bibliothèque publiée. Une bibliothèque abonnée contient soit des copies des fichiers de la bibliothèque publiée, soit uniquement les métadonnées associées aux éléments de cette bibliothèque. La bibliothèque publiée peut se trouver sur la même instance de vCenter Server que la bibliothèque abonnée, mais cette dernière peut aussi faire référence à une bibliothèque publiée située sur une autre instance de vCenter Server. Vous ne pouvez pas ajouter d'éléments dans une bibliothèque abonnée. Vous ne pouvez ajouter des éléments que dans une bibliothèque locale ou publiée. Après synchronisation, les deux bibliothèques contiennent les mêmes éléments, sauf si la bibliothèque abonnée contient uniquement les métadonnées de ces éléments.

7-23 Laboratoires

Laboratoire 8 : Utilisation des modèles et des clones

Laboratoire 9 : Utilisation des bibliothèques de contenu

7-24 Laboratoire 8 : Utilisation des modèles et des clones

Déployer une nouvelle machine virtuelle à partir d'un modèle et cloner une machine virtuelle

1. Créer une bibliothèque de contenu
2. Cloner un modèle de VM vers un modèle chargé dans une bibliothèque de contenu
3. Déployer une machine virtuelle à partir d'un modèle de VM chargé dans la bibliothèque de contenu
4. Supprimer une bibliothèque de contenu

7-25 Laboratoire 9 : Utilisation des bibliothèques de contenu

Créer une bibliothèque de contenu pour cloner et déployer des machines virtuelles

1. Créer une bibliothèque de contenu
2. Cloner un modèle de VM vers un modèle chargé dans une bibliothèque de contenu
3. Déployer une machine virtuelle à partir d'un modèle de VM chargé dans la bibliothèque de contenu
4. Supprimer une bibliothèque de contenu

7-26 Rappel des objectifs de la formation

Vous devriez être en mesure d’atteindre les objectifs suivants :

- Identifier les avantages liés aux bibliothèques de contenu
- Décrire les différents types de bibliothèque de contenu
- Déployer une machine virtuelle à partir de la bibliothèque de contenu

7-27 Leçon 3 : Modification de machines virtuelles

7-28 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les paramètres et les options des machines virtuelles
- Ajouter un périphérique installable à chaud
- Augmenter la taille d'un disque virtuel de manière dynamique
- Ajouter un disque de mappage de périphérique brut (RDM) à une machine virtuelle

Vous pouvez être amené à modifier la configuration d'une machine virtuelle afin, par exemple, d'ajouter un adaptateur réseau ou un disque virtuel. Toutes les modifications apportées à une machine virtuelle peuvent être apportées lorsque celle-ci est hors tension. Certains changements matériels peuvent être opérés alors que la machine virtuelle est sous tension.

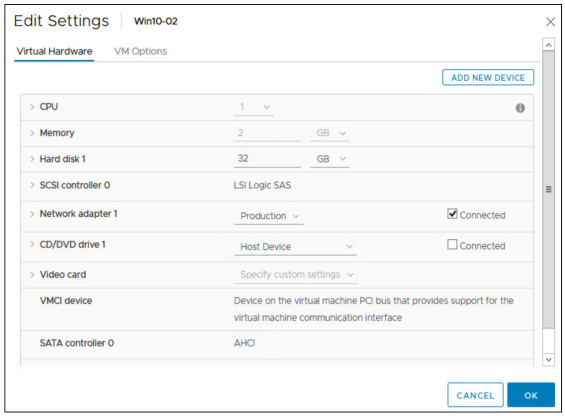
Vous avez la possibilité d'ajouter ou de supprimer du matériel virtuel, mais aussi de redéfinir diverses options de la machine virtuelle.

La configuration d'une machine virtuelle s'effectue depuis la boîte de dialogue Edit Settings de cette machine virtuelle.

7-29 Modification des paramètres d'une machine virtuelle

Vous pouvez modifier la configuration d'une machine virtuelle en accédant à sa boîte de dialogue « Edit Settings » :

- L'ajout de matériel virtuel :
  - il est possible d'ajouter certains composants matériels alors que la machine virtuelle est sous tension.
- La suppression de matériel virtuel :
  - certains composants matériels ne peuvent être supprimés que si la machine virtuelle est hors tension.
- La configuration des options de machine virtuelle.
- Le contrôle des ressources CPU et mémoire d'une machine virtuelle.



Le fait d'ajouter ou de supprimer des périphériques sur un serveur physique vous oblige à intervenir physiquement sur ce serveur au sein du Data Center. Lorsque vous utilisez des machines virtuelles, l'ajout de ressources s'effectue de manière dynamique et sans interruption de service. Il est nécessaire d'arrêter une machine virtuelle pour retirer des composants matériels, mais vous pouvez reconfigurer cette machine virtuelle sans accéder physiquement au Data Center.

Il est possible d'ajouter des ressources CPU et mémoire alors que la machine virtuelle est sous tension. Ces options, dites d'enfichage à chaud de CPU et d'ajout à chaud de mémoire, ne sont disponibles que si le système d'exploitation prend effectivement ces fonctionnalités en charge. Ces options sont désactivées par défaut. L'utilisation des fonctionnalités d'enfichage et d'ajout à chaud présuppose que les conditions suivantes soient satisfaites :

- Vous devez installer VMware Tools.
- La machine virtuelle doit utiliser la version 7 ou une version ultérieure du matériel.
- Le système d'exploitation client de la machine virtuelle doit prendre en charge les options d'ajout à chaud de CPU et de mémoire.
- Les options d'enfichage et d'ajout à chaud doivent être activées sous les options **CPU** ou **Memory** de l'onglet **Virtual Hardware**.

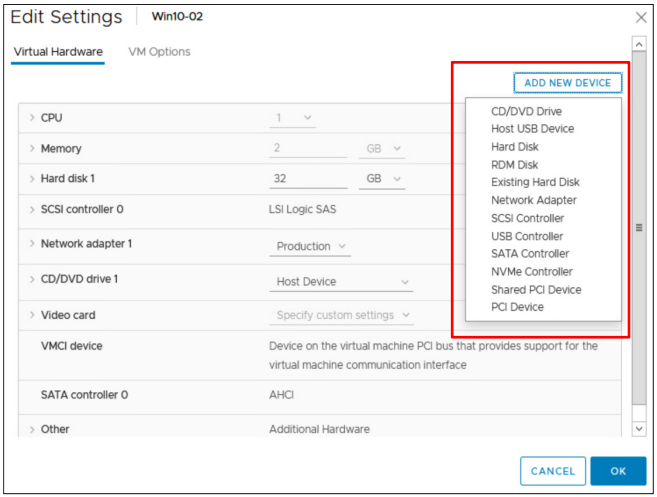
Reportez-vous au *Guide d'administration d'une machine virtuelle vSphere*, disponible à l'adresse suivante : http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

7-30 Périphériques installables à chaud

L'option d'enfichage à chaud vous permet d'ajouter des ressources à une machine virtuelle en cours d'exécution.

Les exemples de périphériques installables à chaud : les contrôleurs USB, les adaptateurs Ethernet et les disques durs.

Avec les systèmes d'exploitation client compatibles, vous pouvez également ajouter des ressources CPU et mémoire à une machine virtuelle en cours d'exécution.



Un mappage de périphériques bruts (RDM) est un fichier doté de l'extension `.vmdk` qui contient uniquement des informations de disque décrivant le mappage vers un LUN configuré sur l'hôte VMware ESXi. Les données proprement dites sont stockées sur le LUN.

Un RDM prend en charge les modes de compatibilité suivants :

- Le mode de compatibilité physique (passthrough) : permet au système d'exploitation client d'accéder directement au matériel. La compatibilité physique est utile si vous exécutez des applications orientées SAN sur la machine virtuelle. En revanche, un LUN configuré pour la compatibilité physique ne peut pas être cloné ni transformé en modèle. Lorsque vous prenez un snapshot d'une machine virtuelle dotée d'un RDM physique, aucun snapshot de ce dernier n'est généré. La taille d'un LUN configuré pour le mode passthrough est limitée à 64 To. Le nom de fichier d'un RDM en mode de compatibilité physique se termine par `-rdmp.vmdk`. Lorsqu'une machine virtuelle dotée d'un RDM en mode de compatibilité physique est sous tension, vous avez la possibilité d'utiliser vSphere Storage vMotion pour migrer cette VM vers une nouvelle banque de données, mais cette opération sera sans effet sur le contenu du LUN. Le fichier `-rdmp.vmdk` migre vers la nouvelle banque de données. Il en va de même lorsqu'une machine virtuelle sous tension fait l'objet d'une migration vSphere vMotion « Shared-Nothing ». Lorsqu'une machine virtuelle dotée d'un RDM en mode de compatibilité physique est hors tension, il est possible de migrer ses fichiers vers une nouvelle banque de données. L'utilisateur peut décider si le contenu du LUN doit être transféré dans un fichier `-flat.vmdk` (c'est-à-dire converti en disque virtuel) sur la nouvelle banque de données, ou s'il doit rester dans le LUN (la migration est alors limitée au fichier `-rdmp.vmdk`).

- Le mode de compatibilité virtuelle : permet à la machine d'utiliser les snapshots et d'autres fonctionnalités avancées de VMware. La compatibilité virtuelle permet au LUN de se comporter comme un disque virtuel. Lorsque vous clonez le disque ou le convertissez en modèle, ou encore lorsque vous le faites migrer (si la migration implique une copie du disque), vous avez la possibilité de copier le contenu du LUN dans un fichier de disque virtuel (`-flat.vmdk`). Quel que soit l'état de fonctionnement de la machine virtuelle, si un RDM en mode de compatibilité virtuelle lui est associé, l'utilisateur a la possibilité de décider si le contenu du LUN doit être transféré dans un fichier `-flat.vmdk` sur la banque de données de destination ou s'il doit conserver sa forme de LUN brut (seul le fichier `-rdm.vmdk` est alors transféré vers la nouvelle banque de données).

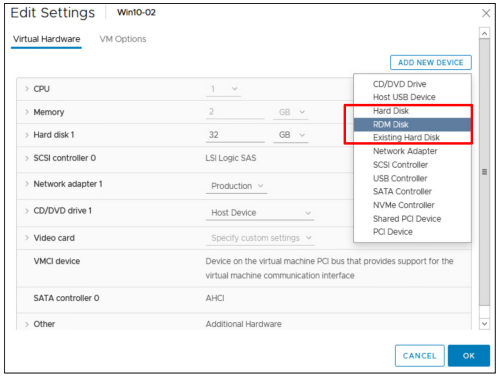
7-31 Création de fichiers de mappage de périphériques bruts (RDM)

Un fichier RDM (`-rdm.vmdk`) permet à une machine virtuelle d'accéder directement à un LUN physique.

L'encapsulation des informations de disque dans le fichier RDM permet à VMkernel de verrouiller le LUN de sorte qu'il accepte uniquement les écritures émanant d'une machine virtuelle donnée.

Lors de la création d'un fichier RDM, vous devez définir les éléments suivants :

- Le LUN cible : Le LUN vers lequel le fichier RDM doit effectuer un mappage
- La banque de données mappée : permet de stocker le fichier RDM avec la machine virtuelle ou dans une autre banque de données
- Le mode de compatibilité :
  - Physique
  - Virtuel
- Le nœud de périphérique virtuel



Vous pouvez augmenter la taille d'un disque virtuel appartenant à une machine virtuelle sous tension à condition que celle-ci ne comporte pas de snapshots.

Après avoir augmenté la taille d'un disque virtuel, vous pouvez être appelé à redimensionner le système de fichiers présent sur ce disque. Recourez à l'outil approprié du système d'exploitation client pour autoriser le système de fichiers à utiliser l'espace disque nouvellement alloué.

Les RDM que vous utilisez peuvent être en mode de compatibilité virtuelle ou de compatibilité physique.

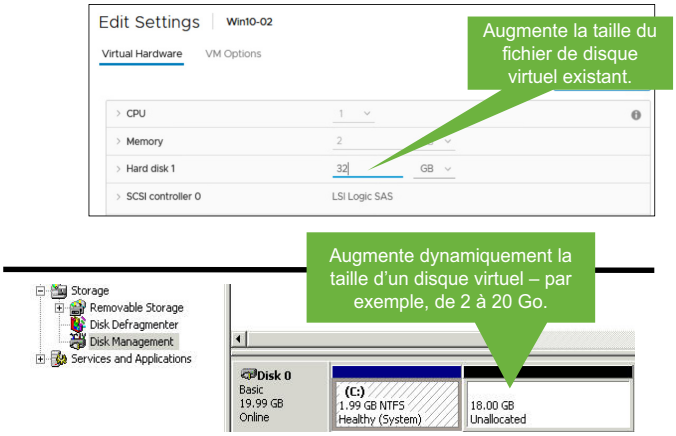
- Le mode virtuel correspond à une virtualisation complète du périphérique mappé. En mode virtuel, VMkernel envoie uniquement des demandes de LECTURE ou d'ÉCRITURE au périphérique mappé. Du point de vue du système d'exploitation client, le périphérique mappé se présente exactement comme un fichier de disque virtuel stocké dans un volume VMFS. Ses caractéristiques matérielles réelles sont masquées. En utilisant un disque brut en mode virtuel, vous pouvez bénéficier des avantages de VMFS, tels que le verrouillage de fichier avancé, pour la protection des données, et les snapshots, pour la rationalisation des processus de développement. Le mode virtuel offre en outre une meilleure portabilité entre matériels de stockage que le mode physique, dans la mesure où il présente le même comportement qu'un fichier de disque virtuel.

- Le mode physique détermine une virtualisation SCSI minimale du périphérique mappé, ce qui garantit une flexibilité optimale pour les logiciels de gestion SAN. En mode physique, VMkernel transmet toutes les commandes SCSI au périphérique à une seule exception près : la commande REPORT LUNs est en effet virtualisée afin que VMkernel puisse isoler le LUN pour la machine virtuelle propriétaire. À part cela, toutes les caractéristiques physiques du matériel sous-jacent sont exposées. Le mode physique est utilisé pour exécuter les agents de gestion SAN ou d'autres logiciels basés sur les cibles SCSI installés sur la machine virtuelle.

7-32 Redimensionnement dynamique d’un disque virtuel

Vous pouvez augmenter la taille d’un disque virtuel appartenant à une machine virtuelle sous tension :

- Ce disque ne doit pas être associé à des snapshots.
- Des outils système seront peut-être nécessaires pour rendre l’espace supplémentaire utilisable.



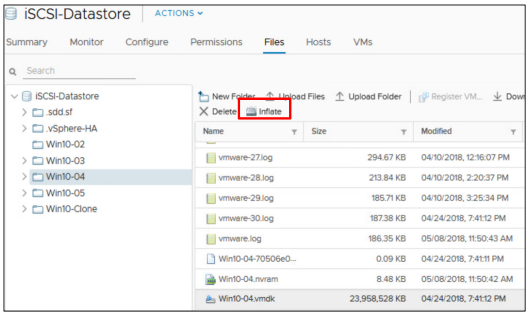
Lorsque vous gonflez un disque à provisionnement fin, le disque virtuel gonflé occupe la totalité de l’espace de banque de données initialement provisionné pour lui. Le fait de gonfler un disque à provisionnement fin convertit celui-ci en disque virtuel à format définitif.

7-33 Gonflage de disques à provisionnement fin

Vous pouvez convertir un disque virtuel à provisionnement fin en disque virtuel de format définitif avec mise à zéro immédiate.

Pour gonfler un disque à provisionnement fin :

- La machine virtuelle doit être hors tension.
- Cliquez avec le bouton droit sur le fichier .vmdk de la machine virtuelle et sélectionnez « Inflate ».



Vous pouvez également utiliser vSphere Storage vMotion et sélectionner un disque à provisionnement définitif comme destination.

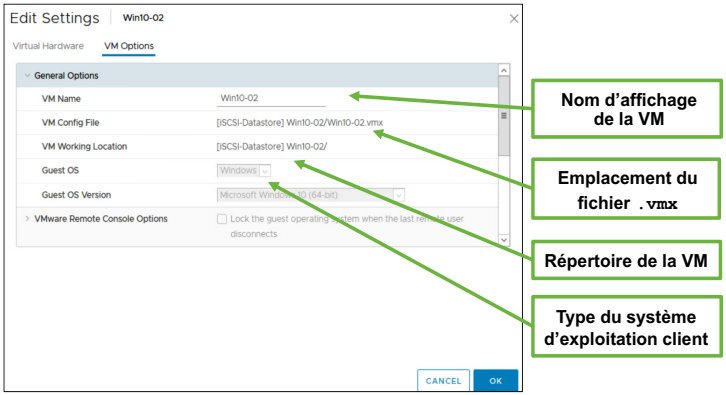
Le volet VM vous permet de modifier différentes caractéristiques de la machine virtuelle, telles que son nom d'affichage ou le type du système d'exploitation client installé. L'emplacement et le nom du fichier de configuration (fichier `.vmx`) ainsi que l'emplacement du répertoire de la machine virtuelle sont également indiqués.

Vous pouvez sélectionner les chaînes de texte correspondant au fichier de configuration et à l'emplacement de travail en vue de les copier et de les coller dans un document. Cependant, seuls le nom d'affichage et le type de système d'exploitation client peuvent être modifiés.-

La modification du nom d'affichage est sans effet sur le nom des fichiers de la machine virtuelle ni sur celui du répertoire dans lequel elle est stockée. Lors de la création d'une machine virtuelle, les noms des fichiers et du répertoire associés sont basés sur son nom d'affichage. En revanche, les modifications ultérieures du nom d'affichage ne se répercutent pas sur ces noms de fichier et de répertoire.

7-34 Options de machine virtuelle

Sous l'onglet **VM Options**, vous pouvez définir ou modifier les options de la machine virtuelle pour exécuter des scripts VMware Tools, contrôler les accès utilisateur à la console distante, configurer le comportement au démarrage, etc.



Le volet VMware Tools détermine la façon dont l'instance de VMware Tools installée sur la machine virtuelle réagit à certains événements externes. Ces options vous permettent de personnaliser les boutons de mise sous tension de la machine virtuelle. La machine virtuelle doit être mise hors tension avant toute modification de ces paramètres.

Vous pouvez cocher la case **Check and upgrade VMware Tools before each power on** de façon à vérifier si une version plus récente de VMware Tools est disponible. S'il existe une version plus récente, VMware Tools est mis à niveau lors du prochain cycle d'alimentation de la machine virtuelle. La case à cocher **Synchronize guest time with host** permet de synchroniser l'horloge du système d'exploitation client avec l'hôte.

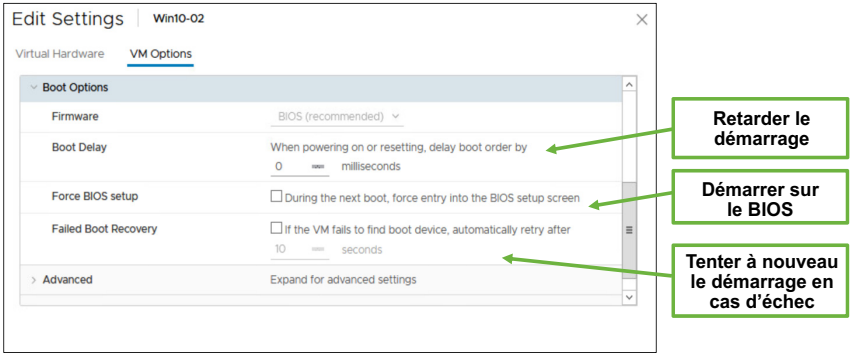
Pour plus d'informations sur les meilleures pratiques de synchronisation concernant les systèmes d'exploitation client que vous utilisez, consultez les articles 1318 et 1006427 de la base de connaissances VMware, disponibles respectivement à l'adresse http://kb.vmware.com/kb/1318 et à l'adresse http://kb.vmware.com/kb/1006427.

7-35 Options de VMware Tools

Vous pouvez parfois être amené à configurer les options de démarrage :

- Lorsque vous créez une machine virtuelle et sélectionnez un système d'exploitation client, l'option **BIOS** ou **EFI** est sélectionnée automatiquement, selon le type de microprogramme pris en charge par le système d'exploitation. Les systèmes d'exploitation client Mac OS X Server prennent uniquement en charge l'option EFI (Extensible Firmware Interface). Si les options BIOS et EFI sont toutes deux prises en charge par le système d'exploitation, vous avez la possibilité de redéfinir l'option de démarrage si nécessaire. Cette modification doit toutefois intervenir avant l'installation du système d'exploitation client.
- Le volet « Boot Delay » vous permet de spécifier un délai d'attente entre la mise sous tension d'une machine virtuelle et le démarrage effectif du système d'exploitation client. Un démarrage retardé permet d'échelonner les démarrages lorsque plusieurs machines virtuelles sont mises sous tension en même temps.
- Le volet « Force BIOS Setup » vous offre la possibilité de redéfinir les paramètres du BIOS, notamment pour forcer une machine virtuelle à démarrer à partir d'un CD/DVD. La prochaine fois que la machine virtuelle sera mise sous tension, elle accédera directement au BIOS. Cet accès forcé au BIOS est nettement plus simple que la manœuvre consistant à mettre la machine virtuelle sous tension, ouvrir une console, puis appuyer aussi rapidement que possible sur la touche F2 pour accéder au BIOS.
- Le volet « Failed Boot Recovery » vous permet de demander à la machine virtuelle d'effectuer une nouvelle tentative de démarrage au bout de 10 secondes (délai par défaut) lorsqu'elle ne détecte aucun périphérique de démarrage.

7-36 Options de démarrage



7-37 Laboratoire 10 : Modification de machines virtuelles

Modifier le matériel d'une machine virtuelle et ajouter un LUN brut à une machine virtuelle

1. Cloner une machine virtuelle sous tension
2. Augmenter la taille d'un fichier de disque de machine virtuelle
3. Régler l'allocation de mémoire d'une machine virtuelle
4. Renommer une machine virtuelle dans l'inventaire vCenter Server Appliance
5. Ajouter ou supprimer un LUN brut sur une machine virtuelle

7-38 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les paramètres et les options des machines virtuelles
- Ajouter un périphérique installable à chaud
- Augmenter la taille d'un disque virtuel de manière dynamique
- Ajouter un disque de mappage de périphérique brut (RDM) à une machine virtuelle

7-39 Leçon 4 : Migration de machines virtuelles

7-40 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Vérifier que les exigences propres à vSphere vMotion sont satisfaites, y compris les contraintes et recommandations en matière de CPU
- Effectuer une migration via vSphere vMotion
- Effectuer une migration via vSphere Storage vMotion
- Effectuer une migration vSphere vMotion « Shared-Nothing »
- Expliquer le fonctionnement d'EVC (Enhanced vMotion Compatibility) en mode « cluster » et en mode « par VM » avec vSphere vMotion

Vous pouvez déplacer des machines virtuelles d'un hôte ou d'un emplacement de stockage à un autre par migration à chaud ou à froid. Par exemple, vSphere vMotion vous permet de retirer des machines virtuelles sous tension d'un hôte pour procéder à des opérations de maintenance, équilibrer les charges, colocaliser des machines virtuelles appelées à communiquer entre elles, séparer des machines virtuelles afin de minimiser un domaine de pannes, migrer vers un nouveau matériel serveur, etc.

Différents types de migration sont envisageables selon le type de ressources de la machine virtuelle :

- Le changement limité aux ressources de calcul : la machine virtuelle est migrée sans ses composants de stockage vers une autre ressource de calcul : le hôte, le cluster, le pool de ressources, vApp, etc.
- Le changement limité au stockage : la machine virtuelle et ses composants de stockage (disques virtuels et fichiers de configuration, en toutes combinaisons) sont migrés vers une autre banque de données disponible pour le même hôte.
- Le changement de ressources de calcul et de stockage : la machine virtuelle est migrée vers un autre hôte, et son disque ou son dossier de machine virtuelle est migré vers une autre banque de données. Lorsque vous déplacez les capacités réseau d'une machine virtuelle d'un commutateur distribué à un autre, la configuration et les règles réseau associées aux adaptateurs réseau de cette VM sont transférées vers le commutateur cible.

7-41 Migration de machines virtuelles

La migration d'une machine virtuelle consiste à déplacer celle-ci d'un hôte, d'une banque de données ou d'un système vCenter Server à un autre hôte, une autre banque de données ou un autre système vCenter Server.

Types de migration :

- À froid : pour migrer une machine virtuelle hors tension vers un nouvel hôte ou une nouvelle banque de données.
- Avec interruption : pour migrer une machine virtuelle interrompue vers un nouvel hôte ou une nouvelle banque de données.
- vSphere vMotion : pour migrer une machine virtuelle sous tension vers un nouvel hôte.
- vSphere Storage vMotion : pour migrer les fichiers d'une machine virtuelle sous tension vers une nouvelle banque de données.
- vSphere vMotion « Shared-Nothing » : pour migrer une machine virtuelle sous tension à la fois vers un nouvel hôte et vers une nouvelle banque de données.

L'un des facteurs déterminants pour le choix d'une technique de migration est l'objectif poursuivi. Par exemple, votre but peut être d'arrêter un hôte à des fins de maintenance sans interrompre le fonctionnement des machines virtuelles. Recourez alors à vSphere vMotion pour migrer les machines virtuelles, plutôt qu'à une migration à froid ou à une migration avec interruption. Si vous devez déplacer les fichiers d'une machine virtuelle vers une autre banque de données en vue de rééquilibrer la charge des disques ou d'effectuer une transition vers une nouvelle baie de stockage, utilisez vSphere Storage vMotion.

Certaines techniques de migration, telles que la migration via vSphere vMotion, exigent une configuration matérielle spécifique pour fonctionner correctement. D'autres techniques, comme la migration à froid ou la migration avec interruption, ne présentent pas de contraintes matérielles particulières.

7-42 Comparaison des types de migration

Type de migration	État de fonctionnement de la VM	Changement d'hôte ou de banque de données ?	Entre différentes instances de vCenter Server ?	Stockage partagé requis ?	Compatibilité des CPU
À froid	Désactivée	Hôte ou banque de données, ou les deux	Oui	Non	CPU de différentes familles autorisés
Avec interruption	Avec interruption	Hôte ou banque de données, ou les deux	Oui	Non	Doit satisfaire aux exigences de compatibilité des CPU
vSphere vMotion	Activé	Hôte	Oui	Oui	Doit satisfaire aux exigences de compatibilité des CPU
vSphere Storage vMotion	Activé	Banque de données	Non	Non	S. o.
vSphere vMotion « Shared-Nothing »	Activé	Les deux	Oui	Non	Doit satisfaire aux exigences de compatibilité des CPU

vSphere vMotion permet de migrer des machines virtuelles d'un hôte VMware ESXi à un autre sans perturbation ni interruption de service. vSphere vMotion est sollicité par vSphere DRS pour migrer des machines virtuelles en cours d'exécution entre les différents hôtes à des fins d'équilibrage de charge.

vSphere vMotion transfère l'intégralité de l'état de la machine virtuelle d'un hôte à un autre tout en maintenant le stockage des données dans la même banque de données.

Les informations d'état comprennent le contenu actuel de la mémoire ainsi que toutes les informations servant à définir et identifier la machine virtuelle. Le contenu de la mémoire inclut les données de transaction et les portions du système d'exploitation ou des applications se trouvant dans la mémoire. Les informations de définition et d'identification stockées dans l'état incluent toutes les données qui correspondent aux éléments matériels de la machine virtuelle, telles que :

- Le BIOS
- Les périphériques
- Les CPU
- Les adresses MAC des cartes Ethernet

7-43 Migration via vSphere vMotion

Une migration via vSphere vMotion déplace une machine virtuelle sous tension d'un hôte à un autre.

vSphere vMotion offre les avantages suivants :

- Une meilleure utilisationglobale du matériel
- Assure la continuité du fonctionnement des machines virtuelles durant les interruptions de service planifiées des composants matériels
- Permet à vSphere DRS d'équilibrer les machines virtuelles entre les différents hôtes

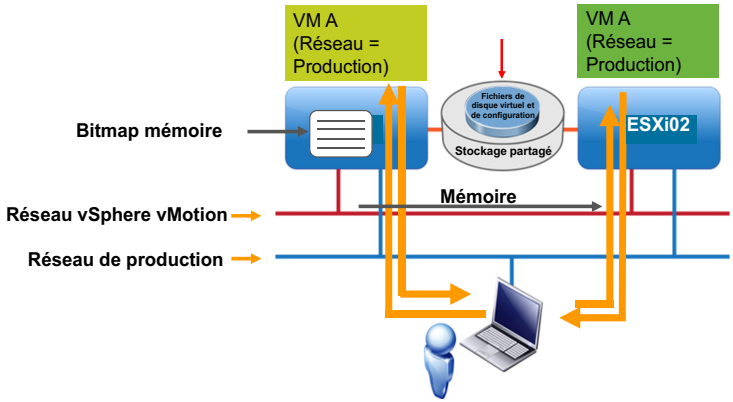
La migration via vSphere vMotion se déroule en plusieurs étapes :

1. Une machine virtuelle fantôme est créée sur l'hôte de destination.
2. L'état de la mémoire de la machine virtuelle est copié de l'hôte source à l'hôte cible via le réseau vSphere vMotion. Les utilisateurs peuvent continuer à accéder à la machine virtuelle et, le cas échéant, à mettre à jour des pages mémoire. La liste des pages modifiées dans la mémoire est conservée sur l'hôte source sous la forme d'un bitmap mémoire.
3. À l'issue de la première passe de copie de l'état de la mémoire, une nouvelle passe de copie de mémoire est exécutée afin de prendre en compte les pages qui auraient été modifiées durant l'itération précédente. Cette itération de la copie de mémoire se poursuit jusqu'à ce qu'il ne reste aucune page modifiée.
4. Une fois que la mémoire de la machine virtuelle a été copiée en quasi-totalité de l'hôte source à l'hôte cible, la machine virtuelle est mise au repos. Aucune autre activité n'a lieu sur la machine virtuelle. Durant la période de mise au repos, vSphere vMotion transfère l'état du périphérique de la machine virtuelle vers l'hôte de destination.

5. Immédiatement après sa mise au repos sur l'hôte source, la machine virtuelle est initialisée et commence à s'exécuter sur l'hôte cible. Une demande GARP (Gratuitous Address Resolution Protocol) notifie au sous-réseau que l'adresse MAC de la machine virtuelle se trouve à présent sur un nouveau port de commutateur.
6. Les utilisateurs accèdent désormais à la machine virtuelle sur l'hôte cible plutôt que sur l'hôte source.
7. Les pages mémoire que la machine virtuelle utilisait sur l'hôte source sont marquées comme disponibles.

7-44 Workflow de la migration via vSphere vMotion

L'hôte source (ESXi01) et l'hôte de destination (ESXi02) ont accès à la banque de données partagée contenant les fichiers de la machine virtuelle.



La migration via vSphere vMotion peut générer une erreur dans certaines conditions. En ce cas, la migration s'interrompt et ne reprend qu'une fois l'erreur corrigée.

Par défaut, la migration d'une machine virtuelle via vSphere vMotion génère une erreur si cette machine virtuelle est connectée à un commutateur virtuel interne (c'est-à-dire un commutateur qui n'est pas directement connecté à une carte d'interface réseau physique). Cette restriction a été établie afin de garantir la disponibilité du serveur durant une migration à chaud, ainsi que pour éviter les problèmes es résultant du fait que l'hôte VMware ESXi cible serait mal configuré et dépourvu de connexion active au réseau physique. Elle ne tient cependant pas compte des cas dans lesquels une machine virtuelle en mode passerelle est utilisée pour filtrer le trafic entre la charge de travail et le réseau physique. Vous pouvez activer vSphere vMotion lors de l'utilisation de machines virtuelles en mode passerelle dédiées à des services de sécurité ou autres. Pour en savoir plus, consultez l'article 1006701 de la base de connaissances VMware, disponible à l'adresse suivante : http://kb.vmware.com/kb/1006701.

Vous ne pouvez pas recourir à vSphere vMotion pour migrer une machine virtuelle exploitant un périphérique virtuel adossé à un périphérique de l'hôte VMware ESXi. Vous devez par conséquent déconnecter ces périphériques avant de procéder à la migration de la machine virtuelle. vSphere vMotion génère également des avertissements dans certaines situations, notamment lorsqu'une machine virtuelle est configurée pour accéder à un lecteur de CD/DVD local ou à une image de disquette alors qu'elle ne leur est pas connectée. La migration via vSphere vMotion peut néanmoins se poursuivre même si les avertissements n'ont pas été traités.

Pour obtenir la liste complète des contraintes liées à la migration via vSphere vMotion, consultez le guide *Gestion de vCenter Server et des hôtes*, disponible à l'adresse suivante : http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

7-45 Contraintes liées à la migration via vSphere vMotion

La machine virtuelle doit satisfaire aux exigences suivantes :

- Elle ne doit pas présenter de connexion active avec un commutateur virtuel interne, car la migration générerait en ce cas une erreur.
- Elle ne doit pas être configurée avec l'affinité CPU.
- Elle ne doit pas être connectée à un périphérique virtuel, tel qu'un lecteur de CD/DVD ou de disquette, sur lequel est montée une image locale.
- Si son fichier d'échange n'est pas accessible à l'hôte de destination, vSphere vMotion doit être en mesure de créer un fichier d'échange qui lui soit accessible avant l'opération de migration.
- Si elle utilise un disque RDM, celui-ci et le LUN correspondant doivent être accessibles à l'hôte de destination.

Un coût en ressources est affecté à chaque opération, telle que la migration via vSphere vMotion ou le clonage d'une machine virtuelle. À chaque hôte, banque de données ou ressource réseau correspond un coût maximal supportable à un moment donné. Toute nouvelle opération de migration ou de provisionnement dont l'exécution immédiate entraînerait un dépassement de ce coût maximal est mise en file d'attente jusqu'à ce que les ressources requises aient été libérées par l'achèvement d'autres opérations. La nouvelle opération n'est traitée que si les limites afférentes à tous les types de ressources (réseau, banque de données et hôte) sont respectées.

Pour obtenir la liste complète des contraintes liées aux migrations simultanées, consultez le guide *Gestion de vCenter Server et des hôtes*, disponible à l'adresse suivante : http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs

Les hôtes source et de destination doivent remplir certaines conditions pour que la migration via vSphere vMotion puisse aboutir :

- La visibilité des disques virtuels du point de vue du SAN
- L'interconnexion Gigabit Ethernet (ou débit supérieur)
- La configuration réseau cohérente, sur les plans physique et virtuel
- Le CPU appartenant à un même groupe de compatibilité sur les serveurs source et de destination

Pour de meilleures performances, vous pouvez configurer plusieurs cartes d'interface réseau pour vMotion. Pour traiter le trafic vMotion sur plusieurs cartes d'interface réseau, vous pouvez dédier plusieurs groupes de ports au trafic vSphere vMotion, en veillant à ce que chacun de ces groupes de ports soit associé à un adaptateur VMkernel vMotion. Vous pouvez alors connecter une ou plusieurs cartes d'interface réseau à chaque groupe de ports. Le trafic vMotion est ainsi pris en charge par plusieurs cartes d'interface réseau physiques, d'où une augmentation de la bande passante. Pour plus de détails sur la procédure de configuration de plusieurs cartes d'interface réseau pour vMotion, consultez l'article 2007467 de la base de connaissances VMware, disponible à l'adresse suivante : https://kb.vmware.com/kb/2007467.

7-46 Configuration hôte requise pour la migration via vSphere vMotion

Les hôtes source et de destination doivent présenter les caractéristiques suivantes :

- L'accessibilité à tous les types de stockage de la machine virtuelle (Fibre Channel, iSCSI ou NAS) :
  - 128 migrations vSphere vMotion simultanées par banque de données VMFS ou NFS.
- Le réseau 1 Gigabit Ethernet (1 GbE) au minimum :
  - Chaque processus vSphere vMotion actif requiert un débit minimal de 250 Mbit/s sur le réseau vSphere vMotion.
  - Le nombre de migrations vSphere vMotion simultanées est limité à quatre sur un réseau 1 Gbit/s.
  - Le nombre de migrations vSphere vMotion simultanées est limité à huit sur un réseau de 10 Gbit/s (ou plus).
  - Pour des performances optimales, dédiez au moins deux groupes de ports au trafic vSphere vMotion.
- La compatibilité des CPU :
  - Les jeux de fonctionnalités CPU des hôtes source et de destination doivent être compatibles.
  - Certaines fonctionnalités peuvent être dissimulées à l'aide d'EVC ou de masques de compatibilité.

L'une des exigences posées par vSphere vMotion réside dans la compatibilité des CPU entre l'hôte source et l'hôte cible. Par exemple, si l'hyperthreading est activé sur l'hôte source et désactivé sur l'hôte de destination, la migration via vSphere vMotion peut aboutir dans la mesure où cette différence dans les caractéristiques CPU est gérée par VMkernel. En revanche, si les instructions SSE4.1 sont prises en charge par le processeur de l'hôte source mais pas sur celui de l'hôte de destination, ces deux hôtes sont considérés comme incompatibles et la migration via vSphere vMotion échoue. Les instructions SSE4.1 sont des instructions de niveau application qui contournent la couche de virtualisation et pourraient provoquer une instabilité de l'application en cas de divergence consécutive à une migration via vSphere vMotion.

7-47 Contraintes de CPU pour la migration via vSphere vMotion

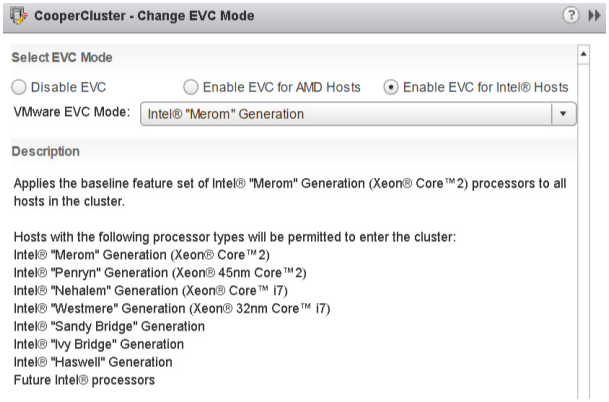
Caractéristiques CPU	Correspondance exacte requise	Motif
Fréquence d'horloge, taille de cache, hyperthreading et nombre de coeurs	S. o.	Ces caractéristiques sont virtualisées par VMkernel.
Fabricant (Intel ou AMD), famille et génération (Opteron4, Intel Westmere)	Oui	Les jeux d'instructions présentent un grand nombre de légères différences.
Présence ou absence des instructions SSE3, SSSE3 ou SSE4.1	Oui	Les instructions multimédias sont utilisables directement par les applications.
Assistance matérielle pour la virtualisation	Pour les VM 32 bits : S. o.	Cette caractéristique est virtualisée par VMkernel.
	Pour les VM 64 bits : Oui	L'implémentation Intel 64 bits avec VMware s'appuie sur Intel VT.

Enhanced vMotion Compatibility (EVC) veille à ce que tous les hôtes d'un cluster présentent le même jeu de fonctionnalités CPU aux machines virtuelles, même si les CPU réels des hôtes sont différents. Le fait de présenter des jeux de fonctionnalités de CPU identiques permet d'éviter que les migrations effectuées via vSphere vMotion échouent en raison d'une incompatibilité entre CPU.

Pour plus d'informations sur la compatibilité des processeurs avec EVC, consultez l'article 1003212 de la base de connaissances VMware, disponible à l'adresse suivante : http://kb.vmware.com/kb/1003212.

7-48 Autres paramètres de cluster : EVC pour la migration via vSphere vMotion

EVC (Enhanced vMotion Compatibility) est une fonctionnalité de cluster permettant d'éviter que les migrations via vSphere vMotion échouent pour des raisons d'incompatibilité entre CPU.



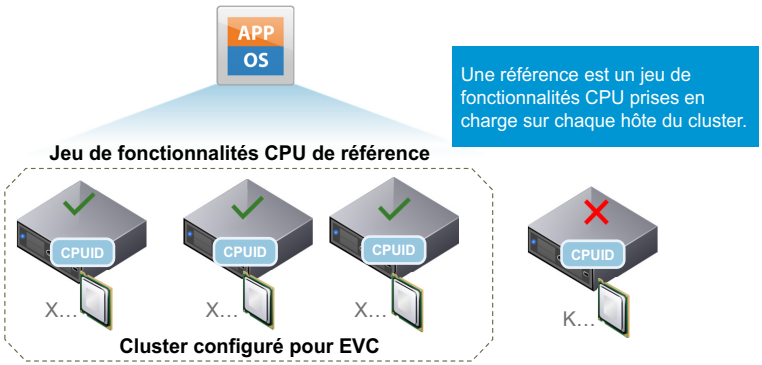
EVC garantit le bon déroulement de la migration vSphere vMotion entre des CPU de différentes générations. Avec EVC, vous pouvez recourir à vSphere vMotion pour migrer des machines virtuelles entre des CPU qui seraient sinon considérés comme incompatibles.

EVC permet à vCenter Server d'assurer la compatibilité vSphere vMotion à l'échelle de tous les hôtes d'un cluster en obligeant ceux-ci à présenter un ensemble de fonctionnalités CPU commun (ou référence) aux machines virtuelles. Une référence est un jeu de fonctionnalités CPU prises en charge sur chaque hôte du cluster. Lors de la configuration d'EVC, vous définissez tous les processeurs hôtes du cluster afin qu'ils présentent les fonctionnalités d'un processeur de référence. Une fois activés pour un cluster, les hôtes qui sont ajoutés à ce cluster sont automatiquement configurés d'après le CPU de référence.

Les hôtes dont la configuration ne peut pas être alignée sur la référence ne sont pas autorisés à rejoindre le cluster. Les machines virtuelles du cluster se voient toujours attribuer un jeu de fonctionnalités CPU identique quel que soit l'hôte sur lequel elles s'exécutent. Étant donné que ce processus est automatique, EVC est simple à utiliser et n'exige aucune connaissance particulière sur les fonctionnalités et les masques CPU.

7-49 CPU de référence pour un cluster EVC

EVC opère au niveau du cluster, et s'appuie sur les CPU de référence pour configurer tous les processeurs du cluster pour lesquels EVC est activé.



Avant de créer un cluster EVC, assurez-vous que les hôtes que vous prévoyez d'ajouter au cluster répondent aux conditions requises.

EVC configure automatiquement les hôtes dont les CPU intègrent la technologie Intel FlexMigration ou AMD-V Extended Migration de telle sorte qu'ils offrent une compatibilité vSphere vMotion avec les hôtes utilisant des CPU plus anciens. EVC veille à ce que tous les hôtes d'un cluster présentent le même jeu de fonctionnalités CPU aux machines virtuelles, même si les CPU réels des hôtes sont différents.

Vous disposez de deux méthodes pour créer un cluster EVC :

- Créer un cluster vide avec la compatibilité EVC activée, puis transférer les hôtes dans ce cluster
- Activer EVC dans un cluster existant

Pour qu'EVC fonctionne correctement, les applications installées sur les machines virtuelles doivent être écrites de manière à utiliser l'instruction CPUID de détection des fonctionnalités CPU conformément aux recommandations des fournisseurs de CPU. vSphere ne peut pas prendre en charge EVC sur les applications qui ne respectent pas les recommandations du fournisseur de CPU concernant la détection des fonctionnalités CPU.

Pour déterminer quels modes EVC sont compatibles avec votre CPU, effectuez une recherche dans le Guide de compatibilité VMware, disponible à l'adresse suivante : http://www.vmware.com/resources/compatibility/search.php?deviceCategory=server. Recherchez le modèle de serveur ou la famille de CPU, puis cliquez sur l'entrée appropriée dans la colonne « CPU Series » afin d'afficher les modes EVC compatibles.

7-50 Conditions requises pour un cluster EVC

Tous les hôtes du cluster doivent satisfaire aux exigences suivantes :

- Utiliser des CPU d'un fournisseur unique, Intel ou AMD :
  - Utiliser des CPU Intel dotés d'une microarchitecture Merom ou ultérieure.
  - Utiliser des processeurs AMD Opteron de première génération ou ultérieurs.
- Être configurés pour la virtualisation matérielle : AMD-V ou Intel VT
- Être configurés pour la technologie Execution-Disable : Technologie AMD No eXecute (NX) ou Intel eXecute Disable (XD)
- Être configurés pour la migration via vSphere vMotion

Les applications exécutées sur les machines virtuelles doivent être compatibles avec l'instruction CPUID.

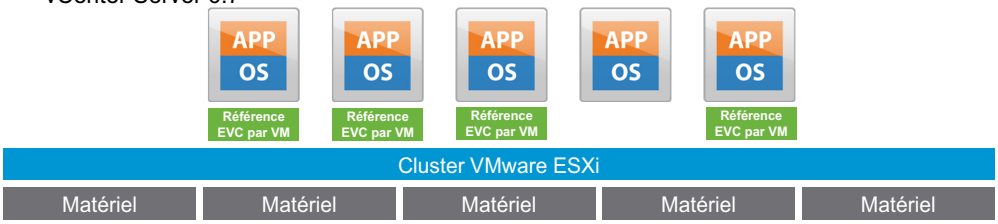
Les caractéristiques CPU du matériel serveur indiquent généralement si les CPU contiennent ou non des fonctions qui affectent leur compatibilité avec vSphere vMotion. Si les spécifications d'un serveur ou ses caractéristiques CPU sont inconnues, vous pouvez les afficher à l'aide de l'utilitaire d'identification de CPU de VMware. Cet utilitaire vous permet de démarrer un serveur et de déterminer si ses CPU intègrent ou non des fonctions telles que SSE3, SSSE3 ou NX/XD.

Vous pouvez télécharger l'utilitaire d'identification de CPU pour les hôtes VMware ESXi depuis l'URL suivante : https://www.vmware.com/support/shared_utilities.html.

7-51 EVC par VM

La fonctionnalité EVC par VM peut être appliquée à tout ou partie des machines virtuelles d'une machine virtuelle.

- Elle facilite la migration des machines virtuelles vers l'extérieur du cluster ou entre différents systèmes vCenter Server ou Data Centers.
- Elle permet d'appliquer des définitions EVC plus granulaires à des VMs déterminées.
- Elle est indépendante du mode EVC défini au niveau du cluster.
- Les conditions requises :
  - ESXi 6.7
  - vCenter Server 6.7



Avec la fonctionnalité Enhanced vMotion Compatibility (EVC) par VM, le mode EVC devient un attribut de la machine virtuelle et remplace la génération de processeur spécifique sur laquelle cette VM a démarré au sein du cluster. Elle permet ainsi une migration transparente entre deux Data Centers exploitant des processeurs différents. De plus, cette fonctionnalité est persistante sur chaque VM, qui conserve ainsi son mode EVC après une migration entre cluster ou d'un cycle d'alimentation à un autre.

Dans ce schéma, EVC n'est pas activé sur le cluster. Ce cluster comprend différents modèles de CPU présentant des jeux de fonctionnalités distincts. Les VMs configurées avec EVC par VM peuvent être exécutées sur n'importe quel hôte VMware ESXi répondant au mode EVC spécifié.

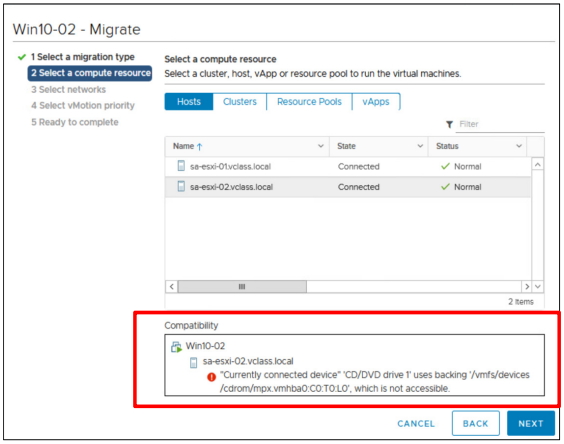
7-52 Modifier les paramètres de masque d'identification de CPU

Le masquage ou la dissimulation de fonctionnalités CPU permet d'élargir la disponibilité d'une machine virtuelle vis-à-vis des hôtes VMware ESXi lors des migrations :

- vCenter Server compare les fonctionnalités CPU accessibles à une machine virtuelle avec celles de l'hôte de destination afin de déterminer s'il convient ou non d'autoriser la migration via vSphere vMotion.
- Le masquage du bit NX/XD empêche la machine virtuelle d'utiliser les fonctionnalités concernées, mais assure en revanche la compatibilité requise pour migrer cette machine virtuelle vers des hôtes VMware ESXi dépourvus de ces fonctionnalités.
- Lorsque le bit NX/XD est visible pour le système d'exploitation client, la machine virtuelle est à même d'exploiter cette fonctionnalité, mais vous ne pouvez migrer cette VM que vers les hôtes sur lesquels la fonctionnalité est activée.

7-53 Vérification des erreurs notifiées par vSphere vMotion

Une fois que vous avez sélectionné l'hôte et le cluster, une validation est effectuée en vue de vérifier que la plupart des exigences de vSphere vMotion sont satisfaites.



Si la validation est concluante, vous pouvez poursuivre avec l'assistant. En cas d'échec, la liste des erreurs et des avertissements générés par vSphere vMotion s'affiche dans le volet « Compatibility ».

Les avertissements sont signalés par un triangle jaune, et les erreurs, par un losange rouge. Les avertissements permettent la poursuite de la migration via vSphere vMotion. En revanche, les erreurs vous empêchent de continuer. Le cas échéant, vous devez quitter l'assistant et résoudre toutes les erreurs signalées avant de tenter à nouveau la migration.

Lorsqu'une migration via vSphere vMotion échoue en cours d'exécution, la machine virtuelle n'est pas migrée et elle continue à s'exécuter sur l'hôte source.

7-54 Migration via vSphere Storage vMotion

VMware vSphere Storage vMotion vous permet de migrer une machine virtuelle et ses fichiers de disque d'une banque de données vers une autre sans interrompre l'exécution de cette machine virtuelle.

vSphere Storage vMotion vous permet d'effectuer les tâches suivantes :

- Retirer des machines virtuelles d'une baie en prévision d'une intervention de maintenance ou de mise à niveau.
- Modifier le type de provisionnement de disque.
- Renommer les fichiers de machine virtuelle transférés dans la banque de données de destination d'après le nom d'inventaire de la machine virtuelle. La migration renomme tous les fichiers de disque virtuel, de configuration, de snapshot et de RAM non volatile (`.nvram`).
- Retirer les machines virtuelles d'un périphérique de stockage, afin de procéder à une opération de maintenance ou de reconfiguration sur ce dernier sans interruption de service sur les machines virtuelles.
- Modifier la répartition des machines virtuelles ou des disques virtuels entre les différents volumes de stockage en vue d'équilibrer la capacité ou d'améliorer les performances.

VMware vSphere Storage vMotion vous permet de migrer une machine virtuelle et ses fichiers de disque d'une banque de données vers une autre sans interrompre l'exécution de cette machine virtuelle. vSphere Storage vMotion vous permet de retirer des machines virtuelles d'une baie en prévision d'une intervention de maintenance ou de mise à niveau. Vous avez également la possibilité d'optimiser les disques en vue d'accroître leurs performances, ou d'en changer le type en vue de récupérer de l'espace.

Vous pouvez choisir de placer la machine virtuelle et tous ses disques à un même emplacement ou bien de sélectionner des emplacements différents pour le fichier de configuration de la machine virtuelle et chacun des disques virtuels. La machine virtuelle ne change pas d'hôte d'exécution lors d'une migration via vSphere Storage vMotion.

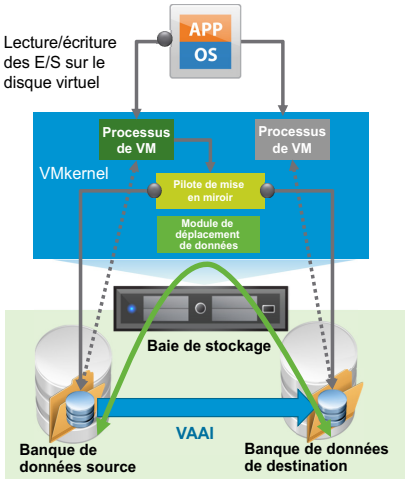
Durant une migration via vSphere Storage vMotion, vous avez la possibilité de redéfinir le type de provisionnement du disque.

Le processus de migration via vSphere Storage vMotion renomme les fichiers de machine virtuelle transférés sur la banque de données de destination d'après le nom d'inventaire de la machine virtuelle. La migration renomme tous les fichiers de disque virtuel, de configuration, de snapshot et de RAM non volatile (`.nvram`). Si les noms cibles dépassent la longueur maximale autorisée pour les noms de fichier, la migration ne peut pas aboutir.

7-55 Fonctionnement de vSphere Storage vMotion

vSphere Storage vMotion exploite une architecture de mise en miroir des E/S pour copier les blocs de disque entre la source et la destination :

1. vSphere Storage vMotion lance la migration du stockage.
2. Il fait appel au module de déplacement de données de VMkernel ou à VMware vSphere® Storage APIs - Array Integration pour copier les données.
3. Il démarre un nouveau processus de machine virtuelle.
4. Il met en miroir les appels d'E/S concernant les blocs de fichier déjà copiés sur un disque virtuel de la banque de données de destination.
5. Il bascule sur le processus de la machine virtuelle de destination pour commencer à accéder à la copie du disque virtuel.



Le processus de migration du stockage copie en une seule passe tous les blocs du disque source vers le disque de destination. Si des blocs sont modifiés après avoir été copiés, ils sont synchronisés depuis la source vers la destination par le pilote de mise en miroir, ce qui permet d'éviter les passes récursives.

Cette approche garantit une parfaite intégrité transactionnelle, ainsi qu'une rapidité suffisante pour rendre le processus imperceptible pour l'utilisateur. Le pilote de mise en miroir utilise le module de déplacement de données de VMkernel pour copier les blocs de données du disque source vers le disque de destination. Ce pilote met en miroir de façon synchrone les écritures effectuées sur les deux disques durant l'exécution de vSphere Storage vMotion.

Enfin, les opérations de vSphere Storage vMotion peuvent s'effectuer en interne sur un seul hôte VMware ESXi ou être sous-traitées à la baie de stockage. Les opérations exécutées en interne sur l'hôte VMware ESXi font appel au module de déplacement de données intégré dans VMkernel. Ces opérations sont sous-traitées à la baie de stockage lorsque celle-ci prend en charge la fonctionnalité d'accélération matérielle VMware vSphere® Storage APIs – Array Integration.

7-56 Consignes et contraintes relatives à vSphere Storage vMotion

Les consignes :

- Planifiez la migration et assurez la coordination avec les administrateurs.
- Effectuez les migrations en période creuse.
- Veillez à ce que l'hôte ait accès aux banques de données source et cible.

Les contraintes :

- Les disques de machine virtuelle indépendants doivent obligatoirement être en mode permanent.

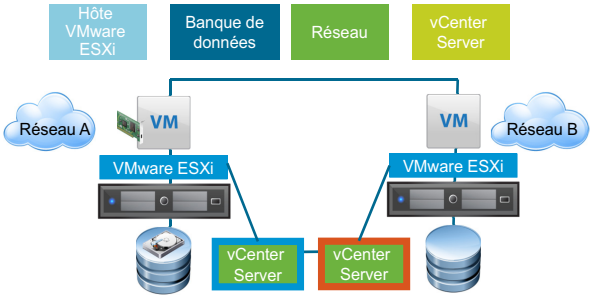
La migration des disques d'une machine virtuelle (VMDK) via vSphere Storage vMotion est soumise à certaines conditions portant sur les ressources et la configuration de cette machine virtuelle et de son système hôte. En particulier, l'hôte sur lequel la machine virtuelle est exécutée doit avoir accès aux banques de données source et cible.

Durant une migration via vSphere Storage vMotion, vous avez la possibilité de redéfinir le type de provisionnement du disque. Le processus de migration via vSphere Storage vMotion renomme les fichiers de machine virtuelle transférés sur la banque de données de destination d'après le nom d'inventaire de la machine virtuelle. La migration renomme tous les fichiers de disque virtuel, de configuration, de snapshot et de RAM non volatile (`.nvram`). Si les noms cibles dépassent la longueur maximale autorisée pour les noms de fichier, la migration ne peut pas aboutir.

7-57 Migration vSphere vMotion « Shared-Nothing »

La migration vSphere vMotion « Shared-Nothing » permet à une machine virtuelle de changer simultanément d'hôte, de banque de données, de réseau et d'instance de vCenter Server, y compris entre deux hôtes dépourvus de stockage partagé.

Cette technique combine les processus vSphere vMotion et vSphere Storage vMotion en une seule opération.



La migration des machines virtuelles peut s'effectuer indépendamment des limitations liées à l'accessibilité du stockage, entre deux hôtes, au sein d'un même cluster ou entre deux clusters, deux Data Centers ou deux instances de vCenter Server.

La fonctionnalité vSphere vMotion « Shared-Nothing » s'avère utile pour les migrations entre clusters, durant lesquelles les systèmes du cluster cible n'ont pas nécessairement accès au stockage du cluster source. Les processus en cours sur la machine virtuelle poursuivent leur exécution durant la migration via vSphere vMotion.

La migration vSphere vMotion « Shared-Nothing » présente notamment un intérêt pour certaines tâches d'administration de l'infrastructure virtuelle :

- La maintenance de l'hôte : La possibilité de retirer les machines virtuelles hébergées sur l'hôte en prévision d'une intervention de maintenance sur celui-ci.
- La maintenance et la reconfiguration du stockage : la possibilité de retirer les machines virtuelles d'un périphérique de stockage afin de procéder à une opération de maintenance ou de reconfiguration, sans interruption de service sur les machines virtuelles.
- La redistribution de la charge de stockage : la possibilité de modifier manuellement la répartition des machines virtuelles ou des disques virtuels entre les différents volumes de stockage en vue d'équilibrer la capacité ou d'améliorer les performances.

Les instances de la fonctionnalité de migration vSphere vMotion « Shared-Nothing » sont décomptées du nombre d'instances simultanées autorisées pour vSphere vMotion et vSphere Storage vMotion. Le nombre de migrations vSphere vMotion « Shared-Nothing » simultanées est limité à deux. L'exécution simultanée de deux instances de migration vSphere vMotion « Shared-Nothing » entraîne la mise en file d'attente de toute demande de création d'instance de vSphere Storage vMotion jusqu'à ce que l'une des instances actives de la migration vSphere vMotion « Shared-Nothing » ait fini de s'exécuter. De même, les instances de migration vSphere vMotion « Shared-Nothing » sont décomptées du nombre maximal d'instances simultanées autorisées pour vSphere vMotion (huit par hôte). Ainsi,

lorsque deux instances de migration vSphere vMotion « Shared-Nothing » sont actives, vous n'avez plus droit qu'à six instances simultanées de vSphere vMotion. Si les huit instances autorisées pour vSphere vMotion sont déjà actives, toute demande de création d'une nouvelle instance de vSphere vMotion « Shared-Nothing » est placée en file d'attente jusqu'à ce que l'une des instances actives de vSphere vMotion ait terminé son exécution.

La fonctionnalité de migration vSphere vMotion « Shared-Nothing » présente exactement le même comportement que vSphere vMotion en ce qui concerne la prise en charge de cartes d'interface réseau multiples. La migration vSphere vMotion « Shared-Nothing » prend également en charge la migration de fichiers d'échange partagés ou non partagés de la même manière que vSphere vMotion, le déplacement du répertoire home d'une machine virtuelle devenant une migration de fichier d'échange non partagé. Le coût plus élevé des instances de migration vSphere vMotion « Shared-Nothing » doit être pris en compte dans les décisions de migration. Ni vSphere DRS ni VMware vSphere® Storage DRS™ n'utilisent la technologie de migration vSphere vMotion « Shared-Nothing ». Bien que la migration vSphere vMotion « Shared-Nothing » ne soit pas proposée par vSphere DRS ni par vSphere Storage DRS, les utilisateurs ont toujours la possibilité d'exécuter manuellement des migrations vSphere vMotion « Shared-Nothing » à l'intérieur d'un cluster vSphere Storage DRS ou vSphere DRS aussi bien qu'entre deux clusters de ce type.

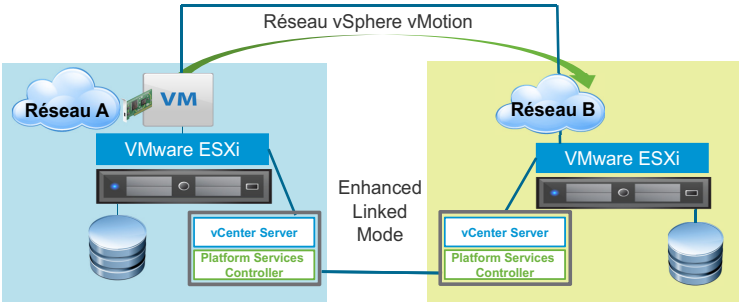
Pour en savoir plus sur les contraintes et limitations liées à la migration vSphere vMotion « Shared-Nothing », consultez le guide *Gestion de vCenter Server et des hôtes*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

7-58 Migrations entre instances de vCenter

vSphere vMotion vous permet de migrer des machines virtuelles entre des systèmes vCenter Server liés.

Les conditions requises :

- Les hôtes VMware ESXi et les systèmes vCenter Server doivent avoir été mis à niveau vers vSphere 6.x.
- Les instances de vCenter Server doivent être configurées en mode Enhanced Linked Mode.
- Les horloges des hôtes doivent être synchronisées.
- Les deux systèmes vCenter Server doivent avoir la même version de vCenter Server.



La migration de machines virtuelles entre des systèmes vCenter Server est utile dans les scénarios de provisionnement de VM suivants :

- Équilibrer les charges de travail entre plusieurs clusters ou instances de vCenter Server.
- Étendre ou réduire la capacité de manière élastique entre les ressources de différentes instances de vCenter Server déployées sur un même site ou dans des zones géographiques distinctes.
- Transférer des machines virtuelles entre des environnements répondant à des objectifs distincts – par exemple, d'un environnement de développement à un environnement de production.
- Transférer des machines virtuelles pour garantir le respect de différents contrats de niveau de service (SLA) concernant l'espace de stockage, les performances, etc.

En cas d'utilisation de vSphere Web Client, les deux instances de vCenter Server doivent être en mode Enhanced Linked Mode et se trouver dans le même domaine vCenter Single Sign-On. L'instance source de vCenter Server aura ainsi la possibilité de s'authentifier auprès de l'instance vCenter Server de destination.

7-59 Couche réseau et pile TCP/IP de VMkernel

La couche de mise en réseau de VMkernel assure la connectivité vers les hôtes et gère le trafic standard de vSphere vMotion, du stockage IP, de vSphere Fault Tolerance, de vSAN, etc.

Vous pouvez également créer des adaptateurs VMkernel sur les hôtes vSphere Replication source et cible pour isoler le trafic des données de réplication.

La pile TCP/IP au niveau de VMkernel :

- La pile TCP/IP par défaut
- La pile TCP/IP de vSphere vMotion
- La pile TCP/IP de provisionnement
- La pile TCP/IP personnalisée

Tenez compte des points ci-après concernant la pile TCP/IP au niveau de VMkernel :

- La pile TCP/IP par défaut : assure la prise en charge de la mise en réseau pour le trafic de gestion entre des hôtes vCenter Server et VMware ESXi et pour le trafic système touchant vSphere vMotion, le stockage IP et VMware vSphere Fault Tolerance.
- La pile TCP/IP de vSphere vMotion : prend en charge le trafic de migration à chaud des machines virtuelles. Utilisez cette pile pour optimiser l'isolation du trafic vSphere vMotion. Une fois l'adaptateur VMkernel créé sur la pile TCP/IP de vSphere vMotion, vous ne pouvez plus utiliser que cette pile pour les migrations vSphere vMotion sur cet hôte. Les adaptateurs VMkernel figurant sur la pile TCP/IP par défaut sont désactivés pour le service vSphere vMotion. Si une migration à chaud utilise la pile TCP/IP par défaut alors que vous configurez des adaptateurs VMkernel avec la pile TCP/IP de vSphere vMotion, cette migration aboutit. Toutefois, les adaptateurs VMkernel impliqués qui figurent sur cette pile TCP/IP par défaut sont désactivés lors des sessions ultérieures de vSphere vMotion.
- La pile TCP/IP de provisionnement : prend en charge le trafic de migration, de clonage ou de création de snapshots de la machine virtuelle à froid. Vous pouvez utiliser la pile TCP/IP de provisionnement pour gérer le trafic NFC (Network File Copy) lors de la migration longue distance de données vSphere vMotion. Les adaptateurs VMkernel configurés avec la pile TCP/IP de provisionnement gèrent le trafic de clonage des disques virtuels des VMs migrées lors de la migration longue distance de données vSphere vMotion. Grâce à cette pile, vous pouvez isoler le trafic des opérations de clonage sur une passerelle distincte. Une fois l'adaptateur VMkernel configuré avec le pilote TCP/IP de provisionnement, tous les adaptateurs de la pile TCP/IP par défaut sont désactivés pour le trafic de provisionnement.

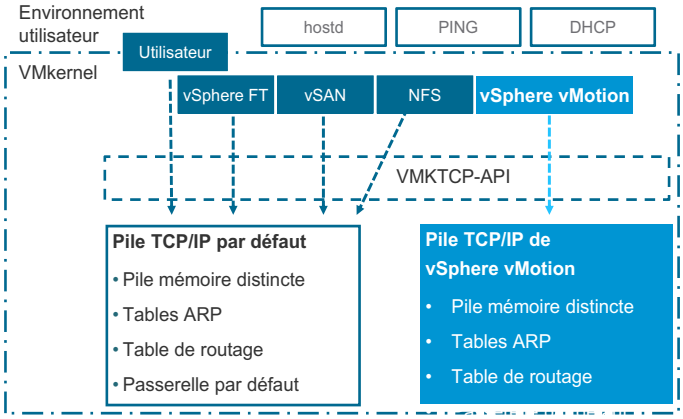
- La pile TCP/IP personnalisée : vous pouvez ajouter une pile TCP/IP personnalisée sur un hôte afin d'acheminer le trafic réseau via une application personnalisée. Ouvrez une connexion SSH à l'hôte et exécutez cette commande vSphere CLI :

```
esxcli network ip netstack add -N="nom_pile"
```

Prenez les mesures de sécurité qui s'imposent pour empêcher tout accès non autorisé au trafic de gestion et système au sein de votre environnement vSphere. Par exemple, vous pouvez isoler le trafic vSphere vMotion sur un réseau distinct, qui inclut uniquement les hôtes VMware ESXi participant à la migration. Isolez le trafic de gestion au sein d'un réseau accessible uniquement aux administrateurs réseau et sécurité.

7-60 Pile TCP/IP de vSphere vMotion

Dans vSphere 6.x, chaque hôte possède une seconde pile TCP/IP dédiée à la migration via vSphere vMotion.



La pile TCP/IP de vSphere vMotion prend en charge le trafic de migration à chaud des machines virtuelles. Utilisez cette pile pour optimiser l'isolation du trafic vSphere vMotion. Une fois l'adaptateur VMkernel créé sur la pile TCP/IP de vSphere vMotion, vous ne pouvez plus utiliser que cette pile pour les migrations vSphere vMotion sur cet hôte.

Les adaptateurs VMkernel figurant sur la pile TCP/IP par défaut sont désactivés pour le service vSphere vMotion. Si une migration à chaud utilise la pile TCP/IP par défaut alors que vous configurez des adaptateurs VMkernel avec la pile TCP/IP de vMotion, cette migration aboutit. Toutefois, les adaptateurs VMkernel impliqués qui figurent sur cette pile TCP/IP par défaut sont désactivés lors des sessions ultérieures de vSphere vMotion.

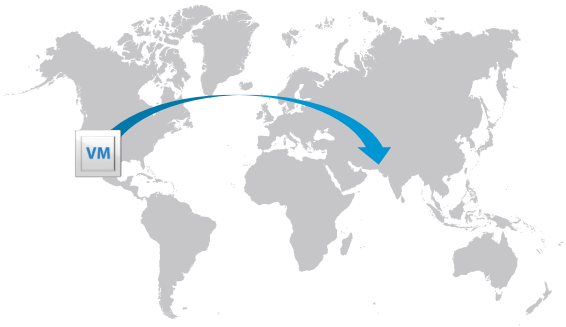
7-61 Migration vSphere vMotion longue distance

La migration vSphere vMotion longue distance correspond à une extension de la migration vSphere vMotion entre différentes instances de vCenter Server.

Ce processus de migration est destiné aux environnements dans lesquels les systèmes vCenter Server sont géographiquement dispersés sur de grandes distances avec une forte latence entre sites.

Cas d'usage pour la migration vSphere vMotion longue distance

- Les migrations permanentes
- La prévention des sinistres
- VMware Site Recovery Manager™ et les tests de prévention des sinistres
- L'équilibrage de charge multisite
- La prise en charge de scénarios d'ajustement aux fuseaux horaires



7-62 Configuration réseau requise pour la migration vSphere vMotion longue distance

Les migrations via vSphere vMotion intervenant entre différentes instances de vCenter Server requièrent des connexions de couche 3 :

- Le réseau de machines virtuelles :
  - La connexion de couche 2 (L2)
  - La même adresse IP de machine virtuelle disponible sur la destination
- Le réseau vSphere vMotion :
  - La connexion de couche 3 (L3)
  - Sécurisé (recommandé en l'absence de vSphere vMotion chiffré, disponible à partir de vSphere 6.5).
  - 250 Mbit/s par opération vSphere vMotion.
  - Le délai d'aller-retour entre les hôtes peut atteindre 150 millisecondes.

7-63 Vérifications de compatibilité réseau pour les migrations entre instances de vCenter Server

vCenter Server procède à plusieurs vérifications de compatibilité réseau visant à prévenir les problèmes de configuration suivants :

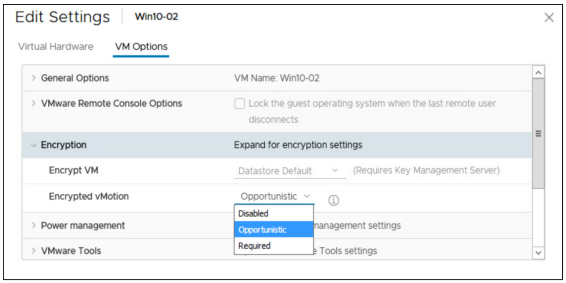
- L'adresse MAC non compatible sur l'hôte de destination
- La migration via vSphere vMotion entre un commutateur distribué et un commutateur standard
- La migration vSphere vMotion entre des commutateurs distribués de versions différentes
- La migration vSphere vMotion vers un réseau interne – par exemple, un réseau sans carte d'interface réseau physique

7-64 vSphere vMotion chiffré

vSphere vMotion utilise systématiquement le chiffrement pour la migration de machines virtuelles chiffrées.

Lorsque les machines virtuelles ne sont pas chiffrées, sélectionnez l'une des options vSphere vMotion proposées pour le paramètre « Encrypted vMotion » :

- **« Disabled »**.
- **« Opportunistic » :** la version chiffrée de vSphere vMotion est utilisée si les hôtes source et de destination la prennent en charge.
- **« Required » :** si la version chiffrée de vSphere vMotion n'est pas prise en charge par l'hôte source ou par l'hôte de destination, la migration via vSphere vMotion échoue.



La version chiffrée de vSphere vMotion garantit la confidentialité, l'intégrité et l'authenticité des données transférées via vSphere vMotion. Elle prend en charge toutes les variantes de vSphere vMotion, y compris la migration entre différents systèmes vCenter Server. La version chiffrée de vSphere Storage vMotion n'est pas prise en charge.

Vous ne pouvez pas désactiver le paramètre vSphere vMotion chiffré pour les machines virtuelles chiffrées.

L'état « Opportunistic » est sélectionné par défaut pour les machines virtuelles non chiffrées.

7-65 Laboratoire 11 : Migration de machines virtuelles

Utiliser vSphere vMotion et vSphere Storage vMotion pour migrer des machines virtuelles

1. Migrer les fichiers d'une machine virtuelle du stockage local vers le stockage partagé
2. Créer un commutateur virtuel et un groupe de ports VMkernel pour la migration via vSphere vMotion
3. Préparer les machines virtuelles pour la démonstration de la migration via vSphere vMotion
4. Faire migrer des machines virtuelles via vSphere vMotion
5. Faire migrer des ressources de calcul et de stockage

7-66 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Vérifier que les exigences propres à vSphere vMotion sont satisfaites, y compris les contraintes et recommandations en matière de CPU
- Effectuer une migration via vSphere vMotion
- Effectuer une migration via vSphere Storage vMotion
- Effectuer une migration vSphere vMotion « Shared-Nothing »
- Expliquer le fonctionnement d'EVC (Enhanced vMotion Compatibility) en mode « cluster » et en mode « par VM » avec vSphere vMotion

7-67 Leçon 5 : Création de snapshots de machine virtuelle

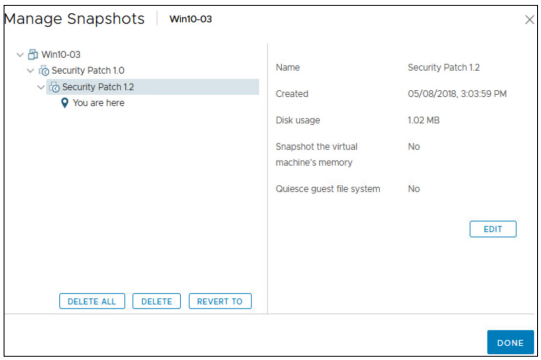
7-68 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Prendre un snapshot d'une machine virtuelle
- Gérer des snapshots multiples
- Supprimer des snapshots de machine virtuelle
- Consolider des snapshots
- Configurer le nombre maximal de snapshots autorisé pour une machine virtuelle :

7-69 Snapshots de machine virtuelle

Les snapshots vous permettent de conserver l'état d'une machine virtuelle de façon à pouvoir restaurer fréquemment ce même état.



Les snapshots offrent notamment la possibilité de restaurer fréquemment un même état sans créer plusieurs machines virtuelles. Par exemple, lors de l'application d'un correctif ou d'une mise à niveau sur le système d'exploitation client d'une machine virtuelle, les snapshots vous permettent de rétablir l'état antérieur si des problèmes apparaissent au cours de ce processus.

Les relations entre snapshots sont du type parent-enfant. Les snapshots sont organisés en arborescence. Chaque snapshot d'une arborescence possède un parent et un ou plusieurs enfants, à l'exception du dernier snapshot, qui est dépourvu d'enfant.

Sur la diapositive, le snapshot nommé Security patch 1.0 possède deux enfants, nommés Security Patch 1.1 et 1.2.

Un snapshot de machine virtuelle comprend essentiellement les états suivants :

- L'état des paramètres : l'état des paramètres (`.nvram` et `.vmx`) et l'état de fonctionnement de la machine virtuelle.
- L'état des disques : l'état des disques associés à la machine virtuelle.
- L'état de la mémoire : contenu de la mémoire de la machine virtuelle (facultatif).

7-70 Prise de snapshots

Vous pouvez prendre un snapshot d'une machine virtuelle alors que celle-ci se trouve à l'état sous tension, hors tension ou interrompu.

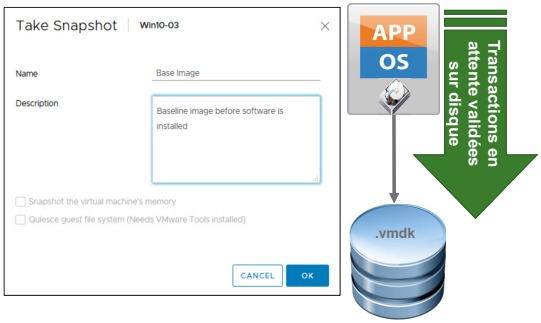
Un snapshot permet de capturer les éléments suivants :

- La configuration de la machine virtuelle
- L'état de la mémoire de la machine virtuelle (facultatif)
- Les disques virtuels
- Les mappages de périphériques bruts (RDM) en mode de compatibilité virtuelle

Un snapshot ne capture pas les éléments suivants :

- Les disques de machine virtuelle indépendants (en mode permanent ou non permanent)
- Les mappages de périphériques bruts (RDM) en mode de compatibilité physique

La prise de snapshots des machines virtuelles n'est pas recommandée en tant que stratégie de sauvegarde.



Chaque snapshot permet de capturer l'intégralité de l'état de la machine virtuelle au moment de la prise de ce snapshot, ce qui inclut les éléments suivants :

- L'état de la mémoire : contenu de la mémoire de la machine virtuelle. L'état de la mémoire n'est capturé que si la machine virtuelle est sous tension et que vous cochez la case **Snapshot the virtual machine's memory** (sélection par défaut).
- L'état des paramètres : l'état des paramètres de la machine virtuelle.
- L'état des disques : l'état de tous les disques de la machine virtuelle.

Au moment de la prise du snapshot, vous avez également la possibilité de mettre au repos le système d'exploitation client. Cette action met uniquement au repos le système de fichiers du système d'exploitation client.

Les snapshots des disques RDM en mode de compatibilité physique ne sont pas pris en charge.

ATTENTION

La prise de snapshots des machines virtuelles n'est pas recommandée en tant que stratégie de sauvegarde.

7-71 Types de snapshot

Un disque delta ou enfant est créé lors de la création d'un snapshot :

- Dans la banque de données VMFS, le disque delta correspond à un disque de format sparse.
- Selon le type de la banque de données, les disques delta utilisent différents formats sparse.

Type de snapshot	Type de banque de données	Nom de fichier	Taille de bloc
VMFSsparse	VMFS5 avec disque virtuel d'une taille inférieure à 2 To	#-delta.vmdk	512 octets
SEsparse	• VMFS6 • VMFS5 avec disque virtuel d'une taille supérieure à 2 To • Format à optimisation d'espace (provisionnement fin) • Permet la récupération de disque (unmap)	#-sesparse.vmdk	4 Ko
vsanSparse	vSAN	Objet delta	4 Mo

Selon le type de votre banque de données, les disques delta utilisent différents formats sparse.

- VMFSsparse : VMFS5 utilise le format VMFSsparse pour les disques virtuels d'une taille inférieure à 2 To. VMFSsparse est implémenté au-dessus de VMFS. La couche VMFSsparse traite les E/S émises vers un snapshot de machine virtuelle. Techniquement, VMFSsparse est un fichier journal Redo initialement vide qui est créé immédiatement après la prise d'un snapshot de machine virtuelle. Ce journal Redo se développe jusqu'à atteindre la taille de son disque virtuel (VMDK) de base, au moment où ce VMDK est entièrement réécrit avec de nouvelles données après la création du snapshot de machine virtuelle. Ce journal Redo correspond à un fichier stocké dans la banque de données VMFS. Lors de la création du snapshot, le VMDK de base associé à la VM est remplacé par le VMDK de format sparse nouvellement créé.
- SEsparse : SEsparse est le format utilisé par défaut pour tous les disques delta stockés dans les banques de données VMFS6. Dans VMFS5, le format SEsparse est utilisé pour les disques virtuels d'une taille égale ou supérieure à 2 To. Le format SEsparse est similaire à VMFSsparse à quelques améliorations près. Il s'agit d'un format à optimisation d'espace prenant en charge la technique de récupération d'espace. La récupération d'espace repose sur le marquage des blocs supprimés par le système d'exploitation client. Le système envoie des commandes à la couche SEsparse de l'hyperviseur afin de démapper ces blocs. Ce démappage permet de récupérer l'espace alloué par SEsparse une fois que le système d'exploitation client a supprimé ces données.

7-72 Fichiers de snapshot de machine virtuelle (1)

Un snapshot se compose d'un ensemble de fichiers.

`-Snapshot#.vmsn` : l'état de la configuration

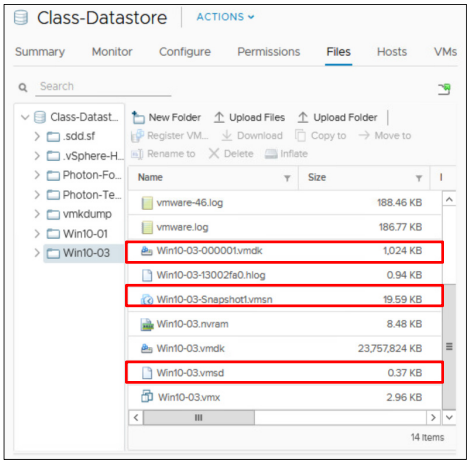
`-Snapshot#.vmem` : l'état de la mémoire (facultatif)

`-00000#.vmdk` : descripteur de disque

`-00000#-delta.vmdk` : delta VMFS5

`-00000#-sesparse.vmdk` : delta VMFS6

Le fichier `.vmsd` contient les noms, les descriptions et les relations de tous les snapshots de la machine virtuelle.



Une machine virtuelle peut être dotée d'un ou plusieurs snapshots. Chaque prise de snapshot entraîne la création des fichiers suivants :

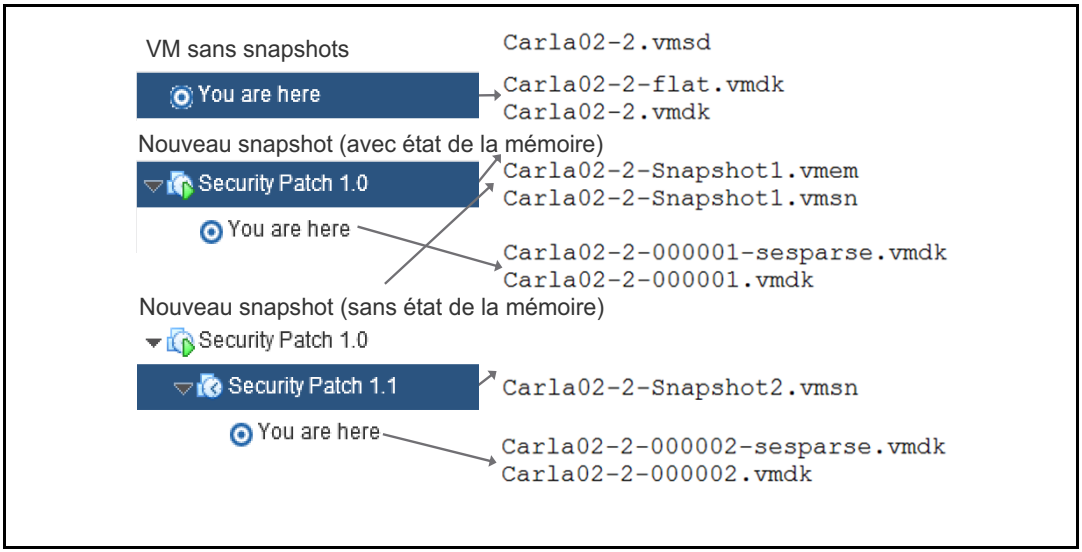
- Le fichier de disque delta : lorsque vous prenez un snapshot d'une machine virtuelle, l'état de chaque disque virtuel est conservé, ce qui exclut les RDM physiques et les disques virtuels marqués comme indépendants. La machine virtuelle cesse d'écrire dans son fichier *nom_VM*-`flat.vmdk` et les écritures sont redirigées vers *nom_VM*-`######-delta.vmdk` (où ###### correspond à un numéro de séquence incrémenté). Vous pouvez exclure un ou plusieurs disques de machine virtuelle d'un snapshot en leur attribuant le statut de disques indépendants. La configuration d'un disque virtuel en mode indépendant intervient généralement lors de la création de ce disque virtuel, mais cette option peut être redéfinie à tout moment dès lors que la machine virtuelle est hors tension.
- Le fchier de descripteur de disque : *nom_VM*-`00000#.vmdk`. Il s'agit d'un petit fichier texte contenant des informations relatives au snapshot.
- Le fichier d'état de configuration : *nom_VM*-`Snapshot#.vmsn`. # correspond à un numéro de séquence incrémenté à partir de 1. Ce fichier contient l'état de la mémoire active de la machine virtuelle au moment de la prise du snapshot, ce qui comprend le matériel virtuel, l'état de fonctionnement et la version du matériel.
- Le fichier d'état de la mémoire : *nom_VM*-`Snapshot#.vmem`. Ce fichier n'est créé que si l'option d'inclusion de l'état de la mémoire était sélectionnée lors de la création du snapshot. Il contient l'intégralité du contenu de la mémoire de la machine virtuelle lors de la prise du snapshot.

- Le fichier delta du snapshot : *nom_VM*-00000#-delta.vmdk. Ce fichier contient les modifications apportées aux données du disque virtuel depuis la prise du snapshot.
- Le fichier de mémoire active de snapshot : *nom_VM*-Snapshot#.vmem. Ce fichier stocke le contenu de la mémoire de la machine virtuelle dans le cas où l'option d'inclusion de la mémoire est sélectionnée lors de la création du snapshot.
- *nom_VM*.vmsd est le fichier contenant la liste des snapshots, créé en même temps que la machine virtuelle. Il permet de tenir à jour les informations relatives aux snapshots de la machine virtuelle en vue de la création de la liste des snapshots affichée dans vSphere Web Client. Ces informations comprennent le nom du fichier de snapshot .vmsn et celui du fichier de disque virtuel.
- Le fichier d'état de snapshot présente l'extension .vmsn et permet de stocker l'état d'une machine virtuelle au moment de la prise d'un snapshot. Un nouveau fichier .vmsn est créé chaque fois que vous prenez un snapshot pour une machine virtuelle. Ce fichier est supprimé lors de la suppression du snapshot correspondant. La taille de ce fichier varie en fonction des options sélectionnées lors de la prise du snapshot. Par exemple, l'inclusion de l'état de la mémoire de la machine virtuelle dans le snapshot a pour effet d'augmenter la taille du fichier .vmsn.

Vous pouvez exclure un ou plusieurs disques de machine virtuelle d'un snapshot en attribuant à l'un des disques virtuels le statut de disque indépendant. L'activation du mode indépendant intervient généralement au moment de la création du disque virtuel. Si le disque virtuel n'a pas été configuré en mode indépendant lors de sa création, vous devez mettre la machine virtuelle hors tension pour activer ce mode.

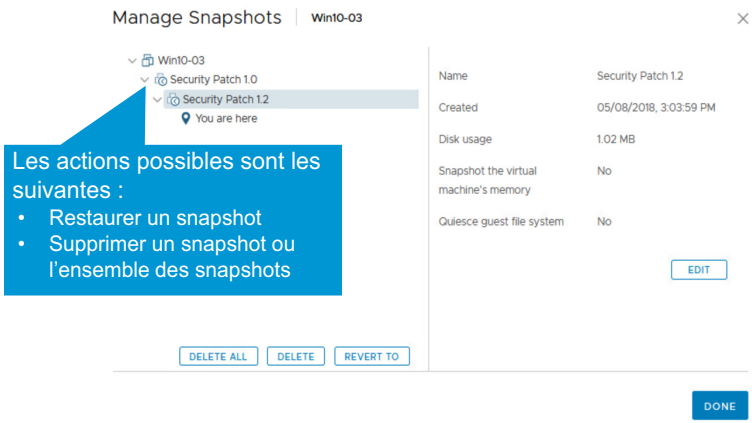
D'autres fichiers peuvent également être créés, selon la version du matériel de machine virtuelle. Par exemple, chaque snapshot d'une machine virtuelle sous tension est associé à un fichier *nom_snapshot_numéro*.vmem contenant la mémoire principale du système d'exploitation client, enregistrée au sein de ce snapshot.

7-73 Fichiers de snapshot de machine virtuelle (2)



7-74 Gestion des snapshots

L'onglet **Snapshot** vous permet d'afficher tous les snapshots générés pour la machine virtuelle active et d'agir directement sur ceux-ci.



L'onglet **Snapshot** propose les actions suivantes :

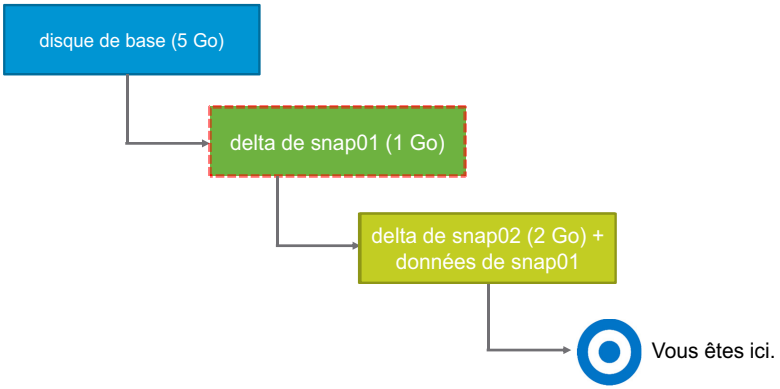
- **Edit Snapshot** : permet de modifier le nom et la description du snapshot.
- **Delete Snapshot** : supprime le snapshot de Snapshot Manager, puis consolide les fichiers de snapshot sur le disque de snapshots parent et procède à une fusion avec le disque de base de la machine virtuelle.
- **Delete All Snapshots** : valide tous les snapshots intermédiaires antérieurs à l'icône d'état actuel (« Vous êtes ici ») dans le fichier de disque de machine virtuelle Tulika01-03, puis supprime tous les snapshots associés à la machine virtuelle concernée.
- **Revert to** : vous permet de restaurer un snapshot déterminé pour rétablir l'état correspondant. Le snapshot que vous restaurez devient le nouveau snapshot actuel.

Le fait de restaurer un snapshot ramène tous les éléments associés à l'état dans lequel ils se trouvaient au moment de la prise de ce snapshot. Si vous souhaitez que la machine virtuelle soit dans un certain état (interrompue, sous tension ou hors tension) lorsque vous la redémarrerez, veillez à ce qu'elle se trouve dans cet état lors que vous prenez le snapshot.

La suppression d'un snapshot (**Delete Snapshot** ou **Delete All Snapshots**) consolide les modifications entre les snapshots et les états de disque antérieurs. Le fait de supprimer un snapshot entraîne également l'écriture sur le disque parent de toutes les données du disque delta contenant les informations relatives au snapshot supprimé. Lorsque vous supprimez le snapshot parent de base, toutes les modifications sont fusionnées avec le disque de base de la machine virtuelle.

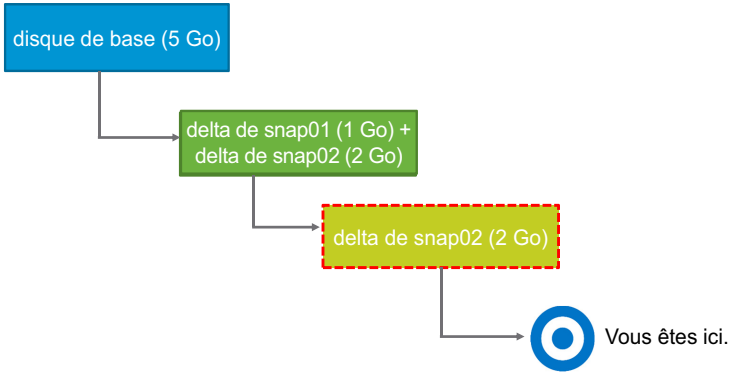
7-75 Suppression de snapshots de machine virtuelle (1)

Si vous supprimez un snapshot se trouvant à un ou plusieurs niveaux en amont de l'icône d'état actuel (« Vous êtes ici »), l'état de ce snapshot est supprimé. Les données de snap01 sont validées au niveau enfant (snap02), et l'état de base pour snap02 est conservé.



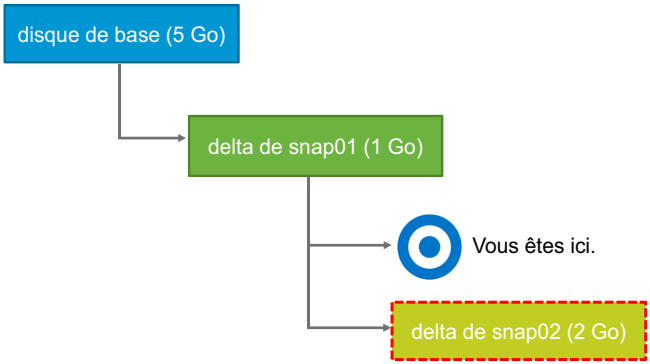
7-76 Suppression de snapshots de machine virtuelle (2)

Si vous supprimez le snapshot actuel, les modifications correspondantes sont validées au niveau de son parent. Les données de snap02 sont validées et fusionnées avec celles de snap01, et le fichier snap02 -delta.vmdk est supprimé.



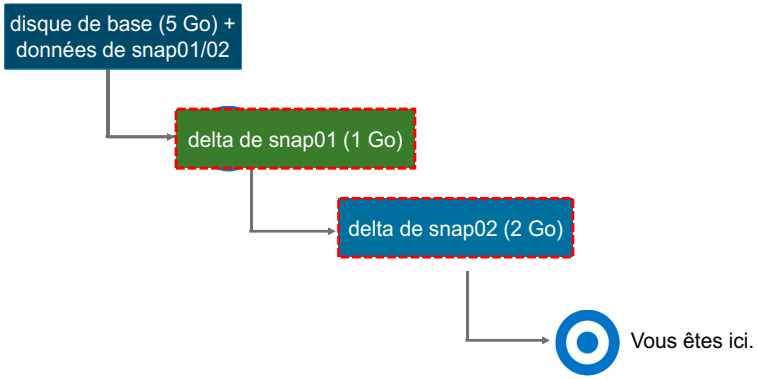
7-77 Suppression de snapshots de machine virtuelle (3)

Si vous supprimez un snapshot situé un ou plusieurs niveaux en aval de l'icône « Vous êtes ici », les snapshots suivants sont également supprimés : vous ne pourrez donc plus restaurer les états correspondants. Le delta snap02 est supprimé.



7-78 Suppression de tous les snapshots d'une machine virtuelle

Le mécanisme de suppression de tous les snapshots optimise l'utilisation de l'espace de stockage. La taille du disque de base n'augmente pas. Comme c'est le cas lors de la suppression d'un seul snapshot, les blocs modifiés dans le snapshot viennent écraser les blocs correspondants du disque de base.



Dans cette diapositive, snap01 est validé dans le disque de base en préalable à la validation de snap02.

Tous les snapshots placés en amont de l'icône « Vous êtes ici » sont validés en remontant jusqu'au disque de base. Tous les snapshots situés en aval de cette icône sont supprimés.

7-79 À propos de la consolidation des snapshots

La consolidation des snapshots est un moyen d'appliquer une chaîne de snapshots sur les disques de base quand Snapshot Manager indique qu'il n'existe aucun snapshot alors que des fichiers delta sont encore présents dans la banque de données.

La consolidation des snapshots vise à résoudre certains problèmes susceptibles de se produire avec les snapshots :

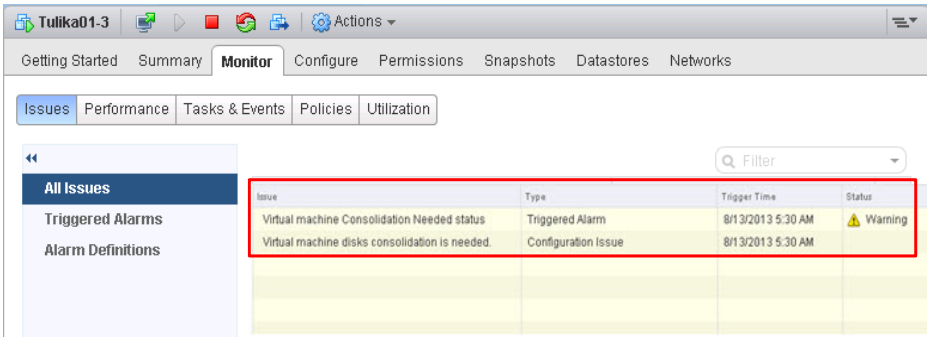
- Le fichier de descripteur de snapshot a été validé correctement, de sorte que la fenêtre **Snapshot** indique que tous les snapshots ont été supprimés.
- Les fichiers de snapshot `(-delta.vmdk)` continuent à faire partie de la machine virtuelle.
- Les fichiers de snapshot continuent à grossir jusqu'à épuiser l'espace de banque de données alloué à la machine virtuelle.

La consolidation des snapshots est un moyen de nettoyer les fichiers delta superflus d'une banque de données. Si une machine virtuelle dépourvue de snapshots comporte néanmoins des fichiers delta de snapshot, la consolidation permet d'appliquer toute la chaîne des snapshots désignés par ces fichiers delta et de supprimer ces derniers.

Sans consolidation des snapshots, les fichiers de snapshot risquent de s'étendre jusqu'à occuper tout l'espace disponible dans la banque de données de la machine virtuelle.

7-80 Détermination du moment où une consolidation des snapshots est nécessaire

Un message d'avertissement apparaît sous l'onglet **Monitor > Issues** de la machine virtuelle pour informer les utilisateurs qu'une consolidation est nécessaire.

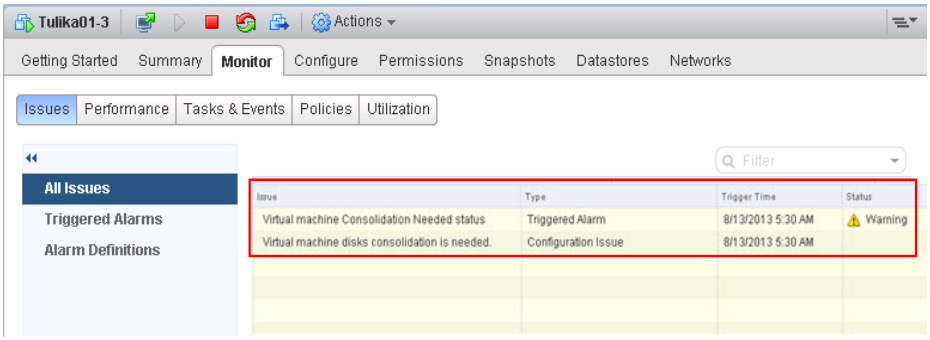


En relation avec la consolidation des snapshots, vCenter Server affiche un avertissement lorsque les fichiers de descripteur et de snapshot ne correspondent pas. Lorsque cet avertissement lui est présenté, l'utilisateur a la possibilité de valider les snapshots via vSphere Web Client plutôt qu'à partir d'une session de ligne de commande.

Dans l'exemple représenté, l'onglet **Monitor** signale un problème de consolidation.

7-81 Détermination du moment où une consolidation des snapshots est nécessaire

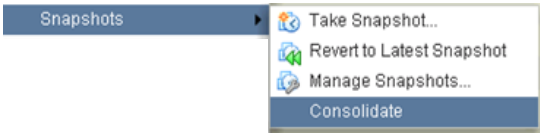
Un message d'avertissement apparaît sous l'onglet **Monitor > Issues** de la machine virtuelle pour informer les utilisateurs qu'une consolidation est nécessaire.



7-82 Exécution de la consolidation des snapshots

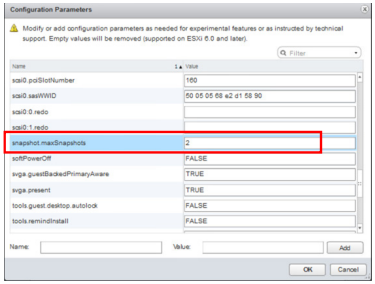
Après avoir reçu le message d'avertissement relatif à la consolidation des snapshots, les utilisateurs peuvent recourir à vSphere Web Client pour consolider les snapshots :

- Pour réconcilier les snapshots, sélectionnez **Snapshots > Consolidate**.
- Tous les disques delta de snapshot sont validés sur les disques de base.



7-83 Configuration du nombre maximal de snapshots autorisé pour une machine virtuelle

Pour définir le nombre maximal de snapshots autorisé pour une machine virtuelle, il vous suffit de modifier la variable snapshot.maxSnapshots = *n* du fichier de configuration.



7-84 Laboratoire 12 : Gestion des machines virtuelles

Effectuer des tâches de gestion des machines virtuelles

1. Annuler l'enregistrement d'une machine virtuelle dans l'inventaire vCenter Server Appliance
2. Enregistrer une machine virtuelle dans l'inventaire vCenter Server Appliance
3. Annuler l'enregistrement des machines virtuelles et les supprimer de la banque de données
4. Prendre des snapshots d'une machine virtuelle
5. Ajouter des fichiers et réaliser un autre snapshot d'une machine virtuelle
6. Restaurer un snapshot de la machine virtuelle
7. Supprimer individuellement un snapshot
8. Supprimer tous les snapshots

7-85 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Prendre un snapshot d'une machine virtuelle
- Gérer des snapshots multiples
- Supprimer des snapshots de machine virtuelle
- Consolider des snapshots
- Configurer le nombre maximal de snapshots autorisé pour une machine virtuelle

7-86 Points clés

- vCenter Server fournit différentes fonctionnalités permettant de provisionner des machines virtuelles, telles que les modèles ou le clonage.
- Le déploiement de machines virtuelles à partir d'un modèle vous permet de créer de nombreuses machines virtuelles de façon rapide et simple.
- Utilisez vSphere vMotion pour déplacer des machines virtuelles alors qu'elles sont sous tension.
- Utilisez vSphere Storage vMotion pour déplacer des machines virtuelles d'une banque de données à un autre.
- Les snapshots de machine virtuelle vous permettent de conserver l'état d'une machine virtuelle de façon à pouvoir restaurer fréquemment ce même état.

Des questions ?

MODULE 8

Gestion et surveillance des ressources

8-2 Vous êtes ici

1. Présentation du cours
2. Présentation de vSphere et du Software-Defined Data Center
3. Création de machines virtuelles
4. vCenter Server
5. Configuration et gestion des réseaux virtuels
6. Configuration et gestion du stockage virtuel
7. Gestion des machines virtuelles
8. **Gestion et surveillance des ressources**
9. vSphere HA, vSphere Fault Tolerance et protection des données
10. vSphere DRS
11. vSphere Update Manager
12. Résolution des problèmes vSphere

8-3 Importance

VMkernel s’efforce, de manière proactive, d’éviter les conflits entre les ressources, mais l’optimisation des performances nécessite malgré tout une analyse des systèmes, ainsi qu’une surveillance en continu.

8-4 Leçons du module

Leçon 1 :	Concepts relatifs aux CPU et à la mémoire virtuels
Leçon 2 :	Contrôles des ressources et pools de ressources
Leçon 3 :	Surveillance du taux d'utilisation des ressources
Leçon 4 :	Utilisation des alarmes

8-5 Leçon 1 : Concepts relatifs aux CPU et à la mémoire virtuels

8-6 Objectifs de la formation

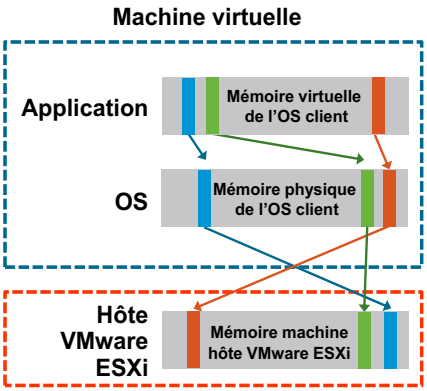
À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Aborder les concepts de mémoire et de CPU au sein d'un environnement virtualisé
- Définir la notion de surdimensionnement des ressources
- Identifier les autres technologies capables d'améliorer l'utilisation de la mémoire
- Décrire le fonctionnement du logiciel VMware vSphere® Virtual Symmetric Multiprocessing et l'utilisation de l'hyperthreading par VMkernel

8-7 Principes de base sur la virtualisation de la mémoire

vSphere présente les couches de mémoire suivantes :

- La mémoire virtuelle du système d'exploitation client est présentée aux applications par le système d'exploitation.
- La mémoire physique du système d'exploitation client est présentée à la machine virtuelle par VMkernel.
- La mémoire hôte gérée par VMkernel offre un espace mémoire adressable et contigu, qui est utilisé par la machine virtuelle.



Lors de l'exécution d'une machine virtuelle, VMkernel crée un espace mémoire adressable contigu pour cette dernière. Cet espace présente les mêmes propriétés que l'espace d'adressage de la mémoire virtuelle présenté aux applications par le système d'exploitation client. Il permet à VMkernel d'exécuter plusieurs machines virtuelles simultanément, tout en protégeant la mémoire de chaque machine contre tout accès par d'autres machines. Du point de vue d'une application exécutée sur la machine virtuelle, VMkernel ajoute une couche supplémentaire de traduction d'adresse, qui mappe l'adresse physique du système client à celle de l'hôte.

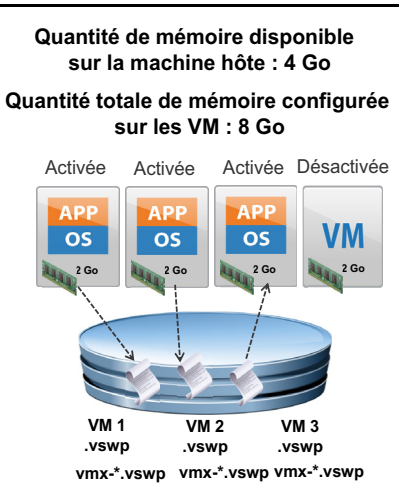
8-8 Surdimensionnement de la mémoire des machines virtuelles

La mémoire est surdimensionnée lorsque l'encombrement mémoire configuré pour l'ensemble des machines virtuelles sous tension dépasse la capacité de mémoire hôte.

Les machines virtuelles n'utilisent pas toujours l'intégralité de la mémoire qui leur est allouée.

Un hôte VMware ESXi transfère la mémoire des machines virtuelles inactives vers les machines virtuelles nécessitant davantage de mémoire, afin d'optimiser l'utilisation de cette dernière.

La capacité supplémentaire de mémoire est stockée dans un fichier d'échange (`.vswp`).



Il peut arriver que la taille totale de la mémoire configurée pour toutes les machines virtuelles dépasse celle de la mémoire physique disponible sur l'hôte. Toutefois, cette condition n'indique pas nécessairement un surdimensionnement de la mémoire. La mémoire est surdimensionnée lorsque la taille de la mémoire de travail de l'ensemble des machines virtuelles dépasse celle de la mémoire physique de l'hôte VMware ESXi.

Grâce aux techniques de gestion de la mémoire utilisées par l'hôte VMware ESXi, les machines virtuelles peuvent utiliser une quantité de RAM virtuelle supérieure à la capacité de RAM physique disponible sur l'hôte. Par exemple, vous pouvez disposer d'un hôte doté de 4 Go de mémoire et exécuter quatre machines virtuelles dotées de 2 Go de mémoire chacune. Dans ce cas, la mémoire est surdimensionnée. Par exemple, si les quatre machines virtuelles sont inactives, la mémoire globale utilisée peut être inférieure à 4 Go. Toutefois, si toutes les machines virtuelles utilisent activement la mémoire, il se peut que l'encombrement mémoire associé dépasse 4 Go et que l'hôte VMware ESXi soit surchargé. Un hôte VMware ESXi peut manquer de mémoire si les machines virtuelles utilisent toute la mémoire réservable dans un environnement au sein duquel la mémoire est surdimensionnée. Bien que les machines virtuelles déjà sous tension ne soient pas affectées, il se peut qu'une nouvelle machine ne puisse pas être allumée pour cause de mémoire insuffisante. Le surdimensionnement se justifie dans la mesure où, en règle générale, certaines machines virtuelles sont peu chargées alors que d'autres le sont beaucoup plus ; de plus, les niveaux d'utilisation relatifs varient au fil du temps.

La mémoire en excès d'une machine virtuelle est stockée au sein d'un fichier d'échange au format `.vswp` . Le processus de surdimensionnement de la mémoire sur l'hôte utilise le fichier d'échange `vmx-*.vswp` pour assurer le stockage et le suivi de la capacité supplémentaire de mémoire. La mémoire disponible dans ce fichier est transférée vers le disque lorsque la mémoire de la machine hôte est surdimensionnée.

8-9 Techniques de récupération de la mémoire

La récupération de mémoire intervient lorsque le pourcentage de capacité de mémoire disponible sur l'hôte est inférieur ou égal à 6 %, ce qui indique que l'hôte ne peut pas satisfaire aux besoins en mémoire.

L'hôte VMware ESXi dispose de plusieurs méthodes pour récupérer de la mémoire auprès des machines virtuelles :

- La rationalisation de l'utilisation des pages de mémoire physique :
  - Le partage de page transparent permet de ne stocker qu'une seule fois les pages qui présentent un contenu identique.
- La réallocation de mémoire d'une machine virtuelle à une autre :
  - Le mécanisme de gonflage de mémoire s'active lorsque la mémoire vient à manquer et oblige les machines virtuelles à utiliser leur propre zone de pagination.
- La compression de mémoire : ce mécanisme vise à rétablir les performances de la mémoire lorsque la contention mémoire est importante.
- L'utilisation de disques SSD au niveau de l'hôte :
  - Le fait d'utiliser un disque SSD sur l'hôte pour stocker un fichier d'échange de cache hôte peut améliorer les performances.
- La pagination de la mémoire des machines virtuelles vers le disque :
  - En raison de son impact négatif sur les performances, l'utilisation de l'espace d'échange de VMkernel constitue le dernier recours.

VMkernel utilise différentes techniques pour récupérer de la mémoire sur un hôte VMware ESXi. Ces techniques sont décrites selon leur ordre d'utilisation par VMkernel :

- La première technique, appelée « partage de page transparent » (« Transparent page sharing », TPS), consiste à rationaliser l'utilisation des pages de mémoire physique. Grâce à elle, les pages qui présentent un contenu identique sont stockées une seule fois. Bien souvent, les charges de travail impliquant plusieurs machines virtuelles utilisent moins de mémoire que si elles étaient exécutées sur des machines physiques. Le partage de pages transparent permet aux hôtes de prendre en charge de manière efficace des niveaux de surdimensionnement de mémoire plus élevés.

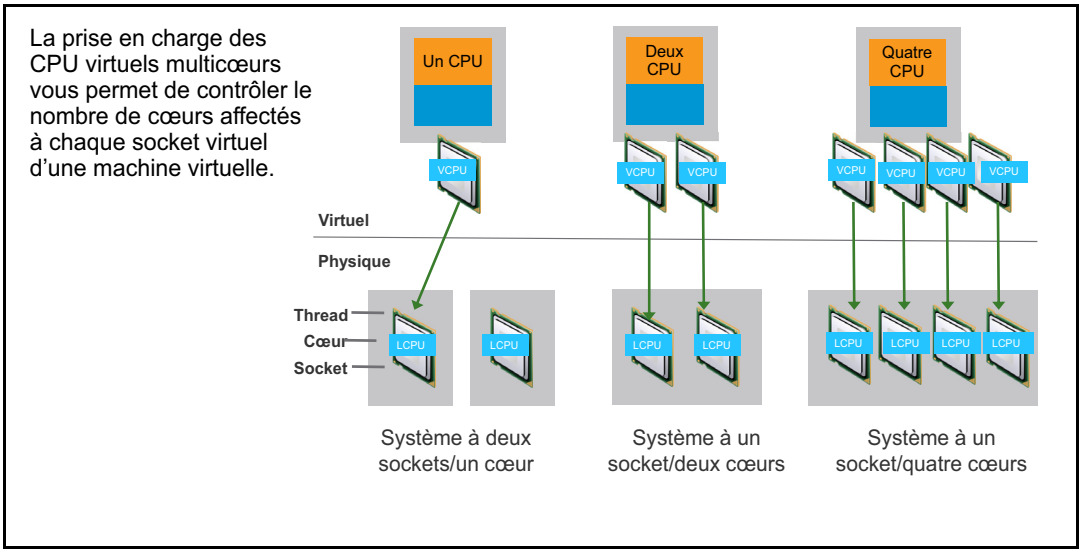
- Lors d'une contention mémoire, VMkernel s'efforce de récupérer la mémoire inactive, ou allouée mais non utilisée, auprès des machines virtuelles. VMkernel transfère la mémoire des machines virtuelles inactives vers celles qui requièrent davantage de mémoire à l'aide du pilote `vmmemctl` (généralement installé avec VMware Tools). Le pilote `vmmemctl` est également appelé « pilote de gonflage de mémoire ».

- VMkernel peut également récupérer la mémoire physique de l'hôte via la compression de mémoire. Cette technique tente de récupérer une partie de la mémoire en compressant les pages pour éviter un transfert vers un fichier d'échange de machine virtuelle en cas de forte contention mémoire.

- Autre méthode de récupération de la mémoire : la création d'un cache hôte sur un disque SSD de la machine hôte. Le système utilise ce cache hôte après avoir tenté les trois autres techniques décrites précédemment (partage de pages transparent, gonflage de mémoire et compression de mémoire) et avant de recourir à un fichier d'échange sur le disque. L'installation d'un fichier de cache d'hôte sur un disque SSD peut améliorer les performances de cette méthode.

- Enfin, la dernière et la moins intéressante des techniques de récupération de mémoire consiste à transférer sur disque la mémoire paginée des machines virtuelles. L'échange sur disque est utilisé lorsque les autres méthodes ne parviennent pas à récupérer la mémoire suffisamment vite pour répondre aux besoins actuels du système. Cette technique entraîne des problèmes de performances importants.

8-10 Configuration de CPU virtuels multicœurs



Vous pouvez configurer une machine virtuelle avec un maximum de 128 VCPU (CPU virtuels). VMkernel inclut un planificateur de CPU, qui planifie les VCPU de manière dynamique sur les CPU physiques du système hôte.

Ce planificateur prend en compte la topologie de type socket/cœur/thread lorsqu'il effectue sa planification. Intel et AMD ont mis au point des processeurs combinant plusieurs cœurs au sein d'un circuit intégré unique, que nous appellerons « socket ». Un socket est un package unique qui peut correspondre à un ou plusieurs CPU physiques, chaque cœur comprenant un ou plusieurs CPU logiques (LCPU), ou « threads ». Les LCPU permettent au cœur de planifier des threads d'exécution ; un LCPU est associé à la planification d'un thread. La diapositive indique que le premier système, à deux sockets monocœurs, comprend deux cœurs et, par conséquent, deux LCPU.

Lorsque l'exécution d'un VCPU, ou d'une machine virtuelle comprenant un ou plusieurs VCPU, doit être planifiée, VMkernel mappe chaque VCPU à un processeur logique disponible.

8-11 À propos de l'hyperthreading

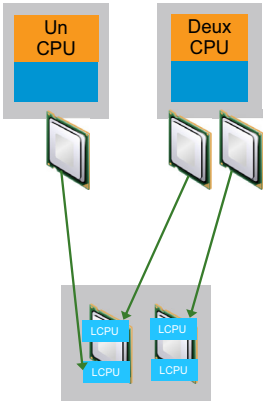
L'hyperthreading permet à un cœur d'exécuter deux threads (ou ensemble d'instructions) en même temps.

Ce mécanisme optimise les performances du planificateur.

Par défaut, le mécanisme d'hyperthreading est activé.

Pour activer ce mécanisme :

- Vérifiez que le système hôte le prend en charge.
- Activez-le dans le BIOS système.
- Vérifiez qu'il est activé pour l'hôte VMware ESXi.



Système à un socket/deux cœurs avec hyperthreading

Si l'hyperthreading est activé sur le système hôte, VMware ESXi peut exécuter deux threads en même temps sur chaque cœur de processeur (CPU physique). Ce mécanisme optimise les performances du planificateur dans la mesure où il fournit plus de CPU logiques sur lesquels planifier les VCPU. L'hyperthreading présente cependant un inconvénient : il ne multiplie pas par deux la puissance d'un cœur. Ainsi, si deux threads d'exécution requièrent simultanément les mêmes ressources sur la puce, l'un d'eux devra patienter. Toutefois, VMware ESXi exploite les récentes améliorations apportées à la technologie de l'hyperthreading, ce qui permet de gagner en performances sur les systèmes utilisant ces améliorations.

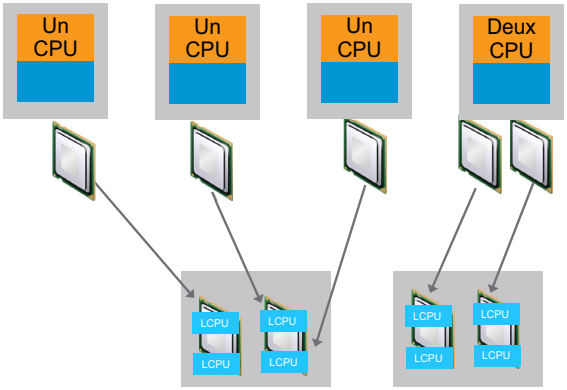
Un hôte VMware ESXi sur lequel cette technologie est activée se comporte quasiment comme un système standard. Les processeurs logiques se trouvant sur un même cœur présentent des numéros de CPU adjacents. Les processeurs logiques 0 et 1 se trouvent sur le premier cœur ; les processeurs logiques 2 et 3, sur le deuxième, et ainsi de suite.

Pour vérifier que l'hyperthreading fonctionne correctement, consultez la documentation associée au matériel, afin de déterminer si le BIOS prend ou non cette technologie en charge. Ensuite, activez-la dans le BIOS système. Certains fabricants qualifient cette option de processeur logique, tandis que d'autres parlent d'activation de l'hyperthreading.

Utilisez vSphere Web Client pour vérifier que l'hyperthreading est activé pour votre hôte. Pour vérifier l'activation de l'hyperthreading, accédez à l'onglet **Summary** et sélectionnez **CPUs** sous « Hardware ».

8-12 Équilibrage de charge CPU

VMkernel équilibre le temps processeur de façon à garantir une répartition équitable de la charge entre les différents cœurs de processeur du système.



Système à deux sockets/deux cœurs avec hyperthreading

Le planificateur de CPU peut utiliser chaque processeur logique de manière indépendante pour exécuter les machines virtuelles, en offrant des fonctions similaires aux systèmes SMP (Symmetric Multi-Processing) traditionnels. VMkernel gère intelligemment le temps processeur de façon à garantir une répartition équitable de la charge entre les différents cœurs de processeur du système. Toutes les 2 à 40 millisecondes (selon la topologie socket/cœur/thread), VMkernel essaie de migrer les VCPU d'un processeur logique vers un autre, afin d'équilibrer la charge. Il s'efforce de planifier au mieux l'exécution des machines virtuelles dotées de plusieurs VCPU sur deux cœurs différents, plutôt que sur deux processeurs logiques sur le même cœur. En cas de besoin, VMkernel peut cependant mapper deux VCPU d'une même machine virtuelle à des threads d'un même cœur.

Si un processeur logique n'a aucune tâche à effectuer, il est mis à l'état *arrêté*. Cette action libère les ressources d'exécution associées et permet à la machine virtuelle exécutée sur l'autre processeur logique d'un même cœur d'utiliser toutes les ressources d'exécution du cœur. Le planificateur VMkernel tient compte de ce temps d'arrêt, de sorte qu'une machine virtuelle exploitant l'intégralité des ressources d'un cœur recevra une charge plus importante qu'une machine virtuelle exécutée sur un demi-cœur. Cette méthode de gestion des processeurs permet de garantir que le serveur ne porte pas atteinte aux règles d'allocation des ressources de VMware ESXi.

8-13 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Aborder les concepts de mémoire et de CPU au sein d'un environnement virtualisé
- Définir la notion de surdimensionnement des ressources
- Identifier les autres technologies capables d'améliorer l'utilisation de la mémoire
- Décrire le fonctionnement du logiciel VMware vSphere® Virtual Symmetric Multiprocessing et l'utilisation de l'hyperthreading par VMkernel

8-14 Leçon 2 : Contrôles des ressources et pools de ressources

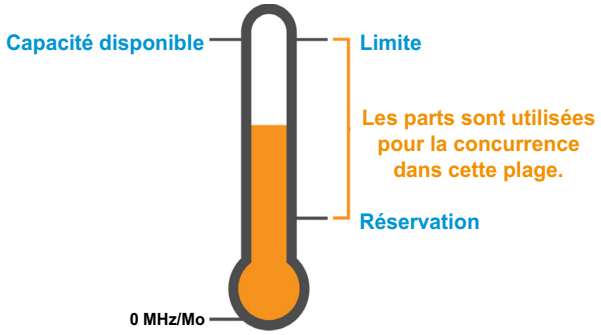
8-15 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Affecter des parts pour les ressources CPU et mémoire
- Décrire le mode de concurrence des machines virtuelles pour l'octroi des ressources
- Créer un pool de ressources
- Définir les attributs des pools de ressources
- Établir les réservations et les limites associées aux ressources CPU et la mémoire
- Décrire les réservations extensibles
- Utiliser une vApp pour gérer des machines virtuelles

8-16 Parts, limites et réservations

Une machine virtuelle ne se met sous tension que si la réservation associée peut être garantie.



Dans la mesure où les machines virtuelles utilisent simultanément les ressources d'un même hôte VMware ESXi, un conflit entre les ressources est susceptible de survenir.

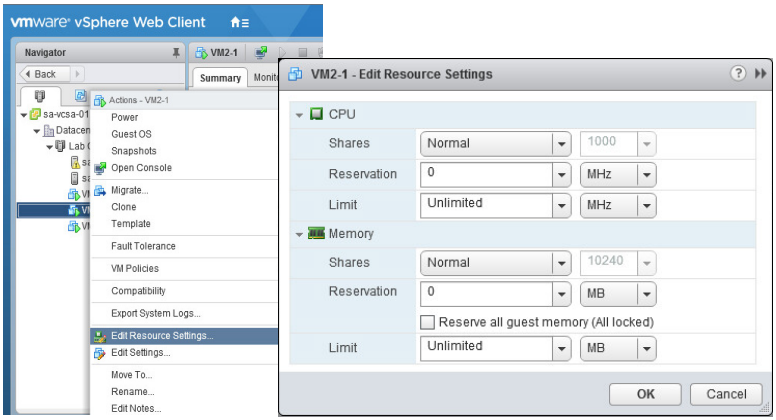
Pour assurer une gestion adéquate des ressources, vSphere propose des mécanismes permettant de réduire, d'augmenter ou de maintenir l'accès à une ressource donnée. De plus, il est possible d'empêcher une machine virtuelle d'utiliser de trop grandes quantités de ressources, ainsi que d'octroyer une quantité garantie de ressources à une machine virtuelle dont les performances sont insuffisantes ou dont le fonctionnement nécessite une certaine quantité de ressources.

Lorsque les ressources mémoire ou CPU de l'hôte sont surdimensionnées, la cible d'allocation d'une machine virtuelle se situe entre la réservation spécifiée et la limite indiquée, selon les parts de la machine virtuelle et la charge du système. vSphere utilise un algorithme d'allocation basé sur les parts (« shares ») afin d'optimiser l'utilisation des ressources pour l'ensemble des machines virtuelles et de garantir l'octroi d'une ressource donnée aux machines virtuelles qui en ont le plus besoin. Trois paramètres configurables contrôlent l'accès d'une machine virtuelle à une ressource donnée :

- Shares : le nombre de parts indique la priorité ou l'importance relatives de l'accès d'une machine virtuelle à une ressource donnée.
- Limit : la limite définit un seuil supérieur pour les ressources de CPU, de mémoire ou d'E/S de stockage pouvant être allouées à une machine virtuelle.
- Reservation : une réservation permet d'indiquer la quantité minimale de ressources garantie à une machine virtuelle.

8-17 Définition des paramètres de ressources pour des VM ponctuelles

Lorsque la capacité des ressources disponibles ne répond pas aux exigences des consommateurs de ressources, vous pouvez être amené à personnaliser les quantités de ressources allouées aux machines virtuelles.



Il importe de bien comprendre le fonctionnement des parts, des limites et des réservations. Si vous surdimensionnez les ressources mémoire et CPU de votre hôte VMware ESXi, vous aurez besoin d'un outil garantissant l'allocation d'une quantité de ressources adéquate aux différentes machines. Telle est précisément la finalité des parts, des limites et des réservations.

Une réservation garantit l'allocation d'une certaine quantité de ressources mémoire ou CPU à une machine virtuelle. Une réservation peut être spécifiée en Mo ou en MHz.

Les parts déterminent l'importance relative d'une machine virtuelle ou d'un pool de ressources. Si une machine virtuelle présente deux fois plus de parts d'une ressource qu'une autre VM, elle a le droit d'utiliser une portion deux fois plus importante de cette ressource lorsque les deux VMs sont en concurrence.

Une limite définit un seuil supérieur pour les ressources de CPU, de mémoire ou d'E/S de stockage pouvant être allouées à une machine virtuelle.

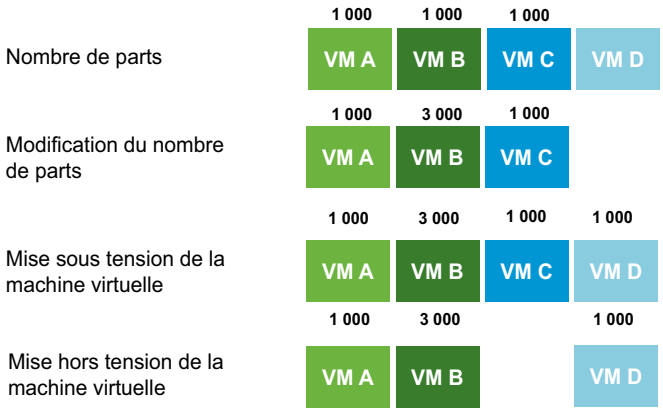
Dans la plupart des cas, il n'est pas nécessaire de spécifier une limite. La spécification d'une limite présente les avantages et les inconvénients suivants :

- Les avantages : L'affectation d'une limite est utile si vous commencez avec un petit nombre de machines virtuelles et souhaitez gérer les attentes de l'utilisateur. Les performances se dégradent à mesure que vous ajoutez des machines virtuelles. Vous pouvez simuler une réduction des ressources disponibles en spécifiant une limite.

- Les inconvénients : En spécifiant une limite, vous courez le risque de gaspiller les ressources inexploitées. Même si le système est sous-utilisé et présente des ressources inutilisées, il ne permet pas aux machines virtuelles d'utiliser une quantité de ressources supérieure à la limite autorisée. Ne spécifiez une limite que si vous avez de bonnes raisons de le faire.

8-18 Partage des ressources par les VMs

Les machines virtuelles consomment des ressources. Les paramètres de ressources affectés par défaut lors de la création fonctionnent très bien pour la plupart des machines.



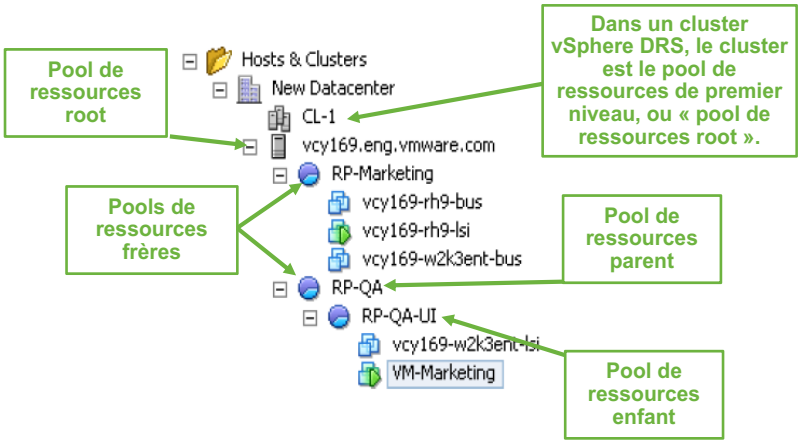
Le mécanisme de partage proportionnel s'applique à l'attribution des ressources de CPU, de mémoire, d'E/S de stockage et d'E/S réseau. Ce mécanisme fonctionne uniquement lorsque plusieurs machines virtuelles sont en concurrence pour l'octroi d'une même ressource.

Les parts garantissent qu'une machine virtuelle reçoit un certain pourcentage d'une ressource (CPU, RAM, E/S de stockage ou E/S réseau). Par exemple, examinez la troisième ligne de la diapositive ci-dessus, dans laquelle la machine virtuelle D bénéficie de 1 000 parts. Avant sa mise sous tension, un total de 5 000 parts était disponible, mais l'ajout de la machine D entraîne une augmentation du nombre de parts total, qui atteint 6 000. En conséquence, la proportion représentée par le nombre de parts des autres machines virtuelles diminue. Cependant, le nombre de parts de chaque machine virtuelle constitue toujours une valeur minimale garantie. La machine virtuelle A bénéficie toujours de 1/6e de la ressource, car elle possède 1/6e des parts.

Vous pouvez ajouter des parts à une machine virtuelle en cours d'exécution, qui bénéficiera ainsi d'un accès étendu à cette ressource (en cas de concurrence pour cette dernière). Lorsque vous ajoutez une machine virtuelle, celle-ci se voit également octroyer des parts. La quantité de parts de la machine virtuelle est incluse dans le calcul du nombre total de parts, mais les machines virtuelles existantes ont la garantie de ne pas être privées de la ressource. Lorsque vous supprimez ou arrêtez une machine virtuelle, le nombre total de parts diminue : les machines virtuelles restant actives bénéficient donc d'un accès plus étendu.

8-19 À propos des pools de ressources

Un pool de ressources est une abstraction logique des ressources mémoire et CPU gérées de manière hiérarchique.



Un pool de ressources est une abstraction logique dédiée à la gestion des ressources. Les pools de ressources peuvent être regroupés en hiérarchies et utilisés pour le partitionnement hiérarchique des ressources mémoire et CPU disponibles. Dans l'exemple de la diapositive, le pool RP-QA est le pool de ressources parent du pool RP-QA-UI. RP-Marketing et RP-QA sont des pools frères.

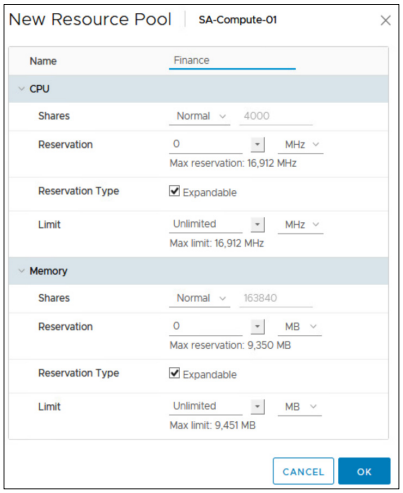
En tant qu'administrateur, le pool de ressources vous permet de répartir et d'allouer les ressources à des machines virtuelles et à d'autres pools de ressources. Un pool de ressource vous permet de contrôler les ressources mémoire et CPU agrégées de la ressource de calcul. Cette ressource peut être un hôte autonome ou un cluster VMware vSphere DRS. Les pools de ressources sont également utiles pour déléguer des droits à d'autres utilisateurs ou groupes.

Le pool de ressources situé au premier niveau est appelé « pool de ressources root ». Chaque hôte autonome ou cluster vSphere DRS inclut un pool de ressources root (invisible) regroupant les ressources de cet hôte ou de ce cluster. Le pool de ressources root est invisible, car les ressources de l'hôte (ou du cluster) et du pool de ressources root sont toujours les mêmes.

8-20 Attributs des pools de ressources

Vous pouvez créer un pool de ressources enfant sous n'importe quel hôte VMware ESXi, pool de ressources ou cluster vSphere DRS :

- « Shares » : niveau faible (« Low »), normal (« Normal »), élevé (« High) ou personnalisé (« Custom »).
- Les réservations : en MHz/GHz, ou en Mo/Go.
- La limite :
  - En MHz/GHz, ou en Mo/Go.
  - L'accès illimité, jusqu'à la quantité maximale de ressources accessible (par défaut).
- « Reservation type » :
  - L'option d'extensibilité sélectionnée : les machines virtuelles et les sous-pools peuvent exploiter les ressources du pool parent de ce pool.
  - L'option d'extensibilité désélectionnée : les machines virtuelles et les sous-pools peuvent uniquement exploiter les ressources de ce pool, même si le pool parent associé inclut des ressources disponibles.



À l'instar des machines virtuelles, un pool de ressources se voit associer une réservation, une limite et des parts pour les ressources mémoire et CPU.

Les pools de ressource présentent également un paramètre autorisant l'extension des réservations. L'attribut de réservation extensible permet à un pool de ressources ne répondant pas aux exigences d'une demande de réservation de parcourir sa hiérarchie afin de trouver la capacité non réservée nécessaire pour satisfaire cette demande.

8-21 Quelques raisons justifiant l'utilisation des pools de ressources

Les pools de ressources offrent les avantages suivants :

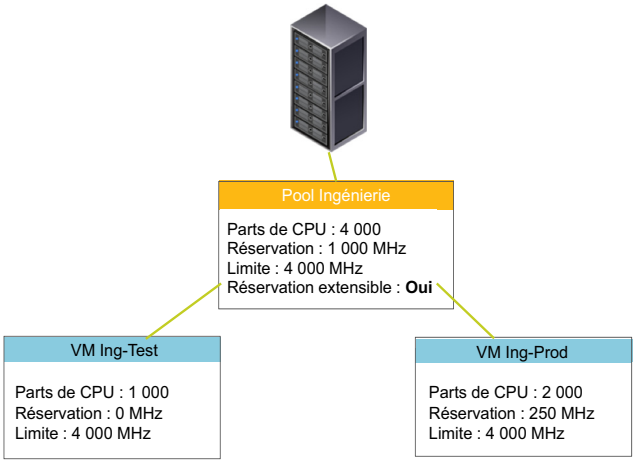
- Une organisation hiérarchique et flexible
- L'isolation entre les pools et le partage dans les pools
- Le contrôle des accès et la délégation
- La séparation entre les ressources et le matériel
- La gestion des ensembles de machines virtuelles exécutant un service à plusieurs niveaux
- La possibilité de classer par priorité les charges de travail des machines virtuelles

Grâce aux pools de ressources, vous pouvez déléguer le contrôle sur les ressources d'un cluster vSphere DRS ou d'un hôte autonome. L'utilisation des pools de ressources peut offrir les avantages suivants :

- Une organisation hiérarchique et flexible : ajoutez, supprimez et réorganisez les pools de ressources, ou modifiez l'allocation des ressources, le cas échéant.
- L'isolation entre les pools et le partage dans les pools : un administrateur de premier niveau peut mettre un pool de ressources à la disposition d'un administrateur de niveau département.
- Le contrôle des accès et la délégation : la création et la gestion des machines virtuelles sont effectuées selon les limites associées aux ressources auxquelles le pool de ressources a droit. La délégation est généralement exécutée d'après les paramètres définissant les permissions.
- La séparation entre les ressources et le matériel : si vous utilisez des clusters vSphere DRS, les ressources de l'ensemble des hôtes sont toujours affectées au cluster.
- La gestion des ensembles de machines virtuelles exécutant un service à plusieurs niveaux : regroupez les machines virtuelles associées à un service à plusieurs niveaux dans un pool de ressources.

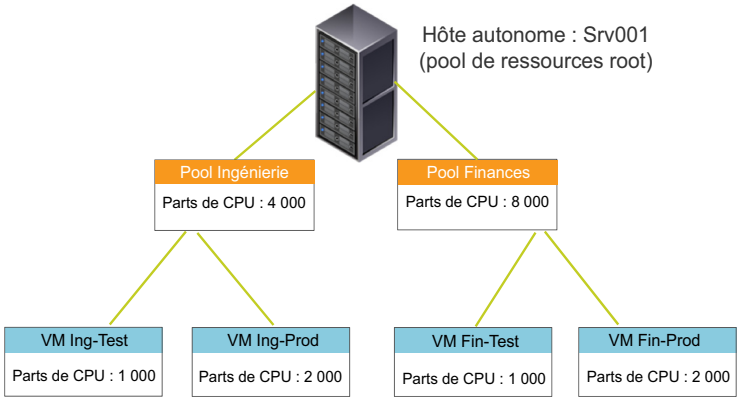
8-22 Exemple de pool de ressources

Cet exemple définit les attributs de ressources qui sont définis sur un pool de ressources.



8-23 Exemple de pool de ressources : Parts de CPU

Dans cet exemple, le pool de ressources du département Finances inclut deux fois plus de parts CPU que celui du département Ingénierie. Le pool de ressources du département Finances a droit à deux fois plus de ressources CPU que celui du département Ingénierie.



Les pools de ressources peuvent être organisés de manière hiérarchique. Le pool de ressources situé au premier niveau est le pool de ressources root. Le pool de ressources root englobe la capacité cumulée de tous les CPU (en MHz) et de toute la RAM installée (en Mo) dans l'environnement de calcul (hôte autonome ou cluster).

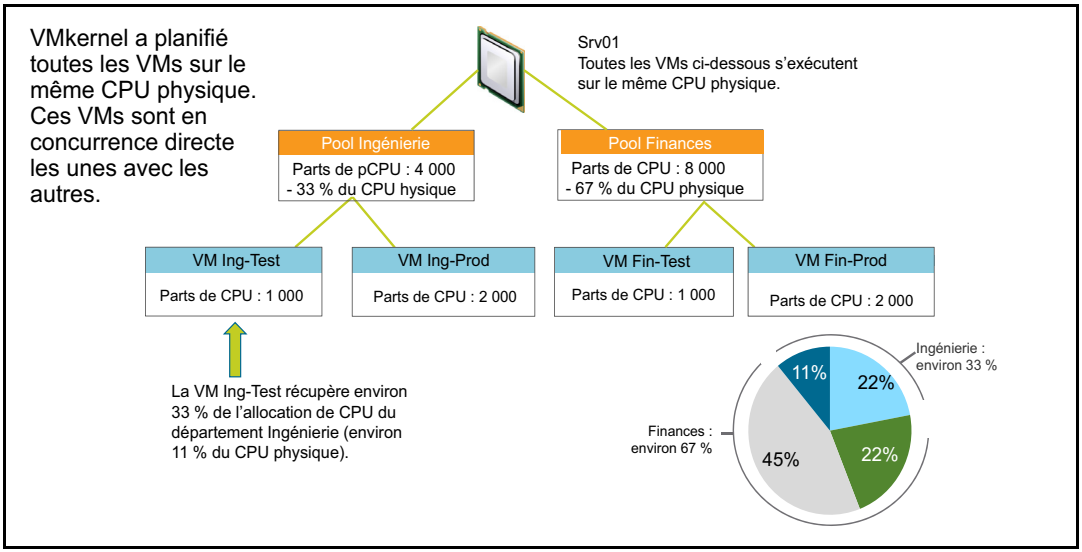
Sur la diapositive ci-dessus, le pool de ressources root correspond à un hôte autonome nommé Svr001. Il offre 12 000 MHz de CPU et 4 Go de RAM, qui peuvent être utilisés par d'autres pools de ressources ou par des machines virtuelles.

Tous les pools de ressources ont un pool parent (sauf le pool de ressources root). Un pool de ressources peut contenir des pools de ressources enfants, ou uniquement les machines virtuelles qu'il alimente.

Un pool de ressources enfant permet d'allouer les ressources du pool parent pour les utilisateurs du pool enfant. Le contrôle d'administration peut également être délégué à des individus ou à des organisations. Un pool de ressources enfant ne peut pas présenter une capacité plus grande que celle du pool de ressources parent. La création d'un pool enfant permet de réserver les ressources du pool parent, que les machines virtuelles du pool enfant soient alimentées ou non.

Les parts déterminent la priorité ou l'importance relatives d'un pool de ressources ou d'une machine virtuelle. Si un pool de ressources présente deux fois plus de parts d'une ressource qu'un autre pool, il a le droit d'utiliser un pourcentage deux fois plus important de cette ressource. Ce principe s'applique également aux machines virtuelles.

8-24 Exemple de pool de ressources : Contention CPU



Le pool Ingénierie obtient 33 % des ressources CPU, qu'il répartit entre les machines virtuelles Ing-Test et Ing-Prod. De même, le pool Finances obtient 67 % des ressources CPU et les répartit entre les machines virtuelles Fin-Test et Fin-Prod. Les paramètres d'attribution des ressources d'une machine virtuelle sont limités par les ressources du pool auquel la machine virtuelle appartient.

La machine virtuelle Ing-Test bénéficie d'environ 33 % de l'allocation du CPU pour le pool de ressources Ingénierie [1 000/(1 000+2 000)]. Ce chiffre correspond à environ 11 % du CPU physique (33 % de 33 %, soit environ 11 %). Chaque machine virtuelle bénéficie d'un pourcentage du CPU physique alloué au pool de ressources associé, sur la base de son allocation de parts individuelle.

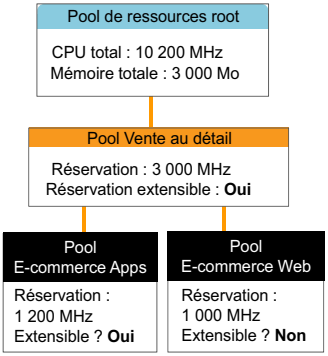
L'exemple indiqué sur la diapositive utilise des valeurs approximatives pour expliquer l'impact du nombre de parts sur la quantité de CPU allouée à une machine virtuelle.

8-25 À propos des réservations extensibles

Les ressources sont empruntées, de manière récursive, auprès des ancêtres du pool de ressources actuel :

- L'option **Expandable Reservation** doit être activée.
- Elle offre une plus grande flexibilité, mais une protection moins importante.

Les extensions de réservation ne sont libérées que lorsque la machine virtuelle à l'origine de l'extension est arrêtée, ou que la réservation qui lui est associée est réduite.



Une réservation extensible mal gérée ou mal dimensionnée risque de récupérer la totalité de la capacité non réservée.

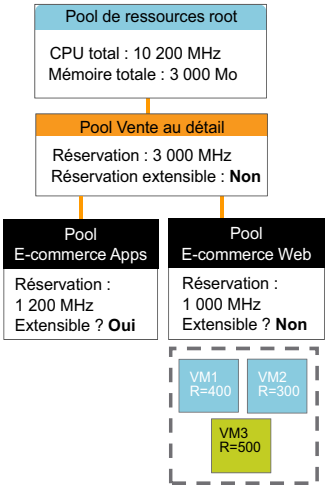
La réservation extensible permet à un pool de ressources ne répondant pas aux exigences d'une demande de réservation de parcourir sa hiérarchie afin de trouver la capacité non réservée nécessaire pour satisfaire cette demande.

Sur la diapositive, vous constatez que l'option **Expandable Reservation** est activée pour le pool de ressources enfant E-commerce Apps. La quantité de réservation d'un pool de ressources enfant ne peut pas dépasser celle de son parent. La recherche de ressources non utilisées porte sur les ancêtres du pool de ressources root, ou sur le premier pool de ressources pour lequel l'option **Expandable Reservation** n'est pas activée.

Toutefois, vous devez utiliser l'option de réservation extensible avec prudence. En effet, un pool de ressources enfant unique peut utiliser l'intégralité des ressources disponibles de son parent, privant ainsi les autres pools enfants de ressources directement accessibles. Cela peut se produire si vous déplacez les machines virtuelles de manière inappropriée, afin de les faire démarrer en fonction des réservations des ressources.

Il peut être souhaitable de désactiver l'option **Expandable Reservation** si vous octroyez une quantité fixe de ressources à un groupe. Ainsi, un administrateur ayant pour clients des entités de son entreprise qui ont payé pour une quantité fixe de ressources mémoire et CPU aura intérêt à désactiver l'option **Expandable Reservation**.

8-26 Exemple de réservation extensible (1)



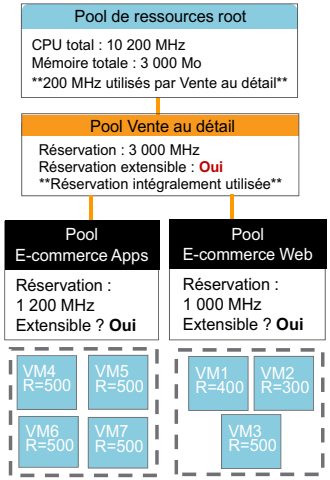
Le pool de ressources E-commerce réserve 2 200 MHz sur les 3 000 MHz réservés par le pool Vente au détail.

Mettez sous tension les machines virtuelles du pool E-commerce Web.

L'option **Expandable Reservation** étant désactivée pour le pool E-commerce Web, il n'est pas possible de démarrer VM3 avec une réservation de 500 MHz :

- Réduisez la réservation de la machine virtuelle.
- Activez l'option **Expandable Reservation**.
- Augmentez la réservation du pool E-commerce Web.

8-27 Exemple de réservation extensible (2)



Activez l'option **Expandable Reservation** pour le pool E-commerce Web.

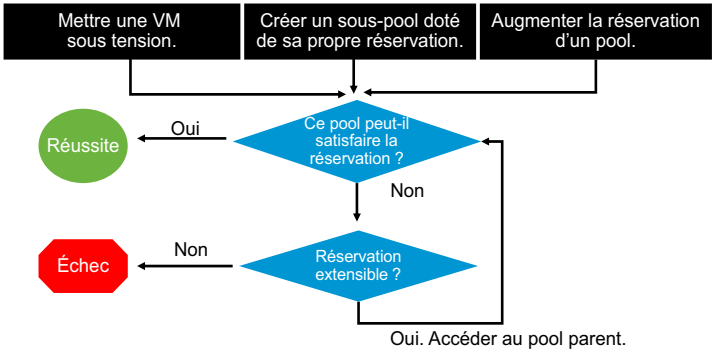
Le système prend en considération les ressources disponibles dans le pool enfant et dans son parent direct.

La réservation de la machine virtuelle est imputée à la réservation du pool E-commerce Web.

La réservation du pool E-commerce Web est imputée à la réservation du pool Vente au détail.

8-28 Contrôle d’admission pour les réservations de CPU et de mémoire

Le contrôle d’admission permet de garantir que vous n’allouez aucune ressource non disponible.



Certaines opérations doivent respecter les exigences de la fonction de contrôle d’admission, à savoir :

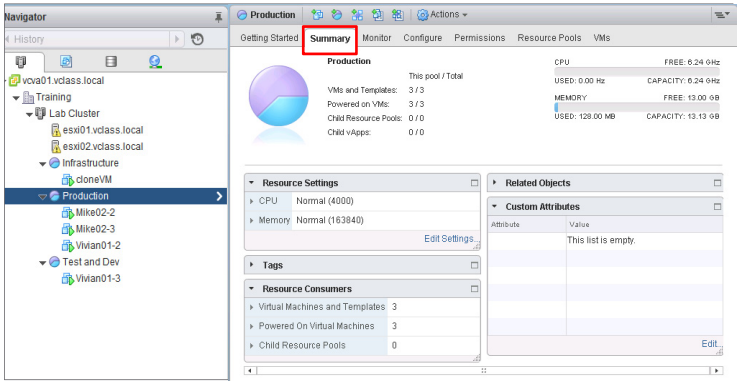
- La mise sous tension d’une machine virtuelle
- La création d’un pool de ressources doté de sa propre réservation
- L’augmentation de la réservation d’un pool de ressources

Si l’objet (machine virtuelle ou pool de ressources) se trouve dans un pool de ressources associé à une réservation extensible, le système consulte le parent du pool de ressources actuel, le cas échéant, afin de satisfaire la réservation.

Il est impossible de surdimensionner les réservations.

8-29 Onglet « Resource Pool Summary Tab »

L'onglet **Summary** du pool de ressources affiche un récapitulatif des informations portant sur la machine hôte et ses ressources.

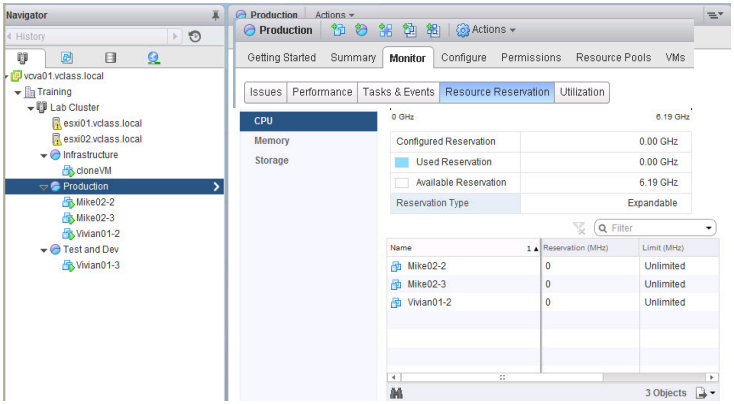


Plusieurs points doivent être pris en considération concernant l'onglet **Summary** :

- Le volet « Resource Settings » affiche les paramètres de partage « CPU » et « Memory ».
- Le volet **Resource Consumers** affiche le nombre total de machines virtuelles et le nombre de machines virtuelles sous tension, ainsi que les pools de ressources enfants inclus dans le pool de ressources sélectionné.
- Le volet **Tags** affiche les balises affectées aux objets qui résident dans le pool de ressources.

8-30 Onglet « Resource Reservation »

Sur l'onglet **Resource Reservation**, vous pouvez afficher des informations sur les ressources de stockage, mémoire et CPU d'un pool de ressources.

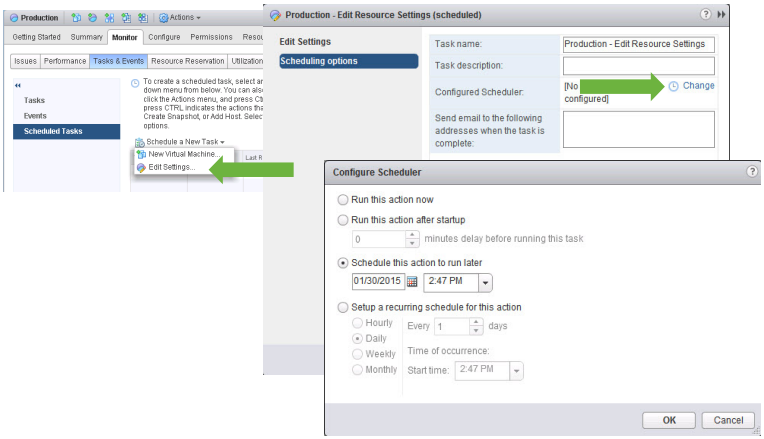


En ce qui concerne les ressources CPU et la mémoire du pool, les informations affichées sont les suivantes :

- La quantité de réservation de CPU et de mémoire qui a été configurée
- Le type de réservation utilisé (extensible ou non)
- La quantité de réservation utilisée par les machines virtuelles et les pools enfants
- La quantité de mémoire et de CPU pouvant être réservée

8-31 Planification des modifications apportées aux paramètres de ressources

Vous pouvez planifier l'exécution d'une tâche qui modifie les paramètres de ressources d'un pool de ressources ou d'une machine virtuelle.



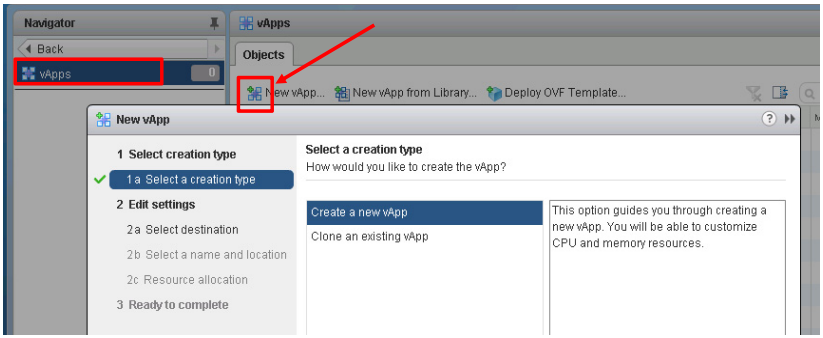
Vous pouvez configurer la tâche afin de modifier les parts, la réservation et la limite associées aux CPU et/ou à la mémoire en fonction des priorités du moment.

Par exemple, à la fin de chaque trimestre, vous pouvez fournir davantage de ressources CPU et mémoire aux applications de gestion financière qu'aux applications internes. Ainsi, dans une entreprise de vente au détail, vous pouvez multiplier par deux les réservations de ressources mémoire et CPU pour les machines virtuelles exécutant les applications de boutique en ligne pendant le mois de décembre.

8-32 Gestion de machines virtuelles à l'aide de vApps

Une vApp est un objet de l'inventaire vCenter Server :

- Une vApp est un conteneur renfermant une ou plusieurs machines virtuelles.
- Une vApp permet de packager et de gérer des applications à plusieurs niveaux.



vSphere peut être utilisé comme une plate-forme pour l'exécution d'applications, notamment dans le cas des applications à plusieurs niveaux. Vous avez la possibilité de packager ces applications de sorte qu'elles s'exécutent directement sur vSphere.

Dans vSphere Web Client, les vApps sont représentées dans les vues « Hosts and Clusters » et « VM and Templates ».

Une vApp est un conteneur renfermant une ou plusieurs machines virtuelles ou autres vApps. Une vApp partage des fonctionnalités avec les machines virtuelles. Une vApp peut être mise sous tension ou hors tension, ainsi que clonée. Les formats de distribution possibles pour une vApp sont OVF (Open Virtualization Format) et OVA (Open Virtualization Appliance). Les différences entre ces formats sont les suivantes :

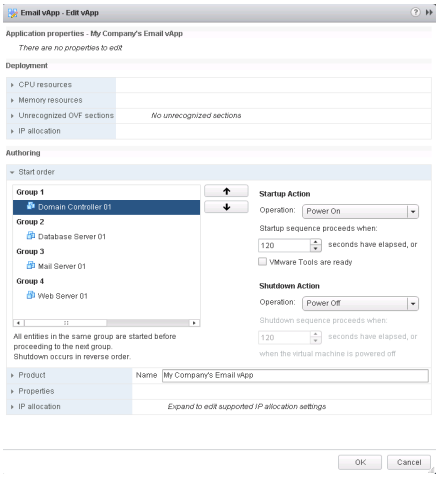
- Un fichier OVF correspond à un ensemble de fichiers de machine virtuelle. Il s'agit d'un fichier XML contenant des informations sur les fichiers de disque virtuel contenus dans le répertoire. L'exportation d'une machine virtuelle sous la forme d'un fichier OVF entraîne la création d'un répertoire contenant un fichier OVF et les fichiers de disque de machine virtuelle (VMDK).
- OVA est le format de machine virtuelle portable utilisé dans le produit tiers XenSource. Le fichier OVA est un fichier unique assimilable à une archive ZIP, qui contient tous les fichiers appartenant au répertoire OVF.

8-33 Caractéristiques d'une vApp

Vous avez la possibilité de configurer plusieurs paramètres d'une vApp en cliquant sur celle-ci avec le bouton droit de la souris :

- Allocation de ressources CPU et mémoire
- Règle d'attribution d'adresse IP

Vous pouvez également configurer l'ordre de démarrage ou d'arrêt des machines virtuelles.



Une fois la vApp créée, vous pouvez modifier certains de ses paramètres :

- L'allocation des ressources : détermine les modalités d'allocation des ressources CPU et mémoire de la vApp.
- La règle d'attribution d'adresse IP : permet de choisir le mode selon lequel les adresses IP sont attribuées à la vApp.
- Les paramètres avancés : comprennent les informations relatives au produit et au fournisseur ainsi que les propriétés personnalisées.

Vous avez la possibilité de modifier l'ordre de démarrage ou d'arrêt des machines virtuelles d'une vApp (ainsi que de ses vApps intégrées) en affectant les machines virtuelles à différents groupes. Toutes les entités appartenant à un même groupe sont démarrées avant celles du groupe suivant. Les arrêts s'échelonnent dans l'ordre inverse. Vous pouvez également spécifier des délais d'attente à respecter et des actions à effectuer au moment du démarrage ou de l'arrêt.

Sur la diapositive, la machine virtuelle Domain Controller 01 est démarrée en premier. La machine virtuelle Database Server 01 démarre 120 secondes plus tard.

Pour en savoir plus sur les vApp, consultez le *Guide d'administration d'une machine virtuelle vSphere*, disponible à l'adresse suivante : http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

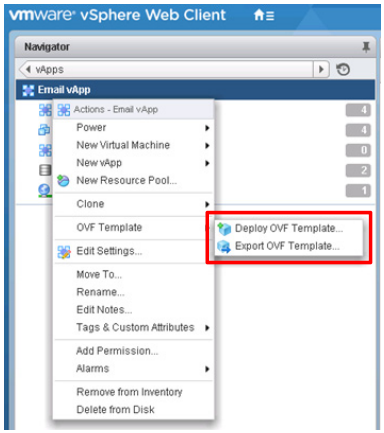
8-34 Exportation et déploiement de vApps

Lorsque vous exportez une vApp en tant que modèle OVF ou OVA :

- Vous pouvez partager cette vApp avec d'autres utilisateurs.
- Vous pouvez l'utiliser à des fins d'archivage.

Lorsque vous déployez un modèle OVF :

- Vous pouvez déployer des vApps à plusieurs niveaux.
- Vous pouvez déployer un OVF à partir du site VMware Virtual Appliance Marketplace.



8-35 Laboratoire 13 : Gestion des pools de ressources

Dans vCenter Server, créer et utiliser des pools de ressources sur un hôte VMware ESXi

1. Créer une contention CPU
2. Créer des pools de ressources
3. Vérifier le bon fonctionnement des pools de ressources

8-36 Rappel des objectifs de la formation

Vous devriez être en mesure d'atteindre les objectifs suivants :

- Affecter des parts pour les ressources CPU et mémoire
- Décrire le mode de concurrence des machines virtuelles pour l'octroi des ressources
- Créer un pool de ressources
- Définir les attributs des pools de ressources
- Établir les réservations et limites associées aux ressources CPU et mémoire
- Décrire les réservations extensibles
- Utiliser une vApp pour gérer des machines virtuelles

•

8-37 Leçon 3 : Surveillance du taux d’utilisation des ressources

8-38 Objectifs de la formation

À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Utiliser la méthodologie de réglage des performances et les outils de surveillance des ressources
- Utiliser les diagrammes de performances pour afficher et améliorer les performances
- Surveiller les facteurs clés susceptibles d'affecter les performances d'une machine virtuelle : utilisation des ressources CPU, mémoire et disque, et de la bande passante réseau

8-39 Méthodologie de réglage des performances

Suivez les meilleures pratiques ci-après pour régler les performances de votre infrastructure vSphere :

- Évaluez les performances :
  - Utilisez les outils de surveillance appropriés.
  - Consignez les résultats d'un test de performances numérique avant d'apporter vos modifications.
- Identifiez la ressource à l'origine de la limitation.
- Augmentez la quantité de ressources disponibles :
  - Allouez des ressources supplémentaires.
  - Réduisez la concurrence.
  - Enregistrez vos modifications.
- Effectuez un nouveau test de performances.

Évitez de modifier inutilement les paramètres des systèmes de production.

En matière de réglage des performances, la meilleure pratique consiste à appliquer, étape par étape, une approche logique :

1. Pour bénéficier d'une vision complète sur la situation d'une machine virtuelle en termes de performances, utilisez les outils de surveillance du système d'exploitation client et de vCenter Server. Consignez les résultats des tests de performances avant d'apporter vos modifications.
2. Identifiez la ressource sur laquelle la machine virtuelle s'appuie le plus souvent. Cette ressource est celle qui risque le plus d'affecter les performances de la machine virtuelle en cas de sous-capacité.
3. Allouez plus de ressources à une machine virtuelle, ou réduisez les ressources allouées aux autres machines virtuelles.
4. Après avoir mis une plus grande quantité de la ressource limitante à la disposition de la machine virtuelle, effectuez un autre test de performances et enregistrez les changements.

Soyez très prudent lorsque vous modifiez des systèmes de production, car ces changements risquent de nuire aux performances des machines virtuelles.

8-40 Outils de surveillance des ressources

vSphere propose aux administrateurs de nombreux outils de surveillance des performances et des ressources.

Au sein du système

DLL Perfmon
Gestionnaire de tâches

En dehors du système

Diagrammes de performances
vCenter Server
vRealize Operations
Journaux système
vSphere/VMware ESXi
Outils `resxtop` et `esxtop`

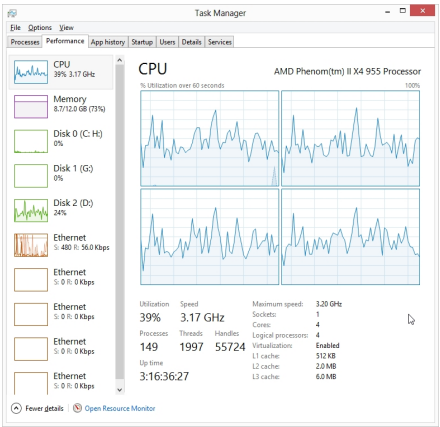
Le système d'exploitation client propose des outils provenant de sources externes à VMware, qui sont utilisés dans différentes applications VMware. Par ailleurs, certains outils qui ne figurent pas dans le système d'exploitation client sont mis à votre disposition par VMware. Vous pouvez les utiliser avec vSphere et d'autres applications.

La diapositive présente une liste non exhaustive des outils de surveillance des ressources proposés.

8-41 Outils de surveillance du système d'exploitation client

Pour surveiller les performances du système d'exploitation client, utilisez des outils que vous maîtrisez, comme le Gestionnaire des tâches de Windows.

Gestionnaire des tâches de Windows

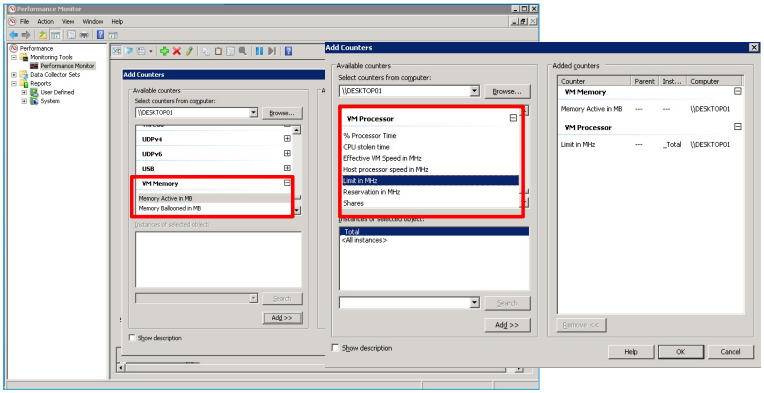


Le Gestionnaire des tâches de Windows vous permet de mesurer l'utilisation des ressources CPU et mémoire sur le système d'exploitation client.

Cependant, les mesures que vous effectuez grâce aux outils du système d'exploitation client reflètent l'utilisation des ressources par ce système, qui ne correspond pas nécessairement à l'utilisation faite par la machine virtuelle.

8-42 Utilisation de l'outil Perfmon pour surveiller les ressources des VMs

La DLL Perfmon de VMware Tools fournit des objets processeur VM et mémoire VM permettant d'accéder aux statistiques relatives aux hôtes depuis une machine virtuelle.



VMware Tools propose une bibliothèque de fonctions désignée comme la DLL Perfmon. Perfmon vous permet d'accéder à des statistiques clés sur l'hôte dans une machine virtuelle cliente. Les objets de performances Perfmon (« VM Processor » et « VM Memory ») vous permettent d'afficher le taux d'utilisation réel du CPU et de la mémoire, ainsi que leur utilisation observée dans le cas du système d'exploitation client.

Ainsi, l'objet « VM Processor » vous permet d'afficher le compteur « % Processor Time », qui surveille la charge actuelle du processeur virtuel de la machine virtuelle. De même, vous pouvez utiliser l'objet « Processor » et afficher le compteur « % Processor Time » (non représenté), qui surveille l'utilisation globale du processeur par l'ensemble des processus en cours d'exécution.

8-43 Utilisation de l'outil esxtop pour surveiller les ressources des VMs

`esxtop` est le principal outil de surveillance des performances en temps réel disponible pour vSphere :

- Vous pouvez lancer cet outil depuis l'instance VMware ESXi Shell locale de l'hôte, en exécutant la commande `esxtop`.
- Cet outil peut également être exécuté à distance depuis vSphere CLI, via la commande `resxtop`.
- Le fonctionnement de l'outil `esxtop` est analogue à celui de l'utilitaire de gestion des performances `top` proposé par les systèmes d'exploitation Linux.

Dans cet exemple, vous entrez `c` (minuscule) puis `V` (majuscule) pour afficher les mesures d'utilisation de CPU relatives aux machines virtuelles.

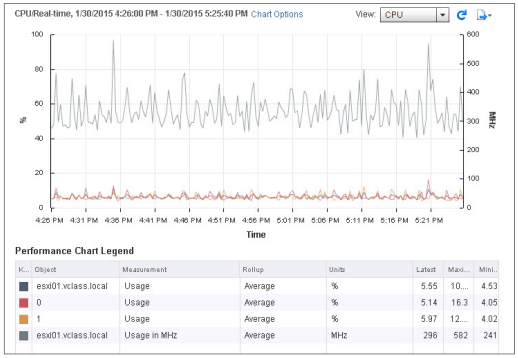
```
 2:48:37pm up 7 days 13:36, 493 worlds, 3 VMs, 3 vCPUs; CPU load average: 0.03, 0.03, 0.02
PCPU USED(%): 1.8 3.9 AVG: 2.8
PCPU UTIL(%): 2.2 4.2 AVG: 3.2

      ID      GID NAME             NWLD   %USED    %RUN    %SYS   %WAIT %VMWAIT    %RDY   %IDLE  %OVRLP   %CSTP
   52127    52127 VM2-1             8    0.15    0.14    0.00  800.00    0.72    0.03   99.67    0.00    0.00
   43316    43316 VM1-2             8    0.11    0.10    0.01  800.00    0.74    0.07   99.67    0.00    0.00
   55009    55009 VM2-2             8    0.11    0.10    0.01  800.00    0.73    0.12   99.63    0.00    0.00
```

Vous pouvez exécuter l'utilitaire `esxtop` via vSphere ESXi Shell pour communiquer avec l'interface de gestion de l'hôte VMware ESXi. Cette action requiert des privilèges d'utilisateur root.

8-44 Surveillance des objets d'inventaire via les diagrammes de performances

Le sous-système de statistiques vSphere collecte des données sur l'utilisation des ressources par les objets d'inventaire :

- Les ompteurs et les groupes de mesures
- Les niveaux et les intervalles de collecte
- La dsponibilité des données



Les données de nombreuses mesures sont recueillies fréquemment, puis traitées et archivées dans la base de données vCenter Server.

Vous pouvez accéder à des informations statistiques via des outils de ligne de commande dédiés à la surveillance, ou en affichant les diagrammes de performances proposés dans vSphere Web Client et dans vSphere Client.

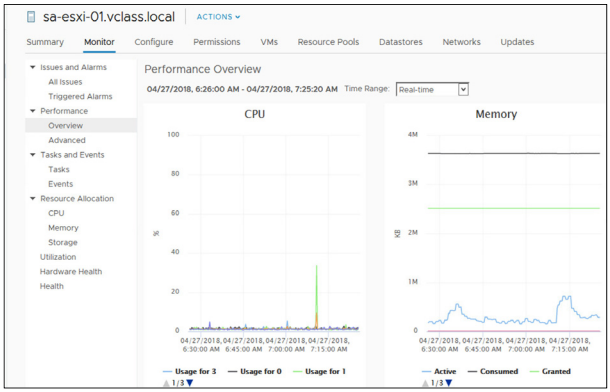
- Les compteurs et les groupes de mesures : les hôtes et les systèmes vCenter Server utilisent des compteurs de données pour demander des statistiques. Un compteur de données est une unité d'information pertinente pour un périphérique ou un objet d'inventaire donné. Chaque compteur collecte des données correspondant à une statistique différente dans un groupe de mesures. Ainsi, le groupe de mesures sur les disques comprend des compteurs distincts pour la collecte des données correspondant aux taux d'utilisation, d'écritures ou de lectures d'un disque. Les statistiques de chaque compteur sont cumulées selon un intervalle de collecte spécifique. Chaque compteur de données comprend différents attributs, qui sont utilisés pour déterminer la valeur statistique collectée.
- Les niveaux et les intervalles de collecte : les niveaux de collecte déterminent le nombre de compteurs pour lequel les données sont regroupées lors de chaque intervalle de collecte. Les intervalles de collecte déterminent la période pendant laquelle les statistiques sont regroupées, calculées, cumulées et archivées dans la base de données vCenter Server. Lorsqu'ils sont associés, le niveau et l'intervalle de collecte déterminent la quantité de données statistiques collectées et stockées dans la base de données vCenter Server.

- La disponibilité des données : les données en temps réel ne sont affichées dans les diagrammes de performances que pour les hôtes et machines virtuelles sous tension. Les données historiques apparaissent pour tous les objets d'inventaire, mais peuvent être indisponibles dans certains cas.

8-45 Utilisation des diagrammes de performances généraux

Les diagrammes de performances du volet « Overview » affichent les mesures les plus courantes concernant un objet de l'inventaire.

Partie du volet « Overview » des diagrammes de performances de l'hôte



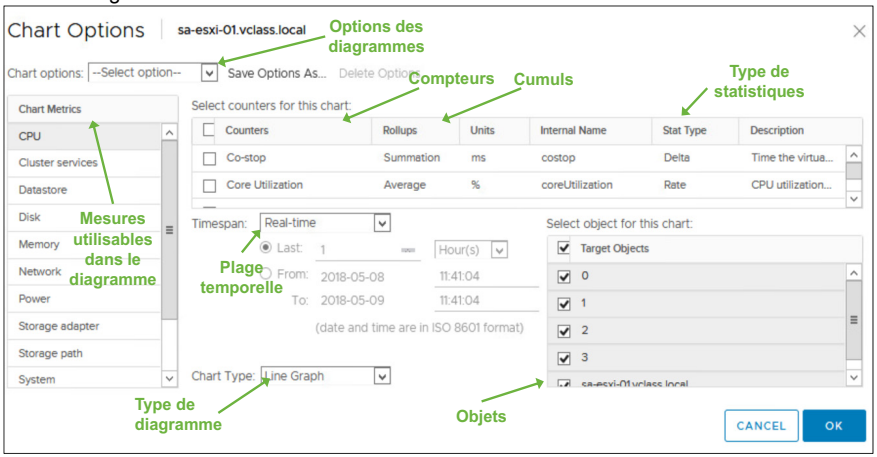
vSphere Web Client propose deux types de diagramme de performances VMware : les diagrammes généraux et les diagrammes avancés.

Un diagramme de performances général affiche les statistiques de performances que VMware considère comme les plus utiles pour surveiller les performances et diagnostiquer les problèmes.

Sur la base de l'objet sélectionné dans l'inventaire, les diagrammes de performances affichés dans le volet « Overview » vous proposent une rapide représentation visuelle des performances de la machine virtuelle ou de l'hôte. Voici une vue partielle des diagrammes de performances généraux portant sur un hôte VMware ESXi.

8-46 Utilisation des diagrammes de performances avancés

Les diagrammes de performances avancés prennent en charge les compteurs de données qui ne sont pas gérés par les autres diagrammes.



vSphere Web Client vous permet de personnaliser l'apparence des diagrammes de performances avancés.

Ces diagrammes incluent les éléments suivants :

- Plus d'informations : passez le curseur de la souris sur un point de données dans un diagramme pour afficher des informations sur ce point.
- Les diagrammes personnalisables : modifiez les paramètres des diagrammes et enregistrez les paramètres personnalisés pour créer les vôtres.
- L'exportation des données vers des feuilles de calcul.
- L'enregistrement des données vers un fichier image ou une feuille de calcul.

8-47 Options des diagrammes : Données en temps réel et historiques

vCenter Server stocke les statistiques à différentes fréquences.

Intervalle	Fréquence des données	Nombre d'échantillons
En temps réel (heure précédente)	20 secondes	180
Jour précédent	5 minutes	288
Semaine précédente	30 minutes	336
Mois précédent	2 heures	360
Année précédente	1 jour	365

Les informations « en temps réel » sont générées pour la période de l'heure précédente, selon une fréquence de 20 secondes. Les informations historiques sont générées pour la période du jour, de la semaine, du mois ou de l'année précédents, selon différentes fréquences.

Par défaut, vCenter Server propose quatre intervalles de collecte : jour, semaine, mois et année. Chaque intervalle détermine une durée d'archivage des statistiques dans la base de données vCenter Server. Vous pouvez configurer les intervalles activés et la durée de conservation correspondante. Il est également possible de définir le nombre de compteurs de données utilisés dans un intervalle de collecte, en déterminant le niveau de collecte. Lorsqu'ils sont associés, le niveau et l'intervalle de collecte déterminent la quantité de données statistiques collectées et stockées dans la base de données vCenter Server. Par exemple, selon le tableau suivant, les statistiques de la journée passée affichent un point de données toutes les 5 minutes, pour un total de 288 échantillons. Quant aux statistiques de l'année précédente, elles affichent un point de données par jour, soit 365 échantillons.

Les statistiques en temps réel ne sont pas stockées dans la base de données. Elles sont stockées dans un fichier plat sur les hôtes VMware ESXi et dans la mémoire sur les systèmes vCenter Server. Les hôtes VMware ESXi collectent des statistiques en temps réel pour l'hôte ou les machines virtuelles disponibles sur l'hôte uniquement. Ces statistiques sont directement collectées sur un hôte VMware ESXi, toutes les 20 secondes. Si vous demandez des statistiques en temps réel, vCenter Server interroge chaque hôte directement pour obtenir des données. vCenter Server ne traite pas les données à ce stade, et se contente de les transmettre à vSphere Web Client et à vSphere Client.

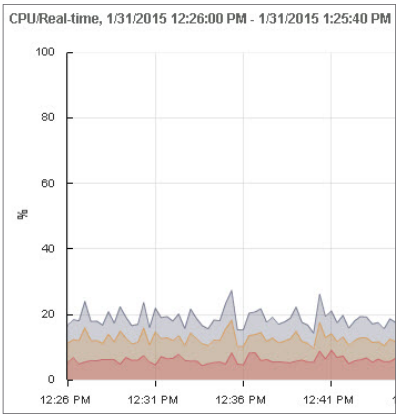
Sur les hôtes VMware ESXi, les statistiques sont conservées pendant une période de 30 minutes, à l'issue de laquelle on dénombre 90 points de données collectés. Les points de données sont regroupés, traités et renvoyés à vCenter Server, qui archive alors les données dans la base de données, sous la forme d'un point de données pour l'intervalle de collecte de la journée.

Afin de vérifier que les performances ne sont pas affectées lors de la collecte et de l'écriture des données dans la base de données, le système émet des requêtes cycliques pour collecter les statistiques des compteurs de données. Ces requêtes sont exécutées selon un intervalle de collecte spécifique. À la fin de chaque intervalle, le calcul des données est effectué.

8-48 À propos des types de diagramme

Le type de mesure et d'objet a une incidence sur la catégorie de diagramme sélectionnée pour l'affichage des mesures de performances :

- Le diagramme à lignes : chaque instance est affichée séparément.
- Le diagramme à barres : chaque instance correspond à une barre dans le diagramme.
- Le diagramme à secteurs : chaque instance correspond à un quartier du diagramme.
- Le diagramme empilé : les diagrammes sont empilés les uns sur les autres.



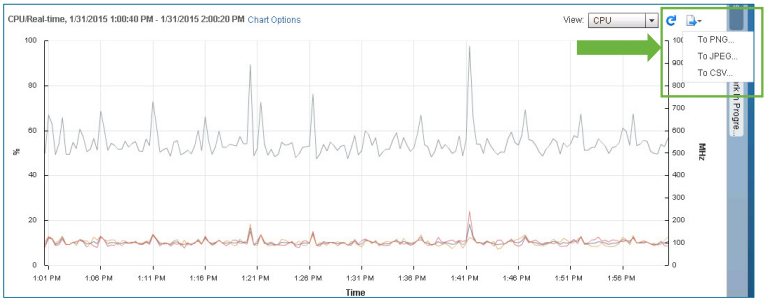
Vous pouvez utiliser des types de diagramme différents pour changer la présentation des mesures :

- Le diagramme à lignes : affiche les mesures d'un objet d'inventaire unique. Les données de chaque compteur de performances sont représentées sur une ligne distincte du diagramme. Par exemple, un diagramme réseau d'un hôte peut contenir deux lignes, l'une représentant le nombre de paquets reçus et l'autre, le nombre de paquets transmis.
- Le diagramme à barres : affiche les mesures du stockage des banques de données dans le Data Center sélectionné. Chaque banque de données correspond à une barre dans le diagramme. Une barre affiche les mesures selon le type de fichier : les disques virtuels, les snapshots, les fichiers d'échange, etc.
- Le diagramme à secteurs : affiche les mesures du stockage d'un objet unique, selon les types de fichier ou les machines virtuelles. Ainsi, un diagramme à secteurs associé à une banque de données peut afficher la quantité d'espace de stockage occupée par les machines virtuelles les plus volumineuses.
- Le diagramme empilé : affiche les mesures des objets enfants présentant les valeurs statistiques les plus élevées. Tous les autres objets sont regroupés et la valeur totale apparaît avec le terme « Other ». Par exemple, un diagramme empilé sur l'utilisation des ressources CPU de l'hôte affiche les mesures relatives à l'utilisation des ressources CPU pour les cinq machines virtuelles qui consomment le plus de ressource CPU sur l'hôte. La quantité « Other » inclut le taux d'utilisation total des ressources CPU par les machines virtuelles restantes. Les mesures relatives à l'hôte lui-même sont affichées dans des diagrammes linéaires distincts. Les diagrammes empilés sont utiles pour la comparaison des valeurs d'allocation et d'utilisation des ressources sur plusieurs hôtes ou machines virtuelles. Par défaut, il s'agit des 10 objets enfants présentant les valeurs de compteur de données les plus élevées.

8-49 Enregistrement des diagrammes

Pour enregistrer les informations d'un diagramme de performances, cliquez sur l'icône **Save Chart** située au-dessus de ce diagramme.

Vous pouvez les enregistrer au format PNG, JPEG ou CSV.



Dans vSphere Web Client, vous pouvez enregistrer les données des diagrammes de performances avancés dans un fichier graphique (différents formats sont disponibles) ou dans un fichier Microsoft Excel. Lorsque vous enregistrez un diagramme, vous choisissez le type de fichier et effectuez la sauvegarde vers l'emplacement de votre choix.

8-50 À propos des objets et des compteurs

Les diagrammes de performances représentent de manière graphique les mesures relatives au stockage, au réseau, aux disques, à la mémoire et aux CPU, pour tous les périphériques et entités gérés par vCenter Server.

Les objets sont des instances ou des agrégations de dispositifs :

- Par exemple, vCPU0, vCPU1, vmhba1:1:2, et l'agrégation sur l'ensemble des cartes réseau

Les compteurs identifient les statistiques à collecter.

- Les exemples :
  - Le CPU : durée d'utilisation, le délai de préparation (« ready time »), le taux d'utilisation
  - La carte d'interface réseau : le nombre de paquets réseau reçus
  - La mémoire : la quantité de mémoire mise en fichier d'échange

vCenter Server permet à l'utilisateur de déterminer la quantité d'informations affichées sur un type de périphérique spécifique. Ainsi, vous pouvez définir le nombre de données affichées par un diagramme en choisissant un ou plusieurs objets et compteurs.

Un objet est une instance pour laquelle une valeur statistique est collectée. Vous pouvez ainsi collecter des statistiques pour un CPU unique, pour tous les CPU, pour un hôte ou pour un périphérique réseau déterminé.

Un compteur représente la valeur statistique réelle que vous collectez. Exemple : le taux d'utilisation des ressources CPU ou le nombre de paquets réseau par seconde pour un périphérique donné.

8-51 À propos des types de statistiques

Le type de statistiques correspond à l'unité de mesure utilisée lors de l'intervalle de collecte de statistiques.

Type de statistiques	Description	Exemple
« Rate »	Valeur correspondant à l'intervalle en cours	Utilisation du CPU (MHz)
« Delta »	Changement par rapport à l'intervalle précédent	Délai de préparation CPU
« Absolute »	Valeur absolue, indépendamment de l'intervalle	Mémoire active

Le type de statistiques indique la mesure utilisée lors de l'intervalle de collecte de statistiques. Il est lié à l'unité de mesure.

Il correspond à l'un des éléments suivants :

- « Rate » : la valeur correspondant à l'intervalle de collecte de statistiques en cours.
- « Delta » : le changement par rapport à l'intervalle de collecte de statistiques précédent.
- « Absolute » : la valeur absolue, indépendamment de l'intervalle de collecte de statistiques.

Ainsi, la valeur « CPU Usage » est un taux (type « Rate »), la valeur « CPU Ready time » est un delta (type « Delta ») et la valeur « Memory Active » est une valeur absolue (type « Absolute »).

8-52 À propos des cumuls

Le cumul correspond à la fonction de conversion entre les intervalles de collecte de statistiques :

- 5 minutes de statistiques calculées pour l'heure précédente sont converties en une valeur pour la journée précédente :
  - Quinze statistiques de 20 secondes sont cumulées en une valeur unique.
- 30 minutes de statistiques calculées pour la journée précédente sont converties en une valeur pour la semaine précédente :
  - Six statistiques de 5 minutes sont cumulées en une valeur unique.
- Autres types de cumul : « minimum » ou « maximum »

Type de cumul	Fonction de conversion	Exemple de statistiques
« Average »	Moyenne des points de données	Utilisation du CPU (en moyenne)
« Summation »	Somme des points de données	Délai de préparation CPU (en millisecondes)
« Latest »	Dernier point de données	Temps disponible (en jours)

Lorsque vous observez différents intervalles historiques, les données sont affichées selon des fréquences distinctes. Les statistiques relatives à l'heure précédente sont affichées à une fréquence de 20 secondes et celles de la journée passée, à une fréquence de 5 minutes. La moyenne calculée pour effectuer la conversion des données d'un intervalle temporel vers un autre est appelée « cumul ».

Différents types de cumul sont disponibles. Le type de cumul détermine la nature des valeurs statistiques renvoyées pour le compteur :

- « Average » : les données collectées durant l'intervalle sont regroupées et leur moyenne est calculée.
- « Minimum » : la valeur minimale est cumulée.
- « Maximum » : la valeur maximale est cumulée.

  Les valeurs minimale et maximale sont collectées et affichées au niveau de collecte 4 uniquement. Les types de cumul « Maximum » et « Minimum » sont utilisés pour capturer des pics de données au cours de l'intervalle. Pour les données en temps réel, la valeur correspond au minimum actuel ou au maximum actuel. En ce qui concerne les données historiques, la valeur correspond au minimum moyen ou au maximum moyen.

Par exemple, les informations du diagramme suivant sur l'utilisation du CPU indiquent que la moyenne est collectée selon l'intervalle de collecte 1 et les valeurs minimum et maximum, selon l'intervalle 4.

- Le compteur : « usage »
- L'unité : « Percentage (%) »
- Le type de cumul : « Average » (« Minimum »/« Maximum »)
- Le niveau de collecte : 1 (4)

Les niveaux de statistiques incluent les paramètres suivants :

- « Summation » : les données collectées sont ajoutées. La mesure affichée dans le diagramme de performances représente la somme des données collectées au cours de l'intervalle.
- « Latest » : les données collectées au cours de l'intervalle correspondent à des valeurs définies. La valeur affichée dans le diagramme de performances représente la valeur actuelle.

Par exemple, si vous consultez le compteur « CPU Used » dans un diagramme de performances des ressources CPU, le type de cumul est « Summation ». Cela signifie que, pour un intervalle donné de 5 minutes, la somme de l'ensemble des échantillons de 20 secondes qui constituent cet intervalle est représentée.

8-53 Interprétation des données produites par les outils

Les outils de surveillance du système d'exploitation client et de vCenter Server offrent des points de vue différents.

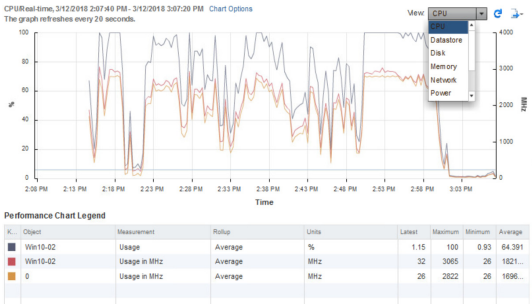
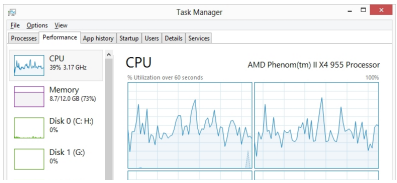


Diagramme relatif à l'utilisation de ressources CPU pour l'hôte



Gestionnaire des tâches dans le système d'exploitation client

Pour interpréter correctement les données de performances, il est crucial d'observer la plage de données selon le point de vue du système d'exploitation client, de la machine virtuelle et de l'hôte.

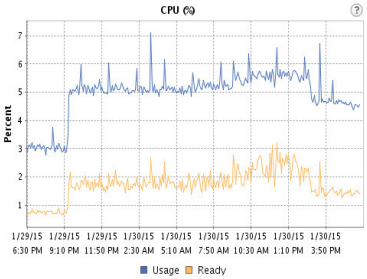
Par exemple, les statistiques d'utilisation des ressources CPU fournies dans le Gestionnaire des tâches ne fournissent qu'une vision parcellaire de cette utilisation. Il est recommandé d'afficher en outre le taux d'utilisation des ressources CPU pour la machine virtuelle et l'hôte qui l'héberge. Utilisez les diagrammes de performances de vCenter Server pour afficher ces données.

8-54 Machines virtuelles limitées en ressources CPU

Un taux d'utilisation des ressources CPU constamment élevé indique que la machine virtuelle est limitée en ressources CPU. Toutefois, il se peut que l'hôte ne dispose pas de ressources CPU suffisantes pour permettre l'exécution d'autres machines virtuelles.

Plusieurs machines virtuelles sont considérées comme limitées en ressources CPU si les conditions suivantes sont réunies :

- Le taux d'utilisation élevé des ressources CPU sur le système d'exploitation client
- Les valeurs de préparation des CPU relativement élevées pour les machines virtuelles



Taux d'utilisation des ressources CPU d'une machine virtuelle unique

Pour vérifier si une machine virtuelle est limitée en ressources CPU, consultez le taux d'utilisation du CPU dans le système d'exploitation client, en utilisant par exemple le Gestionnaire des tâches.

Si ce taux est élevé, vérifiez celui de la machine virtuelle. Dans vSphere Web Client ou dans vSphere Client, sélectionnez la machine virtuelle dans l'inventaire et cliquez sur l'onglet **Monitor**, puis sur le bouton **Performance**. Vous pouvez utiliser les diagrammes généraux ou avancés pour afficher le taux d'utilisation du CPU. La diapositive présente un diagramme avancé retraçant le taux d'utilisation des ressources CPU par une machine virtuelle.

Si ce taux reste élevé pendant un certain temps, cela signifie que la machine virtuelle est limitée en ressources CPU. Il se peut que les autres machines virtuelles de l'hôte disposent de ressources CPU suffisantes pour répondre à leurs besoins.

Si plusieurs machines virtuelles sont limitées en ressources CPU, l'indicateur clé est le délai de préparation CPU. Ce délai porte sur l'intervalle de temps pendant lequel la machine virtuelle est prête à exécuter des instructions mais ne peut pas le faire faute de pouvoir être planifiée sur un CPU. Cette valeur est affectée par plusieurs facteurs :

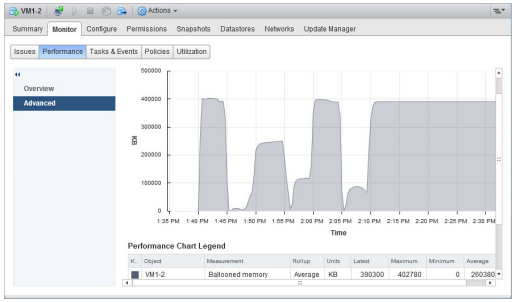
- Le taux d'utilisation global des ressources CPU : le délai de préparation a plus de chances d'augmenter lorsque le taux d'utilisation est élevé, car le CPU est alors plus susceptible d'être occupé lorsqu'une nouvelle machine virtuelle est prête à se lancer.
- Le nombre de consommateurs de ressources (en l'occurrence, les systèmes d'exploitation clients) : lorsqu'un hôte exécute un plus grand nombre de machines virtuelles, le planificateur est plus susceptible de reléguer une machine virtuelle en file d'attente après les autres machines virtuelles déjà en cours d'exécution ou en attente.

La valeur de délai de préparation acceptable varie selon la charge de travail. Pour obtenir une valeur de délai de préparation adaptée à votre charge de travail, collectez des données sur ce délai pendant une certaine période et pour chaque machine virtuelle. Une fois ces données de délai de préparation collectées pour chacune des machines virtuelles, estimez la part du délai de préparation par rapport au temps de réponse observé. S'il apparaît que le non-respect des temps de réponse cibles des applications provient principalement d'un délai de préparation excessif, prenez les mesures requises pour réduire celui-ci.

8-55 VM limitées en ressources mémoire

Vérifiez l'activité de gonflage de mémoire pour déterminer si la machine virtuelle est limitée en ressources mémoire :

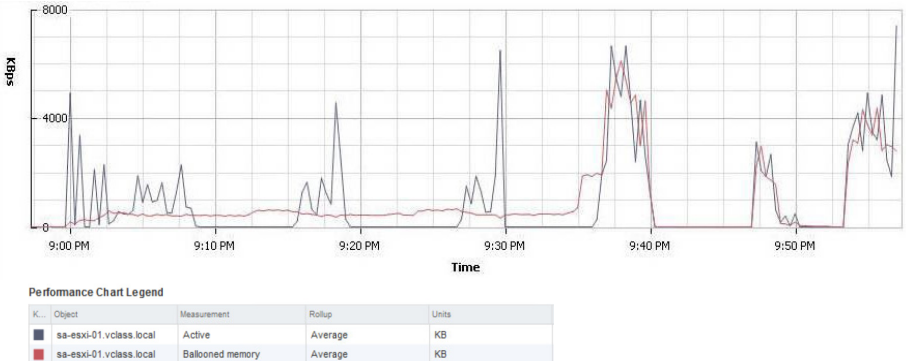
- Une activité de gonflage importante ne constitue pas nécessairement un problème dès lors que toutes les machines virtuelles disposent de suffisamment de mémoire.
- En revanche, une forte activité de gonflage associée à une activité d'échange sur le système d'exploitation client indique que la machine virtuelle est limitée en mémoire.



Lorsqu'une machine virtuelle fait l'objet d'un gonflage de mémoire, une partie de la mémoire physique du système d'exploitation client est récupérée auprès de cette machine virtuelle par le pilote de gonflage de mémoire. Des valeurs de gonflage de mémoire élevée ne constituent pas nécessairement un problème dès lors la machine virtuelle continue à disposer de suffisamment de mémoire. En revanche, si une machine virtuelle connaît une forte activité de gonflage et que son système d'exploitation client commence à paginer la mémoire, il se peut que cette machine virtuelle soit limitée en mémoire.

8-56 Hôtes limités en ressources mémoire

Une activité d'échange au niveau de l'hôte est le signe d'un surdimensionnement de la mémoire hôte.



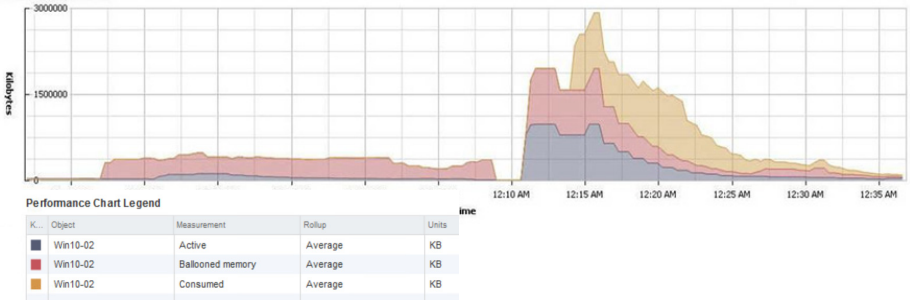
Si plusieurs machines virtuelles sont limitées en ressources mémoire, vous constatez une forte activité de gonflage de mémoire accompagnée d'une pagination de la mémoire par le système d'exploitation client. Par ailleurs, la machine virtuelle elle-même est transférée vers et depuis le système par VMkernel. Cette situation préoccupante indique que la mémoire hôte est surdimensionnée et doit être augmentée.

8-57 Surveillance de la mémoire active des VMs

Vous avez la possibilité de surveiller la mémoire active de l'hôte pour détecter les éventuelles augmentations.

La mémoire active de l'hôte correspond à la mémoire physique active utilisée par les machines virtuelles et VMkernel.

Si la quantité de mémoire active est élevée, il se peut que les machines virtuelles commencent à être limitées en ressources mémoire.



L'un des compteurs de mémoire à surveiller dans la durée est le compteur de mémoire active d'un hôte. Par « mémoire active de l'hôte », on entend la quantité de mémoire physique activement utilisée par les machines virtuelles et VMkernel. Si la quantité de mémoire active de certaines machines virtuelles est continuellement élevée, cela peut entraîner une sous-capacité de mémoire pour ces machines.

8-58 Machines virtuelles limitées en ressources disque

Les applications qui font une forte utilisation des ressources disque peuvent saturer l'espace de stockage ou le chemin d'accès à celui-ci.

Si vous pensez qu'une machine virtuelle est limitée par les accès disque, procédez comme suit :

- Évaluez le débit et la latence entre la machine virtuelle et le stockage.
- Utilisez les diagrammes de performances avancés pour surveiller les paramètres suivants :
  - Le taux de lectures et d'écritures
  - La latence en lecture et en écriture

Les problèmes touchant les performances des disques sont généralement causés par la saturation du matériel de stockage physique sous-jacent. Vous pouvez utiliser les diagrammes de performances avancés de vCenter Server pour évaluer les performances du stockage à différents niveaux. En vous permettant de surveiller tous les composants (depuis la banque de données d'une VM jusqu'à un chemin d'accès au stockage spécifique), ces diagrammes fournissent des indications utiles sur les performances de cette machine virtuelle.

Si vous choisissez un objet hôte, vous pouvez afficher le débit et la latence d'une banque de données, d'un adaptateur de stockage ou d'un chemin d'accès au stockage. Les diagrammes relatifs aux adaptateurs de stockage ne sont disponibles que pour le stockage Fibre Channel. Des diagrammes portant sur les chemins d'accès au stockage sont proposés pour le stockage Fibre Channel et iSCSI, mais pas pour le stockage NFS.

Si vous choisissez un objet de machine virtuelle, vous pouvez afficher le débit et la latence d'un disque virtuel spécifique ou de la banque de données de cette machine.

Pour surveiller un débit, affichez les compteurs « Read rate » et « Write rate ». Pour surveiller une latence, affichez les compteurs « Read latency » et « Write latency ».

8-59 Surveillance de la latence de disque

Pour identifier les problèmes de performances des disques, surveillez deux compteurs de données relatifs à la latence de disque :

- « Kernel command latency » :
  - Ce compteur indique le temps moyen passé dans VMkernel par une commande SCSI.
  - Des valeurs élevées (supérieures à 2 ou 3 millisecondes) indiquent qu'une baie ou un hôte sont surchargés.
- « Physical device command latency » :
  - Ce compteur indique le temps moyen que prend l'exécution d'une commande SCSI par un périphérique physique.
  - Des valeurs élevées (supérieures à 15 ou 20 millisecondes) indiquent qu'une baie est surchargée ou trop lente.

Une méthode fiable pour déterminer si l'environnement vSphere rencontre ou non des problèmes de disques consiste à surveiller les compteurs de données de latence de ces disques. Utilisez les diagrammes de performances avancés pour surveiller ces statistiques. Penchez-vous tout particulièrement sur les compteurs suivants :

- « Kernel command latency » : ce compteur de données mesure le temps moyen (en millisecondes) que passe VMkernel à traiter une commande SCSI. Pour des performances optimales, la valeur obtenue doit se situer entre 0 et 1. Une valeur supérieure à 4 millisecondes indique que les machines virtuelles de l'hôte VMware ESXi tentent d'envoyer des données au système de stockage à un débit plus élevé que celui qui est pris en charge par la configuration.
- « Physical device command latency » : ce compteur de données mesure le temps moyen que passe le périphérique physique à exécuter une commande SCSI (en millisecondes). Selon le matériel, une valeur supérieure à 15 millisecondes indique que la baie de stockage est peut-être trop lente ou surchargée.